

Oracle® Fusion Middleware

User Reference for Oracle Identity Management

11g Release 1 (11.1.1)

E10035-01

May 2009

Oracle Fusion Middleware User Reference for Oracle Identity Management 11g Release 1 (11.1.1)

E10035-01

Copyright © 2005, 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Ellen Desmond

Contributing Author: Don Biasotti

Contributors: Olfat Aly, Manish Arora, Vasuki Ashok, Krishna Chander, Giriraj Chauhan, Margaret Chou, Quan Dinh, Vinoth Janakiraman, Ajay Keni, Buddhika Kottahachchi, Stephen Lee, Paul Li, David Lin, Venkat Medam, Karthi Purushothaman, Lakshmi Ramadoss, Loganathan Ramasamy, Ramaprakash Sathyanarayan, Amit Sharma, Rajiv Sharma, Daniel Shih, Jerry Smith, Baogang Song, Olaf Stullich, Dipankar Thakuria, Arun Theebaprakasam, Satishkumar Venkatasamy, Shawn Vincent, Frances Wu

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xxix
Audience	xxix
Documentation Accessibility	xxix
Related Documents	xxx
Conventions	xxx
Part I Command-Line Tool Reference	
1 Command-Line Tools Overview	
Using Passwords with Command-Line Tools	1-1
Configuring Your Environment	1-2
Oracle Identity Management Command-Line Tool Categories	1-2
2 Oracle Internet Directory Administration Tools	
oidpasswd	2-1
Syntax for oidpasswd	2-2
Arguments for oidpasswd	2-2
Tasks and Examples for oidpasswd	2-2
Changing the Password to the Oracle Internet Directory Database	2-3
Creating Wallets for Oracle Internet Directory Database and Oracle Directory Replication Server Passwords	2-3
Unlocking the Superuser Account	2-3
Resetting the Superuser Password	2-4
Managing Superuser Access Control Points	2-4
Related Command-Line Tools for oidpasswd	2-4
oidctl	2-5
Syntax for oidctl	2-5
Arguments for oidctl	2-5
OIDLDAPD Flags	2-6
OIDREPLD Flags	2-7
Tasks and Examples for oidctl	2-7
Creating an Oracle Internet Directory Instance in an Existing Component	2-8
Deleting an Oracle Internet Directory Instance in a Component	2-8
Starting an Oracle Internet Directory Server Instance	2-8
Stopping an Oracle Internet Directory Server Instance	2-8

Restarting an Oracle Internet Directory Server Instance	2-8
Starting a Directory Replication Server Instance.....	2-9
Stopping a Directory Replication Server Instance	2-9
Starting and Stopping a Server Instance on a Virtual Host or Cluster Node	2-9
Reporting the Status of Each Server	2-9
Reporting Diagnostics	2-10
Related Command-Line Tools for oidctl	2-10
oiddiag	2-11
Syntax for oiddiag.....	2-11
Arguments for oiddiag.....	2-12
Tasks and Examples for oiddiag.....	2-12
Collecting All Diagnostic Information.....	2-13
Collecting Selected Diagnostic Information.....	2-13
Collecting Stack Trace Information	2-13
oidmon	2-13
Syntax for oidmon.....	2-13
Arguments for oidmon.....	2-14
Tasks and Examples for oidmon.....	2-14
Starting Oracle Internet Directory Monitor.....	2-14
Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node	2-14
Stopping Oracle Internet Directory Monitor	2-14
Related Command-Line Tools for oidmon.....	2-15
opmnctl	2-15
Syntax for opmnctl.....	2-15
Arguments for opmnctl.....	2-15
Commands.....	2-16
WebLogic Administration Server Properties.....	2-16
Instance Properties.....	2-17
OPMN Configuration Properties.....	2-17
Component Properties for Oracle Internet Directory	2-17
Oracle Internet Directory Component Configuration Properties.....	2-17
Tasks and Examples for opmnctl.....	2-18
Creating an Oracle Internet Directory Component	2-18
Registering an Oracle Instance.....	2-19
Unregistering an Oracle Instance	2-19
Updating the Component Registration of an Oracle Instance	2-19
Deleting an Oracle Internet Directory Component.....	2-19
Stopping All Oracle Internet Directory Server Components	2-20
Starting All Oracle Internet Directory Server Components.....	2-20
Stopping a Specific Oracle Internet Directory Server Component	2-20
Starting a Specific Oracle Internet Directory Server Component	2-20
Getting Status Information	2-20
Related Command-Line Tools for opmnctl.....	2-20
oidstats.sql	2-21
Syntax for oidstats.sql.....	2-21
Arguments for oidstats.sql.....	2-21
Tasks and Examples for oidstats.sql.....	2-21

Running the Oracle Internet Directory Database Statistics Collection Tool	2-21
Related Command-Line Tools for oidstats.sql.....	2-21
oidcred	2-22
Syntax for oidcred	2-22
Arguments for oidcred.....	2-22
Tasks and Examples for oidcred	2-22
oidrealm	2-22
Syntax for oidrealm.....	2-22
Arguments for oidrealm	2-23
Example for oidrealm	2-23

3 Oracle Internet Directory Data Management Tools

bulkdelete	3-1
Syntax for bulkdelete	3-2
Arguments for bulkdelete	3-2
Tasks and Examples for bulkdelete.....	3-2
Deleting All Entries in a Naming Context and Making Them Tombstone Entries.....	3-3
Completely Deleting All Entries in a Naming Context	3-3
Deleting Entries in Multiple Naming Contexts	3-3
Related Command-Line Tools for bulkdelete.....	3-3
bulkload	3-3
Syntax for bulkload.....	3-5
Arguments for bulkload.....	3-5
Tasks and Examples for bulkload.....	3-7
Loading Data in Bulk Mode	3-7
Loading Data for Multiple Nodes in a Replicated Environment.....	3-7
Loading Data in Incremental Mode	3-7
Verifying Indexes	3-8
Recreating Indexes.....	3-8
Recovering Data After a Load Error	3-8
Related Command-Line Tools for bulkload.....	3-8
bulkmodify	3-8
Syntax for bulkmodify.....	3-9
Arguments for bulkmodify.....	3-10
Tasks and Examples for bulkmodify.....	3-10
Updating an Attribute for Multiple Entries at Once.....	3-11
Limitations of bulkmodify	3-11
Related Command-Line Tools for bulkmodify.....	3-11
catalog	3-11
Syntax for catalog.....	3-12
Arguments for catalog.....	3-12
Tasks and Examples for catalog.....	3-12
Indexing a Single Attribute	3-13
Indexing Multiple Attributes	3-13
Removing an Attribute from the List of Indexed Attributes.....	3-13
Related Command-Line Tools for catalog.....	3-13
ldapadd	3-13

Syntax for ldapadd.....	3-13
Arguments for ldapadd.....	3-13
Tasks and Examples for ldapadd.....	3-16
Adding Data to the Directory Using an LDIF File	3-16
Adding Data to the Directory Using a DSML File	3-17
Previewing an Add Operation.....	3-17
Related Command-Line Tools for ldapadd.....	3-17
ldapaddmt	3-17
Syntax for ldapaddmt.....	3-18
Arguments for ldapaddmt.....	3-18
Tasks and Examples for ldapaddmt.....	3-20
Adding Concurrent Entries to the Directory Using an LDIF File.....	3-20
Related Command-Line Tools for ldapaddmt.....	3-21
ldapbind	3-21
Syntax for ldapbind	3-21
Arguments for ldapbind	3-21
Tasks and Examples for ldapbind	3-22
Validating Authentication Credentials.....	3-23
Related Command-Line Tools for ldapbind	3-23
ldapcompare	3-23
Syntax for ldapcompare	3-23
Arguments for ldapcompare	3-23
Tasks and Examples for ldapcompare	3-25
Comparing Attribute Values for an Entry.....	3-25
Related Command-Line Tools for ldapcompare	3-25
ldapdelete	3-25
Syntax for ldapdelete.....	3-26
Arguments for ldapdelete.....	3-26
Tasks and Examples for ldapdelete.....	3-28
Deleting a Single Entry.....	3-28
Deleting Multiple Entries Using an LDIF File	3-28
Related Command-Line Tools for ldapdelete.....	3-28
ldapmoddn	3-28
Syntax for ldapmoddn.....	3-28
Arguments for ldapmoddn.....	3-28
Tasks and Examples for ldapmoddn.....	3-30
Changing the RDN of an Entry.....	3-30
Moving an Entry	3-30
Related Command-Line Tools for ldapmoddn.....	3-31
ldapmodify	3-31
Syntax for ldapmodify.....	3-31
Arguments for ldapmodify.....	3-31
Tasks and Examples for ldapmodify.....	3-34
Modifying the Directory Schema.....	3-34
Modifying an Entry	3-34
Related Command-Line Tools for ldapmodify.....	3-34
ldapmodifymt	3-35

Syntax for ldapmodifymt.....	3-35
Arguments for ldapmodifymt.....	3-35
Tasks and Examples for ldapmodifymt.....	3-38
Modifying Multiple Entries Concurrently	3-38
Related Command-Line Tools for ldapmodifymt.....	3-38
ldapsearch	3-38
Syntax for ldapsearch	3-38
Arguments for ldapsearch	3-39
Tasks and Examples for ldapsearch	3-43
Performing a Base Object Search	3-43
Performing a One-Level Search	3-43
Performing a Subtree Search	3-43
Searching for Attribute Values of Entries.....	3-43
Searching for Entries with Attribute Options.....	3-44
Searching for All User Attributes and Specified Operational Attributes.....	3-44
Searching for Entries (More Examples)	3-45
Related Command-Line Tools for ldapsearch	3-45
ldifmigrator	3-45
Syntax for ldifmigrator	3-45
Arguments for ldifmigrator.....	3-46
Tasks and Examples for ldifmigrator.....	3-47
Using the Data Migration Tool in Lookup Mode.....	3-47
Overriding Data Migration Values in Lookup Mode.....	3-47
Using the Data Migration Tool by Supplying Your Own Values.....	3-48
Loading and Reconciling Data Using the Data Migration Tool.....	3-48
Related Command-Line Tools for ldifmigrator.....	3-48
Error Messages for ldifmigrator.....	3-48
ldifwrite	3-49
Syntax for ldifwrite	3-50
Arguments for ldifwrite	3-50
Tasks and Examples for ldifwrite	3-51
Converting All Entries under a Naming Context to an LDIF File.....	3-51
Converting a Partial Naming Context to an LDIF File.....	3-51
Converting Entries that Match Criteria to an LDIF File.....	3-51
Related Command-Line Tools for ldifwrite	3-52
upgradecert.pl	3-52
Syntax for upgradecert.pl	3-52
Arguments for upgradecert.pl	3-52
Tasks and Examples for upgradecert.pl	3-53
Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2	3-53
Related Command-Line Tools for upgradecert.pl	3-53

4 Oracle Internet Directory Replication Management Tools

ManageHiq.retry and ManageHiq.purge	4-1
Syntax for ManageHiq.retry and ManageHiq.purge.....	4-2
Examples for ManageHiq.retry	4-2
Examples for ManageHiq.purge.....	4-3

oidcmprec	4-3
Syntax for oidcmprec.....	4-4
Arguments for oidcmprec.....	4-5
Tasks and Examples for oidcmprec.....	4-17
Comparing and Reconciling Individual Entries in Two Directories.....	4-18
Comparing and Reconciling Subtrees in Two Directories.....	4-18
Comparing and Reconciling Entire Directories.....	4-19
Performing User-Defined Compare and Reconcile Operations.....	4-19
Merging Two Directories.....	4-20
Including and Excluding Attributes	4-20
Using a Filter.....	4-20
Overriding Default Conflict Resolution Rules	4-21
Using a Parameter File	4-21
Using a Parameter File in XML Format	4-21
Generating Change Logs	4-22
Performing Directory Schema Operations	4-23
remtool	4-23
Syntax for remtool.....	4-23
Terminology Used in remtool Argument Descriptions	4-24
Arguments for remtool.....	4-24
The remtool -asr2ldap Operation	4-26
Syntax for remtool -asr2ldap	4-26
Arguments for remtool -asr2ldap.....	4-26
Tasks and Examples for remtool -asr2ldap.....	4-26
Converting an Oracle Database Advanced Replication-Based Agreement to an LDAP-Based Agreement.....	4-26
The remtool -addnode Operation	4-27
Syntax for remtool -addnode	4-27
Arguments for remtool -addnode	4-27
Tasks and Examples for remtool -addnode	4-27
Adding a New Node to an Oracle Database Advanced Replication-based DRG... ..	4-27
The remtool -asrcleanup Operation	4-29
Syntax for remtool -asrcleanup.....	4-29
Arguments for remtool -asrcleanup.....	4-30
Tasks and Examples for remtool -asrcleanup.....	4-30
Cleaning Up an Oracle Database Advanced Replication-based DRG Setup	4-30
The remtool -asrrectify Operation	4-31
Syntax for remtool -asrrectify.....	4-31
Arguments for remtool -asrrectify.....	4-31
Tasks and Examples for remtool -asrrectify.....	4-31
Detecting and Correcting Errors in an Oracle Database Advanced Replication-Based DRG Setup	4-31
The remtool -asrsetup Operation.....	4-32
Syntax for remtool -asrsetup	4-33
Arguments for remtool -asrsetup	4-33
Tasks and Examples for remtool -asrsetup	4-33
Creating an Oracle Database Advanced Replication-based DRG	4-33
The remtool -asrverify Operation	4-35

Syntax for remtool -asrverify	4-36
Arguments for remtool -asrverify	4-36
Tasks and Examples for remtool -asrverify	4-36
Detecting Errors in an Oracle Database Advanced Replication-Based DRG Setup	4-36
The remtool -backupmetadata Operation	4-37
Syntax for remtool -backupmetadata.....	4-37
Arguments for remtool -backupmetadata.....	4-38
Tasks and Examples for remtool -backupmetadata.....	4-38
Adding the Metadata of a Pilot Replica to a Master Replica.....	4-38
Backing Up the Metadata of a Pilot Replica to an LDIF File	4-39
The remtool -chgpwd Operation	4-39
Syntax for remtool -chgpwd.....	4-39
Arguments for remtool -chgpwd.....	4-39
Tasks and Examples for remtool -chgpwd.....	4-39
Changing the Replication Administrator Password for an Oracle Database Advanced Replication-based DRG.....	4-40
The remtool -delnode Operation	4-40
Syntax for remtool -delnode.....	4-41
Arguments for remtool -delnode.....	4-41
Tasks and Examples for remtool -delnode.....	4-41
Removing a RMS Node from an Oracle Database Advanced Replication-Based DRG	4-41
The remtool -dispasrerr Operation.....	4-42
Syntax for remtool -dispasrerr	4-42
Arguments for remtool -dispasrerr	4-43
Tasks and Examples for remtool -dispasrerr	4-43
Displaying Errors for an Oracle Database Advanced Replication-based DRG	4-43
The remtool -dispqstat Operation.....	4-44
Syntax for remtool -dispqstat.....	4-44
Arguments for remtool -dispqstat.....	4-44
Tasks and Examples for remtool -dispqstat.....	4-44
Displaying Queue Statistics for an Oracle Database Advanced Replication-Based DRG	4-44
The remtool -paddnode Operation.....	4-45
Syntax for remtool -paddnode.....	4-45
Arguments for remtool -paddnode	4-45
Tasks and Examples for remtool -paddnode	4-46
Adding a Read-Only Replica to a DRG.....	4-46
Adding a Partial Replica to a DRG.....	4-47
The remtool -pdisplay Operation	4-49
Arguments to remtool -pdisplay	4-49
The remtool -pchgmaster Operation.....	4-49
Syntax for remtool -pchgmaster	4-50
Arguments for remtool -pchgmaster	4-50
Tasks and Examples for remtool -pchgmaster	4-50
Breaking a Supplier Agreement and Creating a New Supplier Agreement for a Consumer.....	4-50

Changing the Primary Node	4-51
The remtool -pchgpwd Operation	4-52
Syntax for remtool -pchgpwd	4-52
Arguments for remtool -pchgpwd	4-52
Tasks and Examples for remtool -pchgpwd	4-52
Changing the Replication DN Password Used for LDAP-Based Replication	4-52
The remtool -pchgwalpwd Operation	4-53
Syntax for remtool -pchgwalpwd.....	4-53
Arguments for remtool -pchgwalpwd.....	4-53
Tasks and Examples for remtool -pchgwalpwd.....	4-53
Changing the Replication DN Password in the Oracle Internet Directory Wallet	4-53
The remtool -pcleanup Operation	4-54
Syntax for remtool -pcleanup.....	4-54
Arguments for remtool -pcleanup.....	4-54
Tasks and Examples for remtool -pcleanup.....	4-54
Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup	4-55
Cleaning Up Specific LDAP Agreements.....	4-56
The remtool -pdelnode Operation	4-56
Syntax for remtool -pdelnode	4-56
Arguments for remtool -pdelnode	4-56
Tasks and Examples for remtool -pdelnode	4-57
Deleting a Read-Only Replica from a DRG	4-57
The remtool -pdispqstat Operation	4-58
Syntax for remtool -pdispqstat.....	4-58
Arguments for remtool -pdispqstat	4-58
Tasks and Examples for remtool -pdispqstat	4-58
Display queue statistics for LDAP-based replicas	4-58
The remtool -pilotreplica Operation.....	4-59
Syntax for remtool -pilotreplica	4-59
Arguments for remtool -pilotreplica.....	4-59
Tasks and Examples for remtool -pilotreplica	4-59
Beginning Pilot Mode for a Replica	4-59
Ending Pilot Mode for a Replica.....	4-59
The remtool -presetpwd Operation.....	4-59
Syntax for remtool -presetpwd	4-60
Arguments for remtool -presetpwd	4-60
Tasks and Examples for remtool -presetpwd	4-60
Resetting the Replication DN Password for a Single Directory.....	4-60
The remtool -pverify Operation	4-60
Syntax for remtool -pverify	4-61
Arguments for remtool -pverify	4-61
Tasks and Examples for remtool -pverify	4-61
Verify Replication Configuration for an LDAP-Based DRG	4-61
The remtool -resumear Operation	4-63
Syntax for remtool -resumear	4-63
Arguments for remtool -resumear.....	4-63
Tasks and Examples for remtool -resumear.....	4-63

Resuming Replication Activity for an Oracle Database Advanced Replication-Based DRG	4-63
The remtool -suspendasr Operation.....	4-64
Syntax for remtool -suspendasr	4-64
Arguments for remtool -suspendasr	4-64
Tasks and Examples for remtool -suspendasr	4-64
Suspending Replication Activity for an Oracle Database Advanced Replication-Based DRG	4-64
The -bind Connection Argument.....	4-65
The -connect Connection Argument	4-65
Related Command-Line Tools for remtool.....	4-65

5 Oracle Directory Integration Platform Tools

manageDIPServerConfig	5-1
Syntax for manageDIPServerConfig	5-1
Arguments for manageDIPServerConfig	5-1
Tasks and Examples for manageDIPServerConfig	5-3
manageSyncProfiles	5-3
Syntax for manageSyncProfiles.....	5-3
Arguments for manageSyncProfiles.....	5-3
Tasks and Examples for manageSyncProfiles.....	5-6
syncProfileBootstrap	5-7
Syntax for syncProfileBootstrap.....	5-7
Arguments for syncProfileBootstrap.....	5-7
Tasks and Examples for syncProfileBootstrap.....	5-8
expressSyncSetup	5-8
Syntax for expressSyncSetup.....	5-8
Arguments for expressSyncSetup.....	5-9
Tasks and Examples for expressSyncSetup.....	5-10
provProfileBulkProv	5-10
Syntax for provProfileBulkProv	5-10
Arguments for provProfileBulkProv.....	5-11
Tasks and Examples for provProfileBulkProv	5-11
oidprovtool	5-11
Syntax for oidprovtool	5-12
Arguments for oidprovtool	5-13
Tasks and Examples for oidprovtool	5-16
Creating a Provisioning Profile.....	5-16
Modifying a Provisioning Profile	5-17
Deleting a Provisioning Profile.....	5-17
Disabling a Provisioning Profile.....	5-17
dipStatus	5-17
Syntax for dipStatus.....	5-17
Arguments for dipStatus.....	5-18
Examples for dipStatus.....	5-18
schemasync	5-18
Syntax for schemasync	5-18

Arguments for schemasync	5-19
Tasks and Examples for schemasync	5-19
Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory	5-20
Related Command-Line Tools for schemasync	5-20

Part II LDAP Schema Reference

6 LDAP Schema Overview

Overview of Directory Schema	6-1
Object Classes	6-1
Attributes.....	6-2
LDAP Controls	6-5
Overview of Oracle Identity Management Schema Elements	6-7
System Operational Schema Elements.....	6-8
Directory Schema	6-8
Access Control.....	6-8
Change Logs	6-8
Password Policy	6-9
Oracle Internet Directory Configuration Schema Elements	6-9
Oracle Internet Directory Server.....	6-9
Oracle Context.....	6-9
Oracle Network Services.....	6-10
Garbage Collection	6-10
Attribute Uniqueness	6-10
Audit and Error Logging Schema Elements	6-10
Server Manageability Schema Elements.....	6-11
Oracle Directory Replication Schema Elements	6-11
Oracle Directory Integration and Provisioning Schema Elements	6-12
Applications.....	6-12
Change Logs	6-12
Events and Objects.....	6-12
Plug-ins and Interfaces.....	6-13
Server Configuration	6-13
Profiles	6-13
Schema.....	6-14
Active Directory Users	6-14
Oracle Delegated Administration Services Schema Elements	6-14
Oracle Application Server Certificate Authority and PKI Schema Elements	6-15
Application Schema Elements.....	6-15
Resource Schema Elements.....	6-15
Plug-in Schema Elements.....	6-15
Directory User Agents Schema Elements	6-16
User, Group, and Subscriber Schema Elements	6-16
Groups	6-16
Dynamic Groups	6-16
Users	6-17

