Oracle® Fusion Middleware

Reference for Oracle Identity Management

12c (12.2.1.4.0)
E95870-03
January 2021

Oracle Fusion Middleware Reference for Oracle Identity Management, 12c (12.2.1.4.0)

E95870-03

Primary Author: Alankrta Prakash

Contents

3 Oracle Internet Directory Data Management Tools

5 Oracle Directory Integration Platform Tools

Part II Schema Reference

6 LDAP Schema Overview

7 LDAP Object Class Reference

Index

List of Tables

Preface

The *Reference for Oracle Identity Management* provides reference information about the command-line tools and LDAP directory schema elements for Oracle Identity Management components.

Audience

The *Reference for Oracle Identity Management* is intended for administrators, developers, and others who perform 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

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following manuals in the Oracle Identity Management 12*c*Release 2(12.2.1.3.0) documentation set:

- *Installing and Configuring Oracle Internet Directory*
- *Administering Oracle Internet Directory*
- *Administering Oracle Directory Integration Platform*
- *Application Developer's Guide for Oracle Identity Management*

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.

What's New in This Guide

This section provides a brief description of the new features introduced with the latest release of Oracle Internet Directory and points you to more information about each new feature.

- Updates in January 2021 Documentation Refresh for 12c (12.2.1.4.0)
- New and Changed Features for 12*c* (12.2.1.4.0)
- New and Changed Features for 12c (12.2.1.3.0)

Updates in January 2021 Documentation Refresh for 12c (12.2.1.4.0)

This revision of *Oracle® Fusion Middleware Reference for Oracle Identity Management* contains feature updates and addresses bug fixes.

Support for Running the Oracle Internet Directory Server Diagnostic Command-Line Tool without SYS User Password

You can now run the Oracle Internet Directory Server Diagnostic command-line tool (`oiddiag`) without providing the SYS database user password. When you do so, the tool only collects diagnostics data that does not require sysdba privileges. See About Oracle Internet Directory Server Diagnostic Command-Line Tool for more information about the tool.

New and Changed Features for 12*c* (12.2.1.4.0)

This section provides a concise summary of the new features in this release.

- New security options for the `backupmetadata` operation. See -backupmetadata.
- New option in the `bulkmodify` command to prompt for a secure value instead of the command line value. See `bulkmodify` Command Reference.
- New enhancements to delete only entries that match a specific LDAP filter condition and to execute `bulkdelete` without stopping OID services. See `bulkdelete` Command Reference.

For a comprehensive listing of the new Oracle Internet Directory features introduced in this release, see New and Changed Features for Oracle Internet Directory 12c (12.2.1.4.0) in *Administering Oracle Internet Directory*.

New and Changed Features for 12*c* (12.2.1.3.0)

This section provides a concise summary of the new features in this release.

- **Improvements in the diagnostic tool**: The Alert logging feature captures the log messages for the events related to the OID deployment. The corresponding detailed dignostic log messages related to each of the events are captured in OID server log files that include database SQL statements and other operational time metrics. Starting from this release, the oiddiag tool is capable of generating HTML summary report that contains vital diagnostic information about the health of the deployed OID server. For more information, see About Oracle Internet Directory Server Diagnostic Command-Line Tool.

For a comprehensive listing of the new Oracle Internet Directory features introduced in this release, see New and Changed Features for Oracle Internet Directory 12c (12.2.1.3.0) in *Administering Oracle Internet Directory*.

Part I
Command-Line Tool Reference

You can understand about the different command-line tools and how they are used to administer Oracle Internet Directory, Oracle Internet Directory Replication and Oracle Directory Integration Platform.

This part contains information about the command-line tools for Oracle Identity Management. It includes the following chapters:

1
Command-Line Tools Overview

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

- Overview of Passwords with Command-Line Tools
- Configuring Your Environment
- Oracle Identity Management Command-Line Tool Categories

1.1 Overview of Passwords with Command-Line Tools

Many command-line tools require you to authenticate by providing a password.

In some cases, you can provide the password in either of two ways:

- In response to a prompt from the command.
- Following an option on the command line

For security reasons, avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen and might appear in output from the `ps` command or in log files. When you supply a password at a prompt, it is not visible on the screen, in output from the `ps` command, or in log files.

The `LDAP` tools have been modified to disable the options `-w` *`password`* and `-P` *`password`* when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to `TRUE` or `1`. If you use `-q` or `-Q`, respectively, the command prompts you for the user password or wallet password. Set this environment variable whenever possible. This feature affects the behavior of the following tools:

- 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)

> **Note:**
>
> When you use the `-q` or `-Q` option and redirect or pipe the output of an LDAP command, you do not see the prompt on the command line. The command still accepts the password you provide. If there is no wallet password and you are using the `-Q` option, when prompted for the password, hit Enter.

If you use the `-w` *`password`* option with an LDAP tool when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to true, you see the following error message, followed by command usage help.

```
Command-line passwords are disabled for LDAP commands.
Use -q option instead of -w <password>. You are prompted for the password.*
```

Similarly, If you use the `-P` *`password`* option with an LDAP tool when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to true, you see the following error message, followed by command usage help.

```
Command-line passwords are disabled for LDAP commands.
Use -Q option instead of -P <password>. You are prompted for the password.
```

1.2 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.

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

- `ORACLE_HOME` - The location of non-writable files in your Oracle Identity Management installation.
- `DOMAIN_HOME` - The location of writable files in your Oracle Identity Management installation.
- `NLS_LANG` (*`APPROPRIATE_LANGUAGE`*`.AL32UTF8`) - The default language set at installation is `AMERICAN_AMERICA`.
- `WLS_HOME` - The location where the WebLogic Server is installed. This environment variable is required for Oracle Directory Integration Platform commands but not Oracle Internet Directory commands.
- `PATH` - The following directory locations should be added to your `PATH`:

  `ORACLE_HOME``/bin`

  `ORACLE_HOME``/ldap/bin`

  `ORACLE_HOME``/ldap/admin`

1.3 Oracle Identity Management Command-Line Tool Categories

The Oracle Identity Management command-line tools are organized into categories based on what actions they are helpful in performing.

- Oracle Internet Directory Administration Tools
- Oracle Internet Directory Data Management Tools
- Oracle Internet Directory Replication Management Tools
- Oracle Directory Integration Platform Tools

See Oracle Internet Directory Administration Tools for more information on the various command-line tools.

2
Oracle Internet Directory Administration Tools

Understand about the various command-line tools and utilities that are used to administer Oracle Internet Directory.

> **Note:**
>
> The term "instance" refers to an Oracle Internet Directory instance in `oidctl` documentation.

- Oracle Internet Directory Database Password Utility
- Oracle Internet Directory Control Utility
- Oracle Internet Directory Server Diagnostic Command-Line Tool
- Oracle Internet Directory Monitor Command
- About Oracle Internet Directory Command Line Utility - WLST
- Oracle Internet Directory Database Statistics Collection Tool
- Oracle Internet Directory Credential Management Tool
- Oracle Internet Directory Realm Tool
- Oracle Internet Directory Administration Tools Command Reference

2.1 Oracle Internet Directory Database Password Utility

Understand about Oracle Internet Directory Database Password Utility (`oidpasswd`) command and how to use it.

- About Oracle Internet Directory Database Password Utility
- Using oidpasswd

For syntax and arguments, see Oracle Internet Directory Database Password Utility Command Reference.

2.1.1 About Oracle Internet Directory Database Password Utility

This section describes the utility of (`oidpasswd`) command in Oracle Internet Directory Database Password Utility.

You can use `oidpasswd` command for:

- 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 Fusion Middleware 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 superuser account, namely, `cn=orcladmin`.
- Reset an access control point (ACP) so that the subtree is accessible by the Oracle Internet Directory superuser.
- Manage the restricted superuser ACL.

2.1.2 Using oidpasswd

You can use the `oidpasswd` utility to change the OID Database password, create wallets for Directory Database, and manage Superuser accounts.

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

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

2.1.2.1 Changing the Password of Oracle Internet Directory Database

The following example shows how to change the Oracle Internet Directory database password.

To change the Oracle Internet Directory database password, perform the following:

```
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.

> **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.

2.1.2.2 Creating Wallets for Directory Database and Replication Server Passwords

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

To create wallets for the Oracle Internet Directory database password and the Directory Replication server password, perform the following:

```
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.

2.1.2.3 Unlocking the Superuser Account

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

To unlock the Oracle Internet Directory superuser account, `cn=orcladmin`, perform the following:

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

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

2.1.2.4 Resetting the Superuser Password

If you forget the Oracle Internet Directory superuser 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 superuser password and Oracle Internet Directory database password are the same. After installation, however, you can change the Oracle Internet Directory superuser password using `ldapmodify`. You can change the Oracle Internet Directory superuser password using the `oidpasswd` tool separately.

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

```
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
```

2.1.2.5 Managing Superuser Access Control Points

The following example shows how to reset a restricted ACP.

When an access control point (ACP) is set with an access control item (ACI) that has the keyword `DenyGroupOverride`, neither the Oracle Internet Directory superuser 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 superuser.

To reset a restricted ACP, use the `oidpasswd` utility prompt to enter the Oracle Internet Directory database password and to choose which superuser restricted ACPs to reset.

```
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 superuser can access them, you can use `ldapmodify` to make the subtrees inaccessible to the superuser again.

2.2 Oracle Internet Directory Control Utility

Understand about the usage of the Oracle Internet Directory Control Utility (`oidctl`) command.

- About Oracle Internet Directory Control Utility
- Using oidctl

For syntax and arguments, see Oracle Internet Directory Control Utility Command Reference.

2.2.1 About Oracle Internet Directory Control Utility

Oracle Internet Directory Control Utility (`oidctl`) is a command-line tool for starting and stopping Oracle Identity Management server instances.

In 12c Release 2 (12.2.1.3.0), it is typically used only to configure, start, and stop the Oracle Directory Replication Server.

> **Note:**
>
> - You must set the environment variables `DOMAIN_HOME`, `ORACLE_HOME`, `INSTANCE_NAME` and `COMPONENT_NAME` before you run the `oidctl` command. Alternatively, you can pass the instance name and component name in the command line as `name=instanceName`, `componentname=componentName`.
> - Best practice is to create new Oracle Internet Directory instances by creating new Oracle Internet Directory components by using `wlst` command- `oid_createInstance`. You should use `oidctl` to create an instance *only if* you plan to run Oracle Internet Directory in standalone mode and not use Oracle Enterprise Manager.
> - The term "instance" refers to an Oracle Internet Directory instance in `oidctl` command documentation.

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 Oracle Internet Directory Monitor Command.

2.2.2 Using oidctl

In 12c Release 2 (12.2.1.3.0), oidctl is used primarily to manage the replication server.

The recommended tools for creating instances and managing the LDAP server are WebLogic Domain Framework tools which includes WLST commands and `startComponent.sh` and `stopComponent.sh`, not `oidctl`. You should only use `oidctl` for these purposes if you plan to run Oracle Internet Directory in standalone mode and never use Oracle Enterprise Manager.

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 Oracle Internet Directory Monitor Command for more information about Oracle Internet Directory Monitor.

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

- Creating an Oracle Internet Directory Instance in an Existing Component
- Deleting an Oracle Internet Directory Instance in a Component
- Starting an Oracle Internet Directory Server Instance
- Stopping an Oracle Internet Directory Server Instance
- Restarting an Oracle Internet Directory 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
- Reporting Diagnostics
- Reporting Server Manageability Information

2.2.2.1 Creating an Oracle Internet Directory Instance in an Existing Component

This section describes the procedure to create an Oracle Internet Directory instance in an exiting component.

To create another Oracle Internet Directory instance within an existing component, type

```
oidctl connect=connect_string server=oidldapd inst=new_instance_number \
   name=instanceName componentname=componentName  \
   flags=port=non_ssl_port sport=ssl_port add
```

The name and component name arguments are required unless the environment variables `INSTANCE_NAME` and `COMPONENT_NAME` have been set. Typically, the `inst` value of the original instance is `1`, the second instance you create is `2`, and so forth.

As an example:

```
oidctl connect=oiddb server=oidldapd inst=2 "flags=port=5678 sport=5679" add
```

2.2.2.2 Deleting an Oracle Internet Directory Instance in a Component

This section describes the procedure to delete an Oracle Internet Directory instance in a component.

To delete one Oracle Internet Directory instance within a component, type

```
oidctl connect=connect_string server=oidldapd inst=new_instance_number \
   name=instanceName componentname=componentName  \
   flags=port=non_ssl_port sport=ssl_port delete
```

Typically, the `inst` value of the original instance is `1`, the second instance you create is `2`, and so forth.

2.2.2.3 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.

Before starting a new instance of `OIDLDAPD`, run the command:

```
oidctl connect=connstr status
```

to make sure `oidmon` is running and that the instance number and ports that you intend to use are not already in use.

For example:

```
oidctl connect=dbs1 server=OIDLDAPD instance=2 flags="-p 3133 \
   -debug 1024  -l false" start
```

2.2.2.4 Stopping an Oracle Internet Directory Server Instance

This section describes the procedure to stop an Oracle Internet Directory server instance using command line.

Perform the following task:

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

2.2.2.5 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.

```
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.

2.2.2.6 Starting a Directory Replication Server Instance

When starting an Oracle Directory Replication server, you must supply the information it needs to connect to the Oracle Internet Directory server. You cannot use the `add` option when starting a replication server.

For example:

```
oidctl connect=dbs1 server=OIDREPL instance=1 flags="-p 3060 \
   -h ldaphost.example.com -d 1024" start
```

This command uses the same instance-specific configuration entry as `instance=1`.

2.2.2.7 Stopping a Directory Replication Server Instance

This example describes the usage of the command to stop a directory replication server instance.

To stop a directory replication server instance, use the following command:

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

2.2.2.8 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 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) on a virtual host.

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

2.2.2.9 Reporting the Status of Each Server

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

To report the status of each server running on the node, follow the below given instruction:

```
oidctl connect=dbs1 status
```

2.2.2.10 Reporting Diagnostics

Use the `-diag` flag with the `status` argument to get detailed diagnostic information that can be useful in resolving performance issues.

The `-diag` flag causes `oidctl` to print information about each LDAP operation as it executes, including the time it spends in the database layer.

For example:

```
oidctl connect=dbs1 status -diag

oidctl : ORACLE_INSTANCE is not set, defaulting to /ade/rsathyan_ldmain5/oracle/
ldap/
oidctl : INSTANCE_NAME   is not set, defaulting to inst1
oidctl : COMPONENT_NAME  is not set, defaulting to oid1
  +-------------------------------------------------------------------------+
  | Process      |  PID   | InstName   | CompName  | Inst# | Port | Sport  |
  +-------------------------------------------------------------------------+
  | oidmon       |  12838 |      inst1 |      oid1 |       |      |        |
+-------------------------------------------------------------------------+
  | oidldapd disp|  12926 |      inst1 |      oid1 |      1| 8856 |      0 |
  | oidldapd serv|  12930 |      inst1 |      oid1 |      1| 8856 |      0 |
  | Config   DN  | cn=oid1,cn=osdldapd,cn=subconfigsubentry                |
  +-------------------------------------------------------------------------+
```

```
  +-------------------------------------------------------------------------+
  |Printing LDAP Operation in progress status ...                           |
  +-------------------------------------------------------------------------+
    Search:
      OIDLDAPD_PID: 12930 WorkerID: 8 DBSID: 162
      ConnDN:
      BaseDN:c=us
      Scope=2
        Filter=(|(uid=a*)(cn=b*)
(objectclass=person))
ReqdAttrs:
      SqlText:
        SELECT /*+ FIRST_ROWS */ dn.entryid FROM ct_dn dn WHERE dn.entryi
        d IN (SELECT /*+ INDEX( at1 VA_uid ) */ entryid FROM CT_uid at1 W
        HERE attrValue  like :0 ESCAPE '\'  UNION SELECT /*+ INDEX( at1 V
        A_cn ) */ entryid FROM CT_cn at1 WHERE attrValue  like :1 ESCAPE
        '\'  UNION SELECT /*+ INDEX( at1 VA_objectclass ) */ entryid FROM
         CT_objectclass at1 WHERE attrValue  = 'person') AND ( (dn.parent
        dn like :bdn  ESCAPE '\' OR (dn.rdn = :rdn AND dn.parentdn = :pdn
        )) ) AND dn.entryid >= :entryThreshold

      Plan Hash Value :          0
      Rows Fetched    :          0
      Number of Sorts :          0
      Disk Read       :          0
      Disk Writes     :          0
      Buffer Gets     :          0
      IO Wait Time    :          0 (ms)
      CPU Time        :          0 (ms)
  +-------------------------------------------------------------------------+
```

2.2.2.11 Reporting Server Manageability Information

This procedure describes the server manageability information reporting.

When you run `oidctl` with `status -opdiag` *`interval`*, `oidctl` reads the shared memory contents for all servers in the running instances associated with the OIDMON in that environment and aggregates the operation count of each type for each OID component. It repeatedly displays current and total operation counts on the standard output at *`interval`* seconds. `oidctl` resets all the current values of operation count in the shared memory so that the directory server starts from zero for each type of operation for the next cycle.

For example:

```
$ oidctl status -opdiag 15
oidctl : ORACLE_INSTANCE is not set, defaulting to
/ade/myOID/oracle/ldap/
oidctl : INSTANCE_NAME   is not set, defaulting to inst1
oidctl : COMPONENT_NAME  is not set, defaulting to oid1

+-------------------------------------------------------------------------+
+-------------------------------------------------------------------------+
 |Printing completed LDAP operation counts ...
| +-----------------------------------------------------------------------+
  ComponentName: oid1       Current    Total
              Bind Count     : 0          0
              Add Count      : 0          0
              Delete Count   : 0          0
              Modify Count   : 0          0
```

```
                ModRdn Count   : 0           0
                Compare Count  : 0           0
                Search Count   : 0           0
                Extended Count : 0           0
. +-------------------------------------------------------------------------+
 +-------------------------------------------------------------------------+
```

2.3 Oracle Internet Directory Server Diagnostic Command-Line Tool

Understand about the usage of Oracle Internet Directory Server Diagnostic command-line tool (`oiddiag`).

This section contains the following topics:

- About Oracle Internet Directory Server Diagnostic Command-Line Tool
- Using oiddiag

For syntax and arguments, see Oracle Internet Directory Server Diagnostic Command Reference.

2.3.1 About Oracle Internet Directory Server Diagnostic Command-Line Tool

The Oracle Internet Directory Server Diagnostic command-line tool (`oiddiag`) collects diagnostic information that helps triage issues reported on Oracle Internet Directory. It is available as `oiddiag` for use on UNIX and Linux platforms and as `oiddiag.bat` for Windows.

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 are 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
- The SYS database user password

  If you do not know the SYS database user password, then you can skip it by pressing the Enter key. In this case, the tool does not collect any diagnostic data that requires sysdba privileges.

- Whether the Oracle Database connection uses SSL or not, only `NoSSL Authentication` (Encryption only) is supported.

If you use `collect_stats=true` argument, in addition to prompting for above information, a range of snapshot timestamps are also listed, and then it prompts you for following information:

- The begin snapshot ID
- The end snapshot ID

The valid range for begin and end snapshot IDs are 1 ~ last ID. If you give an invalid one or leave empty, begin snapshot ID will default to 2nd last ID (or last one if there's only one snapshot ID), and end snapshot ID will default to the last ID. Also, if entered begin snapshot ID is greater than end snapshot ID, it'll be automatically swapped.

Additional directory details are prompted for generating replication related statistics:

- The hostname of host running OID server
- The port on which OID server is listening
- The replication dn password

You can find the host name, port number and service name in the file `tnsnames.ora`, located by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config/`. For example, in the following `tnsnames.ora` file, the hostname, port number and service names are, respectively, `sun16.example.com`, `1521`, and `orcl.example.com`:

```
OIDDB =
 (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = sun16.example.com)(PORT = 1521))
   (CONNECT_DATA =
     (SERVER = DEDICATED)
     (SERVICE_NAME = orcl.example.com)
   )
 )
```

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

2.3.2 Using oiddiag

Using the Oracle Internet Directory diagnostic tool, you can collect diagnostics and stack trace information.

- Collecting All Diagnostic Information
- Collecting Selected Diagnostic Information
- Collecting Stack Trace Information
- Collecting Diagnostic Information in HTML Format

2.3.2.1 Collecting All Diagnostic Information

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

.

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

2.3.2.2 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 *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/tools/oiddiag.txt` (for the list) and *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/tools/oiddiag`*`timestamp`*`.log` (for the output file).

```
oiddiag listdiags=true
oiddiag collect_sub=true
```

2.3.2.3 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
```

2.3.2.4 Collecting Diagnostic Information in HTML Format

By giving `collect_stats=true [outfile=`*`filename`*`]` command line argument, you can collect following statistics within a specified timestamp range and generate an HTML report:

- Instance Statistics
- Operations Statistics
- Top Operations Statistics
- Memory/CPU Usage Statistics
- Network Bytes Sent/Received
- Client Connections/Operations Statistics

- DB Connections Statistics
- LDAP Connections Statistics
- Replication Operations Statistics
- Replication Queue Statistics (for all replication agreements)

The following example shows how to collect above diagnostic information in html format and write to the specified output file:

```
oiddiag collect_stats=true outfile=/mypath/oiddiag.html
```

If output file is not supplied, the default output file would be *$DOMAIN_HOME*`/tools/OID/logs/oiddiag<timestamp>.html`

2.4 Oracle Internet Directory Monitor Command

Understand about the usage of Oracle Internet Directory Monitor command-line tool (`oidmon`).

This section contains the following topics:

- About Oracle Internet Directory Monitor Command
- Using oidmon

For syntax and arguments, see Oracle Internet Directory Monitor Command Reference.

2.4.1 About Oracle Internet Directory Monitor Command

In 12c Release 2 (12.2.1.3.0), you typically manage Oracle Internet Directory by using Oracle Enterprise Manager or the WebLogic Domain Framework tools which includes WLST commands and `startComponent.sh` and `stopComponent.sh`.

2.4.2 Using oidmon

Using Oracle Internet Directory Monitor, you can start and stop Oracle Internet Directory Monitor.

This section contains the following topics:

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

2.4.2.1 Starting Oracle Internet Directory Monitor

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

For example:

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

2.4.2.2 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.

For example:

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

2.4.2.3 Stopping Oracle Internet Directory Monitor

Stopping Oracle Internet Directory Monitor also stops 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 starts all the server processes it had stopped previously.

For example:

```
oidmon connect=dbs1 stop
```

2.5 About Oracle Internet Directory Command Line Utility - WLST

Understand about the usage of Oracle Internet Directory Server Diagnostic command-line tool (`wlst`).

This section contains the following topics:

- Using WLST Command Line Utility

2.5.1 Using WLST Command Line Utility

Using the WLST command Utility, you can perform the Oracle Internet Directory server management tasks.

You can perform Oracle Internet Directory-related tasks from the command line by using WLST Commands.

See Managing Oracle Internet Directory Components by Using WLST Commands in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

2.6 Oracle Internet Directory Database Statistics Collection Tool

This section describes the Oracle Internet Directory Server Diagnostic command-line tool (`oiddiag`).

This section includes the following:

- About Oracle Internet Directory Database Statistics Collection Tool
- Running the Oracle Internet Directory Database Statistics Collection Tool

For syntax and arguments, see Oracle Internet Directory Database Statistics Collection Tool Command Reference.

2.6.1 About Oracle Internet Directory Database Statistics Collection Tool

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`), 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 processes.

> **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.

2.6.2 Running the Oracle Internet Directory Database Statistics Collection Tool

Use the command provided in this topic to run the Oracle Internet Directory database statistics collection tool.

Execute the command as given below:

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

2.7 Oracle Internet Directory Credential Management Tool

The Oracle Internet Directory Credential Management Tool is used to add, update, or delete a credential that has been created in the Credential Store Framework.

For more information, see Updating Credential Required by Enterprise Manager to manage OID - oid_setProperties().

2.8 Oracle Internet Directory Realm Tool

The Oracle Internet Directory realm tool is used to create multiple realms in Oracle Internet Directory. The individual realms can be managed separately, so you can use `oidrealm` as a replacement for Delegated Administration Services.

The `oidrealm` tool supports creation, but not deletion, of a realm. A procedure for deleting a realm is provided in Note 604884.1, which is available on My Oracle Support at `https://support.oracle.com/`

For more information, see Oracle Internet Directory Realm Tool Command Reference.

2.9 Oracle Internet Directory Administration Tools Command Reference

Understand about the Oracle Internet Directory Administration Tools Command and its usage from the following topics.

This section contains the following topics:

- Oracle Internet Directory Database Password Utility Command Reference
- Oracle Internet Directory Control Utility Command Reference
- Oracle Internet Directory Server Diagnostic Command Reference
- Oracle Internet Directory Monitor Command Reference
- About Oracle Internet Directory Command Line Utility - WLST
- Oracle Internet Directory Database Statistics Collection Tool Command Reference
- Oracle Internet Directory Realm Tool Command Reference

2.9.1 Oracle Internet Directory Database Password Utility Command Reference

Understand about the `oidpasswd` syntax and arguments.

- Syntax for oidpasswd
- Arguments for oidpasswd
- Related Command-Line Tools for oidpasswd

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

Arguments for oidpasswd are as follows:

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 by default in *`ORACLE_HOME`*`/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

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 prompts you for additional information. The following choices are available:

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

  > **Note:**
  >
  > In an Oracle Real Application Clusters (Oracle RAC) environment, if you update the password on one Oracle RAC node, then you must update the wallet on the other Oracle RAC nodes. Refer to Changing the Password of the ODS Schema Used by Oracle Internet Directory topic in *Additional Oracle Internet Directory High Availability Issues* section in *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 from the connected database.

  You must 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 Fusion Middleware administrator.

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

Related Command-Line Tools for oidpasswd

- See ldapmodify
- Oracle Internet Directory Monitor Command

2.9.2 Oracle Internet Directory Control Utility Command Reference

Understand about the `oidctl` syntax and arguments.

Refer to the following sections:

- Syntax for oidctl

Syntax for oidctl

```
oidctl [connect=connect_string] { server=OIDLDAPD | OIDREPLD }
instance=instance_number [name=instance_name] [componentname=component_name]
[host=host_name] [flags="flagname=value ..." ] [
{start | stop | add | delete | status [-diag | -odiag interval]}
```

Arguments for oidctl

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 by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

server=*server*
Required. The options are:

- `OIDLDAPD` — Oracle Internet Directory server
- `OIDREPLD` — Directory Replication server

instance=*instance_number*
Required. The numerical value of the instance. The value must be greater than 0 but less than 100.

host=*host_name*
Optional. Name of the logical host where the server is located or will be added. If you are using this argument, make sure `oidmon` is also started with the `host=host_name` parameter.

name=*instance_name*
Optional. Name of the instance to be used. The default is `inst1`.

componentname=*component_name*
Optional. Name of the component to be used. The default is `oid1`.

flags="*flagname=value* | *-flag value...*"
The flags argument is needed only while starting the server. If the flags consist of UNIX-style keywords, then the keyword-value pairs must be separated by spaces.

start | stop | restart | add | delete | status
Required. The operation to perform on the given server process.

- start — Start the server=*server* instance=*instance_number* [name=*instance_name* componentName=*component_name*]
- stop — Stop the server=*server* instance=*instance_number* [name=*instance_name* componentName=*component_name*]
- add — Add the instance-specific configuration entry and start the server instance.
- delete — Stop the server instance and delete the instance-specific configuration entry

- status [-diag | -opdiag] — Report the status of running server instances. Use `-diag` with `status` to get diagnostic information. Use `-opdiag`, followed by *`interval`*, an integer value, with `status` to get the operation count for each operation for each Oracle Internet Directory component.

OIDLDAPD Flags

In 12c Release 2 (12.2.1.3.0), the recommended tools for creating instances and managing the LDAP server are WebLogic Domain Framework tools which includes WLST commands and `startComponent.sh` and `stopComponent.sh`, not `oidctl`. You should only use `oidctl` for these purposes if you plan to run Oracle Internet Directory in standalone mode and never use Oracle Enterprise Manager.

-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`. This option has effect only when creating an Oracle Internet Directory instance.

-p *ldap_port*
Optional. Specifies the LDAP port that this Oracle Internet Directory server instance will use. If not specified the default 3060 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 3133 is used.

-work *maximum_threads*
The maximum number of worker threads for this server.

OIDREPLD Flags

-p *directory_port_number*
Required for a start operation. Port number used to connect to Oracle Internet Directory server. The default is 3060.

-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.

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

-sizelimit *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.

Related Command-Line Tools for oidctl

See Oracle Internet Directory Monitor Command.

2.9.3 Oracle Internet Directory Server Diagnostic Command Reference

Understand about the `oiddiag` syntax and arguments.

Refer to the following sections:

Syntax for oiddiag

```
oiddiag {listdiags=true [targetfile=filename]} | {collect_all=true
[outfile=filename]} |
{collect_sub=true [infile=filename] [outfile=filename]} |{collect_stats=true
[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 *$DOMAIN_HOME*`/config/fmwconfig/components/OID/tools/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 *$DOMAIN_HOME*`/config/fmwconfig/components/OID/tools/oiddiag.txt`.

collect_all=true
Collect all of the diagnostic information available and writes it to an output file. You are 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 *$DOMAIN_HOME*`/tools/OID/logs/oiddiag<timestamp>.[log|html]`.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 are 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 *$DOMAIN_HOME*/config/fmwconfig/components/OID/tools/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.

collect_stats=true
Collects the following diagnostic information available and writes it to an output file in html format:

- Instance Statistics
- Operations Statistics
- Top Operations Statistics
- Memory/CPU Usage Statistics
- Network Bytes Sent/Received
- Client Connections/Operations Statistics
- DB Connections Statistics
- LDAP Connections Statistics
- Replication Operations
- StatisticsReplication
- Queue Statistics (for all replication agreements)

You are prompted to provide the Oracle Internet Directory database host name, listener port, net service name, ODS and SYS database users password, begin and end snapshot IDs, and additional directory details for replication related statistics (hostname, OID server port, replication dn password).