Password Policy Schema Elements	6-17
Password Verifier Schema Elements.....	6-17

7 Object Class Reference

Standard LDAP Object Classes	7-1
Oracle Identity Management Object Class Reference	7-3
duaConfigProfile	7-3
orclADGroup	7-4
orclADUser	7-4
orclApplicationEntity	7-4
orclAppSpecificUserInfo	7-5
orclAppUserEntry	7-5
orclAuditOC.....	7-6
orclCertIdMapping	7-6
orclChangeSubscriber.....	7-7
orclCommonAttributes	7-7
orclCommonAttributesV2	7-8
orclConfigSet.....	7-8
orclContainer	7-8
orclDASAppContainer	7-9
orclDASAttrCategory	7-9
orclDASConfigAttr	7-10
orclDASConfigPublicGroup.....	7-10
orclDASLOVVal	7-10
orclDASOperationURL	7-11
orclDASSubscriberContainer	7-11
orclIDMapping	7-12
orclDSAConfig.....	7-12
orclDynamicGroup	7-13
orclEventLog.....	7-13
orclEvents	7-14
orclGeneralStats.....	7-14
orclGroup	7-14
orclHealthStats.....	7-15
orclIndexOC.....	7-15
orclLDAPInstance	7-16
orclLDAPSubConfig.....	7-16
orclNTUser	7-17
orclODIPApplicationCommonConfig	7-17
orclODIPAppSubscription.....	7-17
orclODIPEventContainer	7-18
orclODIPIntegrationProfile.....	7-18
orclODIPObject.....	7-19
orclODIPPlugin	7-19
orclODIPPluginContainer.....	7-20
orclODIPProvEventDefn.....	7-20
orclODIPProvEventTypeConfig	7-20

orclODIPProvInterfaceDetails.....	7-21
orclODIPProvisioningIntegrationInBoundProfileV2	7-21
orclODIPProvisioningIntegrationOutBoundProfile	7-22
orclODIPProvisioningIntegrationOutBoundProfileV2	7-22
orclODIPProvisioningIntegrationProfile.....	7-23
orclODIPProvisioningIntegrationProfileV2.....	7-23
orclODIPProfile.....	7-24
orclODIPSchemaDetails	7-24
orclODIPServerConfig.....	7-25
orclODISConfig	7-25
orclODIServer	7-26
orclODISInstance.....	7-26
orclPerfStats	7-26
orclPKICRL	7-27
orclPKIVaIMecCl.....	7-27
orclPluginConfig	7-28
orclPluginContainer.....	7-28
orclPluginUser	7-29
orclPurgeConfig	7-29
orclPwdVerifierPolicy	7-29
orclPwdVerifierProfile	7-30
orclReplAgreementEntry	7-30
orclReplicaSubentry	7-31
orclReplInstance	7-31
orclReplNameCtxConfig.....	7-32
orclReplSubConfig	7-32
orclResourceDescriptor	7-32
orclResourceType.....	7-33
orclRootContext.....	7-33
orclSchemaVersion.....	7-34
orclSecRefreshEvents.....	7-34
orclService	7-35
orclServiceInstance.....	7-35
orclServiceInstanceReference	7-35
orclServiceRecipient.....	7-36
orclServiceSubscriptionDetail	7-36
orclServiceSuite	7-37
orclSM	7-37
orclSubscriber	7-38
orclSysResourceEvents.....	7-38
orclTraceConfig	7-38
orclUniqueConfig.....	7-39
orclUserStats	7-39
orclUserV2.....	7-40
pwdpolicy.....	7-40
subentry	7-41
subregistry.....	7-41

subschema	7-42
tombstone	7-42
top	7-43

8 Attribute Reference

Standard LDAP Attributes	8-1
Oracle Identity Management Attribute Reference	8-5
attributeMap	8-5
attributeTypes	8-5
authenticationMethod	8-6
authPassword	8-6
bindTimeLimit	8-7
c	8-7
changestatus	8-7
cn	8-8
contentRules	8-8
createTimestamp	8-8
creatorsName	8-9
credentialLevel	8-9
defaultSearchBase	8-10
defaultSearchScope	8-10
defaultServerList	8-10
description	8-11
displayName	8-11
followReferrals	8-11
javaClassName	8-12
jpegPhoto	8-12
krbPrincipalName	8-12
labeledURI	8-13
ldapSyntaxes	8-13
mail	8-13
matchingRules	8-14
middleName	8-14
modifiersName	8-14
modifyTimestamp	8-15
namingContexts	8-15
objectClass	8-16
objectClasses	8-16
objectClassMap	8-16
orclACI	8-17
orclACLResultsLatency	8-17
orclActivateReplication	8-17
orclActiveConn	8-18
orclActiveEndDate	8-18
orclActiveStartdate	8-18
orclActiveThreads	8-19
orclAgreementId	8-19

orclagreementtype	8-19
orclAnonymousBindsFlag	8-20
orclAppFullName	8-20
orclAppId	8-20
orclApplicationAddress	8-21
orclApplicationCommonName.....	8-21
orclApplicationType	8-21
orclAssocDB.....	8-22
orclAssocIasInstance.....	8-22
orclAttrACLEvalLatency	8-22
orclAudCustEvents.....	8-23
orclAudFilterPreset.....	8-23
orclAuditAttribute	8-23
orclAuditMessage	8-24
orclAudSplUsers	8-24
orclBERgenLatency	8-24
orclCatalogEntryDN	8-25
orclCategory.....	8-25
orclCertExtensionAttribute.....	8-25
orclCertExtensionOID	8-26
orclCertificateHash	8-26
orclCertificateMatch	8-27
orclCertMappingAttribute.....	8-27
orclChangeLogLife.....	8-27
orclChangeRetryCount.....	8-28
orclCommonAutoRegEnabled	8-28
orclCommonContextMap	8-29
orclCommonDefaultUserCreateBase	8-29
orclCommonGroupCreateBase	8-29
orclCommonNamingAttribute	8-30
orclCommonNicknameAttribute.....	8-30
orclCommonSASLRealm	8-30
orclCommonUserSearchBase	8-31
orclCommonVerifierEnable.....	8-31
orclConfigSetNumber.....	8-31
orclconflresolution	8-32
orclConnectByAttribute	8-32
orclConnectBySearchBase.....	8-32
orclConnectByStartingValue	8-33
orclConnectionFormat.....	8-33
orclContact	8-33
orclCryptoScheme.....	8-34
orclDASAdminModifiable.....	8-34
orclDASAttrDispOrder	8-34
orclDASAttrName.....	8-35
orclDASEnableProductLogo	8-35
orclDASEnableSubscriberLogo.....	8-35

orclDASIsEnabled	8-36
orclDASIsMandatory	8-36
orclDASIsPersonal	8-37
orclDASLOV	8-37
orclDASPublicGroupDNs	8-37
orclDASSearchable	8-38
orclDASSearchColIndex	8-38
orclDASSearchFilter	8-38
orclDASSearchSizeLimit	8-39
orclDASSelfModifiable	8-39
orclDASUIType	8-39
orclDASURL	8-40
orclDASURLBase	8-40
orclDASValidatePwdReset	8-41
orclDASViewable	8-41
orcldataprivacymode	8-41
orclDateOfBirth	8-42
orclDBConnCreationFailed	8-42
orclDBLatency	8-42
orclDBSchemaIdentifier	8-43
orclDBType	8-43
orclDebugFlag	8-43
orclDebugForceFlush	8-44
orcldebuglevel	8-44
orclDebugOp	8-45
orclDefaultProfileGroup	8-45
orclDefaultSubscriber	8-46
orclDIMEonlyLatency	8-46
orclDIPRepository	8-46
orclDirectoryVersion	8-47
orclDirReplGroupAgreement	8-47
orclDirReplGroupDSAs	8-47
orclDisplayPersonalInfo	8-48
OrclDispThreads	8-48
orclDITRoot	8-48
orclDNSUnavailable	8-49
orclEcacheEnabled	8-49
orclEcacheHitRatio	8-50
orclEcacheMaxEntries	8-50
orclEcacheMaxEntSize	8-50
orclEcacheMaxSize	8-51
orclEcacheNumEntries	8-51
orclEcacheSize	8-51
orclEnabled	8-52
orclEnableGroupCache	8-52
orclencryptedattributes	8-53
orclEntryACLEvalLatency	8-53

orclEntryLevelACI	8-53
orclEventLevel	8-54
orclEventTime	8-54
orclEventType	8-55
orclExcludedAttributes	8-55
orclExcludedNamingContexts	8-55
orclFDIncreaseError	8-56
orclFilterACLEvalLatency	8-56
orclFlexAttribute1	8-56
orclFlexAttribute2	8-57
orclFlexAttribute3	8-57
orclFrontLatency	8-57
orclGender	8-58
orclgeneratechangelog	8-58
orclGenObjLatency	8-58
orclGetNearACLLatency	8-59
orclGlobalID	8-59
orclGUID	8-59
orclGUPassword	8-60
orclHIQSchedule	8-60
orclHireDate	8-61
orclHostedCreditCardExpireDate	8-61
orclHostedCreditCardNumber	8-61
orclHostedCreditCardType	8-62
orclHostedDunsNumber	8-62
orclHostedPaymentTerm	8-62
orclHostname	8-63
orclIdleConn	8-63
orclIdleThreads	8-63
orclIncludedNamingContexts	8-64
orclIndexedAttribute	8-64
orclInitialServerMemSize	8-65
orclinmemfiltprocess	8-65
orclInterval	8-65
orclIpAddress	8-66
orclIsEnabled	8-66
orclIsVisible	8-66
orclLastAppliedChangeNumber	8-67
orclLDAPConnKeepALive	8-67
orclLDAPConnTimeout	8-67
orclLDAPInstanceID	8-68
orclLDAPPProcessID	8-68
orclMaidenName	8-68
orclMappedDN	8-69
orclMasterNode	8-69
orclMatchDnEnabled	8-69
orclMaxCC	8-70

orclMaxConnInCache	8-70
orclMaxFDLimitReached	8-71
orclmaxfiltsize.....	8-71
OrclMaxLdapConns	8-71
orclmaxlogfiles.....	8-72
orclmaxlogfilesize	8-72
orclMaxProcessLimitReached	8-72
orclMaxServerRespTime	8-73
orclMemAllocError	8-73
orclNetDescName	8-73
orclNetDescString	8-74
orclNonSSLPort	8-74
orclNormDN	8-74
orclNWCongested.....	8-75
orclNwrwTimeout	8-75
orclNwUnavailable	8-76
orclObjectGUID	8-76
orclObjectSID	8-76
orclODIPAgent	8-77
orclODIPAgentConfigInfo.....	8-77
orclODIPAgentControl	8-78
orclODIPAgentExeCommand.....	8-78
orclODIPAgentHostName.....	8-78
orclODIPAgentName	8-79
orclODIPAgentPassword.....	8-79
orclODIPApplicationName	8-79
orclODIPApplicationsLocation.....	8-80
orclODIPAttributeMappingRules	8-80
orclODIPBootStrapStatus.....	8-80
orclODIPCommand	8-81
orclODIPConDirAccessAccount.....	8-81
orclODIPConDirAccessPassword	8-82
orclODIPConDirLastAppliedChgNum	8-82
orclODIPConDirMatchingFilter.....	8-82
orclODIPConDirURL.....	8-83
orclODIPConfigDNs.....	8-83
orclODIPConfigRefreshFlag.....	8-84
orclODIPDbConnectInfo.....	8-84
orclODIPEncryptedAttrKey	8-84
orclODIPEventFilter	8-85
orclODIPEventSubscriptions.....	8-85
orclODIPFilterAttrCriteria.....	8-85
orclODIPInstancesLocation	8-86
orclODIPInstanceStatus	8-86
orclODIPInterfaceType	8-87
orclODIPLastExecutionTime.....	8-87
orclODIPLastSuccessfulExecutionTime.....	8-87

orclODIPMustAttrCriteria	8-88
orclODIPObjectCriteria	8-88
orclODIPObjectDefnLocation	8-89
orclODIPObjectEvents.....	8-89
orclODIPObjectName	8-89
orclODIPObjectSyncBase	8-90
orclODIPOIDMatchingFilter	8-90
orclODIPOperationMode.....	8-90
orclODIPOptAttrCriteria	8-91
orclODIPPluginAddInfo	8-91
orclODIPPluginConfigInfo	8-91
orclODIPPluginEvents	8-92
orclODIPPluginExecData.....	8-92
orclODIPPluginExecName	8-92
orclODIPProfileDataLocation	8-93
orclODIPProfileDebugLevel.....	8-93
orclODIPProfileExecGroupID.....	8-93
orclODIPProfileInterfaceAdditionalInformation	8-94
orclODIPProfileInterfaceConnectInformation.....	8-94
orclODIPProfileInterfaceName	8-94
orclODIPProfileInterfaceType.....	8-95
orclODIPProfileInterfaceVersion	8-95
orclODIPProfileLastAppliedAppEventID.....	8-96
orclODIPProfileLastProcessingTime.....	8-96
orclODIPProfileLastSuccessfulProcessingTime	8-96
orclODIPProfileMaxErrors	8-97
orclODIPProfileMaxEventsPerInvocation.....	8-97
orclODIPProfileMaxEventsPerSchedule	8-97
orclODIPProfileMaxRetries	8-98
orclODIPProfileName	8-98
orclODIPProfileProcessingErrors	8-99
orclODIPProfileProcessingStatus	8-99
orclODIPProfileProvSubscriptionMode	8-99
orclODIPProfileSchedule	8-100
orclODIPProfileStatusUpdate	8-100
orclODIPProvEventCriteria.....	8-100
orclODIPProvEventLDAPChangeType.....	8-101
orclODIPProvEventObjectType	8-101
orclODIPProvEventRule	8-101
orclODIPProvEventRuleDTD	8-102
orclODIPProvInterfaceFilter	8-102
orclODIPProvInterfaceProcessor	8-103
orclODIPProvisioningAppGUID.....	8-103
orclODIPProvisioningAppName.....	8-103
orclODIPProvisioningEventMappingRules.....	8-104
orclODIPProvisioningEventPermittedOperations.....	8-104
orclODIPProvisioningEventSubscription.....	8-105

orclODIPProvisioningOrgGUID.....	8-105
orclODIPProvisioningOrgName.....	8-105
orclODIPProvProfileLocation	8-106
orclODIPRootLocation	8-106
orclODIPSchedulingInterval	8-107
orclODIPSchemaVersion.....	8-107
orclODIPSearchCountLimit.....	8-107
orclODIPSearchTimeLimit.....	8-108
orclODIPServerCommitSize.....	8-108
orclODIPServerConfigLocation	8-108
orclODIPServerDebugLevel	8-109
orclODIPServerRefreshIntvl.....	8-109
orclODIPServerSSLMode.....	8-109
orclODIPServerWalletLoc.....	8-110
orclODIPSynchronizationErrors	8-110
orclODIPSynchronizationMode.....	8-111
orclODIPSynchronizationStatus	8-111
orclODIPSyncProfileLocation	8-111
orclODIPSyncRetryCount.....	8-112
orclOidComponentName	8-112
orclOidInstanceName.....	8-112
orclOpAbandoned	8-113
orclOpCompleted.....	8-113
orclOpenConn	8-113
orclOpFailed.....	8-114
orclOpInitiated	8-114
orclOpLatency	8-114
orclOpPending.....	8-115
orclOpResult	8-115
orclOpSucceeded.....	8-115
orclOpTimedOut	8-116
orcloptracklevel	8-116
orcloptrackmaxtotalsize	8-116
orcloptracknumelemcontainers	8-117
orclORA28error	8-117
orclORA3113error	8-117
orclORA3114error	8-118
orclOracleHome	8-118
orclOwnerGUID	8-118
orclPassword.....	8-119
orclPasswordAttribute	8-119
orclPasswordHint	8-119
orclPasswordHintAnswer.....	8-120
orclPasswordVerifier	8-120
orclPilotMode	8-121
orclPKCS12Hint.....	8-121
orclPKIMatchingRule	8-121

orclPKINextUpdate.....	8-122
orclPKIVaIMecAttr	8-122
orclPluginAttributeList	8-122
orclPluginCheckEntryExist.....	8-123
orclPluginEnable	8-123
orclPluginEntryProperties	8-124
orclPluginIsReplace	8-124
orclPluginBinaryFlexfield	8-124
orclPluginFlexfield	8-125
orclPluginSecuredFlexfield.....	8-125
orclPluginKind	8-125
orclPluginLDAPOperation	8-126
orclPluginName	8-126
orclPluginPort.....	8-127
orclPluginRequestGroup	8-127
orclPluginRequestNegGroup	8-127
orclPluginResultCode.....	8-128
orclPluginSASLCallBack	8-128
orclPluginSearchNotFound	8-129
orclPluginShareLibLocation	8-129
orclPluginSubscriberDNList.....	8-129
orclPluginTiming	8-130
orclPluginType	8-130
orclPluginVersion.....	8-131
OrclPluginWorkers	8-131
orclPrName	8-131
orclProductVersion	8-132
orclPrPassword.....	8-132
orclPurgeBase	8-132
orclPurgeDebug.....	8-133
orclPurgeEnable	8-133
orclPurgeFileLoc.....	8-133
orclPurgeFileName	8-134
orclPurgeFilter	8-134
orclPurgeInterval	8-135
orclPurgeNow.....	8-135
orclPurgePackage.....	8-135
orclPurgeSchedule	8-136
orclPurgeStart	8-136
orclPurgeTargetAge.....	8-136
orclPurgeTranSize	8-137
orclPwdAccountUnlock	8-137
orclPwdAllowHashCompare	8-138
orclPwdAlphaNumeric	8-138
orclPwdEncryptionEnable	8-138
orclPwdIllegalValues.....	8-139
orclPwdIPAccountLockedTime	8-139

orclPwDIPIFailureTime	8-140
orclPwDIPLockout	8-140
orclPwDIPLockoutDuration	8-140
orclPwDIPIMaxFailure.....	8-141
orclPwDPolicyEnable.....	8-141
orclPwDVerifierParams	8-141
orclQueueDepth	8-142
orclQueueLatency	8-142
orclReadWaitThreads	8-143
orclrefreshdgrmems.....	8-143
orclReplAgreements	8-143
orclreplautotune	8-144
orclReplicaDN	8-144
orclReplicaID	8-144
orclReplicaSecondaryURI	8-145
orclReplicaState	8-145
orclreplicationid	8-146
orclReplicationProtocol	8-146
orclReplicationState	8-146
orclReplicaType	8-147
orclReplicaURI.....	8-147
orclReplicaVersion	8-147
orclreplmaxworkers.....	8-148
orclreplusesasl;digest-md5	8-148
orclResourceIdentifier	8-148
orclResourceName	8-149
orclResourceTypeName	8-149
orclResourceViewers	8-149
orclRevPwD	8-149
orclrienabled	8-150
orclSAMAccountName	8-150
orclSASLAuthenticationMode	8-151
orclSASLCipherChoice.....	8-151
orclSASLMechanism.....	8-151
orclsDumpFlag	8-152
orclSearchBaseDN	8-152
orclSearchFilter	8-152
orclSearchScope	8-153
orclSecondaryUID	8-153
orclSequence	8-153
orclServerAvgMemGrowth	8-154
orclServerMode	8-154
orclServerProcs.....	8-155
orclServiceInstanceLocation	8-155
orclServiceMember	8-155
orclServiceSubscriptionLocation.....	8-156
orclServiceSubType.....	8-156

orclServiceType	8-156
orclSID	8-157
orclsimplemodchglogattributes	8-157
orclSizeLimit	8-157
orclSkewedAttribute.....	8-158
orclSkipRefInSQL.....	8-158
orclSMSpec.....	8-158
orclSQLexeFetchLatency	8-159
orclSQLGenReusedParsed.....	8-159
orclSSLAuthentication.....	8-159
orclSSLCipherSuite	8-160
orclSSLEnable	8-161
orclsslinteropmode	8-161
orclSSLPort.....	8-162
orclSSLVersion.....	8-162
orclSSLWalletURL.....	8-162
orclStatsDN	8-163
orclStatsFlag.....	8-163
orclStatsLevel.....	8-164
orclStatsOp	8-164
orclStatsPeriodicity	8-164
orclStatus	8-165
orclSUAccountLocked	8-165
orclSubscriberDisable	8-165
orclSubscriberFullName.....	8-166
orclSubscriberNickNameAttribute.....	8-166
orclSubscriberSearchBase.....	8-166
orclSubscriberType	8-167
orclSuffix.....	8-167
orclSuiteType	8-168
orclSULoginFailureCount	8-168
orclSUName	8-168
orclSUPassword	8-169
orclSystemName	8-169
orclTcpConnToClose	8-169
orclTcpConnToShutDown.....	8-170
orclThreadSpawnFailed	8-170
orclThreadsPerSupplier.....	8-170
orclTimeLimit	8-171
orclTimeZone.....	8-171
orclTLimitMode.....	8-171
orclTotFreePhyMem	8-172
orclTraceDimesionLevel	8-172
orclTraceFileLocation	8-173
orclTraceFileSize.....	8-173
orclTraceLevel.....	8-173
orclTraceMode	8-174

orclTrustedApplicationGroup.....	8-174
orclUIAccessibilityMode.....	8-174
orclUniqueAttrName.....	8-175
orclUniqueEnable.....	8-175
orclUniqueObjectClass.....	8-175
orclUniqueScope.....	8-176
orclUniqueSubtree.....	8-176
orclUnsyncRevPwd.....	8-177
orclUpdateSchedule.....	8-177
orclUpgradeInProgress.....	8-177
orclUserDN.....	8-178
orclUserIDAttribute.....	8-178
orclUserModifiable.....	8-178
orclUserObjectClasses.....	8-179
orclUserPrincipalName.....	8-179
orclVersion.....	8-179
orclWirelessAccountNumber.....	8-180
orclWorkflowNotificationPref.....	8-180
orclWriteWaitThreads.....	8-180
owner.....	8-181
pilotStartTime.....	8-181
preferredServerList.....	8-181
profileTTL.....	8-182
protocolInformation.....	8-182
pwdAccountLockedTime.....	8-183
pwdAllowUserChange.....	8-183
pwdChangedTime.....	8-184
pwdCheckSyntax.....	8-184
pwdExpirationWarned.....	8-184
pwdExpireWarning.....	8-185
pwdFailureCountInterval.....	8-185
pwdFailureTime.....	8-186
pwdGraceLoginLimit.....	8-186
pwdGraceLoginTimeLimit.....	8-186
pwdGraceUseTime.....	8-187
pwdHistory.....	8-187
pwdInHistory.....	8-188
pwdLockout.....	8-188
pwdLockoutDuration.....	8-188
pwdMaxAge.....	8-189
pwdMaxFailure.....	8-189
pwdMinAge.....	8-190
pwdMinLength.....	8-190
pwdMustChange.....	8-190
pwdpolicysubentry.....	8-191
pwdReset.....	8-191
pwdSafeModify.....	8-192

ref.....	8-192
seeAlso.....	8-192
serverName.....	8-193
serviceAuthenticationMethod.....	8-193
serviceCredentialLevel.....	8-193
serviceSearchDescriptor.....	8-194
sn.....	8-194
supportedcontrol.....	8-194
supportedextension.....	8-194
supportedldapversion.....	8-195
uniqueMember.....	8-195
supportedsaslmmechanisms.....	8-195
userCertificate;binary.....	8-195
userPassword.....	8-196
userPKCS12.....	8-196
x509issuer.....	8-196

Part III Appendixes

A LDIF File Format

General LDIF Formatting Rules.....	A-1
Line Types and White Space.....	A-1
Sequencing of Entries.....	A-2
Binary Files.....	A-2
Non-Printing Characters in Attribute Values.....	A-2
LDIF Format for Entries.....	A-2
LDIF Format for Adding Entries.....	A-3
LDIF Format for Deleting Entries.....	A-3
LDIF Format for Modifying Entries.....	A-4
LDIF Format for Modifying the RDN of an Entry.....	A-4
LDIF Format for Modifying the DN of an Entry.....	A-5
LDIF Format for Adding Schema Elements.....	A-5
LDIF Format for Migrating Entries.....	A-6
Substitution Variables for Migration Input Files.....	A-6
Predefined Substitution Variables.....	A-7
Reconcile Options for Migrated Entries.....	A-8

List of Tables

3-1	Error Messages of the Data Migration Tool	3-48
4-1	Default Values for the entos Argument.....	4-10
4-2	Default Values for the entod Argument.....	4-10
4-3	Default Values for the atos Argument	4-11
4-4	Default Values for the atrod Argument.....	4-11
4-5	Default Values for the svatrdif Argument	4-13
4-6	Default Values for the mvatrdif Argument	4-13
4-7	Default Values for the mvatrdif Argument	4-14
4-8	Default Values for the odefos Argument	4-14
4-9	Default Values for the odefod Argument.....	4-15
4-10	Default Values for the odefdif Argument	4-15
4-11	Default Values for the adefos Argument.....	4-16
4-12	Default Values for the adefod Argument.....	4-16
4-13	Default Values for the adefdif Argument	4-17
6-1	Attribute Syntax Commonly Used in Oracle Internet Directory	6-3
6-2	Request Controls Supported by Oracle Internet Directory	6-6
6-3	Response Controls Supported by Oracle Internet Directory.....	6-7
7-1	Standard LDAP Object Classes Used By Oracle Internet Directory.....	7-1
8-1	Standard LDAP Attributes Used By Oracle Internet Directory	8-1
8-2	Event Levels.....	8-54
8-3	SSL Cipher Suites Supported in Oracle Internet Directory	8-160
A-1	Predefined Substitution Variables.....	A-7

Preface

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

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request

process. Information about TRS is available at <http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

Related Documents

For more information, see the following manuals in the Oracle Identity Management 11g Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Getting Started with Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management*

If you are using Oracle Delegated Administration Services or Oracle Single Sign-On 10g (10.1.4.3.0) or later, please refer to the following documents in the Oracle Application Server 10g (10.1.4.0.1) library:

- *Oracle Identity Management Guide to Delegated Administration*
- *Oracle Application Server Single Sign-On Administrator's Guide*

Conventions

The following text conventions are used in this document:

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

Part I

Command-Line Tool Reference

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

Part I contains the following chapters:

- [Chapter 1, "Command-Line Tools Overview"](#)
- [Chapter 2, "Oracle Internet Directory Administration Tools"](#)
- [Chapter 3, "Oracle Internet Directory Data Management Tools"](#)
- [Chapter 4, "Oracle Internet Directory Replication Management Tools"](#)
- [Chapter 5, "Oracle Directory Integration Platform Tools"](#)

Command-Line Tools Overview

This chapter provides useful information about using the command-line tools available for Oracle Identity Management. It contains the following topics:

- [Using Passwords with Command-Line Tools](#)
- [Configuring Your Environment](#)
- [Oracle Identity Management Command-Line Tool Categories](#)

Using 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)

If you use the `-w password` option with an LDAP tool when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to true, you will 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 will 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.
```

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.
- `ORACLE_INSTANCE` - 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
```

Oracle Identity Management Command-Line Tool Categories

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

- [Oracle Internet Directory Administration Tools](#)
- [Oracle Internet Directory Data Management Tools](#)
- [Oracle Internet Directory Replication Management Tools](#)
- [Oracle Directory Integration Platform Tools](#)

Oracle Internet Directory Administration Tools

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

- `oidpasswd` (Database Password Utility)
- `oidctl` (Oracle Internet Directory Control)
- `oiddiag` (Oracle Internet Directory Server Diagnostic Tool)
- `oidmon` (Oracle Internet Directory Monitor)
- `opmnctl` (Oracle Process Manager and Notification Server Control)
- `oidstats.sql` (Oracle Internet Directory Database Statistics Collection Tool)
- `oidcred` (Oracle Internet Directory Credential Management Tool)
- `oidrealm` (Oracle Internet Directory Realm Creation Tool)

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

`oidpasswd`

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

- Change the password to the Oracle Internet Directory database.
Oracle Internet Directory uses a password when connecting to an Oracle database. The default for this password matches the value you specified during installation for the Oracle 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.

Syntax for oidpasswd

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

Arguments for oidpasswd

connect=connect_string

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 (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 "About Changing the ODS Password on an Oracle RAC System" in the *Oracle Application Server High Availability Guide* for more information.

- `create_wallet=true` - Create a wallet named `oidpwdlldap1` for the Oracle Internet Directory database password, and a wallet, named `oidpwdrsid`, 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.

Tasks and Examples for oidpasswd

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

- [Changing the Password to the Oracle Internet Directory Database](#)
- [Creating Wallets for Oracle Internet Directory Database and Oracle Directory Replication Server Passwords](#)

- [Unlocking the Superuser Account](#)
- [Resetting the Superuser Password](#)
- [Managing Superuser Access Control Points](#)

Changing the Password to the Oracle Internet Directory Database

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

Example:

```
oidpasswd
current password: oldpassword
new password: newpassword
confirm password: newpassword
password set.
```

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

Note:

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

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

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

Example:

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

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

Unlocking the Superuser Account

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

Example:

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

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

Resetting the 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.

Example:

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

Managing Superuser Access Control Points

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

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

Example:

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

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

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

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

Related Command-Line Tools for `oidpasswd`

- See "[ldapmodify](#)" on page 3-31.
- See "[oidmon](#)" on page 2-13.

oidctl

Oracle Internet Directory Control Utility (`oidctl`) is a command-line tool for starting and stopping Oracle Identity Management server instances. In 11g Release 1 (11.1.1), it is typically used only to configure, start, and stop the Oracle Directory Replication Server.

Note:

- You must set the environment variables `ORACLE_INSTANCE`, `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 with `opmnctl createcomponent`. See "[opmnctl](#)" on page 2-15. You should only use `oidctl` to create an instance if you plan to run Oracle Internet Directory in standalone mode and never use Oracle Enterprise Manager Fusion Middleware Control.
 - 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 "[oidmon](#)" on page 2-13.

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]}
```

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 `ORACLE_INSTANCE/config`. (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. If `oidmon` is started by `opmn`, then make sure the `hostname` parameter exists in the file `ORACLE_INSTANCE/config/OPMN/opmn/opmn.xml`.

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.

- "OIDLDAPD Flags" on page 2-6
- "OIDREPLD Flags" on page 2-7

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]` — Report the status of running server instances. Use `-diag` with `-status` to get diagnostic information.

OIDLDAPD Flags

In 11g Release 1 (11.1.1), the recommended tool for creating instances and managing the LDAP server is `opmnctl`, not `oidctl`. See "[opmnctl](#)" on page 2-15. 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 Fusion Middleware Control.

-l true | false

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

-p ldap_port

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

Tasks and Examples for oidctl

In 11g Release 1 (11.1.1), `oidctl` is used primarily to manage the replication server. The recommended tool for creating instances and managing the LDAP server is `opmnctl`, not `oidctl`. See "[opmnctl](#)" on page 2-15. 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 Fusion Middleware Control.

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

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

See "[oidmon](#)" on page 2-13 for more information about Oracle Internet Directory Monitor.

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

- [Starting an Oracle Internet Directory Server Instance](#)
- [Stopping an Oracle Internet Directory Server Instance](#)
- [Restarting an Oracle Internet Directory Server Instance](#)
- [Starting 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](#)

Creating an Oracle Internet Directory Instance in an Existing 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 componentname 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
```

Deleting 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.

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.

Example:

```
oidctl connect=dbst1 server=OIDLDAPD instance=2 flags="-p 3133 \  
  -debug 1024 -l false" start
```

Stopping an Oracle Internet Directory Server Instance

Example:

```
oidctl connect=dbst1 server=OIDLDAPD instance=2 stop
```

Restarting an Oracle Internet Directory Server Instance

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

For example, if you changed a configuration set that was being referenced by an active instance of Oracle Internet Directory server, you could update it by restarting that

server instance. You do not need to supply the `configset` argument again, as it is maintained from the prior start operation.

Example:

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

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

Starting 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.

Example:

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

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

Stopping a Directory Replication Server Instance

Example:

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

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

Use the `host` argument to specify a virtual host name when starting an Oracle Internet Directory server 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.

Example:

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

Reporting the Status of Each Server

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

Example:

```
oidctl connect=dbs1 status
```

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=osldapd,cn=subconfigsentry |
|-----+-----|
| 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.entryid
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)
```

Related Command-Line Tools for oidctl

- See "[oidmon](#)" on page 2-13

oiddiag

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

You can find the hostname, port number and service name in the file `tnsnames.ora`, located by default in `ORACLE_INSTANCE/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`:

```
ORCL =
  (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 `OIDDIA` tool.

Syntax for oiddiag

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

Arguments for oiddiag

listdiags=true

Writes a list of available diagnostics that can be collected. The list is written to an output file, which is *ORACLE_INSTANCE/diagnostics/logs/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 *ORACLE_INSTANCE/diagnostics/logs/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 *ORACLE_INSTANCE/diagnostics/logs/OID/tools/oiddiag/timestamp.log*. The timestamp format is *YYYYMMDDHHmmss*.

collect_sub=true

Collects a subset of diagnostic information (based on the diagnostics specified in the input file) and writes it to an output file. You 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 *ORACLE_INSTANCE/diagnostics/logs/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.

Tasks and Examples for oiddiag

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

- [Collecting All Diagnostic Information](#)
- [Collecting Selected Diagnostic Information](#)

- [Collecting Stack Trace Information](#)

Collecting All Diagnostic Information

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

Example:

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

Collecting Selected Diagnostic Information

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

Example:

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

Collecting Stack Trace Information

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

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

oidmon

In 11g Release 1 (11.1.1), you typically manage Oracle Internet Directory by using Oracle Enterprise Manager Fusion Middleware Control or the command-line utility `opmnctl`. Both `opmnctl` and Fusion Middleware Control use the Oracle Process Manager and Notification Server to issue commands to the Oracle Internet Directory Monitor, `oidmon`, which initiates, monitors, and terminates directory server processes.

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 `ORACLE_INSTANCE/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).

Tasks and Examples for oidmon

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

- [Starting Oracle Internet Directory Monitor](#)
- [Starting Oracle Internet Directory Monitor on a Virtual Host or Cluster Node](#)
- [Stopping Oracle Internet Directory Monitor](#)

Starting Oracle Internet Directory Monitor

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

Example:

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

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

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

Example:

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

Stopping Oracle Internet Directory Monitor

Stopping Oracle Internet Directory Monitor will also stop all other Oracle Internet Directory processes. The `oidmon` tool does not remove server instance information from the `ODS_PROCESS` table. When an `oidmon start` operation is executed, it will start all the server processes it had stopped previously.

Example:

```
oidmon connect=dbs1 stop
```

Related Command-Line Tools for oidmon

- See "[oidctl](#)" on page 2-5

opmnctl

The Oracle Process Manager and Notification Server Control Utility (`opmnctl`) enables you to manage system components, such as Oracle Internet Directory, in an integrated way.

The term "instance" refers to an Oracle instance in `opmnctl` command descriptions.

Notes:

- This section only discusses how to use the OPMN Control Utility to manage Oracle Internet Directory components. For detailed information on how to use the OPMN Control Utility, see *Oracle Fusion Middleware Oracle Process Manager and Notification Server Administrator's Guide*.
- Arguments to `opmnctl` are case-sensitive. Be sure to type them exactly as shown. For example, `-adminUsername` must have only the letter U in upper case.

Syntax for opmnctl

```
opmnctl startproc ias-component=componentName

opmnctl stopproc ias-component=componentName

opmnctl createcomponent [admin_server_properties] [instance_properties]
[opmn_properties] [component_properties] [component_configuration_properties]

opmnctl deletecomponent [admin_server_properties] [instance_properties]
[opmn_properties] [component_properties] [component_configuration_properties]

opmnctl registerinstance [admin_server_properties] [instance_properties]
[component_configuration_properties]

opmnctl updatecomponentregistration [admin_server_properties] [instance_
properties] [component_configuration_properties]

opmnctl status [-l]
```

Arguments for opmnctl

Arguments for `opmnctl` consist of commands and several types of properties. This section describes the following types of arguments:

- [Commands](#)
- [WebLogic Administration Server Properties](#)
- [Instance Properties](#)

- [OPMN Configuration Properties](#)
- [Component Properties for Oracle Internet Directory](#)
- [Oracle Internet Directory Component Configuration Properties](#)

Note: Arguments to `opmnctl` are case-sensitive. Be sure to type them exactly as shown. For example, `-adminUsername` must have only the letter `U` in upper case.

Commands

The command indicates the operation to perform. The following commands are relevant to Oracle Internet Directory:

startproc

Starts server process

stopproc

Stops server process

createcomponent

Creates a componen and automatically registers the component with a WebLogic domain, as long as the instance is in a registered state.

deletecomponent

Deletes a component

registerinstance

Registers an Oracle instance that was not previously registered with a domain. This scenario occurs if you chose **No Domain** during installation of Oracle Internet Directory or if you created an Oracle instance from the command line and did not register the instance.

status [-l]

Shows the status of components. Add the `-l` option for detailed information.

updatecomponentregistration

Registers an existing Oracle Internet Directory component that was not previously registered with a domain. This scenario occurs if you created a new component in an Oracle instance using `opmnctl createcomponent` and did not register the component.

WebLogic Administration Server Properties

The following administration server properties are relevant to Oracle Internet Directory:

-adminHost

The WebLogic Administration Server host name

-adminPort

The WebLogic Administration Server port. The default is 7001.

-adminUsername

The WebLogic administrator user name.

-adminPasswordFile

A text file containing the WebLogic administrator password. You are prompted for the administrator password if this parameter is missing. Best security practice is to provide the password in response to a prompt. If you must use a file containing the password in clear text, protect it with file permissions and delete it when it is no longer needed.

Instance Properties

You do not need to specify instance properties with the `opmnctl` command, as long as you invoke the command as `ORACLE_INSTANCE/bin/opmnctl`.

OPMN Configuration Properties

No OPMN configuration properties are required with the `opmnctl` commands shown in this chapter.

Component Properties for Oracle Internet Directory

The following component properties are relevant to Oracle Internet Directory.

-componentType

For Oracle Internet Directory, this is always `OID`. This is required for `createcomponent`.

-componentName

The name of an Oracle Internet Directory component, such as `oid1`. The component name must be unique within the Oracle instance.

Oracle Internet Directory Component Configuration Properties

These arguments are specific to Oracle Internet Directory

-Db_info

Specifies the name, TNS port, and service name of the Oracle Database associated with this Oracle Internet Directory component, in the format:

DBHostName: TNSPORT: DBSERVICE_NAME

For example:

`linux12.example.com:1521:orcl.example.com`

-Ods_Password_File

Optional. The file that contains the ODS password in cleartext. You are prompted for the ODS password if this parameter is missing. Best security practice is to provide the password in response to a prompt. If you must use a file containing the password in clear text, protect it with file permissions and delete it when it is no longer needed.

-Sm_Password_File

Optional. The file that contains the ODSSM password in cleartext. You are prompted for the ODSSM password if this parameter is missing. Best security practice is to provide the password in response to a prompt. If you must use a file containing the

password in clear text, protect it with file permissions and delete it when it is no longer needed.

-Namespace

Required only for the first Oracle Internet Directory component in an instance. The Oracle Internet Directory namespace. For example: "dc=us,dc=example,dc=com".

-Admin_Password_File

Optional. The file that contains the password for the Oracle Internet Directory superuser account `cn=orcladmin`. You are prompted for the Oracle Internet Directory superuser password if this parameter is missing.

-Port

Optional. The non-SSL port for this Oracle Internet Directory component. The command will use a default available port if this parameter is missing.

-Sport

Optional. The SSL port for this Oracle Internet Directory component. The command will use a default available port if this parameter is missing.

Tasks and Examples for opmnctl

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

- [Creating an Oracle Internet Directory Component](#)
- [Unregistering an Oracle Instance](#)
- [Updating the Component Registration of an Oracle Instance](#)
- [Deleting an Oracle Internet Directory Component](#)
- [Stopping All Oracle Internet Directory Server Components](#)
- [Starting All Oracle Internet Directory Server Components](#)
- [Stopping a Specific Oracle Internet Directory Server Component](#)
- [Starting a Specific Oracle Internet Directory Server Component](#)
- [Getting Status Information](#)

Creating an Oracle Internet Directory Component

This command creates a component and registers it with a WebLogic domain, as long as the instance is in a registered state:

```
opmnctl createcomponent
  -componentType OID
  -componentName oid2
  -adminHost myhost
  -adminPort 7001
  -Db_info "linux12.example.com:1521:orcl.example.com"
  -Namespace "dc=domain_component1,dc=domain_component2..."
```

The `opmnctl` command prompts for the WebLogic administrator's user name if you do not supply it. It also prompts for the passwords if you do not supply password file names on the command line. The `opmnctl` command also uses available ports if you do not specify `-Port` or `-Sport`

Registering an Oracle Instance

This example registers an Oracle instance with a WebLogic server:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance \  
-adminHost myhost \  
-adminPort 7001 \  
-adminUsername weblogic
```

You will be prompted for the WebLogic administrator's user name and password.

Unregistering an Oracle Instance

This example unregisters an Oracle instance with a WebLogic server:

```
ORACLE_INSTANCE/bin/opmnctl unregisterinstance \  
-adminHost myhost \  
-adminPort 7001 \  
-adminUsername weblogic
```

You will be prompted for the WebLogic administrator's user name and password if you do not supply them.

Updating the Component Registration of an Oracle Instance

You must update the registration of an Oracle Internet Directory component in a registered Oracle instance whenever you change any of the configuration attributes `orclhostname`, `orclnonsslport`, or `orclnonsslport` in the instance-specific configuration entry, or if you change the password for the EMD administrator by using `oidpasswd`. If you do not update the component registration, you will be unable to use Fusion Middleware Control or `wlst` to manage that component.

This example updates the component registration of an Oracle instance that has been registered.

```
ORACLE_INSTANCE/bin/opmnctl updatecomponentregistration \  
-adminHost myhost \  
-adminPort 7001 \  
-adminUsername weblogic \  
-componentType OID \  
-componentName oid2 \  
-Port 6589
```

You are prompted for the WebLogic administrator's user name and password if you do not supply them.

Deleting an Oracle Internet Directory Component

This example deletes an Oracle Internet Directory component that has been registered with a WebLogic server:

```
ORACLE_INSTANCE/bin/opmnctl deletecomponent \  
-adminHost myhost \  
-adminPort 7001 \  
-adminUsername weblogic \  
-componentType OID \  
-componentName oid2
```

You will be prompted for the WebLogic administrator's user name and password if you do not supply them.

oidstats.sql

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

If you load data into the directory by any means other than the bulk load tool (`bulkload`), 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.

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 `$ORACLE_HOME/INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

Tasks and Examples for oidstats.sql

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

- [Running the Oracle Internet Directory Database Statistics Collection Tool](#)

Running the Oracle Internet Directory Database Statistics Collection Tool

Example:

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

Related Command-Line Tools for oidstats.sql

- See "[bulkload](#)" on page 3-3.

oidcred

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. It determines the instance name from the *opmn.xml* file

Syntax for oidcred

```
oidcred user_name option [InstancePath]
```

Arguments for oidcred

The `oidcred` command takes the following arguments:

user_name

Required. Value can be `odssm` or `emd`.

option

Required. Value can be `update` or `delete`. The `update` option adds the credential if it does not exist or updates it if it exists.

InstancePath

Required if `ORACLE_INSTANCE` environment is not set. Path of Oracle Instance directory.

If not specified on the command line, `oidcred` will use `ORACLE_INSTANCE` environment variable if set.

Tasks and Examples for oidcred

Update the password for user `odssm` in the Credential Store Framework.

```
oidcred odssm update /scratch/mydir/fmw_home/asinst_1
Enter password:
Confirm password:
Password set in CSF
```

oidrealm

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.

Syntax for oidrealm

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 *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Arguments for oidrealm

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  
...  
...  
...  
...
```

Oracle Internet Directory Data Management Tools

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

- [bulkdelete](#)
- [bulkload](#)
- [bulkmodify](#)
- [catalog](#)
- [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)
- [ldifwrite](#) (Data Export Tool)
- [ldifmigrator](#) (Data Migration Tool)
- [upgradecert.pl](#) (Certificate Upgrade Tool)

bulkdelete

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

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

Note: The `bulkdelete` command requires that the environment variable `ORACLE_INSTANCE` be set.

Syntax for bulkdelete

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

Arguments for bulkdelete

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (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.

cleandb

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

size

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

encode

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

debug

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `bulkdelete.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

threads

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

verbose

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

Tasks and Examples for bulkdelete

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

- [Deleting All Entries in a Naming Context and Making Them Tombstone Entries](#)
- [Completely Deleting All Entries in a Naming Context](#)
- [Deleting Entries in Multiple Naming Contexts](#)

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

Example:

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

Completely Deleting All Entries in a Naming Context

Example:

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

Deleting Entries in Multiple Naming Contexts

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

Example:

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

Related Command-Line Tools for bulkdelete

- See ["bulkload"](#) on page 3-3
- See ["bulkmodify"](#) on page 3-8
- See ["ldapdelete"](#) on page 3-25

bulkload

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

Intermediate files used by `bulkload` are stored in `ORACLE_INSTANCE/OID/load` by default.

Note:

- The `bulkload` command requires that the environment variable `ORACLE_INSTANCE` be set.
 - If a directory server instance is participating in a replication agreement, do not use the `bulkload` tool to add data into the node. Instead, use `ldapadd`.
-
-

Overview of the Bulk Loading Tool Operations

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

1. Check

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

2. Generate

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

3. Load

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

■ Incremental Mode Loading

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

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

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

■ Bulk Mode Loading

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

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

Notes:

- 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 any referential integrity violations occurred, however, referential integrity is disabled, and you will see the message:

There is a violation of Referential Integrity and hence it is Disabled now. Run the OIDDIAAG 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`.

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 *Oracle Fusion Middleware Upgrade Planning Guide* for any special instructions about upgrading `orclguids` before you begin.

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 `ORACLE_INSTANCE/config`. (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 will be 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 `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

verbose

This is used to run the command in verbose mode.

Tasks and Examples for bulkload

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

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

Loading Data in Bulk Mode

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

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

Example:

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

Loading Data for Multiple Nodes in a Replicated Environment

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

Loading Data in Incremental Mode

If you 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.

Example:

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

Verifying Indexes

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

Example:

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

Recreating Indexes

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

Example:

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

Recovering Data After a Load Error

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

Example:

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

Related Command-Line Tools for bulkload

- See "[bulkdelete](#)" on page 3-1
- See "[bulkmodify](#)" on page 3-8
- See "[ldapadd](#)" on page 3-13
- See "[ldapaddmt](#)" on page 3-17

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 `ORACLE_INSTANCE` be set.

The `bulkmodify` tool supports the following:

- Subtree based modification
- LDAP search filter. For example, the filter could be `objectclass=*`, `objectclass=oneclass`, or `'(&(sn=Baileys)(cn=Kalid Baileys))'`.
- Attribute value addition and replacement. It modifies all matched entries in bulk.

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

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

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

Note:

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

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

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

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

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

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

Syntax for `bulkmodify`

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

Arguments for bulkmodify

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (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.

filter

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

size

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

threads

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

debug

Optional. The debug option reports the logging level. This is useful in case the command runs into errors. The output is logged to the `bulkmodify.log` file. This file can be found under `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

encode

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

verbose

This is used to run the command in verbose mode.

Tasks and Examples for bulkmodify

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

- [Updating an Attribute for Multiple Entries at Once](#)

Updating an Attribute for Multiple Entries at Once

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

Example:

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

Limitations of bulkmodify

`bulkmodify` has the following limitations:

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

Related Command-Line Tools for bulkmodify

- See "[bulkdelete](#)" on page 3-1
- See "[bulkload](#)" on page 3-3
- See "[ldapmodify](#)" on page 3-31
- See "[ldapmodifymt](#)" on page 3-35

catalog

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

- An equality matching rule
- Matching rules supported by Oracle Internet Directory (see "[Matching Rules](#)" on page 6-4)

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

Note: The `catalog` command requires that the environment variable `ORACLE_INSTANCE` be set.

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

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

Syntax for catalog

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

Arguments for catalog

connect

Required. The directory database connect string. If you already have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (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 `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

verbose

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

Tasks and Examples for catalog

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

- [Indexing a Single Attribute](#)
- [Indexing Multiple Attributes](#)

- [Removing an Attribute from the List of Indexed Attributes](#)

Indexing a Single Attribute

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

Example:

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

Indexing Multiple Attributes

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

Example:

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

Removing an Attribute from the List of Indexed Attributes

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

Example:

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

Related Command-Line Tools for catalog

- N/A

ldapadd

The `ldapadd` command-line tool enables you to add entries, their object classes, attributes, and values to the directory. To add attributes to an existing entry, use the `ldapmodify` command, explained in "[ldapmodify](#)" on page 3-31.

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

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 dsm1_filename}
[-b] [-n] [-c [-o log_file_name]] [-M] [-v] [-O ref_hop_limit] [-i 1|0]
[-k|-K] [-U SSL_auth_mode {-W wallet_location -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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-Y "proxy_dn"

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

-p ldap_port

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 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 [Appendix A, "LDIF File Format"](#) on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See ["Adding Data to the Directory Using a DSML File"](#) on page 3-17 for more information about formatting a DSML file.

-b

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

-n

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

-c

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

-o log_file_name

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

-M

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

-v

Optional. Runs the tool in verbose mode.

-O ref_hop_limit

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

-i 1 | 0

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

-k | -K

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

-U SSL_auth_mode

Optional. The SSL authentication mode:

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

-W wallet_location

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

Example for UNIX:

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

Example for Microsoft Windows:

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-d *debug_level*

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

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

-E *character_set*

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

Tasks and Examples for ldapadd

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

- [Adding Data to the Directory Using an LDIF File](#)
- [Adding Data to the Directory Using a DSML File](#)
- [Previewing an Add Operation](#)

Adding Data to the Directory Using an LDIF File

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

Example:

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

Adding Data to the Directory Using a DSML File

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

Example:

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

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

Example:

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

Previewing an Add Operation

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

Example:

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

Related Command-Line Tools for ldapadd

- See "[ldapaddmt](#)" on page 3-17
- See "[ldapmodify](#)" on page 3-31
- See "[bulkload](#)" on page 3-3

ldapaddmt

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

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

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

Syntax for ldapaddmt

```
ldapaddmt -h oid_hostname -D "binddn" -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] [-k|-K] [-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-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 [Appendix A, "LDIF File Format"](#) on page A-1 for information on formatting an LDIF file.

Use the `-x` argument to supply a Directory Service Markup Language (DSML) file. See ["Adding Data to the Directory Using a DSML File"](#) on page 3-17 for more information about formatting a DSML file.

-b

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

-c

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

-M

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

-O *ref_hop_limit*

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

-k | -K

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

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

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

-W *wallet_location*

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

Example for UNIX:

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

Example for Microsoft Windows:

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-d *debug_level*

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

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

-E *character_set*

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

Tasks and Examples for ldapaddmt

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

- [Adding Concurrent Entries to the Directory Using an LDIF File](#)

Adding Concurrent Entries to the Directory Using an LDIF File

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

Example:

```
ldapaddmt -h myhost.company.com -D "cn=orcladmin" -q -T 5 -p 3060 \
```

```
-f ~/myfiles/input.ldif -v
```

Related Command-Line Tools for ldapaddmt

- See "ldapadd" on page 3-13
- See "bulkload" on page 3-3

ldapbind

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

Syntax for ldapbind

```
ldapbind -h oid_hostname -D "binddn" -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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-E character_set

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

Tasks and Examples for ldapbind

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

- [Validating Authentication Credentials](#)

Validating Authentication Credentials

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

Example:

```
ldapbind -h myhost.company.com -D "cn-orcladmin" -q -p 3133 \
-U 2 -W "file:/home/my_dir/my_wallet" -Q
```

Related Command-Line Tools for ldapbind

- N/A

ldapcompare

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

Syntax for ldapcompare

```
ldapcompare -h oid_hostname -D "binddn" -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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-Y "*proxy_dn*"

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

-p ldap_port

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-d debug_level

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

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

-E character_set

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

Tasks and Examples for ldapcompare

Using `ldapcompare` you can perform the following task:

- [Comparing Attribute Values for an Entry](#)

Comparing Attribute Values for an Entry

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

Example:

```
ldapcompare -h myhost.company.com -D "cn=orcladmin" -q -p 3060 -a title \
  -b "cn=Anne Smith,ou=Sales,o=IMC,c=US" -v "Manager"
```

Related Command-Line Tools for ldapcompare

- N/A

ldapdelete

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

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

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] [-k|-K]
[-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-Y "proxy_dn"

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

-p ldap_port

Optional. The port number used to connect to the Oracle Internet Directory server. Defaults to port 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 DN's you want to delete, or a single entry DN supplied on the command-line.

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

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

-n

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

-M

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

-v

Optional. Runs the tool in verbose mode.

-O *ref_hop_limit*

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

-k | -K

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

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

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

-W *wallet_location*

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

Example for UNIX:

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

Example for Microsoft Windows:

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-E character_set

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

Tasks and Examples for ldapdelete

Using `ldapdelete` you can perform the following tasks:

- [Deleting a Single Entry](#)
- [Deleting Multiple Entries Using an LDIF File](#)

Deleting a Single Entry

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

Example:

```
ldapdelete -h myhost.company.com -D "cn=orcladmin" -q \
  -p 3060 "cn=Anne Smith,ou=Sales,o=IMC,c=US"
```

Deleting Multiple Entries Using an LDIF File

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

Example:

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

Related Command-Line Tools for ldapdelete

- See [bulkdelete](#) on page 3-1

ldapmoddn

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

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

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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-E character_set

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

Tasks and Examples for ldapmoddn

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

- [Changing the RDN of an Entry](#)
- [Moving an Entry](#)

Changing the RDN of an Entry

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

Example:

```
ldapmoddn -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
  -b "cn=Mary Smith,dc=Americas,dc=IMC,dc=com" -R "cn=Mary Jones" -r
```

Moving an Entry

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

Example:

```
ldapmoddn -h myhost.company.com -D "cn=orcladmin" -q -p 3060 \
  -b "cn=Mary Smith,dc=Americas,dc=IMC,dc=com" -N "dc=Australia,dc=IMC,dc=com"
```

Related Command-Line Tools for ldapmoddn

- See "ldapmodify" on page 3-31

ldapmodify

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

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

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

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] [-k|-K]
[-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 will be 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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-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 [Appendix A, "LDIF File Format"](#) on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See ["Adding Data to the Directory Using a DSML File"](#) on page 3-17 for more information about formatting a DSML file.

-a

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

-b

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

-c

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

-n

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

-v

Optional. Runs the tool in verbose mode.

-o *log_file_name*

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

-M

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

-O *ref_hop_limit*

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

-i | 0

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

-k | -K

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

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

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

-W *wallet_location*

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

Example for UNIX:

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

Example for Microsoft Windows:

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-E *character_set*

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

-d *debug_level*

Optional. If not specified the default of 0 (not enabled) is used. Debug levels are additive. Add the numbers representing the functions that you want to activate, and use the sum of those in the command-line option. For example, to trace search filter

processing (512) and active connection management (256), enter 768 as the debug level (512 + 256 = 768). Debug levels are as follows:

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

Tasks and Examples for ldapmodify

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

- [Modifying the Directory Schema](#)
- [Modifying an Entry](#)

Modifying the Directory Schema

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

Example:

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

Modifying an Entry

To modify the attributes or attribute values for an entry, you must first prepare your LDIF file correctly. See "[LDIF Format for Modifying Entries](#)" on page A-4 for examples. Once you have a properly formatted LDIF file, you can use the `ldapmodify` tool to import the changes.

Example:

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

Related Command-Line Tools for ldapmodify

- See "[ldapadd](#)" on page 3-13

- See ["ldapdelete"](#) on page 3-25
- See ["ldapmoddn"](#) on page 3-28

ldapmodifymt

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

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

Syntax for ldapmodifymt

```
ldapmodifymt -h oid_hostname -D "binddn" -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] [-k|-K]
[-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-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 [Appendix A, "LDIF File Format"](#) on page A-1 for information on formatting an LDIF file.