2.9.4 Oracle Internet Directory Monitor Command Reference

Understand about the oidmon syntax and arguments.

Refer to the following sections:

- Syntax for oidmon
- Arguments for oidmon
- Related Command-Line Tools for oidmon

Syntax for oidmon

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

Arguments for oidmon

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 by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

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).

Related Command-Line Tools for oidmon

See Oracle Internet Directory Control Utility.

2.9.5 Oracle Internet Directory Database Statistics Collection Tool Command Reference

Understand about the usage of Oracle Internet Directory Database Statistics Collection Tool `oidstats.sql` syntax and arguments.

Refer to the following sections:

- Syntax for oidstats.sql
- Arguments for oidstats.sql
- Related Command-Line Tools for oidstats.sql

Syntax for oidstats.sql

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

Arguments for oidstats.sql

If you do not supply the ODS password on the command line, `sqlplus` prompts for it. Note that the default ODS password is the same as that for the Oracle Application Server administrator. (For security reasons, avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. When you supply a password at a prompt, it is not visible on the screen.)

connect_string
Required. The connect string for the ODS database. This is the network service name set in the `tnsnames.ora` file, which is located by default in *`$DOMAIN_HOME/`*

`config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

Related Command-Line Tools for oidstats.sql

See bulkload.

2.9.6 Oracle Internet Directory Realm Tool Command Reference

Understand about the `oidrealm` syntax and arguments.

Refer to the following sections:

- Syntax for oidrealm
- Arguments for oidrealm
- Example for oidrealm

Syntax for oidrealm

The syntax for Syntax for oidrealm are as follows:

On UNIX or Linux:

```
oidrealm oid_host oid_port DN [-SSL]
```

On Windows:

```
oidrealm.bat oid_host oid_port DN [-SSL]
```

> **Note:**
>
> If you specify an SSL port, that port must be configured in SSL No Authentication Mode, that is, `orclsslauthentication` must be `1`. For more information, see the section on SSL authentication modes in SSL Authentication Modes in *Oracle Internet Directory*.

Arguments for oidrealm

The arguments for oidrealm are as follows:

oid_host
Name of host where Oracle Internet Directory is running.

oid_port
Specifies the port number to use, which can be either SSL or non-SSL

DN
DN of realm to add

[-SSL]
Specifies that the port is an SSL port. Only no-auth mode is supported.

Example for oidrealm

```
$ oidrealm myhost.example.com 3133 'dc=newrealm,dc=com' -SSL
Enter OID Admin Password: password

[info] ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidSubscriberCreateCommon.lst *
Feb 2, 2009 9:22:57 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO: ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidSubscriberCreateCommon.lst *
[info]    ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreate.lst *
Feb 2, 2009 9:22:57 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO:    ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/oidContextCreate.lst *
[info]       -> LOADING:  /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextCreateCommon.sbs
Feb 2, 2009 9:22:57 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO:       -> LOADING:  /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextCreateCommon.sbs
[info]       ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextUpgradeFrom81600.lst *Feb 2, 2009 9:22:58 PM
oracle.ldap.util.LDIFLoader recursiveLoad
INFO:       ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextUpgradeFrom81600.lst*
[info]          -> LOADING:  /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextUpgradeFrom81600Common.sbs
Feb 2, 2009 9:22:58 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO:          -> LOADING:  /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextUpgradeFrom81600Common.sbs
[info]       ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextCreate90100Changes.lst *
Feb 2, 2009 9:23:00 PM oracle.ldap.util.LDIFLoader recursiveLoad
INFO:       ->> /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextCreate90100Changes.lst *
[info]          -> LOADING:  /scratch/mydir/mwhome/idm3/ldap/schema/oid/
oidContextUpgradeFrom90000Common.sbs
Feb 2, 2009 9:23:00 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
...
...
...
...
```

3

Oracle Internet Directory Data Management Tools

You can use the data management command-line tools to administer the entries and data stored in Oracle Internet Directory.
This section contains the following topics:

> **Note:**
>
> - The bulk tools do not support attribute uniqueness.
> - If your schema were created during installation of a version prior to 11g Release 1 (11.1.1.6.0), you must add data files to the OLTS_CT_STORE and OLTS_ATTRSTORE tablespaces if you intend to add more than a million entries to Oracle Internet Directory. Perform this step prior to the `bulkload` or `ldapadd` operation. For details, see the section Creating Data Files and Adding Data Files to a Tablespace in *Oracle Database Administrator's Guide*.

3.1 bulkdelete

The `bulkdelete` command-line tool enables you to delete one or more subtrees efficiently.

The `bulkdelete` command 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.

You must restrict LDAP activity against the subtree during deletion.

> **Note:**
>
> The `bulkdelete` command requires that the environment variable `DOMAIN_HOME` be set.

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

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

You can delete all entries in a naming context and make them tombstone entries by using `bulkdelete` command.

Execute the following command:

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

3.1.2 Completely Deleting All Entries in a Naming Context

You can completely delete all the entries in a naming context by using `bulkdelete` command without proving any `cleandb` option.

Execute the following command:

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

3.1.3 Deleting Entries in Multiple Naming Contexts

You can delete entries in multiple naming contexts by providing a file containing the list of DNs to be deleted.

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

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

3.2 bulkload

The `bulkload` command-line tool is useful for loading large number of entries into a directory server.

The `bulkload` command 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 LDIF File Format for the correct format and syntax of an LDIF file.

Intermediate files used by `bulkload` are stored in*$DOMAIN_HOME*`/tools/OID/load` by default. For more information, refer to the following sections:

- Using bulkload with Replication
- Overview of the Bulk Loading Tool Operations
- Prerequisites for Using the Bulkload Tool
- Tasks and Examples for bulkload

3.2.1 Using bulkload with Replication

When you add data to a node that is part of a Directory Replication Group (DRG), you can use either bulk tools or LDAP tools, depending on the circumstances.

> **Note:**
>
> The `bulkload` command requires that the environment variable `DOMAIN_HOME` be set.

When you add data to a node that is part of a Directory Replication Group (DRG), you can use either bulk tools or LDAP tools, depending on the circumstances. The following rules apply:

- When you add new entries to all nodes in the DRG, you can use either bulk tools or LDAP tools. For more than 20K entries, bulk tools are significantly faster. If you use LDAP tools, add the entries to only one node in the DRG and let replication propagate the entries. If you use bulk tools, generate the intermediate file only once from the LDIF file and use that intermediate file to load the entries onto all the nodes in the DRG.
- When you copy existing entries from one node to another in the same replication group, use bulk tools. Use the `bulkload` option `restore=true` when you upload the data.
- If the LDIF file contains operational attributes, which it does when created with `ldifwrite`, use `bulkload` to add the entries.
- If the replication agreement is a partial replication agreement, use `ldifwrite` with the base DN as the replication agreement DN to write the entries to the LDIF file. Then use `bulkload` with the `restore=true` option to load the data.

3.2.2 Overview of the Bulk Loading Tool Operations

The Bulk Loading tool performs **Check**, **Generate**, **Load** actvities.

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 reports 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.

> **Note:**
>
> - Running the `bulkload -load` operation sets the server mode to read-write. If you require a different mode, reset it after performing the `load` operation.
> - At the start of the load operation, `bulkload` determines the current configured value of `orclRIenabled`, then disables referential integrity. At the end of load phase, bulkload returns `orclRIenabled` to its original value. If is any referential integrity violations occurred, however, referential integrity is disabled, and you see the message:
>
>   ```
>   There is a violation of Referential Integrity and hence
>   it is Disabled now. Run the OIDDIAG tool with diagnostic
>   option to collect the Entries which have dangling DN
>   attribute values and Fix the violation
>   ```
>
>   Fix the violation and then set orclRIenabled to the desired value.

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`.

3.2.3 Prerequisites for Using the Bulkload Tool

Ensure these prerequisites are met 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. Take a cold backup of the Oracle Internet Directory database.
3. If loading data in incremental mode, you do not need to stop the directory server, although you must put the directory server in read-modify mode. Read-modify mode restricts add, delete, and modify DN operations.
4. If loading an LDIF file with data from an older version of Oracle Internet Directory, see the *Planning an Upgrade of Oracle Fusion Middleware* in *Oracle Fusion Middleware Planning an Upgrade of Oracle Fusion Middleware* for any special instructions about upgrading `orclguids` before you begin.

3.2.4 Tasks and Examples for bulkload

You can load data in various modes and verify and recreate indexes using the `bulkloadtool`.

This section contains the following topics:

3.2.4.1 Loading Data in Bulk Mode

This task describes the procedure for 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.

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

3.2.4.2 Loading Data for Multiple Nodes in a Replicated Environment

This task describes the procedure to load data for multiple nodes in a replicate 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).

3.2.4.3 Loading Data in Incremental Mode

This task describes the procedure to load data in incremental mode.

If you must 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.

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

3.2.4.4 Verifying Indexes

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

Execute the following command:

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

3.2.4.5 Recreating Indexes

This task describes the procedure to recreate 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.

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

3.2.4.6 Recovering Data After a Load Error

This task describes the procedure to recover 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`.

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

3.3 bulkmodify

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

> **Note:**
>
> The `bulkmodify` command requires that the environment variable `DOMAIN_HOME` be set.

For more information, refer to the following sections:

- About `bulkmodify` Tool
- Attributes Excluded from `add` or `replace` Operations Using the `bulkmodify` Tool
- Limitations of bulkmodify
- Updating an Attribute for Multiple Entries at Once

3.3.1 About `bulkmodify` Tool

Understand about the usage of `bulkmodify` tool.

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.

3.3.2 Attributes Excluded from `add` or `replace` Operations Using the `bulkmodify` Tool

Understand about the concept of excluding `add` or `replace` attributes while performing `bulkmodify`.

The `bulkmodify` tool does not allow `add` or `replace` operations on the following attributes:

- `dn` (use `ldapmoddn` instead)
- `cn` (use `ldapmodify` instead)
- `userpassword` (use `ldapmodify` instead)
- `orclpassword` (use `ldapmodify` instead)
- `orclentrylevelaci` (use `ldapmodify` instead)

- `orclaci` (use `ldapmodify` instead)
- `orclcertificatehash`
- `orclcertificatematch`
- any binary attribute
- any operational attribute

It does not allow `replace` operation on the attribute `objectclass`.

It does not allow `add` for single-valued attributes.

3.3.3 Limitations of bulkmodify

Understand about the limitations of `bulkmodify`command.

`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.

3.3.4 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"
```

3.4 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 "Attribute Values Matching Rules")

3.4.1 About catalog

As of Oracle Internet Directory 11g Release 1 (11.1.1.6.0) a new autocatalog feature is enabled by default in fresh installs.

You can also enable it if you have upgraded from a previous release. When this feature is enabled, Oracle Internet Directory automatically invokes the `catalog` command to index attributes when you search for them. If the autocatalog feature is not enabled, and you want to use previously uncataloged attributes in search filters, you must add them to the catalog entry, as in previous releases.

If the autocatalog feature is not enabled, and 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 Services Manager. However, if the attribute already exists, then you can index it only by using `ldapmodify` or the Catalog Management Tool (`catalog`).

> **Note:**
>
> - As of Oracle Internet Directory 11g Release 1 (11.1.1.6.0), you can use the LDAP tool `ldapmodify` to create and drop indexes from attributes. The `ldapmodify` tool actually invokes `catalog`, and you can still use `catalog` for this purpose.
> - The `catalog` command requires that the environment variable `DOMAIN_HOME` be set.
> - The `catalog` command cannot index more than 1000 attributes at a time. If more than 1000 attributes are present in the file, the tool throws an error. If you need to index more than 1000 attributes, use multiple files.

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

> **Note:**
>
> 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.

3.4.2 Tasks and Examples for catalog

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

- Indexing a Single Attribute
- Indexing Multiple Attributes

3.4.2.1 Indexing a Single Attribute

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

Example

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

3.4.2.2 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 prompts you for the Oracle Internet Directory superuser password.

Example

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

3.4.2.3 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 prompts you for the Oracle Internet Directory superuser password.

Example:

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

3.4.2.4 Indexing an Attribute Using the IOT Option

The following example indexes the specified attribute and creates an IOT table to improve performance by not creating an additional index.

The `catalog` tool prompts you for the Oracle Internet Directory superuser password.

Example:

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

3.5 ldapadd

Using the example, understand how to index the specified attribute and create an IOT table to improve performance by not creating an additional index.

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.

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

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

3.5.1 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 LDIF File Format for information about formatting an LDIF file.

Example:

```
ldapadd -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
   -f ~/myfiles/input.ldif -v
```

3.5.2 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" -q -p 3060 \
    -X ~/myfiles/input.xml -v
```

3.5.3 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" -q -p 3060 \
    -X ~/myfiles/input.xml -v -n
```

3.6 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.

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 LDIF File Format for information about formatting an LDIF file.

Example:

```
ldapaddmt -h myhost.company.com -D "cn=orcladmin" -q -T 5 -p 3060 \
    -f ~/myfiles/input.ldif -v
```

3.7 ldapbind

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

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" -q -p 3133 \
    -U 2 -W "file:/home/my_dir/my_wallet" -Q
```

3.8 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.

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" -q -p 3060 -a title \
    -b "cn=Anne Smith,ou=Sales,o=IMC,c=US" -v "Manager"
```

3.9 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 *Administering Oracle Internet Directory*.

3.9.1 Tasks and Examples for ldapdelete

You can perform single and multiple deletes using `ldapdelete`.

Using `ldapdelete` you can perform the following tasks:

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

3.9.1.1 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" -q \
   -p 3060 "cn=Anne Smith,ou=Sales,o=IMC,c=US"
```

3.9.1.2 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 LDIF File Format for information about formatting an LDIF file.

Example:

```
ldapdelete -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \      -f /home/
mydir/delete.ldif
```

3.10 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 *Administering Oracle Internet Directory*.

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

- Changing the RDN of an Entry
- Moving an Entry

3.10.1 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" -q -p 3060 \
    -b "cn=Mary Smith,dc=Americas,dc=IMC,dc=com" -R "cn=Mary Jones" -r
```

3.10.2 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" -q -p 3060 \
    -b "cn=Mary Smith,dc=Americas,dc=IMC,dc=com" -N "dc=Australia,dc=IMC,dc=com"
```

3.11 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 LDIF File Format 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 *Administering Oracle Internet Directory*.

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

- Modifying the Directory Schema
- Modifying an Entry
- Indexing an Attribute

3.11.1 Modifying the Directory Schema

You must first prepare your LDIF file to define the new schema elements you want to add. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the new schema definitions into the directory schema.

See Adding Schema Elements for examples.

Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -q -p 3060  \
    -f /home/myfiles/modify.ldif  -v
```

3.11.2 Modifying an Entry

You must first prepare your LDIF file correctly to modify the attributes or attribute values for an entry. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the changes.

See LDIF Format for Modifying Entries for examples.

Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -q \
    -p 3060 -f /home/myfiles/modify.ldif  -v
```

3.11.3 Indexing an Attribute

You can add or drop an attribute in the catalog entry by using `ldapmodify`.

As of Oracle Internet Directory 11g Release 1 (11.1.1.6.0) a new autocatalog feature is enabled by default in fresh installs. You can also enable it if you have upgraded from a previous release. When this feature is enabled, Oracle Internet Directory automatically invokes the `catalog` command to index attributes when you search for them. If the autocatalog feature is not enabled, and you want to use previously uncataloged attributes in search filters, you must add them to the catalog entry, as in previous releases.

To add an attribute, import an LDIF file by using `ldapmodify`. For example, to index the attribute `displayName`, import the following LDIF file by using `ldapmodify`:

Example:

```
dn: cn=catalogs
changetype: modify
add: orclindexedattribute
orclindexedattribute: displayName
```

Type a command similar to the following at the system prompt:

```
ldapmodify -D "cn=orcladmin" -q -h host -p port -f ldif_file_name
```

To index the attribute, the `ldapmodify` command invokes the Catalog Management tool, `catalog`. For information about that tool, see catalog.

To drop an index from an attribute by using `ldapmodify`, specify `delete` in the LDIF file. For example:

```
dn: cn=catalogs
changetype: modify
delete: orclindexedattribute
orclindexedattribute: displayName
```

3.12 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 LDIF File Format for more information about the correct formatting of LDIF files.

Modifying Multiple Entries Concurrently

To modify multiple entries at once, you must first prepare your LDIF file correctly. See LDIF File Format 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 3060 \
    -T 5 -f /home/myfiles/modify.ldif  -v
```

3.13 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 might 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 *Administering Oracle Internet Directory*

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 Operational Attributes of Entries
- Searching for Entries with Attribute Options
- Searching for All User Attributes and Specified Operational Attributes
- Searching for Entries (More Examples)
- Attribute Case in ldapsearch Output

3.13.1 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 3060 -h myhost -b "" -s base -v "objectclass=*"
```

3.13.2 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 3060 -h myhost -b "ou=HR, ou=Americas, o=IMC, c=US" -s one \
           -v "objectclass=*"
```

3.13.3 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 3060 -h myhost -b "c=US" -s sub -v "cn=Person*"
```

3.13.4 Searching for Attribute Values of Entries

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

Example:

```
ldapsearch -p 3060 -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 3060 -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 3060 -h myhost -b "c=US" -s sub -v "cn=Person*" dn sn description \
    -T sn -j 10
```

3.13.5 Searching for Operational Attributes of Entries

You can search for operational attributes using the ldapsearch command.

The following example returns only operational attributes:

```
$ ldapsearch -h adc2190517 -p 3060 -D cn=orcladmin -w welcome -b "c=uk" -L -s
base "(objectclass=*)" +
```

3.13.6 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 3060 -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 3060 -h myhost -b "c=us" -s sub "cn;lang-it=Giovanni"
```

3.13.7 Searching for All User Attributes and Specified Operational Attributes

With the help of examples, learn how to search for all user attributes and specified operational attributes.

Example:

```
ldapsearch -p 3060 -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` to index these two attributes. Then, restart the Oracle directory server before issuing the two previous ldapsearch commands.

3.13.8 Searching for Entries (More Examples)

Each of the following examples searches on port 3060 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 3060 -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 3060 -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 3060 -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 3060 -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 3060 -h sun1 -b "ou=hr, o=acme, c=us" \
           -s subtree "employeenumber<=10000"
```

3.13.9 Attribute Case in ldapsearch Output

In the output from the `ldapsearch` command, the attribute names are shown in lower case if the attribute `orclReqattrCase`in the instance-specific configuration entry is `0`. If `orclReqattrCase` is set to `1`, the attribute names in the output are shown in the same case in which they were entered on the command line.

Example:

```
ldapsearch -h localhost -p 389 -b "dc=oracle,dc=com" -s base -L "objectclass=*"
DC
```

If `orclReqattrCase` is `0` the output looks like this:

```
dn: dc=oracle,dc=comdc: oracle
```

If `orclReqattrCase` is `1`, the output looks like this:

```
dn: dc=oracle,dc=comDC: oracle
```

3.14 ldifmigrator

The Oracle Internet Directory Data Migration Tool is used to convert LDIF files output from other directories or application-specific repositories into a format recognized by Oracle Ineternet Direcotry.

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 for the correct format of the LDIF input file for this tool.

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

- Using the Data Migration Tool in Lookup Mode
- Loading Data for Multiple Nodes in a Replicated Environment
- 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 for examples of correctly formatted LDIF input files for use with the Data Migration Tool.

3.14.1 Using the Data Migration Tool in Lookup Mode

The migration tool looks up the directory server to figure out certain substitution variables specified in the LDIF input file.

In this example, Oracle Internet Directory server is present in the environment, and the migration tool looks up 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"
```

3.14.2 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"
```

3.14.3 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"
```

3.14.4 Loading and Reconciling Data Using the Data Migration Tool

The Data Migration Tool gives your the option of loading the data directly into the directory.

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
```

3.15 ldifwrite

The `ldifwrite` command-line tool enables you to convert to LDIF all or part of the information residing in a directory.

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` command requires that the environment variable `DOMAIN_HOME` be set.

> **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.

- Using ldifwrite with Replication
- Tasks and Examples for ldifwrite

3.15.1 Using ldifwrite with Replication

When you add data to a node that is part of a Directory Replication Group (DRG), you can use either bulk tools or LDAP tools, depending on the circumstances.

The following rules apply:

- When you add new entries to all nodes in the DRG, you can use either bulk tools or LDAP tools. For more than 20K entries, bulk tools are significantly faster. If you use LDAP tools, add the entries to only one node in the DRG and let replication propagate the entries. If you use bulk tools, generate the intermediate file only once from the LDIF file and use that intermediate file to load the entries onto all the nodes in the DRG.
- When you copy existing entries from one node to another in the same replication group, use bulk tools. Use the `bulkload` option `restore=true` when you upload the data.

- If the LDIF file contains operational attributes, which it does when created with `ldifwrite`, use `bulkload` to add the entries.
- If the replication agreement is a partial replication agreement, use `ldifwrite` with the base DN as the replication agreement DN to write the entries to the LDIF file. Then use `bulkload` with the `restore=true` option to load the data.

3.15.2 Tasks and Examples for ldifwrite

Using the `ldifwrite` command-line tool, you can convert entries to an LDIF file in various ways.

This section contains the following topics:

3.15.2.1 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.

Example:

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

3.15.2.2 Converting a Partial Naming Context to an LDIF File

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

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" \
          ldiffile="output2.ldif"
```

3.15.2.3 Converting Entries that Match 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"
```

3.16 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.

This section contains the following topics:

3.16.1 Before Running the upgradecert.pl Tool

Ensure the following conditions before running the `upgradecert.pl` command.

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.

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

Learn how to upgrades user certificates stored in the directory from releases prior to 10.1.2 by executing the command specified in this section.

To upgrade the user certificates:

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

3.17 Oracle Internet Directory Data Management Tools Command Reference

Learn about the syntax, attributes, and related commands for all Oracle Internet Directory Data Management Tools Command.

This section contains the following topics:

3.17.1 `bulkdelete` Command Reference

The following topics list and describe the `bulkdelete` syntax and arguments.

Syntax for `bulkdelete`

```
bulkdelete connect=connect_string {[basedn=Base_DN]|[file=file_name]}
[filter="LDAP_search_filter"] [encode=character_set] [debug="TRUE"|"FALSE"]
[cleandb="TRUE"|"FALSE"] [skipcheck="TRUE"|"FALSE"] [size=transaction_size]
[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 by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

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.

filter

Optional. The LDAP filter for entries to be deleted. This filter option allows you to delete only entries that match a specific LDAP filter condition. Using this option, you can delete a huge amount of data in a reasonable amount of time.

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 *`$DOMAIN_HOME/tools/OID/logs`*.

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.

skipcheck

Optional. The `skipcheck` option allows you to execute `bulkdelete` without stopping OID services. This is possible by passing `skipcheck="TRUE"` in the command line. Default is `skipcheck="FALSE"`.

size

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

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.

Related Command-Line Tools for bulkdelete

- See bulkload
- See bulkmodify
- See ldapdelete

3.17.2 `bulkload` Command Reference

The following topics list and describe the `bulkload` syntax and arguments.

- Syntax for bulkload
- Arguments for bulkload
- Related Command-Line Tools for bulkload

Syntax for bulkload

```
bulkload [connect=connect_string]
{[check="TRUE"|"FALSE"  [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"] [missing="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 by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.) 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:

```
bulkload connect="orcl1,orcl2,orcl3"
```

check | generate | load | recover | index | missing

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.
>
> – `bulkload` updates the mode to read-only when performing a 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 stopped. 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.
- `missing` - Creates only missing indexes on 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.

When the `restore` option is set to `TRUE`, then the operational attributes specified in the LDIF file are honored. If restore option is not specified or it is set to `FALSE`, then the operational attributes might not be retained, depending on the type of attribute. Best practice is to avoid having operational attributes in the LDIF file when the restore option value is FALSE.

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 *`DOMAIN_HOME`*`/tools/OID/logs`.

verbose

This is used to run the command in verbose mode.

Related Command-Line Tools for bulkload

- See bulkdelete
- See bulkmodify
- See ldapadd
- See ldapaddmt

3.17.3 `bulkmodify` Command Reference

The following topics list and describe the `bulkmodify` syntax and arguments.

- Syntax for bulkmodify
- Arguments for bulkmodify
- Related Command-Line Tools for bulkmodify

Syntax for bulkmodify

```
bulkmodify connect=connect_string basedn=Base_DN
{[add="TRUE"|"FALSE"]|[replace="TRUE"|"FALSE"]} attribute=attribute_name
value=attribute_value [-q] [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 by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

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.

-q

Optional. The `-q` option causes the command to prompt for a secure value instead of the command line value. A secure value supplied at the command prompt is not visible on the screen.

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 *`$DOMAIN_HOME`*`/tools/OID/logs`.

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.

Related Command-Line Tools for bulkmodify

- See bulkdelete
- See bulkload
- See ldapmodify
- See ldapmodifymt

3.17.4 `catalog` Command Reference

The following topics list and describe the `catalog` syntax and arguments.

- Syntax for catalog
- Arguments for catalog
- Related Command-Line Tools for catalog

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"] [iot="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 by default in *`$DOMAIN_HOME`*`/config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

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 *`$DOMAIN_HOME`*`/tools/OID/logs`.

iot

Optional. If set to TRUE, this option causes an Index Organized Table (IOT) to be created for the specified attribute without creating an additional index. The IOT option improves both read and write performance for a normal LDAP operation and reduces the storage as well. Use the IOT option when you expect lot of updates for the cataloging attribute. The default is FALSE.

verbose

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

Related Command-Line Tools for catalog

- N/A

3.17.5 `ldapadd` Command Reference

The following topics list and describe the `ldapadd` syntax and arguments.

- Syntax for ldapadd
- Arguments for ldapadd

- Related Command-Line Tools for ldapadd

Syntax for ldapadd

```
ldapadd -h oid_hostname -D "binddn" -q | -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]
[-U SSL_auth_mode {-W wallet_location -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w password` option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-Y ""*proxy_dn*

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

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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 LDIF File Format 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 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 are reported. If the `-c` argument is not used, the tool stops 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 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).

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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`.

Related Command-Line Tools for ldapadd

- See ldapaddmt
- See ldapmodify
- See bulkload

3.17.6 `ldapaddmt` Command Reference

The following topics list and describe the `ldapaddmt` syntax and arguments.

- Syntax for ldapaddmt
- Arguments for ldapaddmt
- Related Command-Line Tools for ldapaddmt

Syntax for ldapaddmt

```
ldapaddmt -h oid_hostname -D "binddn" -q | -w password -T number_threads
[-p ldap_port] [-V ldap_version] {-f ldif_filename | -X dsml_filename}  [-b] [-c]
[-M] [-O ref_hop_limit] [-U SSL_auth_mode {-W wallet_location -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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 3060.

-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 LDIF File Format 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 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 are reported. If the `-c` argument is not used, the tool stops 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.