Use the `-X` argument to supply a Directory Service Markup Language (DSML) file. See ["Adding Data to the Directory Using a DSML File"](#) on page 3-17 for more information about formatting a DSML file.

-a

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

-b

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

-c

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

-o *log_file_name*

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

-M

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

-O *ref_hop_limit*

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

-k | -K

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

-U *SSL_auth_mode*

Optional. The SSL authentication mode:

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

-W *wallet_location*

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

Example for UNIX:

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

Example for Microsoft Windows:

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-E *character_set*

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

-d *debug_level*

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

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

Tasks and Examples for ldapmodifymt

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

- [Modifying Multiple Entries Concurrently](#)

Modifying Multiple Entries Concurrently

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

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

Example:

```
ldapmodify -h myhost.company.com -D "cn=orcladmin" -w password -p 3060 \
-T 5 -f /home/myfiles/modify.ldif -v
```

Related Command-Line Tools for ldapmodifymt

- See "[ldapaddmt](#)" on page 3-17
- See "[ldapmodify](#)" on page 3-31

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 *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-Y "*proxy_dn*"

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

-p *ldap_port*

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

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

-F separator

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

-T [-]sort_attribute

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

-j page_size

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

-A

Optional. Retrieves attribute names only (no values).

-a never | always | search | find

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

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

-S attr

Optional. Sorts the results by the attribute specified.

-R

Optional. Disables the automatic following of referrals.

-i 1 | 0

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

-t

Optional. Writes files to `/tmp`.

-u

Optional. Includes user-friendly names in the output.

-L | -X

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

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: [Appendix A, "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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-d *debug_level*

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

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

-E *character_set*

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

-C

Optional. `ldapsearch -C` option causes `ldapsearch` to traverse a hierarchy and report direct memberships. The `ldapsearch -C` option essentially includes the `CONNECT_BY` control (2.16.840.1.113894.1.8.3) in the request sent to the client. `ldapsearch` doesn't have any means to pass values with a control. So, it sends the `CONNECT_BY` control without values. In this case the default values are assumed, that is, the hierarchy-establishing attribute name is obtained from the filter, and the number of

levels is 0. Thus, the `-C` option can only be used to fetch *all containers of a containee* queries, for example, fetch all groups of a user, fetch all employees of a manager and so forth. Also, all levels of the hierarchy are traversed. For more information refer to [Table 6-2, "Request Controls Supported by Oracle Internet Directory"](#).

See Also: The "Performing Hierarchical Searches" section in Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management

Tasks and Examples for ldapsearch

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

- [Performing a Base Object Search](#)
- [Performing a One-Level Search](#)
- [Performing a Subtree Search](#)
- [Searching for Attribute Values of Entries](#)
- [Searching for Entries with Attribute Options](#)
- [Searching for All User Attributes and Specified Operational Attributes](#)
- [Searching for Entries \(More Examples\)](#)

Performing a Base Object Search

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

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

Example:

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

Performing a One-Level Search

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

Example:

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

Performing a Subtree Search

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

Example:

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

Searching for Attribute Values of Entries

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

Example:

```
ldapsearch -p 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
```

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"
```

Searching for All User Attributes and Specified Operational Attributes

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

Example:

```
ldapsearch -p 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.

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" 
```

Related Command-Line Tools for `ldapsearch`

- See "[ldapcompare](#)" on page 3-23
- See "[catalog](#)" on page 3-11

ldifmigrator

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

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

Syntax for `ldifmigrator`

```
ldifmigrator "input_file=filename" "output_file=filename"
[-lookup -h oid_hostname -D "binddn" -w password [-p ldap_port]
```

```
[subscriber=subscriberDN] ["s_VariableName1=replacement_value"  
"s_VariableName2=replacement_value"...]  
[-load -reconcile SAFE|SAFE_EXTENDED|NORMAL]
```

Arguments for ldifmigrator

"input_file=filename"

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

"output_file=filename"

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

-lookup

If this flag is specified, then values of certain substitution variables will be obtained by looking up the correct values in the directory server. See ["Substitution Variables for Migration Input Files"](#) on page A-6 for a list of substitution variables that can be looked up.

-h oid_hostname

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

-D "binddn"

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

subscriber=subscriberDN

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

"s_VariableName=replacement_value"

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

-load

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

-reconcile SAFE | SAFE_EXTENDED | NORMAL

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

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

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

Tasks and Examples for Ldifmigrator

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

- [Using the Data Migration Tool in Lookup Mode](#)
- [Overriding Data Migration Values in Lookup Mode](#)
- [Using the Data Migration Tool by Supplying Your Own Values](#)
- [Loading and Reconciling Data Using the Data Migration Tool](#)

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

Using the Data Migration Tool in Lookup Mode

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

Example:

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

Overriding Data Migration Values in Lookup Mode

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

Example:

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

Using the Data Migration Tool by Supplying Your Own Values

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

Example:

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

Loading and Reconciling Data Using the Data Migration Tool

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

Example:

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

Related Command-Line Tools for ldifmigrator

- See "[ldapadd](#)" on page 3-13
- See "[ldapmodify](#)" on page 3-31
- See "[ldifwrite](#)" on page 3-49

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 ORACLE_INSTANCE not defined	ORACLE_INSTANCE is not defined.	Set the environment variable ORACLE_INSTANCE
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 <code>-help</code> 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 <code>-help</code> 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 <code>-help</code> option to print the usage.
The specified input file does not exist	The specified file location is invalid.	Check the input file path

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

Message	Reason	Remedial Action
Check the input file. Zero byte input file	The input file does not contain any entries.	Provide a valid file with pseudo LDIF entries
Cannot create the output file. Output file already exists	The output file already exists	Check the Output_File flag
Access denied, cannot read from the input file	The specified input file does not have read permission	Check the read permission of the input file.
Access denied, cannot create the output file	You do not have permission to create the output file.	Check the permission of the directory under which the output file needs to be created.
Directory server name not specified. When -lookup option is used the host parameter should be specified	When the -lookup option is specified, the host parameter is mandatory.	Specify the host parameter.
Bind Dn parameter name not specified. When -lookup option is used the dn parameter should be specified	When the -lookup option is specified, the DN parameter is mandatory.	Specify the DN parameter.
The port number specified is invalid	The port number should be a numeric value.	Check the port number parameter
Unable to establish connection to directory. Please verify the input parameters: host, port, dn & password	The directory server may not be running on the specified host and port, or credentials may be invalid.	Check the host, port, DN and password parameters. Check <code>ORACLE_INSTANCE/diagnostics/logs/OID/tools/</code> .
Naming exception occurred while retrieving the subscriber information from the directory. Please verify the input parameters	The specified identity management realm does not exist in the directory	Check the realm parameter
Not all the substitution variables are defined in the directory server specified	If the identity management realm entry does not contain the required attributes, then this error occurs.	Check the realm entry in the directory
Error occurred while migrating LDIF data to Oracle Internet Directory	This might occur if something goes wrong in the middle of a process—for example, a failure of the directory server or disk.	Report the error message to the administrator

When an error condition occurs, the log messages are logged to this file:

`ORACLE_INSTANCE/ldap/install/LDIFMig_YYYY_MM_DD_HH_SS.log`.

ldifwrite

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

Note: The `ldifwrite` command requires that the environment variable `ORACLE_INSTANCE` 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.

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 `ORACLE_INSTANCE/config`. (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 `ORACLE_INSTANCE/diagnostics/logs/OID/tools`.

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

Tasks and Examples for ldifwrite

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

- [Converting All Entries under a Naming Context to an LDIF File](#)
- [Converting a Partial Naming Context to an LDIF File](#)
- [Converting Entries that Match Criteria to an LDIF File](#)

Converting All Entries under a Naming Context to an LDIF File

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

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

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

When prompted for the Oracle Internet Directory password, enter the password of the ODS database user account.

Example:

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

Converting a Partial Naming Context to an LDIF File

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

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

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

Example:

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

Converting Entries that Match Criteria to an LDIF File

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

Example:

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

Related Command-Line Tools for Idifwrite

- ["ldapsearch"](#) on page 3-38
- ["ldifmigrator"](#) on page 3-45
- ["bulkload"](#) on page 3-3

upgradecert.pl

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

Before running the `upgradecert.pl` tool:

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

```
perl -version
```

3. Make sure that the environment variable `PERL5LIB` is set to the proper PERL library location.
4. Check that you can run `ldapmodify` and `ldapsearch` from your command prompt.
5. Determine whether you have enough disk space to run the tool. The amount of disk space required depends upon the number of certificates stored.

Syntax for upgradecert.pl

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

Arguments for upgradecert.pl

-h *oid_hostname*

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

-D "*binddn*"

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

-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 ["Using Passwords with Command-Line Tools"](#) on page 1-1.

-t temp_dir

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

Tasks and Examples for upgradecert.pl

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

- [Upgrading User Certificates Stored in the Directory from Releases Prior to 10.1.2](#)

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

Example:

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

Related Command-Line Tools for upgradecert.pl

- N/A

Oracle Internet Directory Replication Management Tools

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

- [ManageHiq.retry](#) and [ManageHiq.purge](#) (Human Intervention Queue Management Tools)
- [oidcmprec](#) (Oracle Internet Directory Compare and Reconcile Tool)
- [remtool](#) (Replication Environment Management Tool)

See Also: The replication chapters in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

ManageHiq.retry and ManageHiq.purge

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 "[oidcmprec](#)" on page 4-3)
3. Either place the change back into the retry queue, by using `ManageHiq.retry`, or into the purge queue, by using `ManageHiq.purge`.

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 will impact 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=osldlapd,cn=subconfigsentry
```

Syntax for ManageHq.retry and ManageHq.purge

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

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

```
$ sqlplus /nolog
SQL> connect ods;
SQL> Enter password
SQL> Set serveroutput ON
SQL> ManageHq.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.

Examples for ManageHq.retry

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

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

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

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

or

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

Examples for ManageHiq.purge

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

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

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

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

Or

```
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

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

oidcmprec

The Compare and Reconcile Tool allows you to compare one Oracle Internet Directory with another, detect conflicts or discrepancies, and optionally resolve them. The directories being compared can be standalone directories or part of the same replication group. You can compare two individual entries, subtrees, or entire directories. You can also compare directory schema.

See Also: The section "Comparing and Reconciling Inconsistent Data by Using oidcmprec" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

The `oidcmprec` tool can detect and resolve the following conflict scenarios:

- Entry only in source directory (`entos`)
- Entry only in destination directory (`entod`)
- Attribute only in source directory (`atros`)
- Attribute only in destination directory (`atrod`)
- Single-valued attribute differs (`svatrdif`)
- Multi-valued attribute differs (`mvatrdif`)
- Entry DN differs (`dndif`)

The `oidcmprec` tool can also detect and resolve the following schema conflict scenarios:

- Object class definition exists only in source directory (`odefos`)
- Object class definition exists only in destination directory (`odefod`)
- Object class definition different in source and destination directory (`odefdif`)
- Attribute definition exists only in source directory (`adefos`)
- Attribute definition exists only in destination directory (`adefod`)
- Attribute definition different in source and destination directory (`adefdif`)

Syntax for oidcmprec

```

oidcmprec operation=compare | reconcile | merge | merge_dryrun | userdefinedcr
source=host:port
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] ]
[ entos=ignore | add | del | log2add | log2del | log ]
[ atod=ignore | add | del | log2add | log2del | log ]
[ atos=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 for oidcmprec

operation=compare | reconcile | merge | merge_dryrun | userdefinedcr

Required. The `operation` to perform. The `operation` argument can take the following values:

- `compare`: Compares the two directories, reports conflicts, and logs the changes that 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.

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 DN 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"](#) on page 4-21.

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"](#) on page 4-21.

dns2exclude=" 'edn1' 'edn2' 'edn3' ..."

Optional. Specifies DN's that are to be excluded from the comparison operation. These DN's must be child entries or subtrees of the DN's 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 DN's specified in the `base` argument are compared. This is the default value.
- `subtree`: Directory information trees (DITs) identified by the DN's specified in the `base` argument are compared.
- `onelevel`: Only the immediate children of the DN's 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 DN's that must be compared.

One DN thread is created, by default. The total number of DN threads and worker threads cannot exceed $6 * \text{Number of CPUs} - 2$. If the total number of DN threads and worker threads exceeds the maximum value, the tool reduces both values proportionately to $6 * \text{Number of CPUs} - 2$.

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 `exclattr`/`inclattr`, 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`.

The option allows limited pattern matching. You can use `attributename*` to match all attributes starting with `attributename`. You can also use `attributename;*` to match all subtypes of `attributename`.

compareby=tool | ldapserver

Optional. Specifies whether the `compare` operation is performed by the `tool` or `ldapserver`. A `compare` operation performed by the `tool` is several times faster than a `compare` operation performed by `ldapserver`.

filename=file_name

Optional. Specifies a base name for the report files that would be generated by the tool. Do not specify an extension with the file name. The tool generates the following files:

- `file_name.rpt`: This file contains the DNs of all entries compared and the compare results. This file is known as the `rpt` file.
- `file_name.s2d.ldif`: This file contains all changes that were applied (or to be applied) to the destination directory. `s2d` stands for source directory to destination directory. This file is known as the `s2d` file.
- `file_name.d2s.ldif`: This file contains all changes that were applied (or to be applied) to the source directory. `d2s` stands for destination directory to source directory. This file is known as the `d2s` file.
- `file_name.eos.rpt`: This file lists DNs of entries that exist only in the source directory. `eos` stands for entries available only in the source directory. This file is known as the `eos` file.
- `file_name.eod.rpt`: This file lists DNs of entries that exist only in the destination directory. `eod` stands for entries available only in the destination directory. This file is known as the `eod` file.
- `file_name.dif.rpt`: This file lists the DNs that are different in the source and destination directories along with the names of the DN attributes that differ. This file is known as the `dif` file.
- `file_name.err`: This file contains all the error messages. It is known as the `err` file.

genchlog=d[efault] | t[rue] | f[alse]

Optional. Determines whether a change log is created for the changes made by the `oidcmprec` tool. The `genchlog` 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 `orclldiprepository` 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 `genchlog`.
- `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[true] | f[false]

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[true] | f[false]

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[true] | f[false]

Optional. Determines whether the tool prompts the user for confirmation before performing the specified operation. The default value is `false`. When set to `true`, the tool will not prompt the user for confirmation before performing the specified operation.

contonerr=t[true] | f[false]

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[true] | f[false]

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[true] | f[false]

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[true] | f[false]

Optional. Controls whether the tool generates the `file_name.d2s.ldif` file. The `logd2s` 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[true] | f[false]

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[true] | f[false]

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[true] | f[false]

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[true] | f[false]

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[true] | f[false]

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

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 nonreplication environments. If the GUID values are the same in both directories, then the source directory wins.
- `log2usesmallguid`: Same as `usesmallguid` except that the change is logged into an LDIF file and not directly effected in the directory.
- `usebigguid`: Check the GUID value to determine if the attribute should be deleted from the directory or added to the peer directory. The directory with the bigger GUID value wins. The GUID values would be the same in the same replication group. This rule is intended for nonreplication environments. If the GUID values are the same in both directories, then the source directory wins.
- `log2usebigguid`: Same as `usebigguid` except that the change is logged into an LDIF file and not directly effected in the directory.
- `log`: Log the conflict in the report file and take no other action.

The default value depends on the operation specified. [Table 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
<code>compare</code>	<code>log2add</code>
<code>reconcile</code>	<code>add</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2delete</code>
<code>reconcile</code>	<code>delete</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

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
<code>compare</code>	<code>log2usesrc</code>
<code>reconcile</code>	<code>usesrc</code>
<code>merge</code>	<code>usesrc</code>
<code>merge_dryrun</code>	<code>log2usesrc</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2usesrc</code>
<code>reconcile</code>	<code>usesrc</code>
<code>merge</code>	<code>merge</code>
<code>merge_dryrun</code>	<code>log2merge</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2usesrc</code>
<code>reconcile</code>	<code>usesrc</code>
<code>merge</code>	<code>log2usesrc</code>
<code>merge_dryrun</code>	<code>usesrc</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2add</code>
<code>reconcile</code>	<code>add</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2add</code>
<code>reconcile</code>	<code>add</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2del</code>
<code>reconcile</code>	<code>del</code>
<code>merge</code>	<code>add</code>
<code>merge_dryrun</code>	<code>log2add</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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
<code>compare</code>	<code>log2usesrc</code>
<code>reconcile</code>	<code>usesrc</code>
<code>merge</code>	<code>usesrc</code>
<code>merge_dryrun</code>	<code>log2usesrc</code>
<code>userdefinedcr</code>	<code>ignore</code>

`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.

Tasks and Examples for `oidcmprec`

This section provides examples for tasks that can be performed using the `oidcmprec` command. The following examples discuss various operations that can be performed with the `oidcmprec` tool:

- [Comparing and Reconciling Individual Entries in Two Directories](#)
- [Comparing and Reconciling Subtrees in Two Directories](#)
- [Comparing and Reconciling Entire Directories](#)
- [Performing User-Defined Compare and Reconcile Operations](#)
- [Merging Two Directories](#)
- [Including and Excluding Attributes](#)
- [Overriding Default Conflict Resolution Rules](#)
- [Using a Parameter File](#)
- [Generating Change Logs](#)
- [Performing Directory Schema Operations](#)

Comparing and Reconciling Individual Entries in Two Directories

This example compares the DN, "cn=Anne Smith, cn=users, dc=uk, dc=acme, dc=com", in the source and destination directories. The default conflict resolution rules for the `compare` operation are used. You are prompted for the source directory and destination directory passwords.

Example

```
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 :
```

The following example compares the DN, cn=Anne Smith, cn=users, dc=uk, dc=acme, dc=com, in the source and destination directories. It resolves the conflicts that are detected. The default conflict resolution rules for the `reconcile` operation are used.

Example

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

Comparing and Reconciling Subtrees in Two Directories

This example compares the naming context, dc=com, in the two directories. The `scope` attribute has been set to `subtree`. This allows the entire directory information tree (DIT) under the base DN, dc=com, to be compared. The `threads` and `dnThreads` arguments specify the number of worker threads and DN threads. The `cmpres` file is used to store the report for the operation.

Example

```
oidcmprec base="'dc=com'" \  
          operation=compare scope=subtree \  
          source=myhost1.mycom.com:3060 \  
          destination=myhost2.mycom.com:3060 \  
          threads=5 dnthreads=2 filename=cmpres
```

The following example performs the `reconcile` operation on two subtrees namely, dc=com and dc=org. The `dns2exclude` argument is used to exclude the c=us, dc=mycom, dc=com and c=uk, dc=myorg, dc=org subtrees from the operation.

Example

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

Comparing and Reconciling Entire Directories

The following example compares a directory residing on `host1` with another directory residing on `host2`. The base argument is set to "" and the scope argument is set to `subtree`.

Example

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

The following example reconciles a directory residing on `myhost1` with another directory residing on `myhost2`. Entire directories are compared except the DN, `c=us,dc=mycom,dc=com`.

Example

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

Note: When you compare entire directories, the following DNs and their subtrees are excluded:

- root DSE entry
- cn=auditlog
- cn=baseschema
- cn=catalogs
- cn=events
- cn=oracle internet directory
- cn=replication configuration
- cn=server configuration
- cn=subconfigsubentry
- cn=subregistrysubentry
- cn=subschemasubentry

You can include these entries by specifying them explicitly in the base argument.

Performing User-Defined Compare and Reconcile Operations

This example makes use of user-defined values for the `-entos`, `-entod`, `-atros`, `-svatrdif`, `-mvatrdif`, and `-dndif` arguments. Conflict resolution arguments not specified on the command line, like `-atrod`, are set to `ignore`.

Example

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

```
entos=add entod=ignore atros=add \  
svatrdif=usesrc mvatrdif=usesrc dndif=ignore \  
threads=5 dnthreads=2 file=myreconcile
```

Merging Two Directories

This example synchronizes the `dc=com` subtree in two directories. The merge operation updates both the source and destination directories.

Example

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

Including and Excluding Attributes

The following example performs a compare operation. It uses the `exclattr` argument to exclude the `orclguid`, `category`, `userpassword`, and `authpassword` attributes. The example makes use of wildcard pattern matching to exclude the `authpassword` attribute subtypes.

Example

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

Example

```
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=cmp
```

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

Example

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

Using a Filter

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

Example

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

```
filter="'(cn=*)'"
```

Overriding Default Conflict Resolution Rules

This example performs a compare operation on two directories. It overrides the default conflict resolution rules used for the `dndif` and `mvatrdif` arguments. The conflict resolution rule for these arguments is set to ignore.

Example

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

Using a Parameter File

This example performs a compare operation on two directories. It uses a parameter file, `comp_param` to specify command-line arguments. The `dnThreads` argument is specified both in the file and at the command line. The command-line value of `dnThreads` overrides the value specified in the parameter file.

Example

```
oidcmprec paramfile=comp_param dnthreads=3
```

The following displays the parameter file that is used:

```
#####
#Parameter file for compare and reconcile tool
#Creator   : John
#Date      : 21-Mar-2006
#File Name : comp_param
#####
operation=compare
source=staqj13:3060
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
```

Using a Parameter File in XML Format

This example performs a compare operation on two directories.

Example

```
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>
    <password>password</password>
    <isSSLPort>>false</isSSLPort>
  </source>
- <destination>
  <host>stadd54</host>
  <port>3060</port>
  <password>password</password>
  <isSSLPort>>true</isSSLPort>
</destination>
<base>cn=oraclecontext</base>
<base>o=apple</base>
<dns2exclude>cn=test instance,cn=oraclecontext</dns2exclude>
<dns2exclude>ou=support,o=apple</dns2exclude>
<scope>subtree</scope>
<filter />
<threads>1</threads>
<dnthreads>1</dnthreads>
<inclattr />
<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.

Generating Change Logs

The following example uses the `genchglog` argument to ensure that change logs are generated for the operation. When `genchglog` is set to `true`, change logs are generated at both the source and destination directories.

Example

```

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

```

Performing Directory Schema Operations

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

Example

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

remtool

The Replication Environment Management Tool is used to manage Oracle Internet Directory replication configuration activities.

More specifically, the Replication Environment Management tool:

- Configures Oracle Database Advanced Replication-based multimaster replication.
- Scans the replication environment and verifies an Oracle Database Advanced Replication-based directory replication group (DRG).
- Rectifies any problems in an Oracle Database Advanced Replication-based DRG. If the tool cannot rectify a problem, it reports the point or points of failure, which you can then fix manually.
- Reports queue statistics, deferred transactions errors, and administrative request errors of an Oracle Database Advanced Replication-based DRG.
- Reconfigures the Oracle Database Advanced Replicationbased DRG.
- Configures LDAP-based replication.
- Reconfigures an LDAP-based directory replication group (DRG).

See Also: The section "Managing and Monitoring Replication by Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Syntax for remtool

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

```
operation := { -addnode      | -asrsetup   | -chgpwd    | -delnode   |
               -asrcleanup  | -asrverify  | -asrrectify| -asrdisplay|
               -dispqstat   | -suspendasr| -resumeasr | -asr2ldap  |
               -dispasrerr  | -paddnode  | -pdelnode  | -pcleanup  |
               -pchgpwd    | -pdisplay  | -pchgmaster [ -multimaster] |
               -pchgwlpwd  | -pdispqstat| -pverify   | -presetpwd | }
```

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

```
                        -connect repl_admin_name@net_service_name }
```

Terminology Used in remtool Argument Descriptions

In an Oracle Database Advanced Replication-based Directory Replication Group (DRG), one node must be identified as the Master Definition Site (MDS). This is the group master. All other nodes in the DRG are termed Remote Master Sites (RMS).

ODS.ASR_CHG_LOG and ODS.ODS_CHG_STAT are tables in Oracle Internet Directory's underlying database that store changelog information. The directory uses change logs to keep track of entries that are being replicated or that are being synchronized by the Oracle Directory Integration and Provisioning.

Arguments for remtool

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:

- `-addnode` - Adds a new node to an Oracle Database Advanced Replication-based directory replication group (DRG). See "[The remtool -addnode Operation](#)" on page 4-27 for more information about this operation.
- `-asrsetup` - Creates a new directory replication group (DRG) by configuring Oracle Database Advanced Replication. See "[The remtool -asrsetup Operation](#)" on page 4-32 for more information about this operation.
- `-chgpwd` - Changes the replication administrator's database account password on all nodes of an Oracle Database Advanced Replication-based DRG. See "[The remtool -chgpwd Operation](#)" on page 4-39 for more information about this operation.
- `-delnode` - Deletes a node from an existing Oracle Database Advanced Replication-based DRG. See "[The remtool -delnode Operation](#)" on page 4-40 for more information about this operation.
- `-asrcleanup` - Cleans up the set up of an Oracle Database Advanced Replication-based DRG. See "[The remtool -asrcleanup Operation](#)" on page 4-29 for more information about this operation.
- `-asrverify` - Verifies the setup of Oracle Database Advanced Replication-based DRG, and reports any problems found. See "[The remtool -asrverify Operation](#)" on page 4-35 for more information about this operation.
- `-asrrectify` - Verifies the setup of Oracle Database Advanced Replication-based DRG, and corrects any problems found. See "[The remtool -asrverify Operation](#)" on page 4-35 for more information about this operation.
- `-asrdisplay` - Display all replica details in the replication group for an Oracle Database Advanced Replication-based setup.
- `-dispqstat` - Displays the queue statistics of all nodes in an Oracle Database Advanced Replication-based DRG. See "[The remtool -dispqstat Operation](#)" on page 4-44 for more information about this operation.
- `-suspendasr` - Suspends replication activity for an Oracle Database Advanced Replication-based DRG. See "[The remtool -suspendasr Operation](#)" on page 4-64 for more information about this operation.
- `-resumeasr` - Resumes replication activity for an Oracle Database Advanced Replication-based DRG. See "[The remtool -resumeasr Operation](#)" on page 4-63 for more information about this operation.

- `-asr2ldap` - Converts an existing Oracle Database Advanced Replication-based agreement to an LDAP multimaster agreement.
- `-dispasrerr` - Displays all deferred transaction errors and administrative request errors for an Oracle Database Advanced Replication-based DRG. See "[The remtool -dispasrerr Operation](#)" on page 4-42 for more information about this operation.
- `-paddnode` - Adds a partial replica to an LDAP-based DRG. See "[The remtool -paddnode Operation](#)" on page 4-45 for more information about this operation.
- `-pdelnode` - Deletes a partial replica from an LDAP-based DRG. See "[The remtool -pdelnode Operation](#)" on page 4-56 for more information about this operation.
- `-pcleanup` - Cleans up the partial replication setup of an LDAP-based DRG. See "[The remtool -pcleanup Operation](#)" on page 4-54 for more information about this operation.
- `-pchgpwd` - Changes the password of a replication DN for a replica in an LDAP-based DRG. See "[The remtool -pchgpwd Operation](#)" on page 4-52 for more information about this operation.
- `-pdisplay` - Displays all replica details in a partial replication group. See "[The remtool -pdisplay Operation](#)" on page 4-49 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 "[The remtool -pchgmaster Operation](#)" on page 4-49 for more information about this operation.
- `-pchgwalpwd` - Changes the wallet password of a replication DN for a replica in an LDAP-based DRG. See "[The remtool -pchgwalpwd Operation](#)" on page 4-53 for more information about this operation.
- `-pdispqstat` - Displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. See "[The remtool -pdispqstat Operation](#)" on page 4-58 for more information about this operation.
- `-pverify` - Verifies the replication configuration for a DRG node that uses LDAP-based replication. See "[The remtool -pverify Operation](#)" on page 4-60 for more information about this operation.
- `-presetpwd` - Resets the password of a replication DN for a replica in an LDAP-based DRG. See "[The remtool -presetpwd Operation](#)" on page 4-59 for more information about this operation.
- `-pilotreplica` - Begins or ends pilot mode for a replica. See "[The remtool -pilotreplica Operation](#)" on page 4-59 for more information about this operation.
- `-backupmetadata` - Adds the metadata of a pilot replica to a master replica or backs up the metadata of a pilot replica into a file. This operation must be executed at the pilot replica. See "[The remtool -backupmetadata Operation](#)" on page 4-37 for more information about this operation.

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 "[The -bind Connection Argument](#)" on page 4-65 for more information.
- `-connect` - Used with Oracle Database Advanced Replication-based replication options to specify the connection string for the master definition site (MDS) or the Remote Master Site (RMS). See "[The -connect Connection Argument](#)" on page 4-65 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 `ORACLE_INSTANCE/OID/log`.

The remtool -asr2ldap Operation

If there is an existing Oracle Database Advanced Replication-based agreement between two or more nodes, you can convert this agreement to an LDAP multimaster agreement by using the `asr2ldap` operation.

Syntax for remtool -asr2ldap

```
remtool -asr2ldap
```

Arguments for remtool -asr2ldap

The tool prompts you for information, as shown in the example.

Tasks and Examples for remtool -asr2ldap

Using the `asr2ldap` operation, you can perform the following tasks:

- [Converting an Oracle Database Advanced Replication-Based Agreement to an LDAP-Based Agreement](#)

Converting an Oracle Database Advanced Replication-Based Agreement to an LDAP-Based Agreement

Example:

```
remtool -asr2ldap
```

The results are:

```
Enter replication administrator's name      : repadmin

Enter replication administrator's password  :
Enter global name of MDS                   : inst1.regress.rdbms.dev.example.com

Directory Replication Group (DRG) details :

-----
Instance Host Name      Global Name              Version      ReplicaId    Site
Name                                                            OID          Type
-----
tst1      stacu14                INST1.REGRESS.RDBMS.DEV 11.1.1.0.   stacu14_tst1 MDS
tst12     stacu14                INST2.REGRESS.RDBMS.DEV 11.1.1.0.   stacu14_tst12 RMS
-----
Do you want to continue? [y/n] : y
```

```

-----
Migrating ASR agreement to LDAP MM agreement...

Enter "SYSTEM" user password for "INST2.REGRESS.RDBMS.DEV.EXAMPLE.COM" database at
"stacu14" host :
Enter "SYSTEM" user password for "INST1.REGRESS.RDBMS.DEV.example.com" database at
"stacu14" host :
-----
ASR setup has been cleaned up.
-----

```

The remtool -addnode Operation

The `addnode` operation adds a new node to an existing directory replication group (DRG). You must first create the DRG using "[The remtool -addnode Operation](#)" on page 4-27. The following usage rules apply to this operation:

- The node to be added must be empty.
- You must know the SYSTEM user password of the new node.
- Oracle Internet Directory processes on the master definition site (MDS) and other remote master sites (RMSs) must be down.
- After the `addnode` operation is complete, Oracle Internet Directory processes can be restarted.

Syntax for remtool -addnode

```
remtool -addnode [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -addnode

The tool will also prompt you for the database global name (as defined in the `tnsnames.ora` file) and SYSTEM password for each node to be added.

-connect repl_admin_name@net_service_name

For more information, see "[The -connect Connection Argument](#)" on page 4-65.

Tasks and Examples for remtool -addnode

Using the `addnode` operation you can perform the following tasks:

- [Adding a New Node to an Oracle Database Advanced Replication-based DRG](#)

Adding a New Node to an Oracle Database Advanced Replication-based DRG In this example, `MY_HOST3.MY_COMPANY.COM` is added to a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

Example:

```
remtool -addnode -v -connect repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :

```

```

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
-----

```

```

Name                                                                                               Type
-----
rid2      my_host      MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0 my_host_rid2  RMS
-----

```

Do you want to continue? [y/n] : y

WARNING:

Make sure that the replication administrator database account does not exist already in the new node to be added to the DRG. If the account exists, that account will be dropped and will be created newly.

Enter global name of new node to be added : MY_HOST3.MY_COMPANY.COM

Enter SYSTEM user password of new node to be added :

Adding a new node...

```

MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Creating purge job...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST3.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...

```

```

MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST3.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST3.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST3.MY_COMPANY.COM : "my_host_rid3" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST3.MY_COMPANY.COM : Verifying initialization parameter...

```

```

-----
Node MY_HOST3.MY_COMPANY.COM has been added to this DRG.
-----

```

```

Directory Replication Group (DRG) details :

```

```

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                           Type
-----
rid1      my_host                  MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2      my_host                  MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
rid3      my_host                  MY_HOST3.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid3  RMS
-----

```

The remtool -asrcleanup Operation

The `asrcleanup` operation cleans up an existing Oracle Database Advanced Replication-based setup. You must know the system password of all nodes taking part in the directory replication group (DRG) to run this operation.

Syntax for remtool -asrcleanup

```
remtool -asrcleanup [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -asrcleanup

The tool prompts you for the SYSTEM user password for each MDS and RMS node in the DRG

-connect repl_admin_name@net_service_name

For more information, see "[The -connect Connection Argument](#)" on page 4-65.

Tasks and Examples for remtool -asrcleanup

Using the asrcleanup operation you can perform the following tasks:

- [Cleaning Up an Oracle Database Advanced Replication-based DRG Setup](#)

Cleaning Up an Oracle Database Advanced Replication-based DRG Setup In this example, setup is cleaned up for a DRG consisting of MY_HOST1.MY_COMPANY.COM and MY_HOST2.MY_COMPANY.COM. The tool prompts you to enter the system password for each site.

Example:

```
remtool -asrcleanup -v
```

The results are:

```
Enter replication administrator's name      : repadmin
```

```
Enter replication administrator's password :
```

```
Enter global name of MDS                   : my_host1.my_company.com
```

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
```

```
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
```

```
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                                            Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

```
Do you want to continue? [y/n] : y
```

```
-----
Cleaning up...
```

```
MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST2.MY_COMPANY.COM from
replication group LDAP_REP...
```

```
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
```

```
MY_HOST2.MY_COMPANY.COM : Unscheduling push job to MY_HOST1.MY_COMPANY.COM...
```

```
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
```

```
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
```

```
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
```

```
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
```

```
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
```

```
MY_HOST1.MY_COMPANY.COM : Unscheduling push job to MY_HOST2.MY_COMPANY.COM...
```

```
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MYCOMPANY.COM...
```

```

MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST1.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
-----
ASR setup has been cleaned up.
-----

```

The remtool -asrrectify Operation

The `asrrectify` operation is used for detecting and rectifying problems in an Oracle Database Advanced Replication-based DRG setup. It reports on errors and corrects them. Oracle Corporation recommends that, before running this operation, you stop Oracle Internet Directory servers.

To use the `asrrectify` operation, all nodes in the DRG must be up and running. The operation will fail if any of the nodes are not running.

If necessary, the `asrrectify` operation prompts for the SYSTEM user password.

Syntax for remtool -asrrectify

```
remtool -asrrectify [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -asrrectify

The tool may also prompt you for the SYSTEM user password for each MDS and RMS node in the DRG.

-connect repl_admin_name@net_service_name

For more information, see "[The -connect Connection Argument](#)" on page 4-65.

Tasks and Examples for remtool -asrrectify

Using the `asrrectify` operation you can perform the following tasks:

- [Detecting and Correcting Errors in an Oracle Database Advanced Replication-Based DRG Setup](#)

Detecting and Correcting Errors in an Oracle Database Advanced Replication-Based DRG Setup

In this example, setup errors are deducted and rectified in a DRG consisting of MY_HOST1.MY_COMPANY.COM and MY_HOST2.MY_COMPANY.COM. The tool detects that a user has changed global name of MY_HOST2.MY_COMPANY.COM to NEWNAME.MY_COMPANY.COM after setting up Advanced Replication. It rectifies this error first before continuing with other checks.

Example:

```
remtool -asrrectify -v -conn repadmin@my_host1.my_company.com
```

The results are:

```

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
Enter "SYSTEM" user password for "MY_HOST2.MY_COMPANY.COM" database at "my_host"
host :
NEWNAME.MY_COMPANY.COM : Renaming global name to MY_HOST2.MY_COMPANY.COM (instance
name : rid2, hostname : my_host)
CORRECTED:
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has
been changed to MY_HOST2.MY_COMPANY.COM.

```

```

MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
CORRECTED:
MY_HOST2.MY_COMPANY.COM : Global name of database "rid2" at host "my_host" has
been changed to MY_HOST2.MY_COMPANY.COM.
Directory Replication Group (DRG) details :

-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                                    Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----

Do you want to continue? [y/n] : y

-----
Rectifying ASR setup...

MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

-----
DB Name          Init   Repl   DB    Purge  Sch.   Repl   Repl
                  Param Admin Links Job    Links Group Agrmt
                  Role
-----
MY_HOST1.MY_COMPANY. Chkd  Chkd  Chkd  Chkd  Chkd  Chkd  Chkd
MY_HOST2.MY_COMPANY. Chkd  Chkd  Chkd  Chkd  Chkd  Chkd  Chkd
-----

Legends :
  Chkd - Checked. No errors.
  Crtd - ASR setup errors were found and corrected.
  Err  - Error occurred while doing ASR setup verification.
  NCrtd - ASR setup has errors, but not corrected.
-----

```

The remtool -asrsetup Operation

The asrsetup operation is used to create a new Oracle Database Advanced Replication-based directory replication group (DRG). A DRG consists of a master definition site (MDS) and one or more remote master sites (RMS).

Before you begin, stop all Oracle Internet Directory server processes on the MDS and RMS sites. After the setup operation is completed, you can restart all Oracle Internet Directory processes and replication server processes.

Syntax for remtool -asrsetup

```
remtool -asrsetup [-v]
```

Arguments for remtool -asrsetup

Only the optional `-v` argument is specified on the command-line. The tool prompts you for the following information.

- The database global name of the MDS (as defined in the `tnsnames.ora` file).
- A replication administrator password for the MDS
- The SYSTEM password for the MDS
- The database global for each RMS (as defined in the `tnsnames.ora` file).
- The SYSTEM password for each RMS

Tasks and Examples for remtool -asrsetup

Using the `asrsetup` operation you can perform the following tasks:

- [Creating an Oracle Database Advanced Replication-based DRG](#)

Creating an Oracle Database Advanced Replication-based DRG In this example, a DRG is created consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

Example:

```
remtool -asrsetup -v
```

The results are as follows:

```
-----
ASR Setup for OID Replication
WARNING:
Make sure that the replication administrator that you
enter below does not exist already in any of the nodes
that will be part of the DRG to be created now. If the
user exists, that user will be dropped and will be
created newly.
-----
Enter replication administrator's name      : repadmin

Enter replication administrator's password :
Reenter replication administrator's password :
Enter Master Definition Site (MDS) details :
Enter global name of MDS                  : MY_HOST1.MY_COMPANY.COM

Enter SYSTEM user password of MDS         :
Enter Remote Master Site (RMS) details    :
Enter global name of RMS # 1              : MY_HOST2.MY_COMPANY.COM

Enter SYSTEM user password of MDS         :
Are there more Remote Master Sites in the group? [y/n/q] : n

Verify the details you had entered.
```

```
-----
Replication administrator's name      : repadmin
Master Definition Site                 : MY_HOST1.MY_COMPANY.COM
Remote Master Site # 1                 : MY_HOST2.MY_COMPANY.COM
Are these details correct? [y/n/q] : y
-----

ASR setup in progress...

MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST1.MY_COMPANY.COM : Creating purge job...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Scheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Creating replication administrator repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Granting privileges or roles required for replication
administrator to repadmin...
MY_HOST2.MY_COMPANY.COM : Creating purge job...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Scheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Creating replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ASR_CHG_LOG to replication group
LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE ODS.ASR_CHG_
LOG...
MY_HOST1.MY_COMPANY.COM : Adding object TABLE ODS.ODS_CHG_STAT to replication
group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Generating replication support for TABLE ODS.ODS_CHG_
STAT...
MY_HOST2.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Adding replication site MY_HOST2.MY_COMPANY.COM to
replication group LDAP_REP...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
```

```

MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST2.MY_COMPANY.COM : Executing deferred administrative requests...
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid1" hostname has been added to replication
agreement entry.
MY_HOST2.MY_COMPANY.COM : Inserting replication agreement entry my_host_rid2...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid2" hostname has been added to replication
agreement entry.
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...

```

```

-----
ASR setup has been configured successfully.
-----

```

```

Directory Replication Group (DRG) details :

```

```

-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                    Type
-----
rid1      my_host                 MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host                 MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----

```

The remtool -asrverify Operation

This `asrverify` operation detects and reports on problems found in an Oracle Database Advanced Replication-based directory replication group (DRG). This operation reports errors, but does not correct them. To run this operation, all nodes in the DRG must be up and running. You do not have to stop your Oracle Internet Directory server processes to run this operation.

The `asrverify` operation will fail or report errors for the following situations. You can use the `asrrectify` operation to correct these errors. See ["The remtool -asrverify Operation"](#) on page 4-35 for more information about that operation.

- If, by mistake, the replication administrator account is dropped in any of the nodes, the `asrverify` operation fails. Use `asrrectify` to re-create the replication administrator account and add it back to the DRG.
- If, by mistake, the password for the replication administrator account has changed on any of the nodes in the DRG, the `asrverify` operation fails. Use `remtool asrrectify` to change the replication administrator account and add it back to the DRG.

- If the global database name of any node has changed after Advanced Replication setup, `asrverify` reports an error and does not proceed further. Use `asrrectify` to revert back to the previous global name and rectify other issues.

Syntax for `remtool -asrverify`

```
remtool -asrverify [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for `remtool -asrverify`

-connect repl_admin_name@net_service_name

For more information, see "[The -connect Connection Argument](#)" on page 4-65.

Tasks and Examples for `remtool -asrverify`

Using the `asrverify` operation you can perform the following tasks:

- [Detecting Errors in an Oracle Database Advanced Replication-Based DRG Setup](#)

Detecting Errors in an Oracle Database Advanced Replication-Based DRG Setup In this example, errors are found in a DRG consisting of two nodes.

Example:

```
remtool -asrverify -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                                            Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

```
Verifying ASR setup...
```

```
MY_HOST1.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST2.MY_COMPANY.COM : Verifying initialization parameter...
MY_HOST1.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST2.MY_COMPANY.COM : Verifying replication administrator roles...
MY_HOST1.MY_COMPANY.COM : Verifying database links...
MY_HOST2.MY_COMPANY.COM : Verifying database links...
MY_HOST1.MY_COMPANY.COM : Verifying purge job...
MY_HOST2.MY_COMPANY.COM : Verifying purge job...
MY_HOST1.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST2.MY_COMPANY.COM : Verifying scheduled links...
MY_HOST1.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST2.MY_COMPANY.COM : Verifying availability of replication objects...
MY_HOST1.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
```

```

CHG_STAT.
MY_HOST2.MY_COMPANY.COM : Verifying replication group...
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.
ASR SETUP ERROR/WARNING:
MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...

```

DB Name	Init Param	Repl Admin Role	DB Links	Purge Job	Sch. Links	Repl Group	Repl Agrmt Entry
MY_HOST1.MY_COMPANY.	Chkd	Chkd	Chkd	Chkd	Chkd	NCrtd	Chkd
MY_HOST2.MY_COMPANY.	Chkd	Chkd	Chkd	Chkd	Chkd	NCrtd	Chkd

Legends :

- Chkd - Checked. No errors.
- Crtd - ASR setup errors were found and corrected.
- Err - Error occurred while doing ASR setup verification.
- NCrtd - ASR setup has errors, but not corrected.

Summary of findings:

```

ASR SETUP ERROR/WARNING:
MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.

```

ASR SETUP ERROR/WARNING:

```

MY_HOST1.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.

```

ASR SETUP ERROR/WARNING:

```

MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ASR_
CHG_LOG.

```

ASR SETUP ERROR/WARNING:

```

MY_HOST2.MY_COMPANY.COM : Replication support is not available for TABLE ODS.ODS_
CHG_STAT.

```

The remtool -backupmetadata Operation

The `backupmetadata` operation adds the metadata of a pilot replica to the master replica, or backs up the metadata of a pilot replica into a file.

Note: The `-backupmetadata` option will not work if anonymous bind is disabled at the pilot replica or master replica.

Syntax for remtool -backupmetadata

```

remtool -backupmetadata -replica pilot_hostname:port {-master master_hostname:port
| -bkup file_name}

```

Arguments for remtool -backupmetadata

-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.

Tasks and Examples for remtool -backupmetadata

Using the `backupmetadata` operation you can perform the following tasks:

- [Adding the Metadata of a Pilot Replica to a Master Replica](#)
- [Backing Up the Metadata of a Pilot Replica to an LDIF File](#)

Adding the Metadata of a Pilot Replica to a Master Replica This example shows how to add the metadata entries from a pilot replica to a master replica.

Example:

```
remtool -backupmetadata -replica mypilot.company.com:3060 \  
-master mymaster.company.com:3060 -bkup /myfiles/backup.ldif
```

In this example, a backup file was specified with `-bkup`. The command output is:

```
Backup of metadata will be stored in /myfiles/backup.ldif  
Metadata copied successfully.
```

Example:

```
remtool -backupmetadata -replica mypilot.company.com:3060 \  
-master mymaster.company.com:3060
```

In this example, no backup file was specified, so `remtool` uses the default location. The command output is:

```
Backup of metadata will be stored in  
ORACLE_INSTANCE/diagnostics/logs/OID/tools/ocbkup.replicaid_pilot.T0.replicaid_  
master.timestamp.ldif.  
Metadata copied successfully.
```

The output will contain the expanded path `ORACLE_INSTANCE`.

Note: If Oracle Delegated Administration Services is not configured, then you might see an error message similar to this when you run `remtool` with the `-backupmetadata` option:

```
Failed to add "orclApplicationCommonName=ias.acme.com,
cn=IAS Instances, cn=IAS, cn=Products, cn=OracleContext"
as "uniquemember" to entry "cn=Associated Mid-tiers,
orclapplicationcommonname=DASApp, cn=DAS,cn=products,
cn=OracleContext at replica ldap://myhost:3060
```

Please ignore this error message.

Backing Up the Metadata of a Pilot Replica to an LDIF File This example shows how to back up the metadata entries for a pilot replica into an LDIF file.

Example:

```
remtool -backupmetadata -replica mypilot.company.com:3060 \
  -bkup /home/myfiles/obckup.ldif
```

The output from this command is:

```
Backup of metadata will be stored in /home/myfiles/obckup.ldif
```

```
Metadata copied successfully
```

The `remtool -chgpwd` Operation

The `chgpwd` operation is used to change the replication administrator password for an Oracle Database Advanced Replication-based directory replication group (DRG) that has already been setup using `asrsetup`.

The replication administrator password is the same for all nodes in an Advanced Replication DRG. This operation will change the password for all nodes in the DRG.

Syntax for `remtool -chgpwd`

```
remtool -chgpwd [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for `remtool -chgpwd`

The tool will also prompt you to enter the new password for the replication administrator.

-connect *repl_admin_name@net_service_name*

For more information, see "[The -connect Connection Argument](#)" on page 4-65.

Tasks and Examples for `remtool -chgpwd`

Using the `chgpwd` operation you can perform the following task:

- [Changing the Replication Administrator Password for an Oracle Database Advanced Replication-based DRG](#)

Changing the Replication Administrator Password for an Oracle Database Advanced Replication-based DRG In this example, the password of the replication administrator of a DRG consisting of MY_HOST1.MY_COMPANY.COM and MY_HOST2.MY_COMPANY.COM is changed.

Example:

```
remtool -chgpwd -v -conn repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                                           Type
-----
rid1      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

```
Enter new password of the replication administrator :
Reenter new password of the replication administrator :
```

```
-----
Changing the password of all nodes...
```

```
MY_HOST1.MY_COMPANY.COM : Changing password of replication administrator
repadmin...
MY_HOST2.MY_COMPANY.COM : Changing password of replication administrator
repadmin...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Creating database link to MY_HOST2.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Creating database link to MY_HOST1.MY_COMPANY.COM...
```

```
-----
Password has been changed.
-----
```

The remtool -delnode Operation

The `delnode` operation removes a remote master site (RMS) node from an existing directory replication group (DRG). You must first create the DRG using "[The remtool -asrsetup Operation](#)" on page 4-32. The following usage rules apply to this operation:

- You can only delete RMS nodes from a DRG, not the master definition site (MDS).
- Oracle Internet Directory processes on the master definition site (MDS) and other remote master sites (RMSs) in the DRG must be stopped before running the operation.
- If the RMS node being deleted is down when the `delnode` operation is invoked, it will be selected for deletion.

- After the `delnode` operation is complete, Oracle Internet Directory processes can be restarted.

Syntax for `remtool -delnode`

```
remtool -delnode [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for `remtool -delnode`

The tool will also prompt you for the global database name (as defined in the `tnsnames.ora` file of the RMS node to be deleted from the DRG.

-connect repl_admin_name@net_service_name

For more information, see "The `-connect` Connection Argument" on page 4-65.