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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`.

Related Command-Line Tools for ldapaddmt

- See ldapadd
- See bulkload

3.17.7 `ldapbind` Command Reference

The following topics list and describe the `ldapbind` syntax and arguments.

- Syntax for ldapbind
- Arguments for ldapbind
- Related Command-Line Tools for ldapbind

Syntax for ldapbind

```
ldapbind -h oid_hostname -D "binddn" -q | -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 -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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`.

Related Command-Line Tools for ldapbind

- N/A

3.17.8 `ldapcompare` Command Reference

The following topics list and describe the `ldapcompare` syntax and arguments.

Syntax for ldapcompare

```
ldapcompare -h oid_hostname -D "binddn" -q | -w password [-Y "proxy_dn"]
[-p ldap_port] -a attribute_name -b "base" -v "attribute_value"
[-U SSL_auth_mode {-W wallet_location -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-Y ""*proxy_dn*

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

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-a *attribute_name*

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

-b "*base*"

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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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`.

Related Command-Line Tools for ldapcompare

- N/A

3.17.9 `ldapdelete` Command Reference

The following topics list and describe the `ldapdelete` syntax and arguments.

- Syntax for ldapdelete
- Arguments for ldapdelete
- Related Command-Line Tools for ldapdelete

Syntax for ldapdelete

```
ldapdelete -h oid_hostname -D "binddn" -q | -w password [-Y proxy_dn]
[-p ldap_port] [-V ldap_version] {-f ldif_filename | "entry_dn"}
[-n] [-M] [-v] [-O ref_hop_limit]
[-U SSL_auth_mode {-W wallet_location -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-Y "*proxy_dn*"

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

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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 LDIF File Format 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.

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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`.

Related Command-Line Tools for ldapdelete

- See bulkdelete

3.17.10 `ldapmoddn` Command Reference

The following topics list and describe the `ldapmoddn` syntax and arguments.

- Syntax for ldapmoddn
- Arguments for ldapmoddn
- Related Command-Line Tools for ldapmoddn

Syntax for ldapmoddn

```
ldapmoddn -h oid_hostname -D "binddn" -q | -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 -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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`.

Related Command-Line Tools for ldapmoddn

- See ldapmodify

3.17.11 `ldapmodify` Command Reference

The following topics list and describe the `ldapmodify` syntax and arguments.

- Syntax for ldapmodify
- Arguments for ldapmodify
- Related Command-Line Tools for ldapmodify

Syntax for ldapmodify

```
ldapmodify -h oid_hostname -D "binddn" [-Y "proxy_dn"] -q | -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] [-U SSL_auth_mode {-W wallet_location -Q | -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 is performed as this user.

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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 LDIF File Format 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 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 are reported. If the `-c` argument is not used, the tool stops 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 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).

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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

Related Command-Line Tools for ldapmodify

- See ldapadd
- See ldapdelete
- See ldapmoddn

3.17.12 `ldapmodifymt` Command Reference

The following topics list and describe the `ldapmodifymt` syntax and arguments.

- Syntax for ldapmodifymt
- Arguments for ldapmodifymt
- Related Command-Line Tools for ldapmodifymt

Syntax for ldapmodifymt

```
ldapmodifymt -h oid_hostname -D "binddn" -q | -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
[-U SSL_auth_mode {-W wallet_location -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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 LDIF File Format 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 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 are reported. If the `-c` argument is not used, the tool stops 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.

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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

Related Command-Line Tools for ldapmodifymt

- See ldapaddmt
- See ldapmodify

3.17.13 `ldapsearch` Command Reference

The following topics list and describe the `ldapsearch` syntax and arguments.

- Syntax for ldapsearch
- Arguments for ldapsearch
- Related Command-Line Tools for ldapsearch

Syntax for ldapsearch

```
ldapsearch -h oid_hostname -D "binddn" -q | -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 -Q | -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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-Y "*proxy_dn*"

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

-p *ldap_port*

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 3060.

-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.

By default, `ldapsearch` does not return operational attributes. If you add the character "**+**" to the list of attributes in the search request, however, `ldapsearch` returns all operational attributes.

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

In the output, the attribute names are shown in lower case if the attribute `orclReqattrCase` is 0 in the instance-specific config entry. If `orclReqattrCase` is set to 1, the attribute names in the output are shown in the same case in which they were entered on the command line. See Attribute Case in ldapsearch Output.

-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 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`).

With the -L option, all attributes, including binary attributes are printed in LDAP Data Interchange Format (LDIF). Binary attributes are transformed into printable characters using BASE64 encoding.

> **See Also:**
>
> LDIF File Format for a description of LDAP Data Interchange Format.

-B

Optional. Allows printing of non-ASCII values. Binary attributes are printed as is, without encoding. The complete value might not be printed, as it might contain non-printable characters.

-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"
```

-Q

Required, unless `-P` is used, if using one way or two way SSL authentication (`-U 2|3`). Causes the command to prompt for the wallet password for the wallet specified in the `-W` argument. A password supplied at the command prompt is not visible on the screen.

-P *wallet_password*

Required, unless `-Q` is used, if using one way or two way SSL authentication (`-U 2|3`). The wallet password for the wallet specified in the `-W` argument. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-P` *`wallet_password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-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, see Table 6-2.

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

Related Command-Line Tools for ldapsearch

- See ldapcompare
- See catalog

3.17.14 `ldifmigrator` Command Reference

The following topics list and describe the `ldifmigrator` syntax and arguments.

- Syntax for ldifmigrator
- Arguments for ldifmigrator
- Related Command-Line Tools for ldifmigrator
- Error Messages for ldifmigrator

Syntax for ldifmigrator

```
ldifmigrator "input_file=filename" "output_file=filename"
[-lookup -h oid_hostname "dn=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 are obtained by looking up the correct values in the directory server. See Substitution Variables for Migration Input Files 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.

"**dn**=*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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

subscriber=*subscriberDN*

Optional. The subscriber whose attribute values is used in place of the substitution variables. If not specified, then the default identity management realm specified in the Root Oracle Context is 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 for instructions on adding a substitution variable to the input LDIF file. The `ldifmigrator` tool replaces 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 is 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 adds 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 Reconciliation Modes for Migrated Entries for more information about LDIF directives supported by the `-reconcile` option.

Related Command-Line Tools for ldifmigrator

- See ldapadd
- See ldapmodify
- See ldifwrite

Error Messages for ldifmigrator

The Data Migration Tool can display these error messages:

Table 3-1 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`
Environment variable `DOMAIN_HOME` not defined	`DOMAIN_HOME` is not defined.	Set the environment variable `DOMAIN_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.

Table 3-1 (Cont.) Error Messages of the Data Migration Tool

Message	Reason	Remedial Action
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 *$DOMAIN_HOME*`/tools/OID/logs`.
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:

$DOMAIN_HOME`/tools/OID/logs/LDIFMig_YYYY_MM_DD_HH_SS.log`.

3.17.15 `ldifwrite` Command Reference

The following topics list and describe the `ldifwrite` syntax and arguments.

- Syntax for ldifwrite
- Arguments for ldifwrite
- Related Command-Line Tools for ldifwrite

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 by default in *$DOMAIN_HOME*`/config/fmwconfig/components/OID/config/ directory`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

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 *`$DOMAIN_HOME`*`/tools/OID/logs`.

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

Related Command-Line Tools for ldifwrite

- ldapsearch
- ldifmigrator
- bulkload

3.17.16 `upgradecert.pl` Command Reference

The following topics list and describe the `upgradecert.pl` syntax and arguments.

- Syntax for upgradecert.pl
- Arguments for upgradecert.pl
- Related Command-Line Tools for upgradecert.pl

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`).

-q

Required unless `-w` is used. Causes the command to prompt for the user password needed to bind to the directory. A password supplied at the command prompt is not visible on the screen.

-w *password*

Required unless `-q` is used. The user password needed to bind to the directory. Avoid supplying a password on the command line whenever possible. A password typed on the command line is visible on your screen. The `-w` *`password`* option is disabled when `LDAP_PASSWORD_PROMPTONLY` is set to true. See Overview of Passwords with Command-Line Tools.

-t *temp_dir*

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

Related Command-Line Tools for upgradecert.pl

- N/A

4

Oracle Internet Directory Replication Management Tools

You can administer Oracle Internet Directory replication using the various management command-line tools.

- Managing Human Intervention Queue Management Tools
- Working with Oracle Internet Directory Compare and Reconcile Tool
- Oracle Internet Directory Compare and Reconcile Tool
- Replication Environment Management Tool

> **Note:**
>
> Refer Understanding Oracle Internet Directory Replication in *Administering Oracle Internet Directory*.

4.1 Managing Human Intervention Queue Management Tools

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.

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 the specified number of retries, 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 must:

1. Examine the change in the human intervention queue.
2. Reconcile the conflicting changes using the Compare and Reconcile Tool (see Working with Oracle Internet Directory Compare and Reconcile Tool.
3. Either place the change back into the retry queue, by using `ManageHiq.retry`, or into the purge queue, by using `ManageHiq.purge`.

This section describes the following topics:

- Invoking the Human Intervention Queue Management Tools
- Moving the Changelogs to the Retry Queue
- Purging the Changelog on a Node

> **Note:**
>
> The Oracle Internet Directory server parameter `orclSizeLimit`, which is 1000 by default, limits the number of entries that the human intervention queue manipulation tools 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 impacts server performance, because `orclSizeLimit` also controls the maximum number of entries to be returned by a search. The DN containing `orclSizeLimit` is
>
> `cn=componentname,cn=osdldapd,cn=subconfigsubentry`

4.1.1 Invoking the Human Intervention Queue Management Tools

You invoke `ManageHiq.retry` and `ManageHiq.purge` as PL/SQL commands at the SQL prompt.

You invoke `ManageHiq.retry` and `ManageHiq.purge` as PL/SQL commands at the SQL prompt, as follows:

```
$ sqlplus /nologSQL> connect ods;
SQL> Enter password
SQL> Set serveroutput ON
SQL> exec ManageHiq.retry(SupplierNode, EqualChgNo, StartChgNo, EndChgNo)
SQL> exit

$ sqlplus /nologSQL> connect ods;
SQL> Enter password
SQL> Set serveroutput ON
SQL> exec (ManageHiq.purgeSupplierNode, EqualChgNo, StartChgNo, EndChgNo)
SQL> exit
```

You must set server output ON to display the success or error message. The arguments are:

EqualChgNo–The change number to be moved to the retry queue.

StartChgNo–The starting number. All the change numbers after this should be moved to the retry queue.

EndChgNo–The ending change. All change numbers less than or equal to this change number that should be moved to the retry queue.

4.1.2 Moving the Changelogs to the Retry Queue

Move the changelog on node1, for change numbers between 300 and 1000 and supplier node2, to the retry queue

To move the changelog on node1, for change numbers between 300 and 1000 and supplier node2, to the retry queue.

```
exec Managehiq.retry('node2_orcl', 0, 300, 1000)
```

Move all the changelogs on node1 for supplier node2_orcl to the retry queue.

```
exec Managehiq.retry('node2_orcl', 0, 0, 0)
```

or

```
exec Managehiq.retry('node2_orcl')
```

4.1.3 Purging the Changelog on a Node

Purge the changelog on node1 where the change number is 2152 and the supplier is node2 (supplierNode = node2_orcl).

To purge the changelog on node1 where the change number is 2152 and the supplier is node2 (supplierNode = node2_orcl):

```
exec Managehiq.purge('node2_orcl', 2152)
```

Purge the changelog on node1 where the change number is greater than 200 and the supplier is node2_orcl.

```
exec Managehiq.purge('node2_orcl', 0, 200)
```

Or

```
exec Managehiq.purge('node2_orcl', 0, 200, 0)
```

Purge the changelog on node1 where the change number is less than 2000 and the supplier is node2_orcl.

```
exec Managehiq.purge('node2_orcl', 0, 0, 2000)
```

4.2 Working with Oracle Internet Directory Compare and Reconcile Tool

You can understand about the Oracle Internet Directory Compare and Reconcile Tool and how to perform tasks using the `oidcmprec` command.

The following topics provide a contextual description and syntax of the Oracle Internet Directory Compare and Reconcile Tool:

- Overview of the Compare and Reconcile Tool
- Operating the Compare and Reconcile Tool

4.2.1 Overview of the Compare and Reconcile Tool

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. You can also compare directory schema. For more information, see in Comparing and Reconciling Inconsistent Data by Using oidcmprec in *Administering Oracle Internet Directory*.

> **Note:**
>
> - The `oidcmprec` 11*g* tool supports data migration from 10*g* to 11*g*. However, data migration is not supported from 11*g* to 10*g*.
> - The Compare and Reconcile Tool, `oidcmprec` does not support One way or Two way Authentication and works only on the No-Authentication mode.

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`)

For more information on the syntax and arguments of the `oidcmprec` tool, see Oracle Internet Directory Compare and Reconcile Tool

4.2.2 Operating the Compare and Reconcile Tool

Using the `oidcmprec` command, you can perform compare and reconcile action on individual entries, subtrees and entire directories. Apart from these, you can perform host of other actions covered in this section using the `oidcmprec` command.

The following examples discuss various operations that can be performed with the `oidcmprec` tool:

- Comparing Individual Entries in Two Directories
- Reconciling Individual Entries in Two Directories
- Comparing Subtrees in Two Directories
- Reconciling Subtrees in Two Directories
- Comparing Entire Directories

- Reconciling Entire Directories
- Performing User-Defined Compare and Reconcile Operations
- Merging Two Directories
- Including and Excluding Attributes
- Using a Filter
- Overriding Default Conflict Resolution Rules
- Using a Parameter File
- Using a Parameter File in XML Format
- Generating Change Logs
- Performing Directory Schema Operations

4.2.2.1 Comparing 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.

```
oidcmprec base="'cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com'" \
          operation=compare \
          source=myhost1.acme.com:3060 \
          destination=myhost2.acme.com:3060

Enter replication DN password of the source directory      :
Enter replication DN password of the destination directory :
```

4.2.2.2 Reconciling Individual Entries in Two Directories

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.

```
oidcmprec base="'cn=Anne Smith,cn=users,dc=uk,dc=acme,dc=com'" \
          operation=reconcile \
          source=myhost1.acme.com:3060 \
          destination=myhost2.acme.com:3060
```

4.2.2.3 Comparing 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.

```
oidcmprec base="'dc=com'" \
          operation=compare scope=subtree \
          source=myhost1.mycom.com:3060 \
```

```
          destination=myhost2.mycom.com:3060 \
          threads=5 dnthreads=2 filename=cmpres
```

4.2.2.4 Reconciling Subtrees in Two Directories

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.

```
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:3060 \
          destination=myhost2.mycom.com:3060 \
```

4.2.2.5 Comparing 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.

```
oidcmprec operation=compare source=host1:3060 \
          destination=host2:3070 \ base="' '" scope=subtree
```

> **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.

4.2.2.6 Reconciling Entire Directories

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.

```
oidcmprec base="' '" \
          dns2exclude="'c=us,dc=mycom,dc=com'"
          operation=reconcile scope=subtree \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          threads=5 dnthreads=2 file=cmpres
```

4.2.2.7 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.

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`.

```
oidcmprec operation=userdefinedcr scope=subtree \
          base="'dc=com'  'dc=org'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          entos=add entod=ignore atros=add \
          svatrdif=usesrc mvatrdif=usesrc dndif=ignore \
          threads=5 dnthreads=2 file=myreconcile
```

4.2.2.8 Merging Two Directories

This example synchronizes the `dc=com` subtree in two directories.

The merge operation updates both the source and destination directories.

```
oidcmprec operation=merge scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          file=merge
```

4.2.2.9 Including and Excluding Attributes

The following example performs a `compare` operation.

This 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.

```
oidcmprec operation=compare scope=subtree base="'dc=com'  'dc=org'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          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.

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          inclattr="userpassword cn sn givenname mail"
          file=cmpr
```

The following example includes all attributes for the compare operation except `orclguid`, `creatorsname`, and `modifiersname` attributes.

```
oidcmprec operation=compare scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          inclattr="*" exclattr="orclguid creatorsname modifiersname"
          file=compare
```

4.2.2.10 Using a Filter

The following example restricts the comparison to entries that match the filter `(cn=*)`.

The following example restricts the comparison to entries that match the filter `(cn=*)`.

```
oidcmprec source=stadd54:3060 destination=stadd54:3060 \
         base="' '" scope=sub operation=compare file=test \
         filter="'(cn=*)'"
```

4.2.2.11 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`.

Execute the following command:

```
oidcmprec source=host1:3060 destination=host2:3070 \
          base="' '" scope=subtree file=temp operation=compare \
          dndif=ignore mvatrdif=ignore
```

4.2.2.12 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.

```
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
destination=staqj13:3070
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
```

4.2.2.13 Using a Parameter File in XML Format

This example performs a `compare` operation on two directories.

Execute the following command:

```
oidcmprec xmlParameterFile=param.xml
```

The following is an example of an XML parameter file:

```
  <?xml version="1.0" standalone="yes" ?>
- <input>
  <operation>compare</operation>
- <source>
   <host>stadd54</host>
   <port>3060</port>
   <binddn>cn=orcladmin</binddn>
   <password>source-password</password>
   <isSSLPort>false</isSSLPort>
  </source>
- <destination>
   <host>stadd54</host>
   <port>3060</port>
   <binddn>cn=orcladmin</binddn>
   <password>destination-password</password>
   <isSSLPort>true</isSSLPort>
  </destination>
  <base>
   <dn>dc=myhost,dc=example,dc=com</dn>
   <dn>cn=OracleSchemaVersion</dn>
  </base>
  <dns2exclude>
   <dn>cn=test instance,cn=oraclecontext</dn>
   <dn>ou=support,o=us</dn>
  </dns2exclude>
  <scope>subtree</scope>
  <filter />
  <threads>1</threads>
  <dnthreads>1</dnthreads>
  <inclattr />
  <exclattr>
   <attribute>orclguid</attribute>
   <attribute>userpassword</attribute>
   <attribute>authpassword</attribute>
  </exclattr>
  <compareby>tool</compareby>
  <filename>test</filename>
  <genchglog>default</genchglog>
  <force>true</force>
  <verbose>false</verbose>
  <contonerr>true</contonerr>
- <!--
  <entod>ignore</entod>
```

```
<entos>ignore</entos>
<atros>ignore</atros>
<atrod>ignore</atrod>
<svatrdif>ignore</svatrdif>
<mvatrdif>ignore</mvatrdif>
<dndif>ignore</dndif>
<adefos>ignore</adefos>
<adefod>ignore</adefod>
<adefdif>ignore</adefdif>
<odefos>ignore</odefos>
<odefod>ignore</odefod>
<odefdif>ignore</odefdif>

-->
</input>
```

Substitute the password for *password* in the example. Because the file contains a password, ensure that it is not readable by unauthorized users.

4.2.2.14 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.

```
oidcmprec operation=merge scope=subtree base="'dc=com'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          inclattr="*" exclattr="orclguid creatorsname modifiersname"
          file=merge  genchglog=true
```

4.2.2.15 Performing Directory Schema Operations

The following example includes the schema for the selected operation by adding the `cn=subschemasubentry` DN to the `base` argument.

The following example includes the schema for the selected operation by adding the `cn=subschemasubentry` DN to the `base` argument.

```
oidcmprec operation=merge scope=subtree \
          base="'dc=com' 'cn=subschemasubentry'" \
          source=myhost1.mycom.com:3060 \
          destination=myhost2.mycom.com:3060 \
          inclattr="*" exclattr="orclguid creatorsname modifiersname" \
          file=merge genchglog=false
```

4.3 Oracle Internet Directory Compare and Reconcile Tool

"oidcmprec" includes the syntax and arguments of the Oracle Internet Directory Compare and Reconcile Tool.

4.3.1 oidcmprec

Understand about the syntax and arguments of the Oracle Internet Directory Compare and Reconcile Tool. You can use the `oidcmprec` tool to compare and reconcile attribute

values, and merge attribute values between source and destination directories. To use this command, you need to provide the arguments, source, destination and base values as a mandatory parameters. Learn about the various optional parameters which offer different functionalities.

> **Note:**
>
> The Compare and Reconcile Tool, `oidcmprec` does not support One way or Two way Authentication and works only on the No-Authentication mode.

Syntax

```
oidcmprec operation=compare | reconcile | merge | merge_dryrun |userdefinedcr
          source=host:port
          destination=host:port
          base="'dn1' 'dn2' 'dn3' ..."
          [ ssslport=true | false ]
          [ dsslport=true | false ]
          [ dns2exclude="'edn1' 'edn2' 'edn3' ..."]
          [ scope=base | subtree | onelevel ]
          [ filter=filter_that_conforms_to_RFC_2254]
          [ threads=number_of_worker_threads ]
          [ dnthreads=number_of_dn_threads ]
          [ exclattr=space_separated_list_of_attributes_to_be_excluded |
            inclattr=space_separated_list_of_attributes_to_be_included ]
          [ compareby=tool | ldapserver ]
          [ filename=file_name_without_extension_to_store_compare_report]
          [ genchglog=d[efault] | t[rue] | f[alse] ]
          [ reconaver=t[rue] | f[alse]]
          [ verbose=t[rue] | f[alse] ]
          [ force=t[rue] | f[alse] ]
          [ contonerr = t[rue] | f[alse]
          [ logrpt = t[rue] | f[alse]
          [ logs2d = t[rue] | f[alse]
          [ logd2s = t[rue] | f[alse]
          [ logeos = t[rue] | f[alse]
          [ logeod = t[rue] | f[alse]
          [ logdif = t[rue] | f[alse]
          [ logerr = t[rue] | f[alse]
          [ qlogfreq=frequency ]
          [ help=t[rue] | f[alse] ]
          sbinddn='("dn")'
          dbinddn='("dn")'
          [schemafile=<Schema_filename for compare/merge/userdefinedcr against
destination schema>]
          [ 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 ]

oidcmprec  paramfile=file_containing_parameters]

oidcmprec [ xmlparamfile=file_containing_parameters_in_XML_format]
```

Arguments

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 must 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 must 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.

By default, the `oidcmprec` tool excludes operational attributes during comparison.That is, `oidcmprec` does not compare the operational attributes values in source and destination directory entries. During reconciliation of user defined attributes however, operational attributes might be changed.

source=host:port

Required. The connection string used to bind to the source Oracle Internet Directory node. You are prompted for the replication DN password. If you do not supply the hostname or port information on the command-line, the tool prompts 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

destination=host:port

Required. The connection string used to bind to the source Oracle Internet Directory node. You are prompted for the replication DN password. If you do not supply the

hostname or port information on the command-line, the tool prompts 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

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.

ssslport=true | false

Optional. Specifies whether the source directory port is SSL or not. The default value is `false`. To specify this in an XML parameter file, use the `isSSLPort` parameter. See the example in Using a Parameter File in XML Format.

dsslport=true | false

Optional. Specifies whether the destination port is SSL or not. The default value is `false`. To specify this in an XML parameter file, use the `isSSLPort` parameter. See the example in Using a Parameter File in XML Format.

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.

filter=filter_that_conforms_to_RFC_2254

Optional. Only the entries that match the filter conditions are compared. The filter must be in the same format you would specify for `ldapsearch`. That is, it must conform to RFC 2254.

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 must 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".

exclattr=space_separated_list_of_attributes_to_be_excluded | inclattr=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 `exclattrclattr`, or specify a list of attributes to be included, using `inclattr`.

All attributes are included by default, except the following operational attributes:

- `creatorsname`
- `createtimestamp`
- `modifiersname`
- `modifytimestamp`
- `orclentrydn`
- `orclnormdn`

> **Note:**
>
> - The `exclattr` and `inclattr` attributes cannot be used together, except when you use "*" for `inclattr`.
> - By default, the `oidcmprec` tool excludes operational attributes during comparison.That is, `oidcmprec` does not compare the operational attributes values in source and destination directory entries. During reconciliation of user defined attributes however, operational attributes might be changed.

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`. The default value is `tool`.

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.

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.

reconaver=t[rue] | f[alse]

Optional. Determines whether attribute version reconciliation support is provided. The default value is false. Source and destination directory versions must be greater than 11.1.1.0.0 or directories must have the appropriate patch.

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 does not prompt the user for confirmation before performing the specified operation.

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`.

logrpt=t[rue] | f[alse]

Optional. Controls whether the tool generates the *`file_name`*`.rpt` file. The logrpt argument can have the following values:

- `true`: The tool generates the file. This is the default.
- `false`: The tool does not generate the file.

logs2d=t[rue] | f[alse]

Optional. Controls whether the tool generates the *`file_name`*`.s2d.ldif` file. The logs2d argument can have the following values:

- `true`: The tool generates the file. This is the default.
- `false`: The tool does not generate the file.

logd2s=t[rue] | f[alse]

Optional. Controls whether the tool generates the *`file_name`*`.d2s.ldif` file. The logs2d argument can have the following values:

- `true`: The tool generates the file. This is the default.
- `false`: The tool does not generate the file.

logeos=t[rue] | f[alse]

Optional. Controls whether the tool generates the *`file_name`*`.eos.rpt` file. The logeos argument can have the following values:

- `true`: The tool generates the file. This is the default.
- `false`: The tool does not generate the file.

logeod=t[rue] | f[alse]

Optional. Controls whether the tool generates the *`file_name`*`.eod.rpt` file. The logeod argument can have the following values:

- `true`: The tool generates the file. This is the default.
- `false`: The tool does not generate the file.

logdif=t[rue] | f[alse]

Optional. Controls whether the tool generates the *file_name*.dif.rpt file. The logdif argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

logerr=t[rue] | f[alse]

Optional. Controls whether the tool generates the *file_name*.err file. The logdif argument can have the following values:

- true: The tool generates the file. This is the default.
- false: The tool does not generate the file.

qlogfreq=frequency

Optional. The tool can dump the total number of entries loaded by the tool in memory and the number of entries in each of oidcmprec's various queues. The entry counts are logged in the file oidcmprec.log. Use the qlogfreq argument to specify how frequently oidcmprec logs this information. Possible values are from 1 to 5000. The lower the value, the shorter the interval. For frequent entry counts, use a value between 5 and 10.

help=t[rue] | f[alse]

Optional. When set to true, the tool displays help on the oidcmprec command. The default value is false.

sbinddn='("dn")'

Optional. Specifies the DN to bind with the source directory. This argument is used if Oracle Virtual Directory is the source.

dbinddn='("dn")'

Optional. Specifies the DN to bind with the destination directory. This argument is used if Oracle Virtual Directory is the destination.

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 4-1 shows the default values of the entos argument, corresponding to the operations specified.

Table 4-1 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 4-2 shows the default values of the `entod` argument, corresponding to the operations specified.

Table 4-2 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 non replication 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 non replication 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 4-3 shows the default values of the `atros` argument, corresponding to the operations specified.

Table 4-3 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 4-4 shows the default values of the `atrod` argument, corresponding to the operations specified.

Table 4-4 Default Values for the atrod Argument

Operation	Default Value
`compare`	`log2delete`

Table 4-4 (Cont.) Default Values for the atrod Argument

Operation	Default Value
`reconcile`	`delete`
`merge`	`add`
`merge_dryrun`	`log2add`
`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 4-5 shows the default values of the `svatrdif` argument, corresponding to the operations specified.

Table 4-5 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 4-6 shows the default values of the `mvatrdif` argument, corresponding to the operations specified.

Table 4-6 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 4-7 shows the default values of the `mvatrdif` argument, corresponding to the operations specified.

Table 4-7 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 4-8 shows the default values of the `odefos` argument, corresponding to the operations specified.

Table 4-8 Default Values for the odefos Argument

Operation	Default Value
`compare`	`log2add`

Table 4-8 (Cont.) Default Values for the odefos Argument

Operation	Default Value
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 4-9 shows the default values of the `odefod` argument, corresponding to the operations specified.

Table 4-9 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 4-10 shows the default values of the `odefdif` argument, corresponding to the operation specified.

Table 4-10 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 4-11 shows the default values of the `adefos` argument, corresponding to the operation specified.

Table 4-11 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 4-12 shows the default values of the `adefod` argument, corresponding to the operation specified.

Table 4-12 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 4-13 shows the default values of the `adefdif` argument, corresponding to the operation specified.

Table 4-13 Default Values for the adefdif Argument

Operation	Default Value
compare	log2usesrc
reconcile	usesrc
merge	usesrc
merge_dryrun	log2usesrc
userdefinedcr	ignore

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.

xmlParamFile=file_containing_parameters_in_XML_format

Optional. Specifies an XML parameter file to supply argument values. 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.

4.4 Replication Environment Management Tool

You can use the `remtool` and its arguments to perform various operations.

"remtool" includes the syntax and arguments of the Replication Environment Management Tool.

The Replication Environment Management Tool includes the following operations:

- -backupmetadata
- connection_argument
- -paddnode
- -pdisplay
- -pchgmaster
- -pchgpwd
- -pchgwalpwd
- -pcleanup
- -pdelnode
- -pdispqstat
- -pilotreplica
- -presetpwd
- -pthput
- -pverify
- -psuspendrepl and -presumerepl

4.4.1 remtool

Learn about the `remtool` syntax and the various command-specific syntax, arguments, and usage.

Syntax

The remtool syntax is as follows:

```
remtool operation [connection_argument] [-v]

operation :=  { -paddnode   | -pdelnode   | -pcleanup   |
                -pchgpwd    | -pdisplay   | -pchgmaster [ -multimaster]|
                -pchgwalpwd | -pdispqstat | -pverify    | -presetpwd |
                -psuspendrepl -fromnode host1:port1 [-tonode host2:port2] |
                -presumerepl -fromnode host1:port1 [-tonode host2:port2]|
                -pthput [-interval time_in_seconds] [-file filename] }


connection_argument := { -bind supplier_hostname:ldap_port }
```

Arguments

operation

Required. The name of the operation to perform using `remtool`. See the appropriate operation documentation for command-specific syntax, arguments, and usage. The following operations are available:

- `-paddnode` - Adds a partial replica to an LDAP-based DRG. See "-paddnode" for more information about this operation.
- `-pdelnode` - Deletes a partial replica from an LDAP-based DRG. See "-pdelnode" for more information about this operation.
- `-pcleanup` - Cleans up the partial replication setup of an LDAP-based DRG. See "-pcleanup" for more information about this operation.
- `-pchgpwd` - Changes the password of a replication DN for a replica in an LDAP-based DRG. See "-pchgpwd" for more information about this operation.
- `-pdisplay` - Displays all replica details in a partial replication group. See "-pdisplay" for more information about this operation.
- `pchgmaster` - Breaks agreement with an old LDAP-based supplier (master copy of the naming context) and reestablishes agreement with a new supplier. See "-pchgmaster" for more information about this operation.
- `-pchgwalpwd` - Changes the wallet password of a replication DN for a replica in an LDAP-based DRG. See "-pchgwalpwd" for more information about this operation.
- `-pdispqstat` - Displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. See "-pdispqstat" for more information about this operation.
- `-pverify` - Verifies the replication configuration for a DRG node that uses LDAP-based replication. See "-pverify" for more information about this operation.
- `-presetpwd` - Resets the password of a replication DN for a replica in an LDAP-based DRG. See "-presetpwd" for more information about this operation.
- `-pilotreplica` - Begins or ends pilot mode for a replica. See "-pilotreplica" 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 "-backupmetadata" for more information about this operation.
- `-psuspendrepl -fromnode` *`host1:port1`* [`-tonode` *`host2:port2`*] - Only used during rolling upgrade. For more information, see the appendix in Performing a Rolling Upgrade in *Administering Oracle Internet Directory*.
- `-presumerepl -fromnode` *`host1:port1`* [`-tonode` *`host2:port2`*] - Only used during rolling upgrade. For more information, see the appendix in Performing a Rolling Upgrade in *Administering Oracle Internet Directory*.
- `-pthput` [`-interval` *`time_in_seconds`*] [`-file` *`filename`*] - Enables you to monitor replication progress in a directory replication group. See "-pthput" for more information.

connection_argument

The connection information to be supplied to `remtool`. The following connection details are available:

- `-bind` - Used with LDAP-based replication operations to specify the hostname and port of the supplier. See "-bind Connection" for more information.

-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 *`$DOMAIN_HOME`*`/tools/OID/logs`.

Related Command-Line Tools

- See Oracle Internet Directory Control Utility

4.4.2 connection_argument

Understand about the `-bind` connection arguments in the Replication Environment Management Tool.

The Replication Environment Management Tool includes the `-bind` connection arguments:

- -bind Connection

-bind Connection

This argument is used with LDAP-based operations to supply the host and port of the supplier. The syntax is:

`bind` *`supplier_hostname`*`:`*`ldap_port`*

You are prompted for the replication DN password. If you omit either the hostname or port or both, `remtool` uses the local host name or default port (3060) or both as arguments. If you omit the -bind argument, you are prompted for the missing information.

4.4.3 -backupmetadata

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 does not work if anonymous bind is disabled at the pilot replica or master replica.

Syntax

```
remtool -backupmetadata -replica pilot_hostname:port {-master
master_hostname:port | -bkup file_name}
[-nwurl file:wallet_location] [-wurl file:wallet_location] [-nsslauth auth_mode]
[-sslauth auth_mode]
```

Arguments

-replica pilot_hostname:port

Required. The connection string for the pilot replica. You are prompted for the password for the replication DN of 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 3060.

-master master_hostname:port

Either `-master` or `-bkup` argument is required. (You can provide both arguments.) The connection string for the master replica. You are prompted for the password for the replication DN of 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 3060.

-bkup file_name

Either `-master` or `-bkup` argument is required. (You can provide both arguments.) The full path and file name of the LDIF output file. The metadata entries are written to this file in LDIF format.

-nwurl file:wallet_location

Optional. Specifies the wallet location for SSL connection to the pilot replica (one-way or two-way).

-wurl file:wallet_location

Optional. Specifies the wallet location for SSL connection to the master replica (one-way or two-way).

-nsslauth auth_mode

Optional. Specifies the SSL authentication mode for the pilot replica. You can use SSL in one of three authentication modes:

- 1 – SSL No Authentication mode
- 2 – SSL Server Authentication Only mode
- 3 – SSL Client and Server Authentication mode

-sslauth auth_mode

Optional. Specifies the SSL authentication mode for the master replica. You can use SSL in one of three authentication modes:

- 1 – SSL No Authentication mode
- 2 – SSL Server Authentication Only mode
- 3 – SSL Client and Server Authentication mode

4.4.4 -paddnode

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 LDAP-based replication.
- 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 replicates 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

```
remtool -paddnode [-bind supplier_hostname:ldap_port] [-v]
```

Arguments

You are prompted for the password for the replication DN on the consumer node. You are prompted for the following arguments if you do not specify them:

- 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.

In addition, the tool prompts you for the following information:

- **Replica ID of Supplier** - If the DRG contains multiple nodes that can be used as the supplier, you are 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

See "-bind Connection" for information.

4.4.5 -pdisplay

The pdisplay operation displays all replica details in a partial replication group.

Syntax

N/A

Arguments

-bind supplier_hostname:ldap_port

See "-bind Connection" for information.

4.4.6 -pchgmaster

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 might 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 "-pcleanup" for details about the `pcleanup` operation.

Syntax

```
remtool -pchgmaster [-bind replica_hostname:ldap_port] [ multimaster ] [-v]
```

Arguments

The tool prompts you for the host names and port numbers of the retiring supplier and the new supplier.

-bind replica_hostname:port_number

See "-bind Connection" for information.

-multimaster

This suboption causes `changeMaster` to change the primary replica in a multimaster agreement.

4.4.7 -pchgpwd

The `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, the password is 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 "-pchgwalpwd" operation.

Syntax

```
remtool -pchgpwd [-bind oid_hostname:ldap_port] [-v]
```

Arguments

In addition to the arguments specified on the command-line, the tool also prompts you for the new replication DN password for the host specified in the bind connection string.

-bind supplier_hostname:ldap_port

See "-bind Connection" for information.

4.4.8 -pchgwalpwd

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

```
remtool -pchgwalpwd [-bind oid_hostname:ldap_port] [-v]
```

Arguments

-bind supplier_hostname:ldap_port

See "-bind Connection" for information.

4.4.9 -pcleanup

The `pcleanup` operation is used to clean up an LDAP-based directory replication group (DRG) setup. It cleans up a replica which has incomplete or flawed LDAP-based DRG setup. It only cleans 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 prompts for the Oracle Internet Directory superuser DN and password.

This operation only cleans up LDAP-based DRG setup.

Syntax

```
remtool -pcleanup [-bind oid_hostname:ldap_port] [-agrmt] [-v]
```

Arguments

-bind supplier_hostname:ldap_port

See "-bind Connection" for information.

-agrmt

Optional. Use this option to clean up dead LDAP agreements at a node. Dead agreements might exist if:

- A node in the DRG was offline when you ran `remtool -pcleanup`.
- The node being deleted was offline when you ran `remtool -delnode`.
- The supplier node was offline when you ran remtool `-pchgmaster`.

Alternatively, in the first two cases, you could run `remtool -pcleanup` (without `-agrmt`) to delete all the agreements.

4.4.10 -pdelnode

The `pdelnode` operation deletes an LDAP-based replica or partial replica from a directory replication group (DRG).

Syntax

```
remtool -pdelnode [-bind hostname:ldap_port] [-v]
```

Arguments

In addition to the arguments specified on the command-line, the tool prompts 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

See "-bind Connection" for information.

4.4.11 -pdispqstat

The `pdispqstat` operation displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication.

Syntax

```
remtool -pdispqstat [-bind hostname:ldap_port] [-v]
```

Arguments

-bind hostname:ldap_port

See "-bind Connection" for information.

4.4.12 -pilotreplica

The `pilotreplica` operation begins or ends pilot mode for a replica.

Syntax

```
remtool -pilotreplica {begin|end} -bind hostname:ldap_port [-bkup file_name]
```

Arguments

begin | end

Required. Begin or end pilot mode.

-bind hostname:ldap_port

See "-bind Connection" for information.

-bkup file_name

Name of backup file in which entries modified after pilot mode is started are to be stored in LDIF format.

4.4.13 -presetpwd

The `presetpwd` operation resets the replication DN password for the given Oracle Internet Directory server in both the directory repository and wallet. It does not reset the passwords for any other directories of the directory replication group (DRG) of which this directory is a member.

You need the Oracle Internet Directory superuser DN and password to reset the replication DN password.

Syntax

```
remtool -presetpwd -bind hostname:ldap_port [-v]
```

Arguments

You are prompted for the new replication DN password. In addition to the password and arguments supplied on the command-line, the tool prompts you for the following information:

- The superuser DN, for example `cn=orcladmin`.
- The superuser password.

-bind hostname:ldap_port

See "-bind Connection" for information.

4.4.14 -pthput

The `-pthput` option enables you to monitor replication progress in a directory replication group. The tool binds to the specified node and collects information about

all the nodes in the directory replication group. It displays this information at intervals of specified duration.

Syntax

```
remtool -pthput [-bind hostname:ldap_port_number] [-interval time_in_seconds] [-file filename]
```

Arguments

-bind hostname:ldap_port_number

See "-bind Connection" for information.

-interval time_in_seconds

The interval for displaying information. This is an optional parameter. Provide its value in seconds. Its default value is 60 seconds.

-file filename

The file to write information to. This is an optional argument. If you specify a `file` argument, the output shown on the command line is logged to that file. Otherwise, the output is logged to a file name based on the timestamp.

4.4.15 -pverify

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

```
remtool -pverify [-bind hostname:ldap_port_number] [-hiqmax hiqmax] [-tbtmax tbtmax] [-v]
```

Arguments

-bind hostname:ldap_port_number

See "-bind Connection" for information.

-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.

4.4.16 -psuspendrepl and -presumerepl

The `-psuspendrepl` and `-presumerepl` operations provide rolling upgrade support for multimaster replication DRGs by suspending and resuming replication, respectively.

Syntax

```
remtool -psuspendrepl -fromnode host1:port1 [-tonode host2:port2]

remtool -presumerepl -fromnode host1:port1 [-tonode host2:port2]
```

> **Note:**
>
> You must apply all required patches before starting the rolling upgrade procedure.

Arguments

-fromnode host1:port1

Specifies the host and port of the node from which replication is to be suspended.

-tonode host2:port2

Specifies the host and port of the node to which replication is to be suspended

If you do not specify the `-tonode` parameter with `-psuspendrepl` or `-presumerepl`, `remtool` displays the replicaids of all the replicas and prompts you for the replica to which to replication is to be suspended or resumed. To suspend or resume replication to all the replicas, enter `all`.

5

Oracle Directory Integration Platform Tools

Learn about the various command-line tools that are used to administer Oracle Directory Integration Platform.

> **Note:**
>
> - Best security practice is to provide a password only in response to a prompt from the command.
> - You must set the environment variables `WLS_HOME` and `ORACLE_HOME` before executing any of the Oracle Directory Integration Platform commands.
> - The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute the Oracle Directory Integration Platform commands in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

5.1 Working With Oracle Directory Integration Platform Utilities

Understand how to work with Oracle Directory Integration Platform utilities.

This section contains the following topics:

- Executing Provisioning Profile Bulk Utility
- Executing DIP Status Utility
- Executing the Schema Synchronization utility for OID and third-party Directory Server
- Comparing the Schema between two Oracle Internet Directory Servers
- Synchronizing the Schema between two Oracle Internet Directory Servers
- Executing the Manage Provisioning Profiles Utility

5.1.1 Executing the Manage DIP Server Configuration Utility

Follow the example to understand how to manage DIP server configuration using `manageDIPServerConfig` utility.

The following example illustrates how to execute the manageDIPServerConfig utility command:

```
manageDIPServerConfig get -h myhost.mycompany.com -p 7005 -D weblogic \
   -attr sslmode

manageDIPServerConfig set -h myhost.mycompany.com -p 7005 -D weblogic \
   -attr sslmode -val 2
```

For more information about the command, see Manage DIP Server Configuration Utility

5.1.2 Executing the Manage Synchronization Profiles Utility

Follow the examples to understand the usage of `manageSyncProfiles` utility.

Perform various actions using `manageSyncProfiles` by following the examples given below:

```
manageSyncProfiles register -h myhost.mycompany.com -p 7005 -D weblogic \
  -f /opt/ldap/odip/iPlImport.profile

manageSyncProfiles deregister -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile

manageSyncProfiles updatechgnum -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile

manageSyncProfiles activate -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile

manageSyncProfiles deactivate -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile

manageSyncProfiles get -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile

manageSyncProfiles testProfile -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile

manageSyncProfiles associateprofile -h myhost.mycompany.com -p 7005 \
   -D weblogic -pf myProfile -assopf myProfile1
```

```
manageSyncProfiles dissociateprofile -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile

manageSyncProfiles getAllAssociatedProfiles -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile

manageSyncProfiles getAssociatedProfile -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile

manageSyncProfiles update -h myhost.mycompany.com -p 7005 \
  -D weblogic -pf myProfile -f /opt/ldap/odip/iPlImport.profile

manageSyncProfiles validateMapRules -h myhost.mycompany.com -p 7005 \
  -D weblogic -f /opt/ldap/odip/iPlImport.map -conDirHost server.example.com \
  -conDirPort 8000 -conDirBindDn administrator@idm2003.net -mode IMPORT \
  -conDirType IPLANET

manageSyncProfiles isexists -h myhost.mycompany.com -p 7005 -D weblogic \
  -pf myProfile

manageSyncProfiles copy -h myhost.mycompany.com -p 7005 -D weblogic \
  -pf myProfile -newpf yourProfile

manageSyncProfiles list -h myhost.mycompany.com -p 7005 -D weblogic -
profileStatus
```

For more information about the command, see Manage Synchronization Profiles Utility

5.1.3 Executing Synchronization Profile Bootstrap Utility

Follow the example to understand how to synchronize profile bootstrap using the `syncProfileBootstrap` utility.

The following example illustrates how to use syncProfileBootstrap utility:

```
manageSyncProfileBootstrap -h myhost.mycompany.com -p 7005 -D weblogic \
  -pf myProfile -lp 5

manageSyncProfileBootstrap -h myhost.mycompany.com -p 7005 -D weblogic \
  -f /opt/ldap/odip/bootstrap.properties -lr 3
```

For more information about the command, see Synchronization Profile Bootstrap Utility

5.1.4 Executing Express Synchronization Setup Utility

Follow the example to understand how to use `expressSyncSetup` utility.

Use the example below to use `expressSyncSetup` utility along with its arguments to express synchronization setup:

```
expressSyncSetup -h myhost.mycompany.com -p 7005 -D weblogic -pf myProfile \
  -conDirType ACTIVEDIRECTORY -conDirUrl server.mycompany.com:5432 \
  -conDirBindDN administrator@idm2003.net -conDirContainer ou=sales,dc=us,dc=com
\
  -enableProfiles false \

expressSyncSetup -help
```

For more information about the command, see Express Synchronization Setup Utility

5.1.5 Executing Provisioning Profile Bulk Utility

Follow the example to use `provProfileBulkProv` utility and its arguments to provision profile bulk utility.

The following example illustrates how to use provProfileBulkProv utility:

```
provProfileBulkprov -h myhost.mycompany.com -p 7005 -D weblogic \
  -f /opt/ldap/odip/users.ldif -realm cn=aaaa,ou=bbbb,dc=cccc
```

For more information about the command, see Provisioning Profile Bulk Utility.

5.1.6 Executing DIP Status Utility

Follow the example to learn how to execute DIP status using the `dipStatus` utility.

The following example illustrates how to use dipStatus utility:

```
dipStatus -h myhost.mycompany.com -p 7005 -D weblogic

dipStatus -help
```

For more information about the command, see Oracle Directory Integration Platform Status Utility

5.1.7 Executing the Schema Synchronization utility for OID and third-party Directory Server

Understand how to synchronize the schema between Oracle Internet Directory and a third-party directory server.

Use the following example to synchronize the schema between Oracle Internet Directory and a third-party directory server.

```
schemasync -srchost myhost1.mycompany.com -srcport 3060 -srcdn "cn=orcladmin" \
   -dsthost myhost2.mycompany.com -dstport 3060 \
   -dstdn "uid=superuser,ou=people,dc=mycompany,dc=com" -ldap
```

For more information about the command, see Schema Elements Synchronization Utility

5.1.8 Comparing the Schema between two Oracle Internet Directory Servers

Use the `schemasync` command-line tool to compare the schema between two Oracle Internet Directory servers:

```
schemasync -srchost myhost1.mycompany.com -srcport 3060 -srcdn
"cn=orcladmin" \
   -dsthost myhost2.mycompany.com -dstport 3060 "cn=orcladmin"
```

5.1.9 Synchronizing the Schema between two Oracle Internet Directory Servers

Use the `schemasync` command-line tool to actually synchronize an OID server schema to another OID server:

```
schemasync -srchost myhost1.mycompany.com -srcport 3060 -srcdn
"cn=orcladmin" \
   -dsthost myhost2.mycompany.com -dstport 3060 "cn=orcladmin" -ldap
```

5.1.10 Executing the Manage Provisioning Profiles Utility

When you install an application that you want to provision, you must create a provisioning integration profile by using the Manage Provisioning Profiles Utility. For more information about the command, see Manage Provisioning Profiles Utility. You can use the Manage Provisioning Profiles Utility to:

- Create a new provisioning profile. A new provisioning profile is created and set to the enabled state so that Oracle Directory Integration and Provisioning can process it.
- Modify an existing provisioning profile.
- Delete an existing provisioning profile.
- Disable an existing provisioning profile.
- Enable a disabled provisioning profile.

To understand how to manage provisioning profiles using the `manageProvProfiles` utility, see Tasks and Examples for manageProvProfiles in *Administering Oracle Directory Integration Platform*.

5.2 Manage DIP Server Configuration Utility

The Manage DIP Server Configuration utility, `manageDIPServerConfig`, allows you to manage the Oracle Directory Integration Platform server configuration.

5.2.1 manageDIPServerConfig

Learn about the syntax of manageDIPServerConfig utility and the accepted arguments.

Syntax

The syntax for manageDIPServerConfig utility is as follows:

```
manageDIPServerConfig {get | set} -h HOST -p PORT -D wlsuser -attribute {sslmode
|
refreshinterval | quartzthreadcount | quartzdbretryinterval | oidhostport |
keystorelocation} [-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE]
[-value ATTRIBUTE_VALUE] [-help]
```

Arguments

The manageDIPServerConfig Utility accepts the following arguments:

get | set

Operation to perform.

- get: Displays the current value of the config parameter in DIP configuration file
- set: Updates the value of the config parameter in DIP configuration file.

-h | -host

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed

-p | -port

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

-D | -wlsuser

WebLogic Server login ID.

> **Note:**
>
> You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `manageDIPServerConfig` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary.

-attr | -attribute

Identifies the attribute that `manageDIPServerConfig` performs the operation on. The following is a list and description of the attributes `manageDIPServerConfig` can perform operations on:

- `sslmode`: The SSL mode Oracle Directory Integration Platform uses to connect to Oracle Internet Directory. Supported values are 1 and 2. Use 1 to connect to Oracle Internet Directory using SSL Mode 1 (No Authentication). Use 2 to connect to Oracle Internet Directory using SSl Mode 2 (Server Only Authentication).
- `refreshinterval`: The time interval (amount of time in seconds) that controls how often the Oracle Directory Integration Platform server refreshes profile configuration details.
- `quartzthreadcount`: Controls how many profiles can be scheduled in parallel. The default value is 15. If you have more than 15 profiles, increase the `quartzthreadcount` attribute accordingly.
- `quartzdbretryinterval`: Controls how often Oracle Directory Integration Platform's Quartz scheduler attempts to reconnect to the Oracle Internet Directory database.

- `oidhostport`: Identifies the host and port of the Oracle Internet Directory associated with Oracle Directory Integration Platform. Specify values for the oidhostport attribute in the form of `host:port`.
- `keystorelocation`: Specifies the absolute path to the Java Keystore (JKS) based on the host where Oracle Directory Integration Platform is deployed. When you specify the value for the `keystorelocation` attribute, be sure you use the appropriate path separators (that is, / for UNIX and Linux platforms, and \ for Windows platforms).

-ssl

Executes the command in SSL mode.

> **Note:**
>
> The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

-keystorePath

The full path to the keystore.

-keystoreType

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

-val | -value

The value to set for the attribute This parameter is required with the set operation.

-help

Provides usage help for the command.

5.3 Manage Synchronization Profiles Utility

You can use the Manage Synchronization Profiles utility, `manageSyncProfiles`, to manage synchronization profiles.

5.3.1 manageSyncProfiles

Learn about the syntax and the arguments accepted by manageSyncProfiles.

Syntax

The syntax followed for using manageSyncProfiles is as follows:

```
manageSyncProfiles {activate | deactivate | copy | deregister | get | isexists |
update | testProfile | validateProfile | validateMapRules | register |
updatechgnum | associateProfile | dissociateProfile | getAllAssociatedProfiles |
getAssociatedProfile | list } -h HOST -p PORT -D wlsuser [-ssl -keystorePath
PATH_TO_KEYSTORE -keystoreType TYPE] [-profile] [-newProfile]
```

```
[-associateProfile][-file] [-params 'prop1 val1 prop2 val2 ...']
[-conDirHost] [-conDirPort] [-conDirBindDn] [-mode] [-conDirType] [-conDirSSL]
[-profileStatus] [-help]
```

Arguments

The manageSyncProfiles utility accepts the following arguments:

Operations

activate

Changes a profile state to ENABLE

deactivate

Changes a profile state to DISABLE

copy

Copies an existing profile to profile *newProfile*

deregister

Deletes an existing profile from OID.

get

Gets the profile details from OID.

isexists

Checks if the profile *profile* exists in OID.

update

Modifies an existing profile *profile* in OID.

testProfile

Changes the state of a disabled profile *profile* to TEST and schedules the profile for testing to ensure the profile successfully performs synchronization. After executing the manageSyncProfiles command with the testProfile operation, the results of the test are available in the following log file, where *DOMAIN_HOME* represents the Oracle WebLogic Server Domain home and *ORACLE_WEBLOGIC_MANAGED_SERVER_NAME* represents the name of the managed server where Oracle Directory Integration and Provisioning is deployed:

$DOMAIN_HOME/servers/*ORACLE_WEBLOGIC_MANAGED_SERVER_NAME*/logs/*ORACLE_WEBLOGIC_MANAGED_SERVER_NAME*.log

> **Note:**
>
> The testProfile operation cannot schedule profiles that are in ENABLE state for testing.

validateProfile

Validates the syntax of the values in the specified profile for correctness.

validateMapRules

Validates the map rules provided.

register

Creates a new profile in OID.

updatechgnum

Updates the last applied change number in the profile to latest.

associateProfile

Associates *associateProfileName* with *profileName* to prevent information back flow.

dissociateProfile

Dissociates an associated profile to *profileName*

getAllAssociatedProfiles

Lists all the profiles to which profile *profileName* is associated.

getAssociatedProfile

Displays the profile name associated with profile *profileName*.

list

Displays all profiles registered in OID.

Options

-h | host

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

-p | -port

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

-D | wlsuser

Oracle WebLogic Server login ID

> **Note:**
>
> You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute a command from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `manageSyncProfiles`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

-ssl

Executes the command in SSL mode.

> **Note:**
>
> The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

-keystorePath

The full path to the keystore.

-keystoreType

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

-pf | -profile

The name of the synchronization profile to use when performing the operation.

-newpf | -newProfile

The name of the new profile which will be a copy of *profile*.

-assopf

The name of the profile that will be associated with *profile*

-f | -file

The full path and file name of the profile properties file containing the properties. See the appendix in Example Properties File for Synchronization Profiles in *Administering Oracle Directory Integration Platform* for an example of such a file.

-params

A value is of the form `prop1 val1 prop2 val2 ...` where `prop` is the name of a profile property and `val` is the new value for that property. This keyword is used only for modification of a profile. You can specify as many key values as required

-conDirHost

Host where connected directory server is running.

-conDirPort

Port at which connected directory server listens.

-conDirBindDn

Connected directory server bind DN.

Examples:

- Active Directory

```
administrator@idm2003.net
```

- Sun ONE or iPlanet

  ```
  cn=Directory Manager
  ```

- Oracle Internet Directory

  ```
  cn=orcladmin
  ```

> **Note:**
>
> You are prompted for the connected directory bind DN password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `manageSyncProfiles` from a script, you can redirect input from a file containing the connected directory bind DN password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `manageSyncProfiles`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

-mode

Synchronization mode map rules to be used: `import` or `export`

-conDirType

Connected directory type. Supported values are `ActiveDirectory`, `EDirectory`, `iPlanet`, `OpenLDAP`, `ADAM`, `Tivoli`, `ExchangeServer2003`, and `OID`.

-conDirSSL

SSL mode value used to connect connected directory server

-prfSt | -profileStatus

Displays status for the profile. Used only with the `list` operation.

-help

Provides command usage help.

5.4 Synchronization Profile Bootstrap Utility

The Synchronization Profile Bootstrap utility, `syncProfileBootstrap`, performs the initial migration of data between a connected directory and Oracle Internet Directory for a synchronization profile.

5.4.1 syncProfileBootstrap

Understand about the syntax and the various arguments of `syncProfileBootstrap` utility. Each argument provides you with an option to perform the initial migration between connected directory and Oracle Internet Directory.

Syntax

The syntax followed for using syncProfileBootstrap is as follows:

```
syncProfileBootstrap -h HOST -p PORT -D wlsuser {-file FILENAME |-profile
-PROFILE_NAME} [-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE]
[-loadParallelism INTEGER] [-loadRetry INTEGER][-help]
```

Arguments

The syncProfileBootstrap utility accepts the following arguments:

-h | -host

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

-p | -port

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

-D | wlsuser

Oracle WebLogic Server login ID

> **Note:**
>
> You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `syncProfileBootstrap` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary.

-f | -file

Bootstrap properties file.

-pf | -profile

The name of the synchronization profile to use when performing the operation.

-ssl

Executes the command in SSL mode.

> **Note:**
>
> The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

-keystorePath

The full path to the keystore.

-keystoreType

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

-lp | -loadParallelism

Indicator that loading to Oracle Internet Directory is to take place in parallel by using multiple threads. For example, -loadparallelism 5 means that 5 threads are to be created, each of which tries to load the entries in parallel to Oracle Internet Directory.

-lr | -loadRetry

The number of times the retry should be made (when the load to the destination fails) before marking the entry as bad entry.

-help

Provides command usage help.

5.5 Express Synchronization Setup Utility

Understand how to use the Express Synchronization Setup utility, `expressSyncSetup`, to create import and export synchronizations profiles.

5.5.1 expressSyncSetup

Understand about the syntax and the various arguments of `expressSyncSetup` utility.

Syntax

The syntax followed for using expressSyncSetup is as follows:

```
expressSyncSetup -h HOST -p PORT -D wlsuser -pf PROFILE
-conDirType CONNECTED_DIRECTORY_TYPE -conDirURL CONNECTED_DIRECTORY_URL
-conDirBindDN CONNECTED_DIRECTORY_BIND_DN -conDircontainer SYNC_CONTAINER
[-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE] [-enableProfiles {true |
false}] [-help]
```

Arguments

The expressSyncSetup utility accepts the following arguments:

-h | -host

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

-p | -port

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

-D | wlsusser

Oracle WebLogic Server login ID

> **Note:**
>
> You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `expressSyncSetup` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `expressSyncSetup`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

-pf | -profile

Profile name.

-conDirType

Connected directory type. Supported values are `ActiveDirectory`, `EDirectory`, `iPlanet`, `OpenLDAP`, `ADAM`, `Tivoli`, `ExchangeServer2003`, and `OID`.

-conDirUrl

URL where the connected directory is running. The format is *host*:*port*.

-conDirBindDN

Connected directory server bind DN. For example:

`administrator@idm2003.net`

`cn=orcladmin`, `cn=Directory Manager`

> **Note:**
>
> You are prompted for the connected directory bind DN password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `expressSyncSetup` from a script, you can redirect input from a file containing the connected directory bind DN password. Use file permissions to protect the file and delete it when it is no longer necessary. If you must provide more than one password to `expressSyncSetup`, put each on a separate line in the file, in the following order: connected directory bind DN password, then Oracle WebLogic Server login password.

-conDirContainer

The synchronization container. For example:

```
ou=sales,dc=us,dc=com
```

```
OU=Groups,DC=imtest,DC=com
```

```
CN=Users,DC=imtest,DC=com
```

-ssl

Executes the command in SSL mode.

> **Note:**
>
> The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

-keystorePath

The full path to the keystore.

-keystoreType

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

-enableProfiles

Specify `true` to enable created profiles, `false` if not.

-help

Provides command usage help.

5.6 Provisioning Profile Bulk Utility

The Provisioning Profile Bulk utility, `provProfileBulkProv`, performs initial migration of data from an LDIF file to Oracle Internet Directory for a provisioning profile.

5.6.1 provProfileBulkProv

Understand about the syntax and the various arguments of `provProfileBulkProv` utility.

Syntax

The syntax followed for using provProfileBulkProv is as follows:

```
provProfileBulkProv -h HOST -p PORT -D wlsuser -file LDIF_FILE -realm REALM_DN
[-ssl -keystorePath PATH_TO_KEYSTORE -keystoreType TYPE]
[-encoding INPUT_ENCODING] [-help]
```

Arguments

The provProfileBulkProv utility accepts the following arguments:

-h | -host

Oracle WebLogic Server host where Oracle Directory Integration Platform is deployed.

-p | -port

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

-D | -wlsuser

Oracle WebLogic Server login ID

> **Note:**
>
> You are prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument. Best security practice is to provide a password only in response to a prompt from the command. If you must execute `provProfileBulkProv` from a script, you can redirect input from a file containing the Oracle WebLogic Server login password. Use file permissions to protect the file and delete it when it is no longer necessary.

-f | -file

LDIF file containing the data to be migrated.

-realm

The realm in which the users are to be provisioned.

-ssl

Executes the command in SSL mode.

> **Note:**
>
> The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

-keystorePath

The full path to the keystore.

-keystoreType

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

-encoding

Input file encoding.

-help

Provides command usage help.

5.7 Oracle Directory Integration Platform Status Utility

The `dipStatus` utility allows you to check the status of Oracle Directory Integration Platform and whether it is registered.

5.7.1 dipStatus

Understand about the syntax and the various arguments of `dipStatus` utility.

Syntax

The syntax followed for using dipStatus is as follows:

```
dipStatus -h HOST -p PORT -D wlsuser [-ssl -keystorePath PATH_TO_KEYSTORE
-keystoreType TYPE] [-help]
```

Arguments

The dipStatus utility accepts the following arguments:

-h | -host

Host name of the WebLogic server running the Managed Server where Oracle Directory Integration Platform is deployed.

-p | -port

Listen port of Oracle WebLogic Managed Server where Oracle Directory Integration Platform application is deployed.

-D | -wlsuser

WebLogic Server login ID.

> **Note:**
>
> You are prompted for the WebLogic server login password. You cannot provide the password as a command-line argument.
>
> Best security practice is to provide a password only in response to a prompt from the command. If you must execute `dipStatus` from a script, you can redirect input from a file containing the WebLogic Server password. Use file permissions to protect the file and delete it when it is no longer necessary.

-ssl

Executes the command in SSL mode.

> **Note:**
>
> The Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed must be configured for SSL to execute this command in SSL mode. Refer to the *Configuring SSL* chapter in *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information.

-keystorePath

The full path to the keystore.

-keystoreType

The type of the keystore identified by `-keystorePath`. For example: `-keystorePath jks` or `-keystorePath PKCS12`

-help

Provides usage help for the command.

5.8 Schema Elements Synchronization Utility

The `schemasync` utility enables you to synchronize schema elements—namely attributes and object classes—between an Oracle Internet Directory server and a third-party LDAP directory.

5.8.1 schemasync

Understand about the syntax, the various arguments and the command-line tools of `schemasync` utility.

Syntax

The syntax followed for using schemasync is as follows:

```
schemasync -srchost hostname -srcport port -srcdn bindDN -srcpwd password  -
dsthost hostname -dstport port -dstdn bindDN -dstpwd password [-ldap]
```

Arguments

The schemasync utility accepts the following arguments:

-srchost *hostname*

Required. The host name of the source directory server.

-srcport *port*

Required. The LDAP listening port of the source directory server, for example 3060.

-srcdn *bindDN*

Required. 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 superuser (`cn=orcladmin`).

-srcpwd *password*

Optional. The user password used to bind to the source directory. If you do not specify the password on the command line, you are prompted for it. Best security practice is to provide the password in response to a prompt.

-dsthost *hostname*

Required. The host name of the destination directory server.

-dstport *port*

Required. The LDAP listening port of the destination directory server, for example 3060.

-dstdn *bindDN*

Optional. 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 superuser.

-dstpwd *password*

Required. The user password used to bind to the destination directory. If you do not specify the password on the command line, you are prompted for it. Best security practice is to provide the password in response to a prompt.

-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 to upload the definitions from these two files, first attribute types and then object classes.

Related Command-Line Tools

To know more about command-line tools for schemasync, See ldapmodify

5.9 Manage Provisioning Profiles Utility

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.

5.9.1 manageProvProfiles

Use the `manageProvProfiles` command to manage provisioning profiles.

When you install an application that you want to provision, you must create a provisioning integration profile using the `manageProvProfiles` command located in the `ORACLE_HOME/bin` directory.

The `manageProvProfiles` utility 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 Unified Directory or 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.

> **Note:**
>
> For improved security, do not enter a password with the `manageProvProfiles` command unless prompted for one.

Syntax

The syntax followed for using `manageProvProfiles` is as follows:

```
manageProvProfiles operation=[create|modify] ldap_host=backend_hostname
ldap_port=port
ldap_user_dn="bindDN"
[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]
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

manageProvProfiles {operation=enable|disable|delete|status|reset}
application_dn=DN [organization_dn=DN] [ldap_host=backend_hostname]
[ldap_port=port]
[ldap_user_dn=bindDN] [profile_debug=debug_level]
```

Arguments

The `manageProvProfiles` utility accepts the following arguments:

`operation=create | modify | enable | disable | delete | status | reset`

is required for the operation to perform using `manageProvProfiles`. 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=backend_hostname`

Optional. The host name of the Oracle Unified Directory or 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 the back-end directory. The default port for Oracle Unified Directory or Oracle Internet Directory is `389`.

`ldap_user_dn=bindDN`

Required. The DN of the superuser or a user that has sufficient permissions to perform provisioning subscription operations. The default is `cn=orcladmin`.The default value for Oracle Unified Directory is `"cn=directory manager"` and for Oracle Internet Directory is `"cn=orcladmin"`.

`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 Unified Directory or 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. The default value is TRUE.

> **Note:**
>
> This argument is for Oracle Delegated Administration Services 10g Releases (10.1.4.x).

`manage_application_default=TRUE | FALSE`

Optional. Determines whether the Oracle Internet Directory manages the application's default values. The default value is TRUE.

> **Note:**
>
> This argument is for Oracle Delegated Administration Services 10g Releases (10.1.4.x).

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.

Oracle Internet Directory supports versions `1.1`, `2.0`, or `3.0`.

Oracle Unified Directory support versions `2.0` and `3.0`.

interface_type=PLSQL | JAVA

Optional. The type of interface to which events will be propagated. The default is `PLSQL`.

> **Note:**
>
> For `JAVA` type, only interface protocol version `3.0` is supported.

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 and Provisioning 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 and Provisioning 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_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.

> **Note:**
>
> For security reasons, the `ldap_user_password` and `interface_connect_info` arguments are no longer accepted on the command line.

Part II
Schema Reference

Understand about the LDAP schema elements for Oracle Identity Management

This section contains the following topics:

6
LDAP Schema Overview

Understand about the basic concepts of the LDAP directory schema and the list of the schema elements for Oracle Identity Management.
This section contains the following topics:

- Overview of Directory Schema
- Overview of Oracle Identity Management Schema Elements

6.1 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. This section includes the following topics:

- About Object Classes
- Overview of Attributes
- LDAP Controls

6.1.1 About 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.

6.1.2 Overview of 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
```

This section contains the following topics:

- Attribute Name Limitations
- Attribute Syntax
- Attribute Aliases
- Attribute Values Matching Rules
- Sizing Attribute Values
- About Single-Valued and Multi-Valued Attributes
- Attribute Usage
- About Not User Modifiable Attributes

6.1.2.1 Attribute Name Limitations

The length of an attribute name must not exceed 127 characters. For more information about attribute management, refer to the Understanding Attributes in *Administering Oracle Internet Directory*.

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: & { } < > " ' ( )

6.1.2.2 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 6-1 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.

Table 6-1 (Cont.) Attribute Syntax Commonly Used in Oracle Internet Directory

Syntax and Object ID	Description
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.

6.1.2.3 Attribute Aliases

As of 11g Release 1 (11.1.1.0.0), 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'  ... )
```

As of 11g Release 1 (11.1.1.0.0), you may optionally specify:

```
attributeTypes=( ObjectIdentifier NAME ( 'AttributeName' 'Alias1'
'Alias2' ...) ... )
```

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 "Understanding Attribute Aliases section in *Administering Oracle Internet Directory*.

6.1.2.4 Attribute Values 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

6.1.2.5 Sizing 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, this syntax limits the attribute `foo` size to 64, but this size limit is not enforced in Oracle Internet Directory:

```
(object_identifier_of_attribute NAME 'foo' EQUALITY caseIgnoreMatch SYNTAX
'object_identifier_of_syntax{64}' )
```

6.1.2.6 About 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.

6.1.2.7 Attribute Usage

Attribute Usage defines how the attribute is used in the directory. The attribute usage types are:

- **User applications attribute**–Default attribute usage if not explicitly defined for the attribute.
- **System Operational attribute**–Attributes that control operation of the directory itself.

> **See Also:**
>
> Managing System Configuration Attributes in *Administering Oracle Internet Directory*

6.1.2.8 About Not User Modifiable Attributes

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.

6.1.3 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. The controls supported by Oracle Internet Directory 12c Release 2 (12.1.2.3.0) are listed in the following sections:

- Request Controls Supported by Oracle Internet Directory
- Response Controls Supported by Oracle Internet Directory

6.1.3.1 Request Controls Supported by Oracle Internet Directory

Table 6-2 Request Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113730.3.4.18	Proxy Authorization	Allows an LDAP client application to bind to Oracle Internet Directory server with its own identity and then to perform operations on behalf of another user or on behalf of multiple users. This control can improve performance especially for proxy operations performed on behalf of multiple users. The LDAP operation does not require a rebind for each user. For example, consider this scenario: 1. A client application named `proxy-app` binds to Oracle Internet Directory server. 2. A user named John Doe sends a request to the `proxy-app` client application. The client must be a member of the proxy authorization group. 3. Instead of passing the request to the Oracle Internet Directory server as `proxy-app`, the client passes the Proxy Authorization control along with the proxy dn (John Doe) to the server. 4. The server performs the LDAP request for John Doe using John Doe's privileges (ACLs). The server can access only the information or perform only the operations that John Doe has privileges to access or perform. Considerations for the Proxy Authorization control are: • If the control is not accompanied by a proxy `dn`, the server throws an exception and returns an error to the client. If the criticality flag is not set to TRUE, the request is rejected with a protocol error. • If the proxy user has the privileges to perform the operation as per the ACLs, the server executes the request; otherwise, the server returns the result code "123". • Oracle Internet Directory server determines if a Proxy Authorization request is to be honored. Anonymous users are not allowed to assume the identity of others. • If the server receives more than one Proxy Authorization control in the same operation, an error is returned to the client application and the operation attempt is unsuccessful.

Table 6-2 (Cont.) Request Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
1.3.6.1.4.1.42.2.27.8.5.1	Password Policy	Allows an LDAP client to request information from Oracle Internet Directory server about the current password policy state for a user. If a password policy is applicable, a client can send this control with these operations: • `ldapbind`, `ldapmodify`, `ldapadd`, or `ldapcompare` • `ldapsearch` Other operations such as `ldapunbind` and `ldapabandon` are not supported. Also, this control does not apply to a replication bind. The password policy request control does not have a `controlValue`, but the response control has return values, which are described in Table 6-3. The password policy is typically applied to the single-valued attribute `userPassword` for the LDAP simple authentication method or password-based Simple Authentication and Security Layer (SASL) authentication. For more information, see "Password Policy for LDAP Directories" at this location: `http://tools.ietf.org/html/draft-behera-ldap-password-policy-09`

2.16.840.1.113730.3.4.3	Persistent Search	Allows an LDAP client to send a persistent search request to Oracle Internet Directory server.
		A persistent search operation is an enhanced search that continues after the initial search results are returned by the server to the client. After the initial search is finished, the connection to the server is kept alive until the client unbinds or abandons the operation. The client can track changes for entries in the search scope and receive an Entry Change Notification response control if an entry is modified.
		The definition for this control is:
		`PersistentSearch ::= SEQUENCE {`
		`  controlType 2.16.840.1.113730.3.4.3`
		`  changeTypes INTEGER,`
		`  changesOnly BOOLEAN,`
		`  returnECs BOOLEAN`
		`}`
		For a description of these fields, see:
		`http://tools.ietf.org/id/draft-ietf-ldapext-psearch-03.txt`

Table 6-2 (Cont.) Request Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113894.1.8.39	Computed Attribute Value Uniqueness	Allows computed attribute value uniqueness for an entry-based combination of multiple attribute values. Usually, attribute uniqueness is configured only for a single attribute. An application that requires uniqueness for a combination of attribute values can send this control, and Oracle Internet Directory server ensures that the computed attribute value is unique across the directory during an operation such as `ldapadd`, `ldapmodify -add`, or `ldapmodify -replace`. If an entry with the computed value already exists, Oracle Internet Directory server returns the LDAP error code: LDAP_ALREADY_EXISTS = 0x44. For example, in a multi-tenant environment, the UID attribute of a user must be unique for a specific tenant but not necessarily unique across the directory. An application creates an LDAP entry with a computed attribute named TenantID_UID, where TenantID is the identifier of the tenant and UID is the attribute. The application that creates the LDAP entry sends this control, and if an entry with the computed attribute already value already exists, Oracle Internet Directory server returns the LDAP_ALREADY_EXISTS error code.
2.16.840.1.113730.3.4.9	OID_SEARCH_VLV_REQ_CONTROL	Allows a client to specify that the server return, for a given LDAP search, a contiguous subset of a large search result set. It can be used to go through the search results one page at a time, which allows a client to retrieve results more quickly and prevents the client from needing to store too many search results at a time. The server returns the OID_SEARCH_VLV_RES_CONTROL 2.16.840.1.113730.3.4.10. The OID_SEARCH_VLV_REQ_CONTROL works only in conjunction with the SORT control (ldapsearch -T argument). If you do not include a SORT control, the request returns LDAP error code 53 - Search operation with VLV request control is missing SORT request control. The SORT control can contain any sort specification valid for the server. When the SORT control is used with the OID_SEARCH_VLV_REQ_CONTROL, the server does not return the complete set of sorted search results, but instead returns a contiguous subset of those entries specified in the control using a target entry as a reference point for results. For more information, see "LDAP Extensions for Scrolling View Browsing of Search Results" at `http://tools.ietf.org/html/draft-ietf-ldapext-ldapv3-vlv-09`.
1.2.840.113556.1.4.319	OID_SEARCH_PAGING_CONTROL	See the Extensions to the LDAP Protocol in *Application Developer's Guide for Oracle Identity Management*
1.2.840.113556.1.4.473	OID_SEARCH_SORTING_REQUEST_CONTROL	See the Extensions to the LDAP Protocol in *Application Developer's Guide for Oracle Identity Management*

Table 6-2 (Cont.) Request 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, "Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories," 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_APPLYUSEPASSWORD_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 does not send the verifiers to the application. It sends an appropriate password policy error.
2.16.840.1.113894.1.8.3	CONNECT_BY	See the Extensions to the LDAP Protocol in *Application Developer's Guide for Oracle Identity Management*
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	PasswordStatusRequestControl	When packaged as part of the LDAP Bind/Compare operation request, this control causes the server to generate a password policy response control. The actual response control depends on the situation. Cases include imminent password expiration, number of grace logins remaining, password expired, and account locked.
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.
2.16.840.1.113894.1.8.16	AccountStatusRequestControl	When packaged with the LDAP search operation associated with the authentication process, the Oracle Internet Directory returns a password policy response control to inform the client application of account state related information like account lockout, password expiration etc. The application can then parse and enforce the results.
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. See the appendix Searching the Directory for User Certificates in *Administering Oracle Internet Directory*.

Table 6-2 (Cont.) Request Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113894.1.8.29	EffectivePolicyControl	This control is packaged as part of an LDAP base search, where the base DN is that of the user entry being tested. The entry need not exist in the directory at the time. Passing this control results in the return of the LDAP entry describing the applicable password policy, assuming the entity performing the search has the access rights to view the password policy entry. If the desired password is provided as the optional testPassword parameter, the directory server returns the response control 2.16.840.1.113894.1.8.32.
2.16.840.1.113894.1.8.36	DelSubtreeControl	When this control is sent with a delete operation, it causes the deletion of the entire subtree below the DN provided. Any user having necessary privileges can perform this operation.
1.2.840.113556.1.4.805	DelSubtreeControl	When this control is sent with a delete operation, it causes the deletion of the entire subtree below the DN provided. Any user having necessary privileges can perform this operation.
1.3.6.1.1.21.2	Transaction Specification Control	This is an LDAPControl indicating association of an operation to a transaction by means of the transaction identifier, which is the value of this control. Its criticality is TRUE.

6.1.3.2 Response Controls Supported by Oracle Internet Directory

Table 6-3 Response Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description

1.3.6.1.4.1.42.2.27.8.5.1	Password Policy	Response control that the Oracle Internet Directory server returns to an LDAP client in response to the Password Policy request control. The response control value is encoded as follows:
		
		`PasswordPolicyResponseValue ::= SEQUENCE {`
		`  warning [0] CHOICE {`
		`  timeBeforeExpiration [0] INTEGER (0 .. maxInt),`
		`  graceAuthNsRemaining [1] INTEGER (0 .. maxInt) } OPTIONAL,`
		`  error  [1] ENUMERATED {`
		`  passwordExpired (0),`
		`  accountLocked (1),`
		`  changeAfterReset (2),`
		`  passwordModNotAllowed (3),`
		`  mustSupplyOldPassword (4),`
		`  insufficientPasswordQuality (5),`
		`  passwordTooShort (6),`
		`  passwordTooYoung (7),`
		`  passwordInHistory (8) } OPTIONAL }`
		
		The server sends either an error or warning in the password policy response control (but not both). Error codes are described in:
		
		http://tools.ietf.org/html/draft-behera-ldap-password-policy-09
		
		Control criticality is not returned in the response. For a non violation of the password policy, the server does not send a response.

Table 6-3 (Cont.) Response Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description

2.16.840.1.113730.3.4.7	Entry Change Notification	Returned by the Oracle Internet Directory server to an LDAP client in response to a Persistent Search control that has the `returnECs` field set to TRUE. This control is returned for each changed entry that matches the persistent search criteria and describes the change made to the specific search entry.
		The definition for this control is:
		`EntryChangeNotification ::= SEQUENCE {`
		`  controlType 2.16.840.1.113730.3.4.7`
		`  changeType ENUMERATED {`
		`  add (1),`
		`  delete (2),`
		`  modify (4),`
		`  modDN (8)`
		`  },`
		`  previousDN LDAPDN OPTIONAL, -- modifyDN ops. only`
		`  changeNumber INTEGER OPTIONAL -- if supported`
		`}`
		For a description of these fields, see:
		http://tools.ietf.org/id/draft-ietf-ldapext-psearch-03.txt

2.16.840.1.113730.3.4.10	OID_SEARCH_VLV_RES_CONTROL	The server sends this control in response to an OID_SEARCH_VLV_REQ_CONTROL 2.16.840.1.113730.3.4.9.
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.
2.16.840.1.113894.1.8.20	OID_PWDEXPIRED_CONTROL	Password policy control. The response control that the server sends when the password has expired, there are no grace logins remaining, and the client sends a request control.
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.
2.16.840.1.113894.1.8.15	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.

Table 6-3 (Cont.) Response Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
2.16.840.1.113894.1.8.32	PasswordValidationControl	The server sends this in response to control 2.16.840.1.113894.1.8.29 when the desired password is provided as the optional testPassword parameter. A client application can parse the validationResult to determine whether the password can be accepted by the server ("Success") or the reason it has been rejected. The same type of error message generated during a failed LDAP modify operation on userpassword is returned as the value.
2.16.840.1.113894.1.8.37	OID_SEARCH_DYNGRP_STATIC_UMEM	When you send a query with filter `(unique)member=value` along with this control, then the server provides search results with entries that includes only the static `(unique)members`.

6.2 Overview of Oracle Identity Management Schema Elements

Oracle Identity Management schema elements are listed 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 and Provisioning 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

6.2.1 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.

Table 6-4 lists system operational schema elements and operational attributes:

Table 6-4 Attributes for System Operational Schema Elements

System Operational Schema Element	Operational Attributes
Directory Schema	attributeTypes, contentRules, ldapSyntaxes, matchingRules,objectClasses **Object Classes:** subschema
Access Control	orclACI, orclEntryLevelACI
Change Logs	createTimestamp, creatorsName, modifiersName, modifyTimestamp
Password Policy	orclPwdAccountUnlock, orclPwdIPAccountLockedTime, orclPwdIPFailureTime, orclRevPwd, orclUnsyncRevPwd, pwdAccountLockedTime, pwdChangedTime, pwdExpirationWarned, pwdFailureTime , pwdGraceUseTime, pwdHistory, pwdReset

6.2.2 Oracle Internet Directory Configuration Schema Elements

Understand about the schema elements that pertain to the various configurations of Oracle Internet Directory.

This section contains the following topics:

- Attributes for Oracle Internet Directory Server Configuration
- Attributes for Oracle Context Configuration
- Attributes for Oracle Network Services Configuration
- Attributes for Garbage Collection Configuration
- Attributes for Attribute Uniqueness Configuration

6.2.2.1 Attributes for Oracle Internet Directory Server Configuration

This section lists the attributes and object classes that pertain to the configuration of Oracle Internet Directory server.

Attributes

namingContexts, orclAnonymousBindsFlag, orclCatalogEntryDN, orclCompatibleVersion, orclCryptoScheme, orclDBType, orclDebugFlag, orclDebugForceFlush, orclDebugOp, orclDIPRepository, orclDirectoryVersion,

orclDITRoot, orclEcacheEnabled, orclEcacheMaxEntries, orclEcacheMaxSize, orclEnableGroupCache, orclEventLevel, orclGUPassword, orclHostname, orclIndexedAttribute, orclIpAddress, orclLDAPConnTimeout, orclMatchDnEnabled, orclMaxCC, 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

6.2.2.2 Attributes for Oracle Context Configuration

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

6.2.2.3 Attributes for Oracle Network Services Configuration

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

6.2.2.4 Attributes for Garbage Collection Configuration

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

6.2.2.5 Attributes for Attribute Uniqueness Configuration

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

6.2.3 Audit and Error Logging Schema Elements

Understand about 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

6.2.4 Server Manageability Schema Elements

Understand about 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

6.2.5 Oracle Directory Replication Schema Elements

Understand about the schema elements for directory replication.

Attributes

orclAgreementId, orclChangeLogLife, orclChangeRetryCount, orclCompatibleVersion, orclDirReplGroupAgreement, orclExcludedAttributes, 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

6.2.6 Oracle Directory Integration and Provisioning Schema Elements

Understand about the schema elements for Oracle Directory Integration and Provisioning.

This section contains the following topics:

- Attributes for Provisioning Applications
- Attributes for Provisioning Change Logs
- Attributes for Provisioning Events and Objects
- Attributes for Provisioning Plug-ins and Interfaces
- Attributes for Provisioning Server Configuration

- Attributes for Provisioning Profiles
- Attributes for Provisioning Schema
- Attributes for Provisioning Active Directory Users

6.2.6.1 Attributes for Provisioning Applications

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning applications.

Attributes

orclApplicationType, orclInterval, orclODIPAgent, orclODIPApplicationName, orclODIPCommand, orclODIPDbConnectInfo, orclODIPEventSubscriptions, orclOwnerGUID, orclStatus, orclVersion

Object Classes

orclODIPApplicationCommonConfig, orclODIPAppSubscription

6.2.6.2 Attributes for Provisioning Change Logs

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning change logs.

Attributes

orclLastAppliedChangeNumber, orclSubscriberDisable, serverName, userPassword

Object Classes

orclChangeSubscriber

6.2.6.3 Attributes for Provisioning Events and Objects

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning 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

6.2.6.4 Attributes for Provisioning Plug-ins and Interfaces

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning plug-ins and interfaces.

Attributes

orclODIPPluginAddInfo, orclODIPPluginConfigInfo, orclODIPPluginEvents, orclODIPPluginExecData, orclODIPPluginExecName, orclODIPProfileProvSubscriptionMode, orclODIPProfileStatusUpdate, orclODIPProvInterfaceFilter , orclODIPProfileInterfaceType, orclODIPProvInterfaceProcessor, orclStatus

Object Classes

orclODIPProvInterfaceDetails, orclODIPPlugin, orclODIPPluginContainer

6.2.6.5 Attributes for Provisioning Server Configuration

This section lists the attributes and object classes for configuring the Oracle Directory Integration and Provisioning server.

Attributes

cn, orclCompatibleVersion, orclHostname, orclODIPConfigDNs, orclODIPConfigRefreshFlag, orclODIPInstanceStatus, orclODIPProfileExecGroupID, orclODIPSearchCountLimit, orclODIPSearchTimeLimit, orclODIPServerCommitSize, orclODIPServerDebugLevel, orclODIPServerRefreshIntvl, orclODIPServerSSLMode, orclODIPServerWalletLoc, orclSSLEnable, orclVersion, seeAlso, userPassword

Object Classes

orclODIPServerConfig, orclODISConfig, orclODIServer, orclODISInstance

6.2.6.6 Attributes for Provisioning Profiles

This section the attributes and object classes for Oracle Directory Integration and Provisioning 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

6.2.6.7 Attributes for Provisioning Schema

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning schema information.

Attributes

orclODIPApplicationsLocation, orclODIPInstancesLocation, orclODIPObjectDefnLocation , orclODIPProvProfileLocation, orclODIPRootLocation, orclODIPSchemaVersion, orclODIPServerConfigLocation, orclODIPSyncProfileLocation

Object Classes

orclODIPSchemaDetails

6.2.6.8 Attributes for Provisioning 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 and Provisioning.

Attributes

orclObjectGUID, orclObjectSID, orclSAMAccountName, orclUserPrincipalName

Object Classes

orclADGroup, orclADUser, orclNTUser

6.2.7 Oracle Delegated Administration Services Schema Elements

Understand about 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

6.2.8 Oracle Application Server Certificate Authority and PKI Schema Elements

Understand about 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

6.2.9 Application Schema Elements

Understand about 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

6.2.10 Resource Schema Elements

Understand about the attributes and object classes that pertain to resources.

Attributes

description, displayName, javaClassName, orclConnectionFormat, orclFlexAttribute1, orclFlexAttribute2, orclFlexAttribute3, orclOwnerGUID, orclPasswordAttribute, orclResourceName, orclResourceViewers, orclUserIDAttribute, orclUserModifiable

Object Classes

orclResourceDescriptor, orclResourceType

6.2.11 Plug-in Schema Elements

Understand about 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

6.2.12 Directory User Agents Schema Elements

Understand about 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, serviceAuthenticationMethod, serviceCredentialLevel, serviceSearchDescriptor

Object Classes

duaConfigProfile

6.2.13 User, Group, and Subscriber Schema Elements

Understand about the attributes and object classes used for users, groups, and subscribers.

This section contains the following topics:

- Attributes for Groups
- Attributes for Dynamic Groups
- Attributes for Users

6.2.13.1 Attributes for 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

6.2.13.2 Attributes for Dynamic Groups

This section lists the attributes and object classes for dynamic groups.

Attributes

labeledURI, mail, orclConnectByAttribute, orclConnectBySearchBase, orclConnectByStartingValue

Object Classes

orclDynamicGroup

6.2.13.3 Attributes for 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, orclTxnMaxOperations, orclVersion, orclWirelessAccountNumber, orclWorkflowNotificationPref, userPKCS12

Object Classes

orclSubscriber, orclUserV2

6.2.14 Password Policy Schema Elements

Understand about 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, pwdMustChange, pwdSafeModify

Object Classes

pwdpolicy

6.2.15 Password Verifier Schema Elements

Understand about the attributes and object classes that pertain to password verifiers.

Attributes

cn, displayName, orclAppId, , owner

Object Classes

orclPwdVerifierProfile

7

LDAP Object Class Reference

Understand about the object class information used by Oracle Identity Management. This section contains the following topics:

- Standard LDAP Object Classes Used in Oracle Internet Directory
- Oracle Identity Management Object Class Reference

For a list of object classes grouped by functional categories, see Overview of Oracle Identity Management Schema Elements.

7.1 Standard LDAP Object Classes Used in Oracle Internet Directory

Oracle Internet Directory supports 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`.

Oracle Internet Directory supports the following standard LDAP object classes.

Table 7-1 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
domain	RFC 1274

Table 7-1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
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
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
posixAccount	RFC 2307

Table 7-1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
posixGroup	RFC 2307
referral	RFC 3296
residentialPerson	RFC 2256
room	RFC 1274
shadowAccount	RFC 2307
simpleSecurityObject	RFC 1274
strongAuthenticationUser	RFC 2256

7.2 Oracle Identity Management Object Class Reference

Oracle Identity Management object classes are the object classes used to create entries pertaining to Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, Oracle 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.

7.2.1 duaConfigProfile

`duaConfigProfile` is a configuration profile for a directory user agent (DUA).

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, serviceAuthenticationMethod, serviceCredentialLevel, serviceSearchDescriptor

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.

7.2.2 orclADGroup

`orclADGroup` 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 and Provisioning 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

7.2.3 orclADUser

`orclADUser` 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 and Provisioning 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

7.2.4 orclApplicationEntity

`orclApplicationEntity` 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, orclApplicationAddress, orclApplicationCommonName, orclCategory, orclDBSchemaIdentifier, orclPasswordVerifier, orclResourceIdentifier, orclTrustedApplicationGroup, orclVersion, protocolInformation, seeAlso, userCertificate;binary, userPassword, userPKCS12

7.2.5 orclAppSpecificUserInfo

`orclAppSpecificUserInfo` is 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

r

Object Class Type

Auxilliary

Required Attributes

orclOwnerGUID

Allowed Attributes

N/A

7.2.6 orclAppUserEntry

`orclAppUserEntry` is the application entity of the associated user.

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

7.2.7 orclAuditOC

`orclAuditOC` is the 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

7.2.8 orclCertIdMapping

`orclCertIdMapping` is the 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

7.2.9 orclChangeSubscriber

`orclChangeSubscriber` is the status information for an Oracle Directory Integration and Provisioning 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

7.2.10 orclCommonAttributes

`orclCommonAttributes` is 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

7.2.11 orclCommonAttributesV2

`orclCommonAttributesV2` is the 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

7.2.12 orclConfigSet

`orclConfigSet` is the 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

7.2.13 orclContainer

`orclContainer` is the 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

7.2.14 orclDASAppContainer

`orclDASAppContainer` is the 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

7.2.15 orclDASAttrCategory

`orclDASAttrCategory` is the 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

7.2.16 orclDASConfigAttr

`orclDASConfigAttr` is 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

7.2.17 orclDASConfigPublicGroup

`orclDASConfigPublicGroup` is 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

7.2.18 orclDASLOVVal

`orclDASLOVVal` is 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

7.2.19 orclDASOperationURL

`orclDASOperationURL` is 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

7.2.20 orclDASSubscriberContainer

`orclDASSubscriberContainer` is 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

7.2.21 orclIDMapping

`orclIDMapping` is 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

7.2.22 orclDSAConfig

`orclDSAConfig` holds the 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, orclCatalogEntryDN, orclCryptoScheme, orclDebugFlag, orclDebugForceFlush, orclDebugOp, orclDIPRepository, orclEcacheEnabled, orclEcacheMaxEntries, orclEcacheMaxSize, orclEnableGroupCache, orclGUPassword, orclIpAddress, orclLDAPConnTimeout, orclMatchDnEnabled, orclMaxConnInCache, orclNwrwTimeout, orclPKIMatchingRule, orclPrName, orclPrPassword, orclReplAgreements, orclReplicaID, orclsDumpFlag, orclServerMode, orclSizeLimit, orclSkewedAttribute, orclSkipRefInSQL, orclStatsDN, orclStatsFlag, orclStatsLevel, orclStatsOp, orclStatsPeriodicity, orclSUAccountLocked, orclSULoginFailureCount, orclSUName, orclSUPassword, orclTimeLimit, orclTLimitMode, orclUpgradeInProgress

7.2.23 orclDynamicGroup

`orclDynamicGroup` is the Object class that is 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. In the case of `orclDynamicGroup` using `labelеduri` attribute, the members of the list are cached.

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

7.2.24 orclDynamicList

`orclDynamicList` is the objectclass that is 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. In the case of orclDynamicList, members are not cached.

Object ID

2.16.840.1.113894.1.1.425

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

labeledURI

Allowed Attributes

N/A

7.2.25 orclEventLog

`orclEventLog` is the object class that is 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

7.2.26 orclEvents

`orclEvents` is the object class that is 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

7.2.27 orclGeneralStats

`orclGeneralStats` is the 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

7.2.28 orclGroup

`orclGroup` is the 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

7.2.29 orclHealthStats

`orclHealthStats` has the 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

7.2.30 orclIndexOC

`orclIndexOC` is the 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

7.2.31 orclLDAPInstance

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, orclCompatibleVersion, orclHostname

Allowed Attributes

description, seeAlso

7.2.32 orclLDAPSubConfig

`orclLDAPSubConfig` contains the 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

7.2.33 orclNTUser

`orclNTUser` contains Microsoft NT user attributes, which are used to synchronize NT user objects with Oracle Internet Directory user objects in an Oracle Directory Integration and Provisioning 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

7.2.34 orclODIPApplicationCommonConfig

`orclODIPApplicationCommonConfig` contains the Oracle Directory Integration and Provisioning configuration attributes.

Object ID

2.16.840.1.13894.8.2.421

Superior Object Class

top

Objet Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

orclApplicationType

7.2.35 orclODIPAppSubscription

`orclODIPAppSubscription` contains the application subscription attributes for Oracle Directory Integration and Provisioning.

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

7.2.36 orclODIPEventContainer

`orclODIPEventContainer` is a container object for an Oracle Directory Integration and Provisioning 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

7.2.37 orclODIPIntegrationProfile

`orclODIPIntegrationProfile` is Oracle Directory Integration and Provisioning 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

7.2.38 orclODIPObject

`orclODIPObject` contains attributes to identify Oracle Directory Integration and Provisioning 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

7.2.39 orclODIPPlugin

Configuration attributes for Oracle Directory Integration and Provisioning 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

7.2.40 orclODIPPluginContainer

`orclODIPPluginContainer` contains configuration attributes for Oracle Directory Integration and Provisioning 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

7.2.41 orclODIPProvEventDefn

`orclODIPProvEventDefn` 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

7.2.42 orclODIPProvEventTypeConfig

`orclODIPProvEventTypeConfig` contains 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

7.2.43 orclODIPProvInterfaceDetails

`orclODIPProvInterfaceDetails` contains 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

7.2.44 orclODIPProvisioningIntegrationInBoundProfileV2

`orclODIPProvisioningIntegrationInBoundProfileV2` defines configuration for an Oracle Directory Integration and Provisioning 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

7.2.45 orclODIPProvisioningIntegrationOutBoundProfile

`orclODIPProvisioningIntegrationOutBoundProfile` contains configuration for an Oracle Directory Integration and Provisioning 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

7.2.46 orclODIPProvisioningIntegrationOutBoundProfileV2

`orclODIPProvisioningIntegrationOutBoundProfileV2` contains configuration for an Oracle Directory Integration and Provisioning 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

7.2.47 orclODIPProvisioningIntegrationProfile

`orclODIPProvisioningIntegrationProfile` contains configuration for an Oracle Directory Integration and Provisioning 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

7.2.48 orclODIPProvisioningIntegrationProfileV2

`orclODIPProvisioningIntegrationProfileV2` contains configuration for an Oracle Directory Integration and Provisioning 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

7.2.49 orclODIProfile

`orclODIProfile` is the profile for Oracle Directory Integration and Provisioning 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

7.2.50 orclODIPSchemaDetails

`orclODIPSchemaDetails` are the Oracle Directory Integration and Provisioning 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

7.2.51 orclODIPServerConfig

`orclODIPServerConfig` contains the configuration attributes for the Oracle Directory Integration and Provisioning 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

7.2.52 orclODISConfig

`orclODISConfig` contains the configuration attributes for the Oracle Directory Integration and Provisioning 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

7.2.53 orclODIServer

`orclODIServer` contains the configuration attributes for the Oracle Directory Integration and Provisioning 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

7.2.54 orclODISInstance

Configuration attributes for the Oracle Directory Integration and Provisioning 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

7.2.55 orclPerfStats

`orclPerfStats` are the 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

7.2.56 orclPKICRL

`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

7.2.57 orclPKIValMecCl

`orclPKIValMecCl` is 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

7.2.58 orclPluginConfig

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

7.2.59 orclPluginContainer

`orclPluginContainer` is the 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

7.2.60 orclPluginUser

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

7.2.61 orclPurgeConfig

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

7.2.62 orclPwdVerifierPolicy

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

7.2.63 orclPwdVerifierProfile

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

7.2.64 orclReplAgreementEntry

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

orclExcludedAttributes, orclHIQSchedule, orclIncludedNamingContexts, orclLastAppliedChangeNumber, orclLDAPConnKeepALive, orclReplicaDN

7.2.65 orclReplicaSubentry

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

7.2.66 orclReplInstance

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, orclCompatibleVersion, orclHostname

Allowed Attributes

description, seeAlso

7.2.67 orclReplNameCtxConfig

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

7.2.68 orclReplSubConfig

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

7.2.69 orclResourceDescriptor

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

7.2.70 orclResourceType

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

7.2.71 orclRootContext

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

7.2.72 orclSchemaVersion

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

7.2.73 orclSecRefreshEvents

`orclSecRefreshEvents` is 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

7.2.74 orclService

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

7.2.75 orclServiceInstance

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

7.2.76 orclServiceInstanceReference

`orclServiceInstanceReference` is a 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

7.2.77 orclServiceRecipient

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

7.2.78 orclServiceSubscriptionDetail

`orclServiceSubscriptionDetail` holds the 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

7.2.79 orclServiceSuite

`orclServiceSuite` is a 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

7.2.80 orclSM

`orclSM` is 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

7.2.81 orclSubscriber

`orclSubscriber` provides 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

7.2.82 orclSysResourceEvents

`orclSysResourceEvents` holds the 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

7.2.83 orclTraceConfig

`orclTraceConfig` is the 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

7.2.84 orclUniqueConfig

`orclUniqueConfig` is the 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

7.2.85 orclUserStats

`orclUserStats` is the 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

7.2.86 orclUserV2

`orclUserV2` is the 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,

orclTxnMaxOperations, orclWirelessAccountNumber, orclWorkflowNotificationPref, userPKCS12

7.2.87 pwdpolicy

`pwdpolicy` 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, pwdMaxFailure, pwdMinAge, pwdMustChange, pwdSafeModify

7.2.88 subentry

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

7.2.89 subregistry

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

7.2.90 subschema

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

7.2.91 tombstone

`tombstone` is the 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

7.2.92 top

`top` 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

8
LDAP Attribute Reference

Understand about the reference information of the LDAP attributes used by Oracle Identity Management.

- 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.

8.1 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 8-1 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
co	RFC 1274
crossCertificatePair	RFC 2256
dc	RFC 2247
deltaRevocationList	RFC 2256

Table 8-1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
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
javaSerializedData	RFC 2713
janetMailbox	RFC 1274
jpegPhoto	RFC 1488
knowledgeInformation	RFC 2256

Table 8-1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
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
postalAddress	RFC 2256
postalCode	RFC 2256
postOfficeBox	RFC 2256
preferredDeliveryMethod	RFC 2256

Table 8-1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
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
uniqueMember	RFC 2256
userCertificate;binary	RFC 2256
userClass	RFC 1274
userPassword	RFC 2256

Table 8-1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
userPKCS12	RFC 2798
userSMIMECertificate	RFC 2798
x121Address	RFC 2256
x500UniqueIdentifier	RFC 2256

8.2 Oracle Identity Management Attribute Reference

Oracle Identity Management attributes are the attributes used in entries pertaining to Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, and Oracle Single Sign-On.

> **Note:**
>
> Oracle Fusion Middleware 11g Release 1 (11.1.1.0.0) does not include Oracle Single Sign-On or Oracle Delegated Administration Services. Oracle Internet Directory 11g Release 1 (11.1.1.0.0), however, is compatible with Oracle Single Sign-On and Oracle Delegated Administration Services 10g (10.1.4.3.0) or later.

> **See Also:**
>
> The chapter on Managing System Configuration Attributes in *Administering Oracle Internet Directory*.

8.2.1 attributeMap

`attributeMap` contains the attribute mapping 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

8.2.2 attributeTypes

`attributeTypes` contains definitions of each attribute type available in 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.

8.2.3 authenticationMethod

`authenticationMethod` 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.

8.2.4 authPassword

`authPassword` is the 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

8.2.5 bindAuthPriv

`bindAuthPriv` allows Oracle Internet Directory server to restrict users who can bind to it.

The administrator creates an LDAP group entry where only members of the group can bind to the server. Each user entry of users who are allowed to bind to the server must contain an `bindAuthPriv` attribute that points to the group. If a user is not a member of the group, bind requests are rejected. Several other considerations are:

- The `bindAuthPriv` attribute can be a collective attribute that allows specific users to inherit it.
- The LDAP group can be a nested group.
- The administrator must ensure the proper ACL for the `bindAuthPriv` attribute, so that the attribute can be added to a user entry only by an administrator.

Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.641

Other

Single-valued attribute.

8.2.6 bindTimeLimit

`bindTimeLimit` is the 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.

8.2.7 c

c 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.

8.2.8 changeloginfo

`changeloginfo` is the attribute that provides additional change log information, such as the value of the client IP address.

For example:

```
changeloginfo=clientip=::ffff:10.229.116.104
```

Syntax

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.510

Other

Single-valued attribute.

8.2.9 changestatus

`changestatus` is the last change number transported by the replication server.

Syntax

DN

Matching Rule

DistinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.22

8.2.10 cn

`cn` is 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 Finance 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

8.2.11 contentRules

`contentRules` 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

8.2.12 createTimestamp

`createTimestamp` is 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.

8.2.13 creatorsName

`creatorsName` is 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.

8.2.14 credentialLevel

`credentialLevel` 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.

8.2.15 defaultSearchBase

`defaultSearchBase` is 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

Other

Single-valued attribute.

8.2.16 defaultSearchScope

`defaultSearchScope` is the 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.

8.2.17 defaultServerList

`defaultServerList` is 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.

8.2.18 description

`description` is 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

8.2.19 displayName

`displayName` is 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.

8.2.20 followReferrals

`followReferrals` 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.

8.2.21 javaClassName

`javaClassName` is the 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.

8.2.22 jpegPhoto

`jpegPhoto` is 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

8.2.23 krbPrincipalName

`krbPrincipalName` 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.

8.2.24 labeledURI

`labeledURI` is a 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

8.2.25 ldapSyntaxes

`ldapSyntaxes` 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.

8.2.26 mail

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@example.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

8.2.27 matchingRules

`matchingRules` 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

Other

Directory operational attribute.

8.2.28 middleName

`middleName` is 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

8.2.29 modifiersName

`modifiersName` is 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.

8.2.30 modifyTimestamp

`modifyTimestamp` is 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.

8.2.31 namingContexts

`namingContexts` is the top-level DNs for the naming contexts contained in this server. You must have superuser 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.

8.2.32 objectClass

`objectClass` is 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

8.2.33 objectClasses

`objectClasses` 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.

8.2.34 objectClassMap

`objectClassMap` is 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

8.2.35 orclACI

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

8.2.36 orclACLResultsLatency

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.

8.2.37 orclActivateReplication

`orclActivateReplication` specifies that replication be activated on the replication server designated by `orclOidInstanceName` and `orclOidComponentName`. 1: Start replication server, 0: Stop replication server.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.616

8.2.38 orclActiveConn

`orclActiveConn` 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.

8.2.39 orclActiveEndDate

`orclActiveEndDate` 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.

8.2.40 orclActiveStartdate

`orclActiveStartdate` 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.

8.2.41 orclActiveThreads

`orclActiveThreads` 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

Other

Single-valued attribute.

8.2.42 orclAgreementId

`orclAgreementId` is the 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.

8.2.43 orclagreementtype

`orclagreementtype` is the replication agreement type.

Replication agreement type: '0-OneWay 1-TwoWay, 2-LDAP Multimaster, 3-ASR Multimaster.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.511

8.2.44 orclAnonymousBindsFlag

`orclAnonymousBindsFlag` specifies whether anonymous binds to the directory are allowed or not.

If set to 2, anonymous binds are allowed, but only search operations on root DSE entry are allowed for anonymous users. If set to 1, then anonymous binds are allowed. If set to 0 (zero), then anonymous binds 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.

8.2.45 orclAppFullName

`orclAppFullName` is 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

8.2.46 orclAppId

`orclAppId` is 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.

8.2.47 orclApplicationAddress

`orclApplicationAddress` is the address of the application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.318

8.2.48 orclApplicationCommonName

`orclApplicationCommonName` is 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

8.2.49 orclApplicationType

`orclApplicationType` identifies the application type, such as Oracle 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.

8.2.50 orclAssocDB

`orclAssocDB` 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

8.2.51 orclAssoclasInstance

`orclAssocIasInstance` 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

8.2.52 orclAttrACLEvalLatency

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.

8.2.53 orclAudCustEvents

`orclAudCustEvents` is a comma-separated list of events and category names to be audited. Custom events are only applicable when `orclAudFilterPreset` is `Custom`.

Examples include:

```
Authentication.SUCCESSESONLY,
Authorization(Permission -eq 'CSFPerfmission")
```

Syntax

IA5 String

Matching Rule

caseExactIAI5Match

Object ID

2.16.840.1.113894.1.1.373

8.2.54 orclAudFilterPreset

`orclAudFilterPreset` replaces the audit levels used in 10g (10.1.4.0.1) and earlier releases.

Values are `None`, `Low`, `Medium`, `All`, and `Custom`.

Syntax

IA5 String

Matching Rule

caseExactIAI5Match

Object ID

2.16.840.1.113894.1.1.372

8.2.55 orclAuditAttribute

`orclAuditAttribute` 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

8.2.56 orclAuditMessage

`orclAuditMessage` 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

8.2.57 orclAudSplUsers

`orclAudSplUsers` is a comma separated list of users for whom auditing is always enabled, even if `orclAudFilterPreset` is `None`.

For example:

```
cn=orcladmin.
```

Syntax

IA5 String

Matching Rule

caseExactIAI5Match

Object ID

2.16.840.1.113894.1.1.374

8.2.58 orclBERgenLatency

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.

8.2.59 orclBlockDNIP

`orclBlockDNIP` is an IP address that causes Oracle Internet Directory server to reject any new connections and close any existing connections from that IP address.

> **Note:**
>
> You need to use the `subtype` property along with this attribute to configure DN or IP address that needs to be blocked. Use the following subtype:
>
> For DN: `dn`
>
> For IP address: `ip`
>
> Consider the following examples:
>
> ```
> orclblockdnip;dn: cn=jdoe,ou=abc,c=us
> orclblockdnip;ip: ffff:11.234.56.789
> ```

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.382

Other

Single-valued attribute.

8.2.60 orclcachenotifyip

`orclcachenotifyip` is a configuration attribute that associates a port number with an IP address in order to allow Oracle Internet Directory servers to communicate with each other in a cluster environment when cached data is changed.

The servers communicate with each other using the LDAP protocol. For example, the following LDIF file, which you can load using the `ldapmodify` command, associates port number 5678 with IP address 10.10.10.4 for the oid1 instance:

```
dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
changetype: modify
add: orclcachenotifyip;5678
orclcachenotifyip;5678: 10.10.10.4
```

When orclcachenotifyip is configured for an Oracle Internet Directory instance, the IP address must be local to the node where the instance is running.

Syntax

1.3.6.1.4.1.1466.115.121.1.44

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.640

8.2.61 orclCatalogEntryDN

`orclCatalogEntryDN` 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.

8.2.62 orclCategory

`orclCategory` 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

8.2.63 orclCertExtensionAttribute

`orclCertExtensionAttribute` 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.

8.2.64 orclCertExtensionOID

`orclCertExtensionOID` 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.

8.2.65 orclCertificateHash

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.

8.2.66 orclCertificateMatch

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.

Refer 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.

8.2.67 orclCertMappingAttribute

`orclCertMappingAttribute` 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.

8.2.68 orclChangeLogLife

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.

8.2.69 orclChangeRetryCount

`orclChangeRetryCount` is 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.

8.2.70 orclCommonAutoRegEnabled

`orclCommonAutoRegEnabled` 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.

8.2.71 orclCommonContextMap

`orclCommonContextMap` 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.

8.2.72 orclCommonDefaultUserCreateBase

`orclCommonDefaultUserCreateBase` 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.

8.2.73 orclCommonGroupCreateBase

`orclCommonGroupCreateBase` 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

8.2.74 orclCommonNamingAttribute

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

8.2.75 orclCommonNicknameAttribute

`orclCommonNicknameAttribute` 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.

8.2.76 orclCommonSASLRealm

`orclCommonSASLRealm` 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.

8.2.77 orclCommonUserSearchBase

`orclCommonUserSearchBase` 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

8.2.78 orclCommonVerifierEnable

If this attribute is enabled then the common verifier is 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.

8.2.79 orclCommonVerifierEnable

If this attribute is enabled then the common verifier is 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.

8.2.80 orclCompatibleVersion

`orclCompatibleVersion` is the Oracle Internet Directory version. Do not modify this attribute. It must be present for Oracle Internet Directory 11.1.1.6.0 or later to work with the schema.

Values can be:

- orclcompatibleversion 11.1.1.6.0
- orclcompatibleversion 11.1.1.7.0

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1302

Other

Multi-valued attribute.

8.2.81 orclComputedAttribute

Attribute that allows a configurable attribute and its value to be dynamically computed based on one or more specific rules.

See Also Managing Computed Attributes in *Administering Oracle Internet Directory*.

Syntax

1.3.6.1.4.1.1466.115.121.1.44

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.628

Other

Multi-valued attribute.

8.2.82 orclconflresolution

Automatically resolve replication conflicts. When this feature is enabled, conflicts in the Human Intervention Queue are automatically moved to the purge queue if the supplier's schema and consumer's schema match.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.828

8.2.83 orclConnectByAttribute

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.

8.2.84 orclConnectBySearchBase

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`. This attribute is currently not used.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1003

Other

Single-valued attribute.

8.2.85 orclConnectByStartingValue

For a dynamic group query, this specifies the DN of the attribute 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.

8.2.86 orclConnectionFormat

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.

8.2.87 orclContact

`orclContact` 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.

8.2.88 orclCryptoScheme

The hash algorithm used to encrypt passwords that are stored in the directory. Options are: MD4, MD5, No encryption, SHA, SSHA,SHA256, SHA384, SHA512, SSHA256, SSHA384, SSHA512, SMD5, or UNIX Crypt. The default is SSHA.

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.

8.2.89 orclDASAdminModifiable

`orclDASAdminModifiable` specifies whether 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.

8.2.90 orclDASAttrDispOrder

`orclDASAttrDispOrder` 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

8.2.91 orclDASAttrName

`orclDASAttrName` 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

8.2.92 orclDASEnableProductLogo

`orclDASEnableProductLogo` specifies whether 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.

8.2.93 orclDASEnableSubscriberLogo

`orclDASEnableSubscriberLogo` specifies whether 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.

8.2.94 orclDASIsEnabled

`orclDASIsEnabled` specifies whether 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.

8.2.95 orclDASIsMandatory

`orclDASIsMandatory` specifies whether 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.

8.2.96 orclDASIsPersonal

`orclDASIsPersonal` specifies whether 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.

8.2.97 orclDASLOV

The list of values to display to users in the UI when the `orclDASUIType` =Predefined List.

See orclDASUIType

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

8.2.98 orclDASPublicGroupDNs

`orclDASPublicGroupDNs` 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

8.2.99 orclDASSearchable

`orclDASSearchable` 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.

8.2.100 orclDASSearchColIndex

`orclDASSearchColIndex` 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.

8.2.101 orclDASSearchFilter

`orclDASSearchFilter` 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.

8.2.102 orclDASSearchSizeLimit

`orclDASSearchSizeLimit` is 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.

8.2.103 orclDASSelfModifiable

`orclDASSelfModifiable` specifies whether 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.

8.2.104 orclDASUIType

`orclDASUIType` 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.

8.2.105 orclDASURL

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

8.2.106 orclDASURLBase

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

8.2.107 orclDASValidatePwdReset

`orclDASValidatePwdReset` specifies whether 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.

8.2.108 orclDASViewable

`orclDASViewable` specifies whether 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.

8.2.109 orcldataprivacymode

`orcldataprivacymode` specifies Data Privacy mode.

Sensitive attributes encrypted when returned.

0: Disabled, 1: Enabled

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.890

8.2.110 orclDateOfBirth

`orclDateOfBirth` 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.

8.2.111 orclDBConnCreationFailed

`orclDBConnCreationFailed` 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.

8.2.112 orclDBLatency

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.

8.2.113 orclDBSchemaIdentifier

`orclDBSchemaIdentifier` is the 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

8.2.114 orclDBType

`orclDBType` indicates 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.

8.2.115 orclDebugFlag

`orclDebugFlag` is the debug level associated with a server instance. The default is 0 (zero). The valid range is 0 to 402653184.

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.

8.2.116 orclDebugForceFlush

`orclDebugForceFlush` 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.

8.2.117 orcldebuglevel

`orcldebuglevel` specifies the Replication server debug level.

Values are additive:

0: No Debug Log, 2097152: Replication Performance Log, 4194304: Replication Debug Log, 8388608: Function Call Trace, 16777216: Heavy Trace Log

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.3

8.2.118 orclDebugOp

To make logging more focused, `orclDebugOp` 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.

8.2.119 orclDefaultProfileGroup

`orclDefaultProfileGroup` 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.

8.2.120 orclDefaultSubscriber

`orclDefaultSubscriber` 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

8.2.121 orclDIMEonlyLatency

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.

8.2.122 orclDIPRepository

`orclDIPRepository` is used to determine if the directory is used as the Oracle Directory Integration and Provisioning 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.

8.2.123 orclDirectoryVersion

`orclDirectoryVersion` is 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.

8.2.124 orclDirReplGroupAgreement

`orclDirReplGroupAgreement` 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.

8.2.125 orclDisplayPersonalInfo

`orclDisplayPersonalInfo` 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.

8.2.126 OrclDispThreads

`OrclDispThreads` is the number of dispatcher threads per server process.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.613

8.2.127 orclDITRoot

`orclDITRoot` is 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.

8.2.128 orclDNSUnavailable

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.

8.2.129 orclcachemaxsize

`orclcachemaxsize` specifies the size in bytes of the result set cache or the metadata cache, depending on the subtype.

The available subtypes are:

- rs: Result set cache. Default and minimum cache size is 64 MB.
- md: Metadata cache. Default and minimum cache size is 128 MB.

Specify the size as M or G, indicating megabytes or gigabytes, respectively. To set a subtype, specify:

`orclcachemaxsize; subtypename: value`

For example:

```
orclcachemaxsize; md: 256M
```

Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.642

Other

Single-valued attribute.

8.2.130 orclEcacheEnabled

`orclEcacheEnabled` specifies whether to enable or disable the Entry Cache or Result Set Cache.

Values can be:

- 0: Disable both the Entry Cache and Result Set Cache.
- 1: Enable the Entry Cache only (default value).
- 2: Enable both the Entry Cache and Result Set Cache.

If you change the attribute value, restart the Oracle Internet Directory server instance for the new value to take effect.

> **Note:**
>
> A new subtype `groups` is available for `orclEcacheEnabled` attribute. This specifies whether to cache group entries or not. It's disabled by default out of the box.
>
> Values can be:
>
> - 0 (default): Not to cache group entries
> - 1: Cache group entries
>
> Example, `orclEcacheEnabled;groups: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.

8.2.131 orclEcacheHitRatio

`orclEcacheHitRatio` 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.

8.2.132 orclEcacheMaxEntries

`orclEcacheMaxEntries` holds the 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.

8.2.133 orclEcacheMaxSize

`orclEcacheMaxSize` is the size of shared memory that can be used for the entry cache. The default is 100 MB.

Specify the size as M or G, indicating megabytes or gigabytes, respectively.

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.

8.2.134 orclEcacheNumEntries

`orclEcacheNumEntries` is 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.

8.2.135 orclEcacheSize

`orclEcacheSize` specifies 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.

8.2.136 orclEnabled

`orclEnabled` 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.

8.2.137 orclEnableGroupCache

`orclEnableGroupCache` specifies whether 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.

8.2.138 orclencryptedattributes

`orclencryptedattributes` specifies the list of attributes to be stored in an encrypted form.

Syntax

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.419

8.2.139 orclEntryACLEvalLatency

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.

8.2.140 orclEntryLevelACI

`orclEntryLevelACI` 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

8.2.141 orclEventLevel

`orclEventLevel` specifies critical events related to security and system resources to be recorded for server manageability statistics.

The default value is 0. Table 8-2 lists the level values.

Table 8-2 Event Levels

Level Value	Critical Event	Information It Provides
1	Superuser login	Super uses bind (successes or failures)

Table 8-2 (Cont.) Event Levels

Level Value	Critical Event	Information It Provides
2	Proxy user login	Proxy user bind (failures)
4	Replication login	Replication bind (failures)
8	Add access	Add access violation
16	Delete access	Delete access violation
32	Write access	Write access violation
64	ORA 3113 error	Loss of connection to database
128	ORA 3114 error	Loss of connection to database
256	ORA 28 error	ORA-28 Error
512	ORA error	ORA errors other an expected 1, 100, or 1403
1024	Oracle Internet Directory server termination count	
2047	All critical events	

For events other than superuser, 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.

8.2.142 orclEventTime

`orclEventTime` is the time when 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

8.2.143 orclEventType

`orclEventType` is 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

8.2.144 orclExcludedAttributes

`orclExcludedAttributes` 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.

8.2.145 orclFDIncreaseError

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.

8.2.146 orclFilterACLEvalLatency

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.

8.2.147 orclFlexAttribute1

`orclFlexAttribute1` is 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

8.2.148 orclFlexAttribute2

`orclFlexAttribute2` is 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

8.2.149 orclFlexAttribute3

`orclFlexAttribute3` is 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

8.2.150 orclFrontLatency

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.

8.2.151 orclGender

`orclGender` specifies 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.

8.2.152 orclgeneratechangelog

`orclgeneratechangelog` enables change log generation.

The options are:

- 1- Generate change log
- 0- Do not generate change log

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.617

8.2.153 orclGenObjLatency

`orclGenObjLatency` 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.

8.2.154 orclGetNearACLLatency

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.

8.2.155 orclGlobalID

`orclGlobalID` 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.

8.2.156 orclGUID

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.

8.2.157 orclGUPassword

`orclGUPassword` is the 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.

8.2.158 orclHashedAttributes

`orclHashedAttributes` is the list of attributes whose values are hashed, using the crypto scheme set in the root DSE attribute `orclcryptoscheme`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (caseIgnoreSubstringsMatch)

Matching Rule

caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.376

Other

Multi-valued attribute

> **Note:**
>
> - Never include the same attribute in both `orclhashedattributes` and `orclencryptedattributes`.
> - Only single-valued attributes can be hashed attributes.

8.2.159 orclHIQSchedule

`orclHIQSchedule` is the interval, in seconds, 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.

8.2.160 orclHireDate

`orclHireDate` 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.

8.2.161 orclHostedCreditCardExpireDate

`orclHostedCreditCardExpireDate` indicates 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.

8.2.162 orclHostedCreditCardNumber

`orclHostedCreditCardNumber` indicates 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.

8.2.163 orclHostedCreditCardType

`orclHostedCreditCardType` indicates 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.

8.2.164 orclHostedDunsNumber

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.

8.2.165 orclHostedPaymentTerm

`orclHostedPaymentTerm` specifies the 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.

8.2.166 orclHostname

`orclHostname` indicates 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.

8.2.167 orclIdleConn

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.

8.2.168 orclIdleThreads

The number of Oracle Internet Directory server 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.

8.2.169 orclIncludedNamingContexts

`orclIncludedNamingContexts` is the naming context included in a partial replica. For each naming context object, you can specify only one unique subtree.

In partial replication, 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 Oracle Database 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.

8.2.170 orclIndexedAttribute

`orclIndexedAttribute` are 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

8.2.171 orclInitialServerMemSize

`orclInitialServerMemSize` is 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.

8.2.172 orclinmemfiltprocess

`orclinmemfiltprocess` specifies the search filters to be processed in memory.

Syntax

Printable String

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.608

Other

Multiple-valued attribute.

8.2.173 orclInterval

`orclInterval` is the time interval in seconds between executions of Oracle Directory Integration and Provisioning 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

8.2.174 orclIpAddress

`orclIpAddress` is 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

8.2.175 orclIsEnabled

`orclIsEnabled` specifies whether 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.

8.2.176 orclIsVisible

This attribute is used to determine if users or groups is visible to applications managed by Oracle Delegated Administration Services, such as Oracle Portal. Oracle 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.

8.2.177 orclLastAppliedChangeNumber

For Oracle Directory Integration and Provisioning export operations, `orclLastAppliedChangeNumber` indicates 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 and Provisioning 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.

8.2.178 orclLastLoginTime

`orclLastLoginTime` indicates the last login time of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.24

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.378

Other

Single-valued attribute

8.2.179 orclLDAPConnKeepALive

For replication, `orclLDAPConnKeepALive` indicates whether 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.

8.2.180 orclLDAPConnTimeout

`orclLDAPConnTimeout` indicates 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.

8.2.181 orclLDAPInstanceID

`orclLDAPInstanceID` indicates 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.

8.2.182 orclLDAPProcessID

`orclLDAPProcessID` indicates 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.

8.2.183 orclMaidenName

`orclMaidenName` indicates 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

8.2.184 orclMappedDN

`orclMappedDN` 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.

8.2.185 orclMaskFilter

`orclMaskFilter` indicates LDAP filter specifying entries to be exposed. Others are masked.

Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.427

Other

Multivalued, User-modifiable

8.2.186 orclMaskRealm

`orclMaskRealm` indicates the list of DIT subtrees that are exposed or hidden.

They are as follows:

- orclMaskRealm contains the DIT subtrees that are exposed in an instance. This attribute is configured in the instance level. The DN configured and its children are visible in the instance. Other entries in the DIT are masked (hidden) for all LDAP operations.
- orclMaskRealm;disallowed contains the DIT subtrees that are hidden in a container for an entire directory for all LDAP operations. This attribute is configured in the DSA configuration entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.34 (DN)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.426

Other

Multivalued, User-modifiable.

8.2.187 orclMasterNode

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.

8.2.188 orclMatchDnEnabled

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.

8.2.189 orclMaxCC

`orclMaxCC` indicates the number of connections established by the Oracle Internet Directory server to its backend data base. The default value is 2.

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.

8.2.190 orclMaxConnInCache

`orclMaxConnInCache` is the number of connection DNs whose privileged groups can be cached is controlled by orclMaxConnInCache in the instance-specific configuration entry. The default value is 100000 identities (connection DNs). Increase the value of orclMaxConnInCache if your installation has more than 25000 users.

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.

8.2.191 orclmaxLatencyLog

`orclmaxLatencyLog` indicates the time in micro seconds after which any Oracle Internet Directory server operations that exceed this time are logged to the alert log. Default is 500 micro seconds, and the minimum value is 10 micro seconds.

Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.643

Other

Single-valued attribute.

8.2.192 orclMaxTcpIdleConnTime

`orclMaxTcpIdleConnTime` indicates the frequency in minutes at which the Oracle Internet Directory server calls `OCIPing`() to send keep alive messages to the Oracle Database. Setting this attribute to a value less than the timeout value of the firewall between Oracle Internet Directory server and its Database (typically 30 minutes) prevents the Database connection from being dropped.

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.

8.2.193 orclMaxFDLimitReached

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.

8.2.194 orclmaxfiltsize

`orclmaxfiltsize` indicates the maximum size of the filter to be allowed for ldap search operation.

Syntax

Matching Rule

Object ID

2.16.840.1.113894.1.1.610

8.2.195 OrclMaxLdapConns

`OrclMaxLdapConns` indicates the maximum LDAP connections per server.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.611

8.2.196 orclmaxlogfiles

`orclmaxlogfiles` indicates maximum number of log files to keep in rotation.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.615

8.2.197 orclmaxlogfilesize

`orclmaxlogfilesize` indicates the maximum size of the log file.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.614

8.2.198 orclmaxpsearchconns

`orclmaxpsearchconns` indicates the maximum number of connections allowed for LDAP persistent search operations. Because persistent search operations keep connections from an LDAP client to the Oracle Internet Server server alive, this attribute can prevent the LDAP connection limit from being reached. Default is 0 (disabled).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.383

Other

Single-valued attribute.

8.2.199 orclMaxProcessLimitReached

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.

8.2.200 orclMaxServerRespTime

`orclMaxServerRespTime` indicates the maximum time in seconds for Server process to respond back to Dispatcher process.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.620

8.2.201 orclMemAllocError

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.

8.2.202 orclMemberOf

This attribute contains the groups to which the entry belongs. This includes static groups and dynamic groups of objectclass orclDynamicGroup, using labeleduri attribute, which are cached. The membership includes both direct groups and nested groups. The attribute values are computed during search and are not stored. As of Oracle Internet Directory 11g Release 1 (11.1.1.7.0), this attribute can be used in search filters.

`orclMemberOf` is an operational attribute and is returned by a search only when explicitly requested in the required attributes list.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.424

Other

Directory operational attribute.

Not user modifiable.

Aliases: memberof, ismemberof.

8.2.203 orclNetDescName

`orclNetDescName` indicates 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.

8.2.204 orclNetDescString

`orclNetDescString` indicates the description string for an Oracle Net Service.

The 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.

8.2.205 orclNonSSLPort

`orclNonSSLPort` indicates 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.

8.2.206 orclNormDN

`orclNormDN` 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.

8.2.207 orclNWCongested

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.

8.2.208 orclNwrwTimeout

`orclNwrwTimeout` 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 controlled 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.

8.2.209 orclNwUnavailable

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.

8.2.210 orclObjectGUID

`orclObjectGUID` 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.

8.2.211 orclObjectSID

`orclObjectSID` 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.

8.2.212 orclODIPAgent

`orclODIPAgent` specifies 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

8.2.213 orclODIPAgentConfigInfo

`orclODIPAgentConfigInfo` is 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:

```
manageSyncProfiles update -h host -p port -D WLS_userid -profile profile_name
-params "odip.profile.configfile ORACLE_HOME/ldap/odi/conf/profile_name.cfg"
```

or

```
manageSyncProfiles update -h host -p port -D WLS_userid -profile profile_name
-file properties_file
```

where *properties_file* specifies odip.profile.configfile=*ORACLE_HOME*`/ldap/odi/conf/profile_name.cfg`.

Do this for both import and export agents.

See Oracle Directory Integration Platform Tools and the Managing Directory Synchronization Profiles in *Administering Oracle Directory Integration Platform* for more information

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

8.2.214 orclODIPAgentControl

`orclODIPAgentControl` indicates 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.

8.2.215 orclODIPAgentExeCommand

`orclODIPAgentExeCommand` is 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.

8.2.216 orclODIPAgentHostName

`orclODIPAgentHostName` is the host name of the Oracle Directory Integration and Provisioning 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.

8.2.217 orclODIPAgentName

`orclODIPAgentName` indicates 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.

8.2.218 orclODIPAgentPassword

`orclODIPAgentPassword` specifies the 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.

8.2.219 orclODIPApplicationName

`orclODIPApplicationName` is 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

8.2.220 orclODIPApplicationsLocation

`orclODIPApplicationsLocation` specifies 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.

8.2.221 orclODIPAttributeMappingRules

`orclODIPAttributeMappingRules` is the 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 Oracle Directory Integration Platform Tools and the Supported **Attribute Mapping Rules and Examples** in *Administering Oracle Directory Integration Platform* 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

8.2.222 orclODIPBootStrapStatus

`orclODIPBootStrapStatus` is 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.

8.2.223 orclODIPCommand

`orclODIPCommand` is 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

8.2.224 orclODIPConDirAccessAccount

`orclODIPConDirAccessAccount` is the 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.

8.2.225 orclODIPConDirAccessPassword

`orclODIPConDirAccessPassword` is the password to be used by the user specified in the `orclODIPConDirAccessAccount` attribute to connect to the connected directory.

See orclODIPConDirAccessAccount. 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

8.2.226 orclODIPConDirLastAppliedChgNum

For Oracle Directory Integration and Provisioning import operations, `orclODIPConDirLastAppliedChgNum` is 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 Oracle Directory Integration Platform Tools and the Bootstrapping a Directory in Oracle Directory Integration Platform in *Administering Oracle Directory Integration Platform* 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.

8.2.227 orclODIPConDirMatchingFilter

This attribute specifies the filter to apply to the third-party directory change log. It is used in the Oracle Directory Integration and Provisioning 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: Note 280474.1, "Setting Up Filtering in a DIP Synchronization Profile" available at My Oracle Support (formerly 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

8.2.228 orclODIPConDirURL

`orclODIPConDirURL` is the 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 Database 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.

8.2.229 orclODIPConfigDNs

`orclODIPConfigDNs` stores the DNs of integration profiles for a particular configuration set in Oracle Directory Integration and Provisioning.

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

8.2.230 orclODIPConfigRefreshFlag

`orclODIPConfigRefreshFlag` stores a flag which indicates whether any integration profiles have been added, deleted, or modified. It is 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.

8.2.231 orclODIPDbConnectInfo

`orclODIPDbConnectInfo` is 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

8.2.232 orclODIPEncryptedAttrKey

`orclODIPEncryptedAttrKey` 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.

8.2.233 orclODIPEventFilter

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

8.2.234 orclODIPEventSubscriptions

`orclODIPEventSubscriptions` 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

8.2.235 orclODIPFilterAttrCriteria

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.

8.2.236 orclODIPInstancesLocation

`orclODIPInstancesLocation` 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.

8.2.237 orclODIPInstanceStatus

`orclODIPInstanceStatus` 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.

8.2.238 orclODIPInterfaceType

`orclODIPInterfaceType` signifies 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.

8.2.239 orclODIPLastExecutionTime

`orclODIPLastExecutionTime` is the status attribute set to the last time the integration profile was executed by the Oracle Directory Integration and Provisioning 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.

8.2.240 orclODIPLastSuccessfulExecutionTime

`orclODIPLastSuccessfulExecutionTime` is the status attribute set to the last time the integration profile was executed successfully by the Oracle Directory Integration and Provisioning 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.

8.2.241 orclODIPMustAttrCriteria

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.

8.2.242 orclODIPObjectCriteria

`orclODIPObjectCriteria` is 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

8.2.243 orclODIPObjectDefnLocation

`orclODIPObjectDefnLocation` 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.

8.2.244 orclODIPObjectEvents

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

8.2.245 orclODIPObjectName

`orclODIPObjectName` is 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.

8.2.246 orclODIPObjectSyncBase

`orclODIPObjectSyncBase` is the search base in the directory for an object associated with an Oracle Directory Integration and Provisioning 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

8.2.247 orclODIPOIDMatchingFilter

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

8.2.248 orclODIPOperationMode

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

8.2.249 orclODIPOptAttrCriteria

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.

8.2.250 orclODIPPluginAddInfo

`orclODIPPluginAddInfo` is the additional information that may be needed by an Oracle Directory Integration and Provisioning 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.

8.2.251 orclODIPPluginConfigInfo

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.

8.2.252 orclODIPPluginEvents

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

8.2.253 orclODIPPluginExecData

`orclODIPPluginExecData` is the Oracle Directory Integration and Provisioning 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

8.2.254 orclODIPPluginExecName

`orclODIPPluginExecName` is the fully qualified name of the Oracle Directory Integration and Provisioning 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.

8.2.255 orclODIPProfileDataLocation

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.

8.2.256 orclODIPProfileDebugLevel

`orclODIPProfileDebugLevel` is the debugging level for an Oracle Directory Integration and Provisioning 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.

> **Note:**
>
> To log all information for a synchronization profile, including entries that are synchronized, set the `orclODIPProfileDebugLevel` to a value of `63` for 10*g* and to a value of `64` for 11*g*.
>
> The `orclodipprofiledebuglevel` attribute corresponds to the `odip.profile.debuglevel` configuration property. The `odip.profile.debuglevel` property refers to the following log levels, which you can set in the Oracle Enterprise Manager Fusion Middleware Control by editing the **Log Level** under the **Advanced** tab:
>
> - Off = `0`
> - Error = `8`
> - Info = `16`
> - Trace = `32`
> - All = `64` (recommended for most sync/profile mapping troubleshooting)

8.2.257 orclODIPProfileExecGroupID

`orclODIPProfileExecGroupID` 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.

8.2.258 orclODIPProfileInterfaceAdditionalInformation

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

8.2.259 orclODIPProfileInterfaceConnectInformation

`orclODIPProfileInterfaceConnectInformation` 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.

8.2.260 orclODIPProfileInterfaceName

`orclODIPProfileInterfaceName` 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.

8.2.261 orclODIPProfileInterfaceType

`orclODIPProfileInterfaceType` specifies the type of interface to which events is 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.

8.2.262 orclODIPProfileInterfaceVersion

`orclODIPProfileInterfaceVersion` specifies the provisioning profile version to which events is 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.

8.2.263 orclODIPProfileLastAppliedAppEventID

`orclODIPProfileLastAppliedAppEventID` 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.

8.2.264 orclODIPProfileLastProcessingTime

`orclODIPProfileLastProcessingTime` is the last time the Oracle Directory Integration and Provisioning 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.

8.2.265 orclODIPProfileLastSuccessfulProcessingTime

`orclODIPProfileLastSuccessfulProcessingTime` denotes the last time the Oracle Directory Integration and Provisioning 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.

8.2.266 orclODIPProfileMaxErrors

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.

8.2.267 orclODIPProfileMaxEventsPerInvocation

`orclODIPProfileMaxEventsPerInvocation` 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.

8.2.268 orclODIPProfileMaxEventsPerSchedule

`orclODIPProfileMaxEventsPerSchedule` 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.

8.2.269 orclODIPProfileMaxRetries

`orclODIPProfileMaxRetries` denotes the maximum number of times an Oracle Directory Integration and Provisioning 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.

8.2.270 orclODIPProfileName

`orclODIPProfileName` denotes the name of the Oracle Directory Integration and Provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.201

Other

Single-valued attribute.

8.2.271 orclODIPProfileProcessingErrors

`orclODIPProfileProcessingErrors` 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

8.2.272 orclODIPProfileProcessingStatus

`orclODIPProfileProcessingStatus` 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.

8.2.273 orclODIPProfileProvSubscriptionMode

`orclODIPProfileProvSubscriptionMode` is 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

8.2.274 orclODIPProfileSchedule

`orclODIPProfileSchedule` denotes the number of seconds between executions of an Oracle Directory Integration and Provisioning 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.

8.2.275 orclODIPProfileStatusUpdate

`orclODIPProfileStatusUpdate` 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.

8.2.276 orclODIPProvEventCriteria

`orclODIPProvEventCriteria` is 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

8.2.277 orclODIPProvEventLDAPChangeType

`orclODIPProvEventLDAPChangeType` is 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

8.2.278 orclODIPProvEventObjectType

`orclODIPProvEventObjectType` isuUsed 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.

8.2.279 orclODIPProvEventRule

`orclODIPProvEventRule` 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.

8.2.280 orclODIPProvEventRuleDTD

`orclODIPProvEventRuleDTD` 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.

8.2.281 orclODIPProvInterfaceFilter

`orclODIPProvInterfaceFilter` is 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

8.2.282 orclODIPProvInterfaceProcessor

`orclODIPProvInterfaceProcessor` is 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.

8.2.283 orclODIPProvisioningAppGUID

`orclODIPProvisioningAppGUID` is 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.

8.2.284 orclODIPProvisioningAppName

`orclODIPProvisioningAppName` is 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.

8.2.285 orclODIPProvisioningEventMappingRules

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

8.2.286 orclODIPProvisioningEventPermittedOperations

`orclODIPProvisioningEventPermittedOperations` defines the types of events that the application is allowed to send to the Oracle Directory Integration and Provisioning 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

8.2.287 orclODIPProvisioningEventSubscription

`orclODIPProvisioningEventSubscription` defines the types of events that the Oracle Directory Integration and Provisioning 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

8.2.288 orclODIPProvisioningOrgGUID

`orclODIPProvisioningOrgGUID` is 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.

8.2.289 orclODIPProvisioningOrgName

`orclODIPProvisioningOrgName` is 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.

8.2.290 orclODIPProvProfileLocation

`orclODIPProvProfileLocation` 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.

8.2.291 orclODIPRootLocation

`orclODIPRootLocation` refers to the root location in the directory tree where the Oracle Directory Integration and Provisioning 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.

8.2.292 orclODIPSchedulingInterval

`orclODIPSchedulingInterval` denotes the time interval in seconds after which a connected directory is synchronized with Oracle Internet Directory. The default is `60`.

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.

8.2.293 orclODIPSchemaVersion

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.

8.2.294 orclODIPSearchCountLimit

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.

8.2.295 orclODIPSearchTimeLimit

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.

8.2.296 orclODIPServerCommitSize

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.

8.2.297 orclODIPServerConfigLocation

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.

8.2.298 orclODIPServerDebugLevel

`orclODIPServerDebugLevel` is the number that corresponds to the debugging level for the Oracle Directory Integration and Provisioning 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.

8.2.299 orclODIPServerRefreshIntvl

`orclODIPServerRefreshIntvl` denotes 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.

8.2.300 orclODIPServerSSLMode

`orclODIPServerSSLMode` is 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.

8.2.301 orclODIPServerWalletLoc

`orclODIPServerWalletLoc` denotes the complete path and file name of the Oracle Directory Integration and Provisioning 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.

8.2.302 orclODIPSynchronizationErrors

`orclODIPSynchronizationErrors` contains messages explaining the errors if the last execution of the synchronization profile failed. This attribute is updated by Oracle Directory Integration and Provisioning 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

8.2.303 orclODIPSynchronizationMode

`orclODIPSynchronizationMode` denotes the 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.

8.2.304 orclODIPSynchronizationStatus

`orclODIPSynchronizationStatus` indicates the 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.

8.2.305 orclODIPSyncProfileLocation

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.

8.2.306 orclODIPSyncRetryCount

`orclODIPSyncRetryCount` indicates the maximum number of times Oracle Directory Integration and Provisioning 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.

8.2.307 orclOidComponentName

`orclOidComponentName` indicates the name of OID component where replication server is started.

Syntax

Directory String

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.832

8.2.308 orclOidInstanceName

`orclOidInstanceName` indicates the name of the instance where replication server is started.

Syntax

Directory String

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.830

8.2.309 orclOpAbandoned

`orclOpAbandoned` 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.

8.2.310 orclOpCompleted

`orclOpCompleted` 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.

8.2.311 orclOpenConn

`orclOpenConn` 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.

8.2.312 orclOpFailed

`orclOpFailed` 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.

8.2.313 orclOpInitiated

`orclOpInitiated` 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.

8.2.314 orclOpLatency

`orclOpLatency` 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.

8.2.315 orclOpPending

`orclOpPending` 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.

8.2.316 orclOpResult

`orclOpResult` 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

8.2.317 orclOpSucceeded

`orclOpSucceeded` 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.

8.2.318 orclOpTimedOut

`orclOpTimedOut` 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.

8.2.319 orcloptracklevel

`orcloptracklevel` is the security event tracking level.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.180

8.2.320 orcloptrackmaxtotalsize

`orcloptrackmaxtotalsize` indicates the maximum number of bytes of RAM that security events tracking can use for each type of operation.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.178

8.2.321 orcloptracknumelemcontainers

`orcloptracknumelemcontainers` indicates the number of in-memory cache containers to be allocated for security event tracking.

The `1stlevel` subtype is for setting the number of in-memory cache containers for storing information about users performing operations. The `2ndlevel` subtype, which is applicable only to compare operation, sets the number of in-memory cache containers for information about the users whose userpassword is compared and tracked when detailed compare operation statistics is programmed.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.181

8.2.322 orclORA28error

`orclORA28error` 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.

8.2.323 orclORA3113error

`orclORA3113error` 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.

8.2.324 orclORA3114error

`orclORA3114error` specifies the number of ORA-3114 errors encountered by Oracle Internet Directory servers.

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.

8.2.325 orclOracleHome

`orclOracleHome` indicates 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.

8.2.326 orclOwnerGUID

`orclOwnerGUID` is 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

8.2.327 orclPassword

`orclPassword` 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

8.2.328 orclPasswordAttribute

`orclPasswordAttribute` 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.

8.2.329 orclPasswordHint

`orclPasswordHint` 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.

8.2.330 orclPasswordHintAnswer

`orclPasswordHintAnswer` is 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.

8.2.331 orclPasswordVerifier

`orclPasswordVerifier` is the 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

8.2.332 orclPilotMode

`orclPilotMode` allows to choose whether to BEGIN or END pilot mode for a replica.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch, equality integermatch

Object ID

2.16.840.1.113894.1.1.824

Other

Single-valued attribute.

8.2.333 orclPKCS12Hint

`orclPKCS12Hint` contains the 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

8.2.334 orclPKIMatchingRule

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.

8.2.335 orclPKINextUpdate

`orclPKINextUpdate` indicates 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

8.2.336 orclPKIValMecAttr

`orclPKIValMecAttr` contains the certificate validation mechanism supported. Currently, only validation with crls is supported, hence the value of this attribute is 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

8.2.337 orclPluginAttributeList

`orclPluginAttributeList` contains 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.

8.2.338 orclPluginCheckEntryExist

`orclPluginCheckEntryExist`, if enabled, indicates that the Plug-in is invoked when the base entry does not exist. This only applies to search operation with scope base.

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.

8.2.339 orclPluginEnable

`orclPluginEnable` indicates whether 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.

8.2.340 orclPluginEntryProperties

`orclPluginEntryProperties` is 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.

8.2.341 orclPluginIsReplace

`orclPluginIsReplace` is used 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.

8.2.342 orclPluginBinaryFlexfield

`orclPluginBinaryFlexfield` contains 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.

8.2.343 orclPluginFlexfield

`orclPluginFlexfield` contains 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.

8.2.344 orclPluginSecuredFlexfield

`orclPluginSecuredFlexfield` contains Custom text information (Java only).

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.

8.2.345 orclPluginKind

`orclPluginKind` indicates 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.

8.2.346 orclPluginLDAPOperation

`orclPluginLDAPOperation` indicates the LDAP operation that this plug-in supplements.

The 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.

8.2.347 orclPluginName

`orclPluginName` indicates 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.

8.2.348 orclPluginPort

`orclPluginPort` is 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.

8.2.349 orclPluginRequestGroup

It is 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.

8.2.350 orclPluginRequestNegGroup

`orclPluginRequestNegGroup` is 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.

8.2.351 orclPluginResultCode

`orclPluginResultCode` is an integer value to specify the LDAP result code.

If this value is specified, then the plug-in is 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.

8.2.352 orclPluginSASLCallBack

`orclPluginSASLCallBack` controls the type of bind used when the LDAP_PLUGIN package connects back to the same Oracle Internet Directory server.

Allowed values are:

- 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.

8.2.353 orclPluginSearchNotFound

This only applies if the value for the `orclPluginTiming` attribute is `POST`. It brings in the external entries if the entry is not found in Oracle Internet Directory. It 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.

8.2.354 orclPluginShareLibLocation

`orclPluginShareLibLocation` contains the 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.

8.2.355 orclPluginSubscriberDNList

`orclPluginSubscriberDNList` is 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.

8.2.356 orclPluginTiming

`orclPluginTiming` 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.

8.2.357 orclPluginType

The valid value of this attribute 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.

8.2.358 orclPluginVersion

`orclPluginVersion` indicates 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.

8.2.359 OrclPluginWorkers

`OrclPluginWorkers` specifies the number of plug-in threads per server process.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.612

8.2.360 orclPrName

`orclPrName` 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.

8.2.361 orclProductVersion

`orclProductVersion` 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

8.2.362 orclPrPassword

`orclPrPassword` 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.

8.2.363 orclPurgeBase

`orclPurgeBase` it is 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.

8.2.364 orclPurgeDebug

`orclPurgeDebug` is the 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.

8.2.365 orclPurgeEnable

`orclPurgeEnable` is a 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.

8.2.366 orclPurgeFileLoc

`orclPurgeFileLoc` is the 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.

8.2.367 orclPurgeFileName

`orclPurgeFileName` is 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.

8.2.368 orclPurgeFilter

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.

8.2.369 orclPurgeInterval

`orclPurgeInterval` is the 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.

8.2.370 orclPurgeNow

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.

8.2.371 orclPurgePackage

`orclPurgePackage` 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.

8.2.372 orclPurgeSchedule

`orclPurgeSchedule` specifies the schedule for purging directory objects.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integermatch

Object ID

2.16.840.1.113894.1.1.24

Other

Single-valued attribute.

DSA operational attribute.

8.2.373 orclPurgeStart

`orclPurgeStart` is 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.

8.2.374 orclPurgeTargetAge

This attribute enables time-based purging of change log records. Set this to the number of hours after which old change logs are 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.

8.2.375 orclPurgeTranSize

`orclPurgeTranSize` is 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.

8.2.376 orclPwdAccountUnlock

`orclPwdAccountUnlock` allows a user with the appropriate administration rights and privileges 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.

8.2.377 orclPwdAllowHashCompare

`orclPwdAllowHashCompare` determines whether to allow password validations by comparing the hash values of encrypted passwords. The 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.

8.2.378 orclPwdAlphaNumeric

`orclPwdAlphaNumeric` indicates 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.

8.2.379 orclPwdEncryptionEnable

`orclPwdEncryptionEnable` takes values 1 and 0. If the value is 1, then the user password is stored in reversible encrypted form. If the value is 0, 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.

8.2.380 orclPwdIllegalValues

`orclPwdIllegalValues` 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

8.2.381 orclPwdIPAccountLockedTime

`orclPwdIPAccountLockedTime` indicates 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.

8.2.382 orclPwdIPFailureTime

`orclPwdIPFailureTime` indicates 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.

8.2.383 orclPwdIPLockout

`orclPwdIPLockout` decides whether to enable account lockouts for a specific IP address. The value can be 1 (for true) or 0 (for 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.

8.2.384 orclPwdIPLockoutDuration

`orclPwdIPLockoutDuration` indicates 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.

8.2.385 orclPwdIPMaxFailure

`orclPwdIPMaxFailure` indicates 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.

8.2.386 orclpwdmaxinactivitytime

`orclpwdmaxinactivitytime` indicates the maximum period of time in seconds after which an inactive account is automatically locked.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.379

Other

Single-valued attribute.

8.2.387 orclPwdMaxRptchars

`orclPwdMaxRptchars` indicates the maximum number of times a single character type can be repeated in a password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.415

Other

Single-valued attribute.

8.2.388 orclPwdMinAlphachars

`orclPwdMinAlphachars` indicates the minimum number of alphabetic characters required in a password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.411

Other

Single-valued attribute.

8.2.389 orclPwdMinSpecialchars

`orclPwdMinSpecialchars` indicates minimum number of non-alphanumeric characters required in a password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.412

Other

Single-valued attribute.

8.2.390 orclPwdMinUppercase

`orclPwdMinUppercase` indicates the minimum number of uppercase characters required in a password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.413

Other

Single-valued attribute.

8.2.391 orclpwdminlowercase

`orclpwdminlowercase` indicates the minimum number of lowercase characters required in a password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.414

Other

Single-valued attribute.

8.2.392 orclPwdPolicyEnable

`orclPwdPolicyEnable` determines whether to enable or disable the password policy. The value can be are 1 (for enable) or 0 (for disable).

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.

8.2.393 orclPwdTrackLogin

`orclPwdTrackLogin` enables or disables tracking of user's last login time; 1 for enabling and 0 for disabling (default).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.377

Other

Single-valued attribute

8.2.394 orclPwdVerifierParams

`orclPwdVerifierParams` contains the values of different password verifier types.

For example:

```
orclpwdverifierparams;authpassword: crypto:SASL/MDS $ realm:dc=com
orclpwdverifierparams;orclpasswordverifier: crypto:ORCLLM
orclpwdverifierparams;authpassword: crypto:ORCLWEBDAV $ realm:dc=com
```

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

8.2.395 orclQosConfig

Mechanism to dynamically configure throttling polices.

Syntax

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.920

Other

Multi-valued attribute

8.2.396 orclQueueDepth

`orclQueueDepth` 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.

8.2.397 orclQueueLatency

`orclQueueLatency` 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.

8.2.398 orclReadWaitThreads

`orclReadWaitThreads` 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.

8.2.399 orclReqAttrCase

`orclReqAttrCase` disables or enables preserving the letter case of required attributes in search result. Allowed values are 0 (disable) or 1 (enable). The default value is 0.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.423

Other

Single-valued attribute

8.2.400 orclrefreshdgrmems

`orclrefreshdgrmems` refreshes Dynamic Group Memberships.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch (Integer)

Object ID

2.16.840.1.113894.1.1.416

Other

Single-valued attribute

8.2.401 orclReplAgreements

`orclReplAgreements` indicates 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

8.2.402 orclReplAttrConfl

`orclReplAttrConfl` specifies whether timestamp or attribute version should be honored first during attribute level conflict resolution. 0 (default): timestamp first, 1: version number first

Syntax

1.3.6.1.4.1.1466.115.121.1.27(Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.899

Other

Single valued attribute

8.2.403 orclreplautotune

`orclreplautotune` is used to dynamically vary the number of threads assigned to transport and apply tasks based on load.

The value 0 indicates Off and 1 indicates On. If you set the server to auto tune, you must specify the number of maximum number of threads to be shared between these tasks. Restart server after changing.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.827

8.2.404 orclReplicaDN

`orclReplicaDN` is the DN of the consumer replica in the replication agreement. This applies for LDAP-based replication only.

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

8.2.405 orclReplicaID

`orclReplicaID` is the 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.

8.2.406 orclReplicaSecondaryURI

`orclReplicaSecondaryURI` contains the set of `ldapURI` formatted addresses that can be used if the `orclReplicaURI` values cannot be used.

See orclReplicaURI.

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

8.2.407 orclReplicaState

`orclReplicaState` 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)
- 6 (database copy based add node)
- 7 (sync schema)
- 8 (boot strap without schema sync)

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.

8.2.408 orclreplicationid

`orclreplicationid` is a unique identifier of a one-way, two-way, or peer-to-peer replication group.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.509

8.2.409 orclReplicationProtocol

`orclReplicationProtocol` defines the replication protocol for change propagation to replica.

It takes the following value:

- 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.

8.2.410 orclReplicationState

`orclReplicationState` indicates the activation state of the replication server. 0 indicates Inactive and 1 indicates Active.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.831

8.2.411 orclReplicaType

`orclReplicaType` 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.

8.2.412 orclReplicaURI

`orclReplicaURI` 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.

8.2.413 orclReplicaVersion

`orclReplicaVersion` is the 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.

8.2.414 orclreplmaxworkers

`orclreplmaxworkers` indicates maximum number of worker threads. Required if `orclreplautotune` is set.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.826

8.2.415 orclreplusesasl;digest-md5

`orclreplusesasl;digest-md5` indicates usage of SASL for replication binds.

Values are `auth`, `auth-int`, and `auth-conf`.

Syntax

Directory String

Matching Rule

caseIgnoreMatch; caseIgnoreSubstringMatch

Object ID

2.16.840.1.113894.1.1.829

8.2.416 orclResourceIdentifier

`orclResourceIdentifier` 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

8.2.417 orclResourceName

`orclResourceName` 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

8.2.418 orclResourceTypeName

`orclResourceTypeName` 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

8.2.419 orclResourceViewers

`orclResourceViewers` 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

8.2.420 orclRevPwd

`orclRevPwd` contains the 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 cannot be queried.

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.

8.2.421 orclrienabled

`orclrienabled` enables referential integrity. 0: disabled, 1: enabled.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.1300

Other

Single-valued attribute

8.2.422 orclrscacheattr

`orclrscacheattr` is the multi-valued attribute that specifies the Result Set Cache attributes.

Default values are:

- dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
- orclrscacheattr: uid
- orclrscacheattr: mail
- orclrscacheattr: cn
- orclrscacheattr: orclguid

> **Note:**
>
> Typically these attributes are not modified for the life of the entry. If an attribute has referential integrity enabled, that attribute should not be used.

Syntax

1.3.6.1.4.1.1466.115.121.1.44

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.624

Other

Multi-valued attribute.

8.2.423 orclTraceConnDN

If `orclDebugFlag` is set to a value other than zero (0) and `orclTraceConnDN` specifies one or more connection DNs, Oracle Internet Directory server logs messages only for connections with specified DNs. Other messages are ignored.

Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.1051

Other

Multi-valued attribute.

8.2.424 orclTraceConnIP

If `orclDebugFlag` is set to a value other than zero (0) and `orclTraceConnIP` specifies one or more connection IP addresses, Oracle Internet Directory server logs messages only for operations performed by the specified connection IP addresses. Other messages are ignored.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.1052

Other

Multi-valued attribute.

8.2.425 orclSAMAccountName

`orclSAMAccountName` 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.

8.2.426 orclSASLAuthenticationMode

`orclSASLAuthenticationMode` 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.

8.2.427 orclSASLCipherChoice

`orclSASLCipherChoice` 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

8.2.428 orclSASLMechanism

`orclSASLMechanism` 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

8.2.429 orclsDumpFlag

`orclsDumpFlag` 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.

8.2.430 orclSearchBaseDN

`orclSearchBaseDN` 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.

8.2.431 orclSearchFilter

`orclSearchFilter` 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.

8.2.432 orclSearchScope

`orclSearchScope` 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.

8.2.433 orclSecondaryUID

`orclSecondaryUID` 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

8.2.434 orclSequence

`orclSequence` specifies the sequence number for audit log entries.

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

8.2.435 orclServerAvgMemGrowth

`orclServerAvgMemGrowth` 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.

8.2.436 orclServerMode

`orclServerMode` 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.

8.2.437 orclServerProcs

`orclServerProcs` indicates the 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.

8.2.438 orclServiceInstanceLocation

`orclServiceInstanceLocation` specifies 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.

8.2.439 orclServiceMember

`orclServiceMember` 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

8.2.440 orclServiceSubscriptionLocation

`orclServiceSubscriptionLocation` 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

8.2.441 orclServiceSubType

`orclServiceSubType` 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

8.2.442 orclServiceType

`orclServiceType` 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

8.2.443 orclSID

`orclSID` 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

8.2.444 orclsimplemodchglogattributes

`orclsimplemodchglogattributes` contains the list of multivalued attributes that, when changed, cause a simplified change log to be generated.

Syntax

DN

Matching Rule

DistinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.823

8.2.445 orclSizeLimit

`orclSizeLimit` indicates the 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

8.2.446 orclSkewedAttribute

`orclSkewedAttribute` 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

8.2.447 orclSkipRefInSQL

`orclSkipRefInSQL` 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

8.2.448 orclSkipSpecialInFilter

Evaluates whether Oracle Internet Directory should skip the processing of special characters specified in filter values during a search operation. Its default value is 0.

0: Process the special characters specified in the filter value.

1: Do not process the special characters specified in the filter value.

Syntax

1.3.6.1.4.1.1466.115.121.1.44

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.629

Other

Single-valued attribute

8.2.449 orclSMSpec

`orclSMSpec` 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

8.2.450 orclSQLexeFetchLatency

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

8.2.451 orclSQLGenReusedParsed

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

8.2.452 orclSSLAuthentication

`orclSSLAuthentication` indicates the 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 is 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

8.2.453 orclSSLCipherSuite

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:

Table 8-3 SSL Cipher Suites Supported in Oracle Internet Directory

Cipher Suite	Authentication	Encryption	Data Integrity
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES	SHA
SSL_RSA_WITH_RC4_128_SHA	RSA	RC4	SHA
SSL_RSA_WITH_RC4_128_MD5	RSA	RC4	MD5
SSL_RSA_WITH_DES_CBC_SHA	RSA	DES	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4_40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40	SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	None	3DES	SHA
SSL_DH_anon_WITH_RC4_128_MD5	None	RC4	MD5
SSL_DH_anon_WITH_DES_CBC_SHA	None	DES	SHA
SSL_RSA_WITH_AES_128_CBC_SHA	RSA	AES	SHA
SSL_RSA_WITH_AES_256_CBC_SHA	RSA	AES	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

8.2.454 orclSSLEnable

`orclSSLEnable` is the 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 `2`.

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

8.2.455 orclsslinteropmode

`orclsslinteropmode` allows you to enable SSL interoperability with Oracle legacy applications using no-auth mode.

Starting with Oracle Internet Directory 11g Release 1 (11.1.1.7.0), the default value is disabled (orclsslinteropmode = 0), in order to be fully compliant with the JDK SSL.

In no-auth mode, Oracle legacy components developed before 11g Release 1 (11.1.1.0.0) such as legacy LDAP C clients can connect with Oracle Internet Directory only by using an instance that has interoperability mode enabled (orclsslinteropmode = 1).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.422

Other

Single-valued attribute

8.2.456 orclSSLPort

`orclSSLPort` is the default SSL port for the directory server. The Default value is 3133.

When you run the directory in the secure mode, it listens at default port 3133 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

8.2.457 orclSSLVersion

`orclSSLVersion` is the 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

8.2.458 orclSSLWalletURL

`orclSSLWalletURL` 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

8.2.459 orclStatsDN

`orclStatsDN` 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

8.2.460 orclStatsFlag

`orclStatsFlag` allows you to 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.

8.2.461 orclStatsLevel

`orclStatsLevel` indicates the level of statistics collection for users. The valid value is 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.

8.2.462 orclStatsOp

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.

8.2.463 orclStatsPeriodicity

`orclStatsPeriodicity` indicates the 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.

8.2.464 orclStatus

Depending on the context of the object that it is applied to, like a service, `orclStatus` 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

8.2.465 orclSUAccountLocked

`orclSUAccountLocked` determines whether a superuser 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.

8.2.466 orclSubscriberDisable

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.

8.2.467 orclSubscriberFullName

`orclSubscriberFullName` 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.

8.2.468 orclSubscriberNickNameAttribute

`orclSubscriberNickNameAttribute` 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.

8.2.469 orclSubscriberSearchBase

`orclSubscriberSearchBase` 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

8.2.470 orclSubscriberType

`orclSubscriberType` 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.

8.2.471 orclSuffix

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.

8.2.472 orclSuiteType

`orclSuiteType` identifies the type of suite, for example, 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.

8.2.473 orclSULoginFailureCount

`orclSULoginFailureCount` indicates the number of failed login attempts for the directory superuser.

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.

8.2.474 orclSUName

`orclSUName` is the distinguished name of the directory superuser 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.

8.2.475 orclSUPassword

`orclSUPassword` is the Oracle Internet Directory superuser 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.

8.2.476 orclSystemName

`orclSystemName` 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.

8.2.477 orclTcpConnToClose

`orclTcpConnToClose` 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.

8.2.478 orclTcpConnToShutDown

`orclTcpConnToShutDown` 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.

8.2.479 orclThreadSpawnFailed

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.

8.2.480 orclThreadsPerSupplier

`orclThreadsPerSupplier` 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

integermatch

Object ID

2.16.840.1.113894.1.1.31

Other

DSA operational attribute.

8.2.481 orclTimeLimit

`orclTimeLimit` indicates the 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.

8.2.482 orclTimeZone

`orclTimeZone` 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

8.2.483 orclTLimitMode

`orclTLimitMode` 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.

8.2.484 orclTotFreePhyMem

`orclTotFreePhyMem` 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.

8.2.485 orclTraceDimesionLevel

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.

8.2.486 orclTraceFileLocation

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.

8.2.487 orclTraceFileSize

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.

8.2.488 orclTraceLevel

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.

8.2.489 orclTraceMode

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.

8.2.490 orclTrustedApplicationGroup

`orclTrustedApplicationGroup` 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

8.2.491 orclTraceMode

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.

8.2.492 orclTxnMaxOperations

`orclTxnMaxOperations` indicates the maximum number of operations allowed in a transaction.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.381

Other

Single-valued attribute

8.2.493 orclTxnTimeLimit

`orclTxnTimeLimit` indicates maximum allowed time in a transaction (sec).

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.380

Other

Single-valued attribute

8.2.494 orclUIAccessibilityMode

`orclUIAccessibilityMode` is 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.

8.2.495 orclUniqueAttrName

`orclUniqueAttrName` is 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.

8.2.496 orclUniqueEnable

`orclUniqueEnable` 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.

8.2.497 orclUniqueObjectClass

`orclUniqueObjectClass` 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.

8.2.498 orclUniqueScope

`orclUniqueScope` indicates 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.

8.2.499 orclUniqueSubtree

When multiple attribute uniqueness constraints have the same values in orclUniqueAttrName, orclUniqueScope and orclUserObjectClasses, but different values in orcluniquesubtree, the union of subtree scopes specified by those attribute uniqueness constraints is checked.

When multiple attribute uniqueness constraints have the same values in orclUniqueAttrName, orclUniqueScope and orclUserObjectClasses, 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.

8.2.500 orclUnsyncRevPwd

`orclUnsyncRevPwd` 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.

8.2.501 orclUpdateSchedule

`orclUpdateSchedule` is the replication update interval for new changes and those being retried. The value is in seconds.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integermatch

Object ID

2.16.840.1.113894.1.1.30

Other

Directory operational attribute.

Not user modifiable.

Single-valued attribute.

8.2.502 orclUpgradeInProgress

`orclUpgradeInProgress` determines 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.

8.2.503 orclUserDN

`orclUserDN` is 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

8.2.504 orclUserIDAttribute

`orclUserIDAttribute` 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.

8.2.505 orclUserModifiable

`orclUserModifiable` 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

8.2.506 orclUserObjectClasses

`orclUserObjectClasses` is 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

8.2.507 orclUserPrincipalName

`orclUserPrincipalName` indicates 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.

8.2.508 orclVersion

`orclVersion` is 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.

8.2.509 orclWirelessAccountNumber

`orclWirelessAccountNumber` 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.

8.2.510 orclWorkflowNotificationPref

`orclWorkflowNotificationPref` 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

8.2.511 orclWriteWaitThreads

`orclWriteWaitThreads` 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.

8.2.512 owner

`owner` 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

8.2.513 pilotStartTime

`pilotStartTime` indicates 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.

8.2.514 preferredServerList

`preferredServerList` contains 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.

8.2.515 profileTTL

`profileTTL` is 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.

8.2.516 protocolInformation

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

8.2.517 pwdAccountLockedTime

`pwdAccountLockedTime` indicates 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.

8.2.518 pwdAllowUserChange

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.

8.2.519 pwdChangedTime

`pwdChangedTime` indicates 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.

8.2.520 pwdCheckSyntax

`pwdCheckSyntax` takes value 1 and 0. 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.

8.2.521 pwdExpirationWarned

`pwdExpirationWarned` indicates 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.

8.2.522 pwdExpireWarning

`pwdExpireWarning` indicates 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.

8.2.523 pwdFailureCountInterval

`pwdFailureCountInterval` indicates 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.

8.2.524 pwdFailureTime

`pwdFailureTime` indicates 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.

8.2.525 pwdGraceLoginLimit

`pwdGraceLoginLimit` indicates the 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.

8.2.526 pwdGraceLoginTimeLimit

`pwdGraceLoginTimeLimit` is the number of seconds after account lockout to allow grace logins.

Syntax

1.3.6.1.4.1.1466.115.121.1.27(Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.418

Other

Single-valued attribute.

8.2.527 pwdGraceUseTime

`pwdGraceUseTime` indicates 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.

8.2.528 pwdHistory

`pwdHistory` contains 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.

8.2.529 pwdInHistory

`pwdInHistory` indicates the number of previous passwords to be stored in the password history.

See 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.

8.2.530 pwdLockout

`pwdLockout` is the specification to determine 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.

8.2.531 pwdLockoutDuration

`pwdLockoutDuration` indicates the number of seconds a user is locked out of the directory on certain conditions as stated in the section below.

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.

8.2.532 pwdMaxAge

`pwdMaxAge` indicates 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.

8.2.533 pwdMaxFailure

`pwdMaxFailure` indicates 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.

8.2.534 pwdMinAge

`pwdMinAge` 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.

8.2.535 pwdMinLength

`pwdMinLength` is 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.

8.2.536 pwdMustChange

`pwdMustChange` is an 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 1 (true) or 0 (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.

8.2.537 pwdpolicysubentry

`pwdpolicysubentry` is the DN of the password policy applicable at the subtree rooted at this DN.

Syntax

1.3.6.1.4.1.1466.115.121.1.34

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.417

8.2.538 pwdReset

`pwdReset` is an 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.

8.2.539 pwdSafeModify

`pwdSafeModify` is an 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.

8.2.540 ref

`ref` is 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.

8.2.541 seeAlso

`seeAlso` 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

8.2.542 serverName

`serverName` is the name of the server involved in an Oracle Directory Integration and Provisioning change subscription.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

caseignoresubstringsmatch

Object ID

2.16.840.1.113894.1.1.34

8.2.543 serviceAuthenticationMethod

`serviceAuthenticationMethod` is 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

8.2.544 serviceCredentialLevel

`serviceCredentialLevel` is 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

8.2.545 serviceSearchDescriptor

`serviceSearchDescriptor` defines how and where an LDAP naming service client should search for information for a particular service. It 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

8.2.546 sn

`sn` is 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

8.2.547 supportedcontrol

`supportedcontrol` is a list of controls supported by directory server.

Syntax

OID

Object ID

1.3.6.1.4.1.1466.101.120.13

8.2.548 supportedextension

`supportedextension` is a list of extended operation supported.

Syntax

OID

Object ID

1.3.6.1.4.1.1466.101.120.7

8.2.549 supportedldapversion

`supportedldapversion` is a list of LDAP versions supported.

Syntax

Integer

Object ID

1.3.6.1.4.1.1466.101.120.15

8.2.550 uniqueMember

`uniqueMember` is 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

8.2.551 supportedsaslmechanisms

`supportedsaslmechanisms` is a list of SASL mechanism supported.

Syntax

Directory String

Matching Rule

Object ID

1.3.6.1.4.1.1466.101.120.14

8.2.552 userCertificate;binary

It is 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

8.2.553 userPassword

`userPassword` is 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.

8.2.554 userPKCS12

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

8.2.555 x509issuer

`x509issuer` is 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:

- LDIF File Format

A
LDIF File Format

Understand about creating LDAP Data Interchange Files (LDIF) that can be used by the Oracle Internet Directory command-line tools
This section contains the following topics:

- General LDIF Formatting Rules
- LDIF Format for Entries
- Adding Schema Elements

A.1 General LDIF Formatting Rules

Understand about the general LDIF formatting rules. These 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.

- Line Types and White Space
- Sequencing of Entries
- Binary Files
- Non-Printing Characters in Attribute Values

A.1.1 Line Types and White Space

Learn about the guidelines for using line types and white spaces in an LDIF file.

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.

A.1.2 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.

A.1.3 Binary Files

Reference binary files, such as photographs, with the absolute address of the file proceeded by a / (forward slash).

Reference binary files, such as photographs, with the absolute address of the file proceeded by a / (forward slash).

A.1.4 Non-Printing Characters in Attribute Values

Non-printing characters and tabs are represented in attribute values as base-64 encoding.

Non-printing characters and tabs are represented in attribute values as base-64 encoding.

A.2 LDIF Format for Entries

Understand about the LDIF format used for creating, modifying, and deleting directory entries and for modifying the RDN and DN of an entry.

This section contains the following topics:

A.2.1 Standard Format for Directory Entries

Understand about the standard format for directory 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
...
```

This section contains the following topics:

- dn Directive for an Entry
- changetype Directive for an Entry
- *attribute_type* Directive for an Entry
- objectClass Directive for an Entry

A.2.1.1 dn Directive for an Entry

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
```

A.2.1.2 changetype Directive for an Entry

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 for syntax and examples.
- `delete` - See LDIF Format for Deleting Entries for syntax and examples.
- `modify` - LDIF Format for Modifying Entries for syntax and examples.
- `modrdn` - See LDIF Format for Modifying the RDN of an Entry for syntax and examples.
- `moddn` - See LDIF Format for Modifying the DN of an Entry 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.

A.2.1.3 *attribute_type* Directive for an Entry

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
```

A.2.1.4 objectClass Directive for an Entry

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:**
>
> If an object class has required attributes, you must supply a value for those attributes using *attribute_type* directives.

A.2.2 LDIF Format for Adding Entries

Understand the LDIF format for adding entries from the following example.

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. 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: Suzie
sn: Smith
mail: ssmith@us.Acme.com
telephoneNumber: 69332
photo: \$DOMAIN_HOME/empdir/photog/ssmith.jpg
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

A.2.3 LDIF Format for Deleting Entries

When deleting an entry by using `ldapmodify` or `ldapmodifymt`, 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.

Perform the following:

```
dn: cn=Suzie Smith,ou=Server Technology,o=Acme, c=US
changetype: delete
```

The `ldapdelete` command only needs a list of DNs. It does not require a changetype operator.

A.2.4 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

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 are 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
```

A.2.5 LDIF Format for Modifying the RDN of an Entry

You can modify the relative distinguished name (RDN) for an entry by supplying the DN of the entry followed by the `changetype: modrdn` directive.

Now 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: dn=Sally Smith-Jones
# deletes old RDN entry
deleteoldrdn: 1
```

A.2.6 LDIF Format for Modifying the DN of an Entry

You can modify the DN for an entry (move the entry to a new node in the DIT) by supplying the DN of the entry followed by the `changetype: moddn` directive.

You must also 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
# keeps old RDN entry
deleteoldrdn: 0
newsuperior: ou=expeople,dc=example,dc=com
```

A.3 Adding Schema Elements

Understand about the procedure to add schema elements. Attribute types and object classes must be added to the Oracle Internet Directory schema before they can be used in entries.

This section contains the following topics:

- Adding an Attribute to the Schema
- Adding an Object Class to the Schema
- Adding A New Object Class to an Entry

A.3.1 Adding an Attribute to the Schema

Learn how to add an attribute to the scheme with the help of an example. 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.

A.3.2 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.

A.3.3 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
```

A.4 LDIF Format for Migrating Entries

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.

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 for more information about the Oracle Internet Directory Migration Tool. Also, see:

- Substitution Variables for Migration Input Files
- Reconciliation Modes for Migrated Entries

A.4.1 Substitution Variables for Migration Input Files

Understand about the substitution variables that are denoted in the LDIF file.

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.

```
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.

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.
%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.

A.4.2 Reconciliation Modes for Migrated Entries

When migrating entries into Oracle Internet Directory from another application, it is possible that there may be conflicts.

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
  ```

Index