Tasks and Examples for `remtool -delnode`

Using the `delnode` operation you can perform the following task:

- [Removing a RMS Node from an Oracle Database Advanced Replication-Based DRG](#)

Removing a RMS Node from an Oracle Database Advanced Replication-Based DRG In this example, `MY_HOST3.MY_COMPANY.COM` is removed from a DRG consisting of `MY_HOST1.MY_COMPANY.COM`, `MY_HOST2.MY_COMPANY.COM` and `MY_HOST3.MY_COMPANY.COM`

Example:

```
remtool -delnode -v -conn repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
MY_HOST3.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId    Site
Name                                                           Type
-----
rid1      my_host                 MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1 MDS
rid2      my_host                 MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2 RMS
rid3      my_host                 MY_HOST3.MY_COMPANY.COM 10.1.2.0.0  my_host_rid3 RMS
-----
```

```
Do you want to continue? [y/n] : y
```

```
Enter globalname of node to be deleted : MY_HOST3.MY_COMPANY.COM
```

```
-----
Deleting an existing node...

MY_HOST1.MY_COMPANY.COM : Dropping replication site MY_HOST3.MY_COMPANY.COM from
replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Dropping replication group LDAP_REP...
MY_HOST3.MY_COMPANY.COM : Unsheduling push job to MY_HOST1.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Unsheduling push job to MY_HOST2.MY_COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
```

```

MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST1.MY_
COMPANY.COM...
MY_HOST3.MY_COMPANY.COM : Dropping database link made to MY_HOST2.MY_
COMPANY.COM...
Enter "SYSTEM" user password for "MY_HOST3.MY_COMPANY.COM" database at "my_host"
host :
MY_HOST3.MY_COMPANY.COM : Dropping replication administrator repadmin...
MY_HOST1.MY_COMPANY.COM : Unsheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Unsheduling push job to MY_HOST3.MY_COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST2.MY_COMPANY.COM : Dropping database link made to MY_HOST3.MY_
COMPANY.COM...
MY_HOST1.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Verifying uniqueness of replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST1.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST1.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from
replication agreement entry as it is not part of DRG or was repeated.
MY_HOST2.MY_COMPANY.COM : Verifying replication agreement entry...
MY_HOST2.MY_COMPANY.COM : Deleting replication agreement entry my_host_rid3...
CORRECTED:
MY_HOST2.MY_COMPANY.COM : "my_host_rid3" hostname has been removed from
replication agreement entry as it is not part of DRG or was repeated.
-----
Node MY_HOST3.MY_COMPANY.COM has been deleted from this DRG.
-----
Directory Replication Group (DRG) details :

-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                     Type
-----
rid1      my_host                 MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2      my_host                 MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
=====

```

The remtool -dispsrerr Operation

The `dispsrerr` operation displays errors for an Oracle Database Advanced Replication-based directory replication group (DRG). It shows both administrative request errors and deferred transaction errors.

Syntax for remtool -dispsrerr

```
remtool -dispsrerr [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -dispasrerr

-connect repl_admin_name@net_service_name

For more information, see "The -connect Connection Argument" on page 4-65.

Tasks and Examples for remtool -dispasrerr

Using the `dispasrerr` operation you can perform the following task:

- [Displaying Errors for an Oracle Database Advanced Replication-based DRG](#)

Displaying Errors for an Oracle Database Advanced Replication-based DRG In this example, the tool reports Advanced Replication errors for a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM`.

Example:

```
remtool -dispasrerr -v -conn repadmin@my_host1.my_company.com
```

MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.

MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.

Directory Replication Group (DRG) details :

```
-----
Instance Host Name      Global Name              Version      ReplicaId    Site
Name                                                           Type
-----
rid      my_host      MY_HOST1.MY_COMPANY.COM 10.1.2.0.0  my_host_rid1  MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM 10.1.2.0.0  my_host_rid2  RMS
-----
```

Following administrative request errors were found at MY_HOST1.MY_COMPANY.COM

```
-----
Admin request      Request raised at      Error
raised by
-----
REPADMIN          MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ASR_CHG_L
REPADMIN          MY_HOST1.MY_COMPANY.  ORA-23309: object ODS.ODS_CHG_S
REPADMIN          MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ODS_CHG
REPADMIN          MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ODS_CHG_S
REPADMIN          MY_HOST1.MY_COMPANY.  ORA-23416: table "ODS"."ASR_CHG
REPADMIN          MY_HOST1.MY_COMPANY.  ORA-23308: object ODS.ASR_CHG_L
-----
```

Following deferred transaction errors were found at MY_HOST1.MY_COMPANY.COM

```
-----
Deferred          Deferred Trans      Destination      Error
Transaction ID    Origin DB
-----
1.2.3733          MY_HOST1.MY_COM    MY_HOST1.MY_COM  ORA-01403: no data found
-----
```

No deferred transaction errors were found at MY_HOST2.MY_COMPANY.COM

The remtool -dispqstat Operation

The `dispqstat` operation displays the queue statistics for a directory replication group (DRG) that uses Oracle Database Advanced Replication. This operation cannot be used for DRGs that use LDAP-based replication. If a DRG uses both Advanced and LDAP-based replication, this operation displays queue statistics for nodes that use Advanced Replication only.

Syntax for remtool -dispqstat

```
remtool -dispqstat [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -dispqstat

-connect repl_admin_name@net_service_name

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). You are prompted for the password for the replication administrator. If you do not supply an argument on the command-line, the tool prompts you for the information. The connect string is composed of the following elements:

- The name of the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

Tasks and Examples for remtool -dispqstat

Using the `dispqstat` operation you can perform the following tasks:

- [Displaying Queue Statistics for an Oracle Database Advanced Replication-Based DRG](#)

Displaying Queue Statistics for an Oracle Database Advanced Replication-Based DRG In this example, queue statistics for an Oracle Database Advanced Replication-based DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` are reported.

Example:

```
remtool -dispqstat -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      Replicaid      Site
Name                                                           Type
-----
rid1    my_host                MY_HOST1.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid1   MDS
rid2    my_host                MY_HOST2.MY_COMPANY.COM  OID 10.1.2.0.0  my_host_rid2   RMS
-----
```

Queue Statistics :

```
-----
Supplier      Consumer      New      Retry      Purge      HIQ      Change #
-----
```

MY_HOST1.MY CO MY_HOST1.MY CO	3	9	10	6	2003
MY_HOST1.MY CO MY_HOST2.MY CO	2	7	8	5	2001
MY_HOST2.MY CO MY_HOST1.MY CO	2	8	5	8	2002
MY_HOST2.MY CO MY_HOST2.MY CO	2	10	7	8	2000

Legends

- New: No. of new change logs
- Retry: No. of change logs in retry queue
- Purge: No. of change logs in purge queue
- HIQ: No. of change logs in Human Intervention Queue (HIQ)
- Change # : Last applied change log no.

The remtool -paddnode Operation

The `paddnode` operation adds a replica or partial replica to a directory replication group (DRG). This operation has the following usage rules:

- The supplier node (the master copy) can be part of a DRG that uses Advanced Replication, LDAP-based replication, or both.
- If you want to specify a supplier node that uses Advanced Replication, you must bind using that node's connection information.
- The new replica to be added should not be a member of any DRG.
- A consumer node (the destination of replication updates) can be any node that uses LDAP-based replication.
- After adding a replica, you can choose the naming context(s) to participate in replication, or choose the entire directory by selecting * (asterisk). Choosing specific naming contexts replicates only that portion of the directory. Choosing the entire directory will replicate all directory data except for directory-specific entries (DSE).
- The `cn=oraclecontext` naming context is included for replication whether or not any naming contexts are specified by the user.

Syntax for remtool -paddnode

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

Arguments for remtool -paddnode

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 "[The -bind Connection Argument](#)" on page 4-65 for information.

Tasks and Examples for remtool -paddnode

Using the paddnode operation you can perform the following tasks:

- [Adding a Read-Only Replica to a DRG](#)
- [Adding a Partial Replica to a DRG](#)

Adding a Read-Only Replica to a DRG In this example, directory server `ldap://my_host:3060` is added as a replica to directory server `ldap://my_host:3040`, which is part of the DRG consisting of `ldap://my_host:3040` and `ldap://my_host:3080`, which both use LDAP-based replication.

Example:

```
remtool -paddnode -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

```
-----
Sl  ReplicaId      Directory Information  Supplier Information  Repl.
No.                                                     Type
-----
001 my_host_rid1   my_host:3040          --                    RW
002 my_host_rid3   my_host:3080          my_host_rid1         RO
-----

Enter consumer directory details:
Enter hostname of host running OID server      : my_host

Enter port on which OID server is listening   : 3060

Enter replication dn password                  :
Enter replica type [1 - LDAP read-only replica; 2 - LDAP updateable replica] : 1
Enter replicaId of the supplier                : my_host_rid1
-----

ldap://my_host:3060 [my_host_r[my_host_rid1]id2] : Modifying entry
orclreplicaId=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaId=my_host_
rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementId=000003,orclreplicaId=my_host_rid,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry orclreplicaId=my_host_
rem2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaId=my_host_rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry orclreplicaId=my_host_
rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaId=my_host_rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaId=my_host_
rem,cn=replication configuration...
```

```

ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000003,orclreplicaid=my_host_rid,cn=replication configuration...
-----
Replica ldap://my_host:3060(my_host_rem2) has been added to this DRG.
-----

```

Directory Replication Group (DRG) details :

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	--	RW
002	my_host_rid2	my_host:3060	my_host_rid1	RO
003	my_host_rid3	my_host:3080	my_host_rid1	RO

Replica ldap://my_host:3060 (my_host_rid2) can be made partial replica by specifying naming contexts to be replicated.

List of available naming contexts in supplier replica ldap://my_host:3040 (my_host_rid1) :

```

1. * [replicate whole directory]
Enter naming context (e-end, q-quit) : e
-----
-----

```

Adding a Partial Replica to a DRG In this example, the directory server ldap://my_host:3060 is added as a partial replica by specifying the naming contexts to be replicated to directory server ldap://my_host:3040.

Example:

```
remtool -paddnode -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid	my_host:3040	--	RW

```

Enter consumer directory details:
Enter hostname of host running OID server      : my_host

Enter port on which OID server is listening   : 3060

Enter replication dn password                  :
Enter replica type [1 - LDAP read-only replica; 2 - LDAP updateable replica] : 2
-----
ldap://my_host:3060 [my_host_rid2] : Modifying entry orclreplicaid=my_host_
rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry orclreplicaid=my_host_
rid2,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaid=my_host_
rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_
prep,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000001,orclagreementid=000002,orclreplicaid=usunnae07_
prep,cn=replication configuration...
-----
Replica ldap://my_host:3060(my_host_rid2) has been added to this DRG.
-----
Directory Replication Group (DRG) details :

--- -----
S1  Replicaid          Directory Information  Supplier Information  Repl.
No.                                                                Type
--- -----
001 my_host_rid1      my_host:3040          --                    RW
002 my_host_rid2      my_host:3060          my_host_rid1         RW
-----

Replica ldap://my_host:3060 (my_host_rem2) can be made partial replica by
specifying naming contexts to be replicated.

-----
List of available naming contexts in supplier replica ldap://my_host:3040 (my_
host_rid1) :

    1. * [replicate whole directory]
    2. dc=com
    3. dc=org
    4. dc=net
    5. dc=edu
Enter naming context (e-end, q-quit) : dc=org

Enter naming context (e-end, q-quit) : dc=edu

```



```

Enter naming context (e-end, q-quit) : e

Following naming contexts will be included for replication:
-----
  1. dc=org
  2. dc=edu
Do you want to continue? [y/n] : y

ldap://my_host:3040 [my_host_rid1] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000002,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry
cn=includednamingcontext000003,orclagreementid=000002,orclreplicaid=my_host_
rid,cn=replication configuration...

-----
Selected naming contexts have been included for replication.
-----

```

The remtool -pdisplay Operation

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

Arguments to remtool -pdisplay

-bind supplier_hostname:ldap_port

See "[The -bind Connection Argument](#)" on page 4-65 for information.

The remtool -pchgmaster Operation

The `pchgmaster` operation is used to break the agreement with the old supplier and reestablish the agreement with a new supplier. This operation is part of configuring replication failover.

See Also: "Configuring Replication Failover" in *Oracle Internet Directory Administrator's Guide* for details on performing the replication failover process

The `pchgmaster` operation has the following usage rules:

1. If you do not supply consumer directory details using the `-bind` option, then you are prompted to specify consumer details.
2. If the consumer details are valid, then `remtool` identifies all nodes in the DRG, if any, and displays their details.
3. You are next prompted for the retiring and new supplier details.
4. After the change master operation completes successfully, you 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 ["The remtool -pcleanup Operation"](#) on page 4-54 for details about the `pcleanup` operation.

Syntax for `remtool -pchgmaster`

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

Arguments for `remtool -pchgmaster`

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 ["The -bind Connection Argument"](#) on page 4-65 for information.

-multimaster

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

Tasks and Examples for `remtool -pchgmaster`

Using the `pchgmaster` operation, you can perform the following tasks:

- [Breaking a Supplier Agreement and Creating a New Supplier Agreement for a Consumer](#)

Breaking a Supplier Agreement and Creating a New Supplier Agreement for a Consumer In this example, the supplier of directory server `ldap://my_host:3060` is changed from directory server `ldap://my_host:3040` to directory server `ldap://my_host:3080`.

Example:

```
remtool -pchgmaster -v -bind my_host:3060
```

The results are:

Directory Replication Group (DRG) details :

```
-----
S1  ReplicaId      Directory Information  Supplier Information  Repl.
No.                                     Type
-----
001 my_host_rid2   my_host:3060          my_host_rid1         RW
002 my_host_rid3   my_host:3080          my_host_rid1         RW
003 my_host_rid1   my_host:3040          my_host_rid3
                               my_host_rid2
-----
```

```
Enter replica ID of the retiring supplier           : my_host_rid1
```

```
-----
Enter hostname of the new supplier                 : my_host
```

```
Enter port number of the new supplier              : 3080
```

```
Enter replication DN password of the new supplier :
```

```

* WARNING *: Moving my_host_rid1 to be consumer of my_host_rid3 might cause
discrepancy in data.
Do you want to continue? [y/n]: y
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry orclreplicaid=my_host_
rid3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry orclreplicaid=my_host_
rid2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
dn,orclreplicaid=my_host_rid2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000002,cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Adding entry
cn=includednamingcontext000001,cn=replication
namecontext,orclagreementid=000004,orclreplicaid=my_host_rid3,cn=replication
configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rid1,cn=replication configuration...

```

Directory Replication Group (DRG) details :

S1 No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid2	my_host:3060	my_host_rid3	RW
002	my_host_rid3	my_host:3080	my_host_rid1 my_host_rid2	RW
003	my_host_rid1	my_host:3040	my_host_rid3	RW

Change master of my_host_rid2 to my_host_rid3 successfully.

Changing the Primary Node In this example, the primary node in a three-node LDAP multimaster agreement is changed from stacu14_tst1 to stacu14_tst13

Example:

```
remtool -pchgmaster -multimaster
```

The result is:

Directory Replication Group (DRG) details :

```

-----
Sl  ReplicaId          Directory Information  Supplier Information  Repl.
No.                                                              Type
-----
001 stacu14_tst1      stacu14:3069          stacu14_tst13        RW
                               stacu14_tst12

002 stacu14_tst13    stacu14:3089          stacu14_tst12        RW
                               stacu14_tst1

003 stacu14_tst12    stacu14:3079          stacu14_tst13        RW
                               stacu14_tst1

-----
Enter new primary replica ID      : stacu14_tst13

Changed primary replica from stacu14_tst1 to stacu14_tst13 successfully.

```

The remtool -pchgpwd Operation

This `pchgpwd` operation changes the replication DN password for an Oracle Internet Directory server. The password is changed in both the directory and in wallet.

If the replica is taking part in replication, then password will be changed in other replicas for the local replica's replication DN. Note that, unlike Advanced Replication, the replication DN password for each replica can be different.

The operation must be run on the host of the Oracle Internet Directory server whose password you are changing in order to update the wallet password at the same time. You can also update the wallet password separately using "[The remtool -pchgpwalpwd Operation](#)" on page 4-53.

Syntax for remtool -pchgpwd

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

Arguments for remtool -pchgpwd

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

-bind supplier_hostname:ldap_port

See "[The -bind Connection Argument](#)" on page 4-65 for information.

Tasks and Examples for remtool -pchgpwd

Using the `pchgpwd` operation you can perform the following tasks:

- [Changing the Replication DN Password Used for LDAP-Based Replication](#)

Changing the Replication DN Password Used for LDAP-Based Replication In this example, the replication DN password of the Oracle Internet Directory server `ldap://my_host:3040` is changed.

Example:

```
remtool -pchgpwd -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

```
-----
Sl  ReplicaId      Directory Information  Supplier Information  Repl.
No.                                     Type
-----
001 my_host_rid1    my_host:3040          --                    RW
002 my_host_rid3    my_host:3080          my_host_rid1         RO
-----
```

```
-----
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid' will be changed.
```

```
Do you want to continue? [y/n] : y
```

```
Enter new password of replication DN      :
```

```
Reenter new password of replication DN    :
```

```
-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
```

```
ldap://my_host:3080 [my_host_rid3] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rem,cn=replication configuration...
```

```
-----
Password has been changed.
-----
```

The remtool -pchgwalpwd Operation

The `pchgwalpwd` operation is used to change the replication DN password only in the wallet of an Oracle Internet Directory server. It sets the wallet password to the same replication DN password stored in the Oracle Internet Directory repository for the host specified in the bind connection string.

Syntax for remtool -pchgwalpwd

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

Arguments for remtool -pchgwalpwd

-bind *supplier_hostname:ldap_port*

See "[The -bind Connection Argument](#)" on page 4-65 for information.

Tasks and Examples for remtool -pchgwalpwd

Using the `pchgwalpwd` operation you can perform the following task:

- [Changing the Replication DN Password in the Oracle Internet Directory Wallet](#)

Changing the Replication DN Password in the Oracle Internet Directory Wallet In this example, the replication DN password for Oracle Internet Directory server `ldap://my_host:3040` is set in wallet to match the password in the repository.

Example:

```
remtool -pchgwalpwd -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	--	RW
002	my_host_rid3	my_host:3080	my_host_rid1	RO

Replication DN password of ldap://my_host:3040 (my_host_rid1) associated with database 'rid' will be set in wallet.

Do you want to continue? [y/n] : y

The remtool -pcleanup Operation

The `pcleanup` operation is used to clean up an LDAP-based directory replication group (DRG) setup. It will clean up a replica which has incomplete or flawed LDAP-based DRG setup. It will only clean up the replica identified by the bind connection string.

If replication configuration information is corrupted, or the replication DN entry is not available, then the tool prompts for the Oracle Internet Directory superuser DN and password.

This operation only cleans up LDAP-based DRG setup. For clean up of an Oracle Database Advanced Replication-based DRG setup, see "[The remtool -asrcleanup Operation](#)" on page 4-29.

Syntax for remtool -pcleanup

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

Arguments for remtool -pcleanup

-bind *supplier_hostname:ldap_port*

See "[The -bind Connection Argument](#)" on page 4-65 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.

Tasks and Examples for remtool -pcleanup

Using the `pcleanup` operation you can perform the following tasks:

- [Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup](#)

■ Cleaning Up Specific LDAP Agreements

Cleaning Up an Incomplete or Flawed LDAP-based DRG Setup In this example, the tool cleans up the replication setup of a DRG that has three replicas taking part in LDAP based replication.

Example:

```
remtool -pcleanup -v -bind my_host:3040
```

The results are:

Directory Replication Group (DRG) details :

```
-----
S1  ReplicaId          Directory Information  Supplier Information  Repl.
No.                                     Type
-----
001 my_host_rid1      my_host:3040         --                    RW
002 my_host_rid3      my_host:3080         my_host_rid1         RO
003 my_host_rid2      my_host:3060         my_host_rid1         RO
-----
```

```
DRG identified by replica ldap://my_host:3040 (my_host_rid1) will be cleaned up.
Do you want to continue? [y/n] : y
```

```
-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000003,orclreplicaid=my_host_rem,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry orclreplicaid=my_host_
rem2,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Modifying entry ...
ldap://my_host:3060 [my_host_rid2] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3060 [my_host_rid2] : Deleting entry cn=replication
dn,orclreplicaid=my_host_rem3,cn=replication configuration...
-----
```

```
Replica ldap://my_host:3040(my_host_rid1) has been cleaned up.
-----
```

Cleaning Up Specific LDAP Agreements In this example, the agreement between directory servers `ldap://my_host:3040` and `ldap://my_host:3060` is cleaned up. The agreement between directory servers `ldap://my_host:3040` and `ldap://my_host:3080` is also cleaned up.

Example:

```
remtool -pcleanup -v -agrmt -bind my_host:3040
```

Directory Replication Group (DRG) details :

```
-----
```

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	my_host_rid2 my_host_rid3	RW
002	my_host_rid3	my_host:3080	my_host_rid1	RW
003	my_host_rid2	my_host:3060	my_host_rid1	RW

```
-----
```

Enter replica ID of replica(s) for which its(their) agreement(s) with replica `ldap://my_host:3040` (`my_host_rid1`) will be cleaned up.

Enter replica ID [Enter "e" to end selection] : `my_host_rid2`

Enter replica ID [Enter "e" to end selection] : `my_host_rid3`

Enter replica ID [Enter "e" to end selection] : `e`

```
-----
```

Agreement(s) with the following replica(s) would be cleaned up:

0. `my_host_rid2`

1. `my_host_rid3`

Do you want to continue? [y/n] : `y`

```
-----
```

Successfully cleaned up agreement between `my_host_rid1` and `my_host_rid2`.
Successfully cleaned up agreement between `my_host_rid1` and `my_host_rid3`.

```
-----
```

Replica `ldap://my_host:3040(my_host_rid1)` has been cleaned up.

```
-----
```

The remtool -pdelnode Operation

The `pdelnode` operation deletes an LDAP-based replica or partial replica from a directory replication group (DRG). To delete an Oracle Database Advanced Replication-based replica, used the "[The remtool -pdelnode Operation](#)" on page 4-56.

Syntax for remtool -pdelnode

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

Arguments for remtool -pdelnode

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 "[The -bind Connection Argument](#)" on page 4-65 for information.

Tasks and Examples for remtool -pdelnode

Using the pdelnode operation you can perform the following tasks:

- "[Deleting a Read-Only Replica from a DRG](#)" on page 4-57

Deleting a Read-Only Replica from a DRG In this example, replica ldap://my_host:3080 is removed from the DRG. This DRG consists of three replicas: ldap://my_host:3040, ldap://my_host:3060, and ldap://my_host:3080, of which ldap://my_host:3040 and ldap://my_host:3060 uses Advanced Replication and ldap://my_host:3040 and ldap://my_host:3080 uses LDAP-based replication. To delete replica ldap://my_host:3080, user has to give bind details of either ldap://my_host:3040 or ldap://my_host:3080.

Example:

```
remtool -pdelnode -v -bind my_host:3040
```

```
-----
Directory Replication Group (DRG) details :
```

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	my_host_rid2	RW
002	my_host_rid2	--	my_host_rid1	RW
003	my_host_rid3	my_host:3080	my_host_rid1	RO

```
-----
Enter replicaid of the replica to be deleted : my_host_rid3
```

```
-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry ...
ldap://my_host:3040 [my_host_rid1] : Deleting entry
orclagreementid=000002,orclreplicaid=my_host_rid1,cn=replication configuration...
ldap://my_host:3040 [my_host_rid1] : Deleting entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry orclreplicaid=my_host_
rem3,cn=replication configuration...
ldap://my_host:3080 [my_host_rid3] : Modifying entry ...
ldap://my_host:3080 [my_host_rid3] : Deleting entry orclreplicaid=my_host_
rem,cn=replication configuration...
-----
```

```
Replica ldap://my_host:3080(my_host_rid3) has been deleted from this DRG.
-----
```

```
Directory Replication Group (DRG) details :
```

Sl No.	Replicaid	Directory Information	Supplier Information	Repl. Type
001	my_host_rid1	my_host:3040	my_host_rid2	RW

```
002 my_host_rid2      --                my_host_rid1      RW
```

The remtool -pdispqstat Operation

The `pdispqstat` operation displays the queue statistics for a directory replication group (DRG) that uses LDAP-based replication. This operation cannot be used for DRGs that use ASR-based (advanced) replication. If a DRG uses both ASR and LDAP-based replication, the `pdispqstat` operation displays queue statistics for nodes that use LDAP-based replication only.

Note: The `dispqstat` operation is used to display the queue statistics for a DRG that uses ASR-based replication.

See Also: "[The remtool -dispqstat Operation](#)" on page 4-44 for more details on displaying the queue statistics for a DRG that uses ASR-based replication

Syntax for remtool -pdispqstat

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

Arguments for remtool -pdispqstat

-bind hostname:ldap_port

See "[The -bind Connection Argument](#)" on page 4-65 for information.

Tasks and Examples for remtool -pdispqstat

Using the `pdispqstat` operation, you can perform the following tasks:

- [Display queue statistics for LDAP-based replicas](#)

Display queue statistics for LDAP-based replicas In this example, queue statistics for a DRG consisting of directory servers `ldap://my_host:3040` and `ldap://my_host:3060` are displayed.

Example:

```
remtool -pdispqstat -v -bind my_host:3040
```

```
Directory Replication Group (DRG) details :
```

```
-----
Sl  ReplicaId      Directory Information  Supplier Information  Repl.
No.                                                     Type
-----
001 my_host_rid1    my_host:3040          my_host_rid2         RW
002 my_host_rid2    my_host:3060          my_host_rid1         RW
-----
```

```
Queue Statistics:
```

```
-----
Supplier      Consumer      PROTO New  Retry  Purge  HIQ  LA  Chg#  Logs  TBP  LT  Chg#
-----
my_host_rid2  my_host_rid1  LDAP  0   0     1     2   2001  0     2001
my_host_rid1  my_host_rid2  LDAP  0   0     2     3   2082  3     70335
-----
```

Legends:

New : No. of new change logs
 Retry : No. of change logs in retry queue
 Purge : No. of change logs in purge queue
 HIQ : No. of change logs in Human Intervention Queue (HIQ)
 LA Chg # : Last applied change log no.
 Logs TBP : Logs to be transported.
 LT Chg # : Last transported change log no.

The remtool -pilotreplica Operation

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

Syntax for remtool -pilotreplica

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

Arguments for remtool -pilotreplica

begin | end

Required. Begin or end pilot mode.

-bind *hostname:ldap_port*

See "[The -bind Connection Argument](#)" on page 4-65 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.

Tasks and Examples for remtool -pilotreplica

Using the `pilotreplica` operation you can perform the following tasks:

- [Beginning Pilot Mode for a Replica](#)
- [Ending Pilot Mode for a Replica](#)

Beginning Pilot Mode for a Replica

Example:

```
remtool -pilotreplica begin -bind myhost:3060
```

Ending Pilot Mode for a Replica

Example:

```
remtool -pilotreplica end -bind myhost:3060
```

The remtool -presetpwd Operation

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

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

Syntax for remtool -presetpwd

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

Arguments for remtool -presetpwd

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 "[The -bind Connection Argument](#)" on page 4-65 for information.

Tasks and Examples for remtool -presetpwd

Using the `presetpwd` operation you can perform the following tasks:

- [Resetting the Replication DN Password for a Single Directory](#)

Resetting the Replication DN Password for a Single Directory In this example, the replication DN password is reset for replica `my_host:3040`.

Example:

```
remtool -presetpwd -v -bind my_host:3040
```

The results are:

```

Enter superuser DN                : cn=orcladmin

Enter superuser password          :
-----
Replication DN password of ldap://my_host:3040 (my_host_rem) associated with
database 'rid1' will be reset.
Do you want to continue? [y/n] : y

Enter new password of replication DN :
Reenter new password of replication DN :
-----
ldap://my_host:3040 [my_host_rid1] : Modifying entry cn=replication
dn,orclreplicaid=my_host_rid1,cn=replication configuration...
-----
Password has been changed.
-----

```

The remtool -pverify Operation

The `pverify` operation verifies the replication configuration for a directory replication group (DRG) that uses LDAP-based replication. This operation cannot be used for a DRG that uses ASR based replication. If a DRG uses both ASR and LDAP-based replication, then this option verifies the replication configuration between nodes that use LDAP-based replication only.

The `pverify` operation has the following usage rules:

- This option only verifies agreements that involve the node specified in the command argument.

- The `REMTTOOL_VERIFY_LOG.rpt` report contains the verification results.

Syntax for remtool -pverify

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

Arguments for remtool -pverify

-bind hostname:ldap_port_number

See "[The -bind Connection Argument](#)" on page 4-65 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.

Tasks and Examples for remtool -pverify

Use the `pverify` operation to perform the following tasks:

- [Verify Replication Configuration for an LDAP-Based DRG](#)

Verify Replication Configuration for an LDAP-Based DRG In this example, the replication configuration for a DRG comprising of directory servers `ldap://my_host:3040`, `ldap://my_host:3060`, and `ldap://my_host:3080` is verified.

Example

```
remtool -pverify -v -bind my_host:3040
```

```
Node ID: my_host_rid1
  Test Category: Connection
    Test Against: my_host_rid1
      Test: Wallet
        Check: Corruption passed
        Check: Authentication passed
        Check: Replicationdn passed

      Test Against: my_host_rid2
        Test: URL
          Check: Format (Primary) passed
          Check: Format (Secondary) passed

      Test Against: my_host_rid3
        Test: URL
          Check: Format (Primary) passed
          Check: Format (Secondary) passed

      Test Against: my_host_rid1
        Test: URL
          Check: Format (Primary) passed
          Check: Format (Secondary) passed

    Test Category: Agreements
```

Test Against: Agrmt 000002
Test: orclreplicadn
Check: Validity passed
Check: Match agreement type passed

Test: agreement DN
Check: Format passed

Test Against: Agrmt 000002 with my_host_rid2
Test: lastAppliedChangeNumber (my_host_rid2 to my_host_rid1)
Check: Format (transport) passed
Check: Logs TBP passed
Check: Format (apply) passed
Check: HIQ passed

Test: Filtering (my_host_rid2 to my_host_rid1)
Check: Format passed
Check: Configuration passed

Test Against: Agrmt 000002 with my_host_rid2
Test: Connection
Check: Authentication passed

Test: Replica Pair
Check: Validity passed
Check: Consistency passed

Test: orclreplicationid
Check: Availability passed

Test: Replication Protocol
Check: Availability passed

Test: lastAppliedChangeNumber (my_host_rid1 to my_host_rid2)
Check: Format (transport) passed
Check: Logs TBP passed
Check: Format (apply) passed
Check: HIQ passed

Test: Filtering (my_host_rid1 to my_host_rid2)
Check: Format passed
Check: Configuration passed

Test Against: Agrmt 000003
Test: orclreplicadn
Check: Validity passed
Check: Match agreement type passed

Test: agreement DN
Check: Format passed

Test Against: Agrmt 000003 with my_host_rid3
Test: lastAppliedChangeNumber (my_host_rid3 to my_host_rid1)
Check: Format (transport) passed
Check: Logs TBP passed
Check: Format (apply) passed
Check: HIQ passed

Test: Filtering (my_host_rid3 to my_host_rid1)
Check: Format passed

```

    Check: Configuration failed

Test Against: Agrmt 000003 with my_host_rid3
Test: Connection
    Check: Authentication passed

Test: Replica Pair
    Check: Validity passed
    Check: Consistency passed

Test: orclreplicationid
    Check: Availability passed

Test: Replication Protocol
    Check: Availability passed

Test: lastAppliedChangeNumber (my_host_rid1 to my_host_rid3)
    Check: Format (transport) passed
    Check: Logs TBP passed
    Check: Format (apply) passed
    Check: HIQ passed

Test: Filtering (my_host_rid1 to my_host_rid3)
    Check: Format passed
    Check: Configuration failed

Verify replication configuration for my_host_rid1 successfully.

Refer to REMTOOL_VERIFY_LOG.rpt for details.

2 checks failed.

```

The remtool -resumeasr Operation

The `resumeasr` operation resumes replication activity for an Oracle Database Advanced Replication-based directory replication group (DRG) that was previously suspended using the "[The remtool -suspendasr Operation](#)" on page 4-64.

Syntax for remtool -resumeasr

```
remtool -resumeasr [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -resumeasr

-connect repl_admin_name@net_service_name

For more information, see "[The -connect Connection Argument](#)" on page 4-65.

Tasks and Examples for remtool -resumeasr

Using the `resumeasr` operation you can perform the following tasks:

- [Resuming Replication Activity for an Oracle Database Advanced Replication-Based DRG](#)

Resuming Replication Activity for an Oracle Database Advanced Replication-Based DRG In this example, replication activity of DRG consisting of MY_HOST1.MY_COMPANY.COM and MY_HOST2.MY_COMPANY.COM is resumed.

Example:

```
remtool -resumeasr -v -conn repadmin@MY_HOST1.MY_COMPANY.COM
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId    Site
Name                                                            Type
-----
rid1      my_host                 MY_HOST1.MY_COMPANY.COM 9.0.4.0.0   my_host_rid1 MDS
rid2      my_host                 MY_HOST2.MY_COMPANY.COM 9.0.4.0.0   my_host_rid2 RMS
-----
```

```
Altering replication status...
```

```
MY_HOST1.MY_COMPANY.COM : Resuming replication activity...
```

```
Replication status has been altered successfully.
-----
```

The remtool -suspendasr Operation

The `suspendasr` operation suspends Oracle Database Advanced Replication activity for a directory replication group (DRG) that uses it for replication. While Advanced Replication activity is suspended, replication will not take place.

Syntax for remtool -suspendasr

```
remtool -suspendasr [-connect repl_admin_name@net_service_name] [-v]
```

Arguments for remtool -suspendasr

-connect repl_admin_name@net_service_name

The connection string for the master definition site (MDS) or the Remote Master Site (RMS). You are prompted for the password for the replication administrator. If you do not supply an argument on the command-line, the tool prompts you for the information. The connect string is composed of the following elements:

- The name of the replication administrator.
- The net service name of the MDS or RMS. If you have a `tnsnames.ora` file configured, then this is the net service name specified in that file, which is located by default in `ORACLE_INSTANCE/config`. (You can set the `TNS_ADMIN` environment variable if you want to use a different location.)

Tasks and Examples for remtool -suspendasr

Using the `suspendasr` operation you can perform the following tasks:

- ["Suspending Replication Activity for an Oracle Database Advanced Replication-Based DRG"](#)

Suspending Replication Activity for an Oracle Database Advanced Replication-Based DRG In this example, replication activity of a DRG consisting of `MY_HOST1.MY_COMPANY.COM` and `MY_HOST2.MY_COMPANY.COM` is suspended.

Example:

```
remtool -suspendasr -v -conn repadmin@my_host1.my_company.com
```

The results are:

```
MY_HOST1.MY_COMPANY.COM is Master Definition Site (MDS). Connected to MDS.
MY_HOST2.MY_COMPANY.COM is Remote Master Site (RMS). Connected to RMS.
Directory Replication Group (DRG) details :
```

```
-----
Instance Host Name      Global Name              Version      ReplicaId      Site
Name                                                            Type
-----
rid      my_host      MY_HOST1.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid1  MDS
rid2     my_host      MY_HOST2.MY_COMPANY.COM OID 10.1.2.0.0 my_host_rid2  RMS
-----
Altering replication status...

MY_HOST1.MY_COMPANY.COM : Quiescing replication activity...
-----
Replication status has been altered successfully.
-----
```

The -bind Connection Argument

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` will use 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.

The -connect Connection Argument

This argument is used with Oracle Database Advanced Replication-based operations to specify connection string for the master definition site (MDS) or the Remote Master Site (RMS). The syntax is:

```
-connect repl_admin_name@net_service_name
```

You are prompted for the replication DN password. If you do not supply an argument on the command-line, the tool prompts you for the information.

Related Command-Line Tools for remtool

- See "[oidctl](#)" on page 2-5
- See "[opmnctl](#)" on page 2-15

Oracle Directory Integration Platform Tools

This chapter describes the following command-line tools used to administer Oracle Directory Integration and Provisioning:

- [manageDIPServerConfig](#)
- [manageSyncProfiles](#)
- [syncProfileBootstrap](#)
- [expressSyncSetup](#)
- [provProfileBulkProv](#)
- [oidprovtool](#) (Provisioning Registration Tool)
- [dipStatus](#)
- [schemasync](#)

Notes:

- 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.
-
-

manageDIPServerConfig

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

Syntax for manageDIPServerConfig

manageDIPServerConfig

```
manageDIPServerConfig {get | set} -h HOST -p PORT -D wlsuser -attribute {sslmode |  
refreshinterval | quartzthreadcount | keystorelocation | oidhostport }  
[-value attribute_value] [-help]
```

Arguments for manageDIPServerConfig

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 ManagedServer 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.
- `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).

-val | -value

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

-help

Provides usage help for the command.

Tasks and Examples for manageDIPServerConfig

```
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
```

manageSyncProfiles

The Manage Synchronization Profiles utility, `manageSyncProfiles`, allows you to manage synchronization profiles.

Syntax for manageSyncProfiles**managSyncProfiles**

```
manageSyncProfiles {activate | deactivate | copy | deregister | get | isexists |
  update | testProfile | validateProfile | validateMapRules | register |
  updatechgnum | associateProfile | dissociateProfile | getAllAssociatedProfiles |
  getAssociatedProfile | list } -h HOST -p PORT -D wlsuser [-profile]
  [-newProfile] [-associateProfile] [-file] [-params 'prop1 val1 prop2 val2 ...']
  [-conDirHost] [-conDirPort] [-conDirBindDn] [-mode] [-conDirType] [-conDirSSL]
  [-profileStatus] [-help]
```

Arguments for manageSyncProfiles**Operations****activate**

Changes a profile state to ENABLE

deactivate

Changes a profile state to DISABLE

copy

Copies an existing profile *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 will successfully perform 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 Platform 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 ManagedServer 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.

-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 "Example Properties File for Synchronization Profiles" appendix in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management* 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.

Tasks and Examples for manageSyncProfiles

```
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

```

syncProfileBootstrap

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

Syntax for syncProfileBootstrap

syncProfileBootstrap

```

syncProfileBootstrap -h HOST -p PORT -D wlsuser {-file | -profile}
[-loadParallelism] [-loadRetry] [-help]

```

Arguments for syncProfileBootstrap

-h | -host

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

-p | -port

Listen port of Oracle WebLogic ManagedServer 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.

-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.

Tasks and Examples for syncProfileBootstrap

```
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
```

expressSyncSetup

The Express Synchronization Setup utility, `expressSyncSetup`, creates import and export synchronizations profiles.

Syntax for expressSyncSetup

expressSyncSetup

```
expressSyncSetup -h hostName -p PORT -D wlsuser -pf profile \  
-conDirType connectedDirectoryType -conDirURL connected_directory_url \  
-conDirBindDN connected_directory_bind_dn -conDircontainer syncContainer \  
[-enableProfiles {true | false}] [-help]
```

Arguments for expressSyncSetup

-h | -host

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

-p | -port

Listen port of Oracle WebLogic ManagedServer 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
```

-enableProfiles

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

-help

Provides command usage help.

Tasks and Examples for `expressSyncSetup`

```
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
```

provProfileBulkProv

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

Syntax for `provProfileBulkProv`

provProfileBulkProv

```
provProfileBulkProv -h HOST -p PORT -D wlsuser -file ldif_file -realm realm_dn \  
[-encoding input_encoding] [-help]
```

Arguments for provProfileBulkProv

-h | -host

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

-p | -port

Listen port of Oracle WebLogic ManagedServer 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.

-encoding

Input file encoding.

-help

Provides command usage help.

Tasks and Examples for provProfileBulkProv

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

oidprovtool

Provisioning enables you to ensure that an application is notified of directory changes, such as changes to user or group information. Such changes can affect whether the application allows a user access to its processes and resources.

When you install an application that you want to provision, you must create a provisioning integration profile by using the Provisioning Registration Tool (`oidprovtool`).

You can use the Provisioning Registration Tool to:

- Create a new provisioning profile. A new provisioning profile is created and set to the enabled state so that Oracle Directory Integration Platform can process it.

- Disable an existing provisioning profile.
- Enable a disabled provisioning profile.
- Modify an existing provisioning profile.
- Delete an existing provisioning profile.
- Get the current status of a given provisioning profile.
- Clear all of the errors in an existing provisioning profile.

The Provisioning Registration Tool shields the location and schema details of the provisioning profile entries from the callers of the tool. From the callers' perspective, the combination of an application and a realm uniquely identify a provisioning profile. The constraint in the system is that there can be only one provisioning profile for each application for each realm.

Once a profile is created, its mode—that is, INBOUND, OUTBOUND, or BOTH—cannot be changed by using the `modify` operation. To change the mode, you must delete, then re-create, the profile.

The Oracle directory integration platform server automatically monitors provisioning profile configuration changes in Oracle Internet Directory, including the creation, modification, and deletion of provisioning profiles. For this reason, you do not need to manually enable or disable a provisioning profile.

Note: For improved security, do not supply a password on the command line. The `oidprovtool` command prompts you for a password if you do not supply one on the command line.

Syntax for oidprovtool

oidprovtool

```
oidprovtool operation=[create|modify] ldap_host=oid_hostname ldap_port=port
ldap_user_dn="bindDN" ldap_user_password=password
[profile_mode=INBOUND|OUTBOUND|BOTH]
application_dn="DN" application_type=type [application_name=name]
[application_display_name=display name] organization_dn=DN
[application_isdasvisible=TRUE|FALSE] [manage_application_defaults=TRUE|FALSE]
[enable_bootstrap=TRUE|FALSE] [user_data_location=DN]
[default_provisioning_policy=PROVISIONING_REQUIRED|PROVISIONING_NOT_REQUIRED]
interface_name=SCHEMA.PACKAGE [interface_type=PLSQL|JAVA]
interface_version=1.1|2.0|3.0 interface_connect_info=connection_string
schedule=number_seconds lastchangenumber=number
max_prov_failure_limit=number
max_events_per_schedule=number max_events_per_invocation=number
event_mapping_rules="OBJECT_TYPE:FILTER:DOMAIN"
event_permitted_operations="OBJECT:DOMAIN:OPERATION(attributes,...)"
event_subscription="USER|GROUP:DOMAIN:OPERATION(attributes,...)"
max_events_per_schedule=number max_retries=number profile_group=number
profile_status=ENABLED | DISABLED profile_debug=debug_level

oidprovtool {operation=enable|disable|delete|status|reset}
application_dn=DN [organization_dn=DN] [ldap_host=oid_hostname] [ldap_port=port]
[ldap_user_dn=bindDN] [ldap_user_password=password] [profile_debug=debug_level]
```

Arguments for oidprovtool

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

Required. The operation to perform using `oidprovtool`. You can only perform one operation at a time. The operations are:

- `create`—Creates a new provisioning profile.
- `modify`—Modifies the given properties of an existing provisioning profile.
- `enable`—Enables a provisioning profile.
- `disable`—Disables a provisioning profile.
- `delete`—Deletes a provisioning profile.
- `status`—Shows the current status of a given provisioning profile.
- `reset`—Clears all errors for a provisioning profile.

ldap_host=oid_hostname

Optional. The host name of the Oracle Internet Directory server. If not provided then the name of the local host is used.

ldap_port=port

Optional. The LDAP listening port of Oracle Internet Directory. The default is 3060.

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`.

ldap_user_password=password

Optional. The user password used to bind to the 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.

profile_mode=OUTBOUND | INBOUND | BOTH

Optional for the `create` operation only. The direction of the provisioning events. The default is `OUTBOUND` (data is provisioned from Oracle Internet Directory to the application).

application_dn=DN

Required. The distinguished name of the application to which the provisioning subscription belongs. The combination of the application DN and organization DN uniquely identifies a provisioning profile. For example, here is the application DN for Portal:

```
"orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext"
```

application_type=type

Required. The type of application being provisioned.

application_name=name

Optional. The name of the application being provisioned. If not provided, defaults to the distinguished name assigned to `application_dn`.

application_display_name=*name*

Optional. The display name of the application being provisioned. If not provided, defaults to the value assigned to `application_name`.

organization_dn=*DN*

Optional. If not provided, defaults to the default identity management realm. The distinguished name of the organization to which the provisioning subscription belongs, for example "dc=company, dc=com". The combination of the application DN and organization DN uniquely identifies a provisioning profile.

application_isdasvisible=TRUE | FALSE

Optional. Determines whether the application is visible as a provisioning-integrated application in the Oracle Internet Directory Provisioning Console. The default value is TRUE.

manage_application_default=TRUE | FALSE

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

enable_bootstrap=TRUE | FALSE

Optional. Indicates whether the application should receive provisioning events for users that existed in Oracle Internet Directory before creating the application's provisioning integration profile. The default value is FALSE.

user_data_location=*DN*

Optional. Identifies the DN of the container in which to store application-specific user information.

default_provisioning_policy=PROVISIONING_REQUIRED | PROVISIONING_NOT_REQUIRED

Optional. Specifies the application's default provisioning policy. The default value is PROVISIONING_REQUIRED.

interface_name=SCHEMA.PACKAGE

Required for `create` or `modify` operations. The database schema name for the PLSQL package. The format of the value is `schema.package_name`, for example here is the schema and PLSQL package information for Portal:

```
interface_name=PORTAL.WWSEC_OID_SYNC
```

interface_version=1.1 | 2.0 | 3.0

The version of the interface protocol. Allowed values are 1.1, 2.0, or 3.0. The default value is 2.0.

interface_type=PLSQL | JAVA

Optional. The type of interface to which events will be propagated. The default is PLSQL.

interface_connect_info=*connection_string*

Required for `create` or `modify` operations. To connect to an Oracle database and propagate events, use one of the following formats for the connection string:

- `DBURL=ldap://ldaphost:ldapport/service:username:password` (recommended)

- *host:port:sid:username:password*
- *DBSVC=service:username:password*

schedule=number_seconds

Optional for `create` and `modify` operations only. The number of seconds between executions of this profile. The default is 3600, which means the profile is scheduled to be executed every hour.

lastchangenumber=number

Optional for `create` and `modify` operations on `OUTBOUND` events only. The last change number in Oracle Internet Directory after which all qualifying events should be provisioned to the application. Defaults to the latest current change number.

max_prov_failure_limit=number

Optional. Determines the number of times the Oracle Provisioning System attempts to provision a user. The default is 1.

max_events_per_schedule=number

Optional for `create` and `modify` operations only. The maximum number of events that the Oracle directory integration platform server sends to an application during one execution of a provisioning profile. The default is 100.

max_events_per_invocation=number

Optional for `create` and `modify` operations only. The maximum number of events that can be packaged and sent to a target in one invocation of the interface.

event_mapping_rules="OBJECT_TYPE:FILTER:DOMAIN"

Required for `create` and `modify` operations on `INBOUND` events only. This rule maps the object type received from the application (using an optional filter condition) to a domain in Oracle Internet Directory. A provisioning profile can have multiple mapping rules defined.

The following example shows two mapping rules. The first rule shows that an employee object (`EMP`) whose locality attribute equals America (`l=AMERICA`) should be mapped to the domain `l=AMER, cn=users, dc=company, dc=com`. The second rule shows that an employee object (`EMP`) should be mapped to the domain `cn=users, dc=company, dc=com` (no filter conditions).

```
event_mapping_rules="EMP:l=AMERICA:l=AMER,cn=users,dc=company,dc=com"
event_mapping_rules="EMP::cn=users,dc=company,dc=com"
```

event_permitted_operations="OBJECT:DOMAIN:OPERATION(attributes,...)"

Required for `create` and `modify` operations on `INBOUND` events only. This property is used to define the types of events that the application is allowed to send to the Oracle Directory Integration Platform service. A provisioning profile can have multiple permitted operations defined.

For example, if you wanted to permit the application to send events whenever a user object was added or deleted, or when certain attributes were modified, you would have three permitted operations such as this:

```
event_permitted_operations="USER:dc=mycompany,dc=com:ADD(*)"
event_permitted_operations="USER:dc=mycompany,dc=com:MODIFY(cn,sn,mail,password)"
event_permitted_operations="USER:dc=mycompany,dc=com:DELETE(*)"
```

event_subscription="USER | GROUP:DOMAIN:OPERATION(attributes,...)"

Required for `create` and `modify` operations on `OUTBOUND` events only. This property is used to define the types of events that the Oracle Directory Integration Platform service should send to the application. A provisioning profile can have multiple event subscriptions defined.

For example, if you wanted the directory integration server to send events to the application whenever a user or group object was added or deleted, you would have four event subscriptions such as this:

```
event_subscription="GROUP:dc=mycompany,dc=com:ADD(*)"  
event_subscription="GROUP:dc=mycompany,dc=com:DELETE(*)"  
event_subscription="USER:dc=mycompany,dc=com:ADD(*)"  
event_subscription="USER:dc=mycompany,dc=com:DELETE(*)"
```

max_events_per_schedule=number

Optional for `create` and `modify` operations only. The maximum number of events to be provisioned in one schedule. The default is 100.

max_retries=number

Optional for `create` and `modify` operations only. The number of times a failed event should be retried. The default is 5.

profile_group=number

Required for `create` and `modify` operations only. The group number of the profile. Default is "DEFAULT". This is required to address scalability issues when different Oracle Directory Integration Platform server instances will be used to execute different selected groups.

profile_status=ENABLED | DISABLED

Required for the `create` operation only. Determines whether the profile is enabled or disabled. The default is `ENABLED`.

profile_debug=debug_level

Required. The debug level for the profile.

Tasks and Examples for oidprovtool

Using the Provisioning Registration Tool (`oidprovtool`) you can perform the following tasks:

- [Creating a Provisioning Profile](#)
- [Modifying a Provisioning Profile](#)
- [Deleting a Provisioning Profile](#)
- [Disabling a Provisioning Profile](#)

Creating a Provisioning Profile

The following example creates a new provisioning profile that makes Portal aware of updates to the user and group information that is maintained in Oracle Internet Directory.

Example:

```
oidprovtool operation=create ldap_host=myhost.mycompany.com ldap_port=3060 \
```

```

ldap_user_dn="cn=orcladmin" application_
dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext" \
organization_dn="dc=us,dc=mycompany,dc=com" interface_name=PORTAL.WWSEC_OID_SYNC \
interface_type=PLSQL interface_connect_info=myhost:1521:iasdb:PORTAL:password \
schedule=360 event_subscription="USER:dc=us,dc=mycompany,dc=com:DELETE" \
event_subscription="GROUP:dc=us,dc=mycompany,dc=com:DELETE" \
event_
subscription="USER:dc=us,dc=mycompany,dc=com:MODIFY(orclDefaultProfileGroup,userpa
ssword)" \
event_subscription="GROUP:dc=us,dc=mycompany,dc=com:MODIFY(uniqueMember)" \
profile_mode=OUTBOUND

```

Modifying a Provisioning Profile

The following example modifies an existing provisioning profile for the Portal application. It changes the event subscription for the attributes that are provisioned when a user entry is modified.

Example:

```

oidprovtool operation=modify ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin" application_
dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext" \
organization_dn="dc=us,dc=mycompany,dc=com" \
subscription="USER:dc=us,dc=mycompany,dc=com:MODIFY(orclDefaultProfileGroup,userpa
ssword,mail,cn,sn)"

```

Deleting a Provisioning Profile

The following example disables a provisioning profile for the Portal application.

Example:

```

oidprovtool operation=delete ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin" application_
dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext" \
organization_dn="dc=us,dc=mycompany,dc=com"

```

Disabling a Provisioning Profile

The following example disables a provisioning profile for the Portal application.

Example:

```

oidprovtool operation=disable ldap_host=myhost.mycompany.com ldap_port=3060 \
ldap_user_dn="cn=orcladmin" application_
dn="orclApplicationCommonName=PORTAL,cn=Portal,cn=Products,cn=OracleContext" \
organization_dn="dc=us,dc=mycompany,dc=com"

```

dipStatus

The `dipStatus` utility allows you to check the status of Oracle Directory Integration Platform and whether or not it is registered.

Syntax for dipStatus

dipStatus

```
dipStatus -h HOST -p PORT -D wlsuser [-help]
```

Arguments for dipStatus

-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 ManagedServer 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.

-help

Provides usage help for the command.

Examples for dipStatus

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

```
dipStatus -help
```

schemasync

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.

The errors that occur during schema synchronization are logged in the following files:

- `ORACLE_HOME/ldap/odi/log/attributetypes.log`
- `ORACLE_HOME/ldap/odi/log/objectclasses.log`

Syntax for schemasync

schemasync

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

Arguments for schemasync

-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"` on page 3-31 to upload the definitions from these two files, first attribute types and then object classes.

Tasks and Examples for schemasync

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

- [Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory](#)

Synchronizing the Schema between Oracle Internet Directory and a Third-Party Directory

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

Example:

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

Related Command-Line Tools for schemasync

- See "[ldapmodify](#)" on page 3-31

Part II

LDAP Schema Reference

Part II of the *Oracle Fusion Middleware User Reference for Oracle Identity Management Suite* contains information about the LDAP schema elements for Oracle Identity Management.

Part II contains the following chapters:

- [Chapter 6, "LDAP Schema Overview"](#)
- [Chapter 7, "Object Class Reference"](#)
- [Chapter 8, "Attribute Reference"](#)

LDAP Schema Overview

This chapter provides an overview of some of the basic concepts of the LDAP directory schema, and provides categorized lists of the schema elements for Oracle Identity Management. This chapter contains the following topics:

- [Overview of Directory Schema](#)
- [Overview of Oracle Identity Management Schema Elements](#)

Overview of Directory Schema

A directory schema specifies, among other rules, the types of objects that a directory may have and the mandatory and optional attributes of each object type. The Lightweight Directory Access Protocol (LDAP) version 3 defines a schema based on the X.500 standard for common objects found in a network, such as countries, localities, organizations, people, groups, and devices. In the LDAP v3, the schema is available from the directory. That is, it is represented as entries in the directory and its information as attributes of those entries.

Object Classes

An object class is an LDAP directory term that denotes the type of object being represented by a directory entry or record. There are also object classes that define an object's relationship to other objects, such as object class `top` denotes that the object may have subordinate objects under it in a hierarchical tree structure. Some LDAP object classes may be combined to create an entry in the directory. For example, an entry for a user uses the `top`, `person`, `organizationalPerson`, `inetOrgPerson`, and `orclUserV2` object classes.

Required and Allowed Attributes

The definition of an object class includes a list of required attributes (MUST) and allowed attributes (MAY). Required attributes include the attributes that must be present in entries using the object class. Allowed attributes include the attributes that may be present in entries using the object class.

Object Class Types

The X.500 1993 specification requires that object classes be assigned to one of four categories:

- **Structural:** Object classes that can have instances in the directory. Structural classes are used to create directory objects or entries.
- **Abstract:** Template object classes that are used only to derive new structural classes. Abstract classes cannot be instantiated in the directory.

- **Auxiliary:** A list of attributes that can be appended to the definition of a Structural or Abstract class. An Auxiliary class cannot be instantiated in the directory.
- **88 Classes:** Assigning object classes to categories was not required in the X.500 1988 specification. Classes that were defined prior to the X.500 1993 standards, default to the 88 class. Do not define new 88 classes.

Object Class Inheritance

Inheritance, which is also referred to as derivation, is the ability to build new object classes from existing object classes. The new object is defined as a subclass of the parent object. A subclass is a class that inherits from some other class; for example, a subclass inherits structure and content rules from the parent. The parent object becomes a superclass of the new object. A superclass is a class from which one or more other classes inherit information.

Attributes

Directory data is represented as attribute-value pairs. Any piece of information in the directory is associated with a descriptive attribute. For example, the `cn` (`commonName`) attribute is used to store a nickname. A person named William (Bill) Smith can be represented in the directory as:

```
cn: Bill Smith
```

Attribute Name Limitations

The length of an attribute name must not exceed 127 characters. For more information about attribute management, refer to the *Oracle Fusion Middleware Administrator's Guide for 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: `& { } < > " ' ()`

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.
Printable String 1.3.6.1.4.1.1466.115.121.1.44	A string that does NOT allow extended characters. Values for this attribute are not case-sensitive.
Telephone Number 1.3.6.1.4.1.1466.115.121.1.50	Values for this attribute are in the form of telephone numbers.

Attribute Aliases

As of 11g Release 1 (11.1.1), you can create aliases for attribute names. For example, you could create the user-friendly alias `surname` for the attribute `sn`. Once you create an alias for an attribute name, a user can specify the alias instead of the attribute name in an LDAP operation.

You define an alias for an attribute in the LDAP schema definition of the attribute. The directory schema operational attribute `attributeTypes` has been enhanced to allow you to include aliases in the attribute name list. In previous releases, the format for an attribute name list was:

```
attributeTypes=( ObjectIdentifier NAME 'AttributeName' ... )
```

As of 11g Release 1 (11.1.1), 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 "Attribute Aliases In the Directory" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

Matching Rules

Matching rules are the rules for matching two attribute values that comply with the same attribute syntax. Oracle Internet Directory recognizes the following matching rule definitions in the schema.

- accessDirectiveMatch
- IntegerMatch
- bitStringMatch
- numericStringMatch
- caseExactMatch
- objectIdentifierFirstComponentMatch
- caseExactIA5Match
- ObjectIdentifierMatch
- caseIgnoreIA5Match
- OctetStringMatch
- caseIgnoreListMatch
- presentationAddressMatch
- caseIgnoreMatch
- protocolInformationMatch
- caseIgnoreOrderingMatch
- telephoneNumberMatch
- distinguishedNameMatch
- uniqueMemberMatch
- generalizedTimeMatch
- generalizedTimeOrderingMatch
- orclpkimatchingrule

Of the matching rules in the previous list, Oracle Internet Directory actually enforces the following when it compares attribute values:

- distinguishedNameMatch
- caseExactMatch
- caseIgnoreMatch
- numericStringMatch
- IntegerMatch
- telephoneNumberMatch
- orclpkimatchingrule

Sizing of Attribute Values

Attribute syntax does not put any specific size constraint on attribute values. You can, however, specify the size of the attribute value when defining the attribute. Some attributes in Oracle Internet Directory may have size constraints defined, however length characteristics of an attribute are not enforced.

For example, to limit an attribute `foo` to a size of 64, you would define the attribute as follows:

```
(object_identifier_of_attribute NAME 'foo' EQUALITY caseIgnoreMatch SYNTAX
'object_identifier_of_syntax{64}' )
```

Single-Valued and Multi-Valued Attributes

By default, most attributes are multi-valued. This means that an entry can contain the same attribute with multiple values. For single-valued attributes, only one instance of the attribute can be specified in an entry. For example, the attribute `orclObjectGUID` attribute can only have one possible value.

Attribute Usage

Attribute Usage defines how the attribute is used in the directory. The attribute usage types are:

- **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 Operational Attributes" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

Not User Modifiable

Attributes that are designated as "not user modifiable" can only be modified by the directory server. They cannot be modified by any other user or process.

LDAP Controls

As an LDAP Version 3 directory, Oracle Internet Directory extends the standard LDAP operations by using controls. These are extra pieces of information carried along with existing operations, altering the behavior of the operation. When a client application passes a control along with the standard LDAP command, the behavior of the commanded operation is altered accordingly.

The controls supported by Oracle Internet Directory 11g Release 1 (11.1.1) are listed in [Table 6–2, "Request Controls Supported by Oracle Internet Directory"](#) and [Table 6–3, "Response Controls Supported by Oracle Internet Directory"](#).

Table 6–2 Request Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
1.2.840.113556.1.4.319	OID_SEARCH_PAGING_CONTROL	See the "Extensions to the LDAP Protocol" chapter in Oracle Fusion Middleware 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" chapter in Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management
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 will not send the verifiers to the application. It will send an appropriate password policy error.
2.16.840.1.113894.1.8.3	CONNECT_BY	See the "Extensions to the LDAP Protocol" chapter in Oracle Fusion Middleware 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	PasswordStatusRequest Control	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.

Table 6–2 (Cont.) Request Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory</i> .
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.

Table 6–3 Response Controls Supported by Oracle Internet Directory

Object Identifier	Name	Description
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.
2.16.840.1.113894.1.8.9	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.
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.

Overview of Oracle Identity Management Schema Elements

This section lists the Oracle Identity Management schema elements by category. Each category contains a list of applicable LDAP object classes and attributes that link to the detailed information for the specified attribute or object class. The schema elements are grouped into the following categories:

- [System Operational Schema Elements](#)
- [Oracle Internet Directory Configuration Schema Elements](#)
- [Audit and Error Logging Schema Elements](#)

- [Server Manageability Schema Elements](#)
- [Oracle Directory Replication Schema Elements](#)
- [Oracle Directory Integration 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](#)

System Operational Schema Elements

System operational schema elements are those used by the directory server. System operational object classes are used by the directory server to create entries that pertain to directory server operations. Certain system operational attributes may be available for use on every entry in the directory, regardless of whether they are defined for the object class of the entry. This section contains the following topics:

- [Directory Schema](#)
- [Access Control](#)
- [Change Logs](#)
- [Password Policy](#)

Directory Schema

This section lists the operational attributes and object classes for the directory schema.

Attributes

[attributeTypes](#), [contentRules](#), [ldapSyntaxes](#), [matchingRules](#), [objectClasses](#)

Object Classes

[subschema](#)

Access Control

This section lists the operational attributes for access control.

Attributes

[orclACI](#), [orclEntryLevelACI](#)

Change Logs

This section lists the operational attributes for change logs.

Attributes

[createTimestamp](#), [creatorsName](#), [modifiersName](#), [modifyTimestamp](#)

Password Policy

This section lists the operational attributes for password policy.

Attributes

[orclPwdAccountUnlock](#), [orclPwdIPAccountLockedTime](#), [orclPwdIPFailureTime](#), [orclRevPwd](#), [orclUnsyncRevPwd](#), [pwdAccountLockedTime](#), [pwdChangedTime](#), [pwdExpirationWarned](#), [pwdFailureTime](#), [pwdGraceUseTime](#), [pwdHistory](#), [pwdReset](#)

Oracle Internet Directory Configuration Schema Elements

This section lists the schema elements that pertain to the configuration of Oracle Internet Directory. It contains the following topics:

- [Oracle Internet Directory Server](#)
- [Oracle Context](#)
- [Oracle Network Services](#)
- [Garbage Collection](#)
- [Attribute Uniqueness](#)

Oracle Internet Directory Server

This section lists the attributes and object classes that pertain to the configuration of Oracle Internet Directory server.

Attributes

[namingContexts](#), [orclAnonymousBindsFlag](#), [orclCatalogEntryDN](#), [orclConfigSetNumber](#), [orclCryptoScheme](#), [orclDBType](#), [orclDebugFlag](#), [orclDebugForceFlush](#), [orclDebugOp](#), [orclDIPRepository](#), [orclDirectoryVersion](#), [orclDITRoot](#), [orclEcacheEnabled](#), [orclEcacheMaxEntries](#), [orclEcacheMaxEntSize](#), [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](#)

Oracle Context

This section lists the attributes and object classes that pertain to the configuration of the Oracle Context.

Attributes

[orclCommonAutoRegEnabled](#), [orclCommonContextMap](#), [orclCommonDefaultUserCreateBase](#), [orclCommonGroupCreateBase](#),

[orclCommonNamingAttribute](#), [orclCommonNicknameAttribute](#),
[orclCommonSASLRealm](#), [orclCommonUserSearchBase](#), [orclDefaultSubscriber](#),
[orclProductVersion](#), [orclSubscriberNickNameAttribute](#), [orclSubscriberSearchBase](#),
[orclUserObjectClasses](#), [orclVersion](#)

Object Classes

[orclCommonAttributes](#), [orclCommonAttributesV2](#), [orclRootContext](#),
[orclSchemaVersion](#)

Oracle Network Services

This section lists the attributes and object classes that pertain to the configuration of Oracle Network Services.

Attributes

[labeledURI](#), [orclActiveEndDate](#), [orclActiveStartdate](#), [orclAssocDB](#),
[orclAssocIasInstance](#), [orclEnabled](#), [orclFlexAttribute1](#), [orclIsEnabled](#), [orclMasterNode](#),
[orclNetDescName](#), [orclNetDescString](#), [orclOracleHome](#), [orclServiceInstanceLocation](#),
[orclServiceMember](#), [orclServiceSubscriptionLocation](#), [orclServiceSubType](#),
[orclServiceType](#), [orclSID](#), [orclSuiteType](#), [orclSystemName](#), [orclVersion](#)

Object Classes

[orclService](#), [orclServiceInstance](#), [orclServiceInstanceReference](#), [orclServiceRecipient](#),
[orclServiceSuite](#), [orclServiceSubscriptionDetail](#)

Garbage Collection

This section lists the attributes and object classes that pertain to the configuration of garbage collection.

Attributes

[orclPurgeBase](#), [orclPurgeDebug](#), [orclPurgeEnable](#), [orclPurgeFileLoc](#),
[orclPurgeFileName](#), [orclPurgeFilter](#), [orclPurgeInterval](#), [orclPurgeNow](#),
[orclPurgePackage](#), [orclPurgeStart](#), [orclPurgeTargetAge](#), [orclPurgeTranSize](#)

Object Classes

[orclPurgeConfig](#), [tombstone](#)

Attribute Uniqueness

This section lists the attributes and object classes that pertain to the configuration of attribute uniqueness.

Attributes

[orclUniqueAttrName](#), [orclUniqueEnable](#), [orclUniqueObjectClass](#), [orclUniqueScope](#),
[orclUniqueSubtree](#)

Object Classes

[orclUniqueConfig](#)

Audit and Error Logging Schema Elements

This section lists the attributes and object classes that pertain to audit logs and error logs.

Attributes

orclAuditAttribute, orclAuditMessage, orclDBConnCreationFailed, orclDNSUnavailable, orclEventTime, orclEventType, orclFDIncreaseError, orclMaxFDLimitReached, orclMaxProcessLimitReached, orclMemAllocError, orclNWCongested, orclNwUnavailable, orclOpResult, orclORA28error, orclORA3113error, orclORA3114error, orclSequence, orclThreadSpawnFailed, orclUserDN

Object Classes

orclAuditOC, orclEventLog, orclEvents, orclSysResourceEvents

Server Manageability Schema Elements

This section lists the schema elements for Oracle Internet Directory server manageability statistics.

Attributes

orclACLResultsLatency, orclActiveConn, orclActiveThreads, orclAttrACLEvalLatency, orclAuditMessage, orclBERgenLatency, orclIDBLatency, orclDIMEonlyLatency, orclEcacheHitRatio, orclEcacheNumEntries, orclEcacheSize, orclEntryACLEvalLatency, orclEventTime, orclEventType, orclFilterACLEvalLatency, orclFrontLatency, orclGenObjLatency, orclGetNearACLLatency, orclHostname, orclIdleConn, orclIdleThreads, orclInitialServerMemSize, orclIpAddress, orclLDAPInstanceID, orclLDAPPProcessID, orclOpAbandoned, orclOpCompleted, orclOpenConn, orclOpFailed, orclOpInitiated, orclOpLatency, orclOpPending, orclOpResult, orclOpSucceeded, orclOpTimedOut, orclQueueDepth, orclQueueLatency, orclReadWaitThreads, orclSequence, orclServerAvgMemGrowth, orclSMSpec, orclSQLexeFetchLatency, orclSQLGenReusedParsed, orclTcpConnToClose, orclTcpConnToShutDown, orclTotFreePhyMem, orclTraceDimesionLevel, orclTraceFileLocation, orclTraceFileSize, orclTraceLevel, orclTraceMode, orclUserDN, orclWriteWaitThreads

Object Classes

orclGeneralStats, orclHealthStats, orclPerfStats, orclSecRefreshEvents, orclSM, orclTraceConfig, orclUserStats

Oracle Directory Replication Schema Elements

This section lists the schema elements for directory replication.

Attributes

orclAgreementId, orclChangeLogLife, orclChangeRetryCount, orclConfigSetNumber, orclDirReplGroupAgreement, orclDirReplGroupDSAs, orclExcludedAttributes, orclExcludedNamingContexts, orclHIQSchedule, orclHostname, orclIncludedNamingContexts, orclLastAppliedChangeNumber, orclLDAPConnKeepALive, orclPilotMode, orclPurgeSchedule, orclReplicaDN, orclReplicaID, orclReplicaSecondaryURI, orclReplicaState, orclReplicationProtocol, orclReplicaType, orclReplicaURI, orclReplicaVersion, orclThreadsPerSupplier, orclUpdateSchedule, pilotStartTime

Object Classes

orclReplAgreementEntry, orclReplInstance, orclReplicaSubentry, orclReplNameCtxConfig, orclReplSubConfig

Oracle Directory Integration and Provisioning Schema Elements

This section lists the schema elements for Oracle Directory Integration and Provisioning. It contains the following topics:

- [Applications](#)
- [Change Logs](#)
- [Events and Objects](#)
- [Plug-ins and Interfaces](#)
- [Server Configuration](#)
- [Profiles](#)
- [Schema](#)
- [Active Directory Users](#)

Applications

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning applications.

Attributes

[orclApplicationType](#), [orclInterval](#), [orclODIPAgent](#), [orclODIPApplicationName](#), [orclODIPCommand](#), [orclODIPDbConnectInfo](#), [orclODIPEventSubscriptions](#), [orclOwnerGUID](#), [orclStatus](#), [orclVersion](#)

Object Classes

[orclODIPApplicationCommonConfig](#), [orclODIPAppSubscription](#)

Change Logs

This section lists the attributes and object classes for Oracle Directory Integration and Provisioning change logs.

Attributes

[orclLastAppliedChangeNumber](#), [orclSubscriberDisable](#), [serverName](#), [userPassword](#)

Object Classes

[orclChangeSubscriber](#)

Events and Objects

This section lists the attributes and object classes for Oracle Directory Integration 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

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

Server Configuration

This section lists the attributes and object classes for configuring the Oracle Directory Integration and Provisioning server.

Attributes

cn, orclConfigSetNumber, orclHostname, orclODIPConfigDNs, orclODIPConfigRefreshFlag, orclODIPInstanceStatus, orclODIPProfileExecGroupID, orclODIPSearchCountLimit, orclODIPSearchTimeLimit, orclODIPServerCommitSize, orclODIPServerDebugLevel, orclODIPServerRefreshIntvl, orclODIPServerSSLMode, orclODIPServerWalletLoc, orclSSLEnable, orclVersion, seeAlso, userPassword

Object Classes

orclODIPServerConfig, orclODISConfig, orclODIServer, orclODISInstance

Profiles

This section the attributes and object classes for Oracle Directory Integration 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, orclODIPProfile, orclODIPProvisioningIntegrationProfile,
orclODIPProvisioningIntegrationProfileV2,
orclODIPProvisioningIntegrationOutBoundProfile,
orclODIPProvisioningIntegrationOutBoundProfileV2

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

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

Oracle Delegated Administration Services Schema Elements

This section lists the attributes and object classes for Oracle Delegated Administration Services.

Attributes

orclDASAdminModifiable, orclDASAttrDispOrder, orclDASAttrName,
orclDASEnableProductLogo, orclDASEnableSubscriberLogo, orclDASIsEnabled,
orclDASIsMandatory, orclDASIsPersonal, orclDASLOV, orclDASPublicGroupDNs,
orclDASSearchable, orclDASSearchColIndex, orclDASSearchFilter,
orclDASSearchSizeLimit, orclDASSelfModifiable, orclDASUIType, orclDASURL,
orclDASURLBase, orclDASValidatePwdReset, orclDASViewable

Object Classes

[orclDASAppContainer](#), [orclDASAttrCategory](#), [orclDASConfigAttr](#),
[orclDASConfigPublicGroup](#), [orclDASLOVVal](#), [orclDASOperationURL](#),
[orclDASSubscriberContainer](#)

Oracle Application Server Certificate Authority and PKI Schema Elements

This section lists the attributes and object classes that pertain to public key infrastructure (PKI), certificates, and Oracle Application Server Certificate Authority.

Attributes

[orclCertExtensionAttribute](#), [orclCertExtensionOID](#), [orclCertificateHash](#),
[orclCertificateMatch](#), [orclCertMappingAttribute](#), [orclPKINextUpdate](#),
[orclPKIValMecAttr](#), [x509issuer](#)

Object Classes

[orclCertIdMapping](#), [orclPKICRL](#), [orclPKIValMecCl](#)

Application Schema Elements

This section lists the attributes and object classes that pertain to applications.

Attributes

[authPassword](#), [description](#), [labeledURI](#), [orclAppFullName](#),
[orclApplicationCommonName](#), [orclCategory](#), [orclDBSchemaIdentifier](#),
[orclOwnerGUID](#), [orclPasswordVerifier](#), [orclResourceIdentifier](#),
[orclTrustedApplicationGroup](#), [orclVersion](#), [protocolInformation](#), [seeAlso](#),
[userCertificate;binary](#), [userPassword](#), [userPKCS12](#)

Object Classes

[orclApplicationEntity](#), [orclAppSpecificUserInfo](#), [orclAppUserEntry](#)

Resource Schema Elements

This section lists the attributes and object classes that pertain to resources.

Attributes

[description](#), [displayName](#), [javaClassName](#), [orclConnectionFormat](#), [orclFlexAttribute1](#),
[orclFlexAttribute2](#), [orclFlexAttribute3](#), [orclOwnerGUID](#), [orclPasswordAttribute](#),
[orclResourceName](#), [orclResourceTypeName](#), [orclResourceViewers](#),
[orclUserIDAttribute](#), [orclUserModifiable](#)

Object Classes

[orclResourceDescriptor](#), [orclResourceType](#)

Plug-in Schema Elements

This section lists the attributes and object classes for configuring Plug-ins for Oracle Internet Directory.

Attributes

[orclPluginAttributeList](#), [orclPluginCheckEntryExist](#), [orclPluginEnable](#),
[orclPluginEntryProperties](#), [orclPluginIsReplace](#), [orclPluginKind](#),

[orclPluginLDAPOperation](#), [orclPluginName](#), [orclPluginPort](#), [orclPluginRequestGroup](#), [orclPluginRequestNegGroup](#), [orclPluginResultCode](#), [orclPluginSASLCallBack](#), [orclPluginSearchNotFound](#), [orclPluginShareLibLocation](#), [orclPluginSubscriberDNList](#), [orclPluginTiming](#), [orclPluginType](#), [orclPluginVersion](#), [userPassword](#)

Object Classes

[orclPluginConfig](#), [orclPluginContainer](#), [orclPluginUser](#)

Directory User Agents Schema Elements

This section lists the attributes and object classes for configuring directory user agents (DUAs).

Attributes

[attributeMap](#), [authenticationMethod](#), [bindTimeLimit](#), [cn](#), [credentialLevel](#), [defaultSearchBase](#), [defaultSearchScope](#), [defaultServerList](#), [followReferrals](#), [objectClass](#), [objectClassMap](#), [preferredServerList](#), [profileTTL](#), [serviceAuthenticationMethod](#), [serviceCredentialLevel](#), [serviceSearchDescriptor](#)

Object Classes

[duaConfigProfile](#)

User, Group, and Subscriber Schema Elements

This section lists the attributes and object classes used for users, groups, and subscribers. It contains the following topics:

- [Groups](#)
- [Dynamic Groups](#)
- [Users](#)

Groups

Oracle Internet Directory uses the standard object classes [groupOfNames](#) and [groupOfUniqueNames](#) as defined in RFC 2256. In addition to the standard attributes and object classes, the following are also used for groups.

Attributes

[displayName](#), [mail](#), [orclGlobalID](#), [orclIsVisible](#)

Object Classes

[orclGroup](#)

Dynamic Groups

This section lists the attributes and object classes for dynamic groups.

Attributes

[labeledURI](#), [mail](#), [orclConnectByAttribute](#), [orclConnectBySearchBase](#), [orclConnectByStartingValue](#)

Object Classes

[orclDynamicGroup](#)

Users

Oracle Internet Directory uses the standard object classes `person` and `inetOrgPerson` as defined in RFC 2256. In addition to the standard attributes and object classes, the following are also used for users.

Attributes

`authPassword`, `c`, `jpegPhoto`, `krbPrincipalName`, `middleName`, `orclActiveEndDate`, `orclActiveStartDate`, `orclContact`, `orclDateOfBirth`, `orclDefaultProfileGroup`, `orclDisplayPersonalInfo`, `orclGender`, `orclHireDate`, `orclHostedCreditCardExpireDate`, `orclHostedCreditCardNumber`, `orclHostedCreditCardType`, `orclHostedDunsNumber`, `orclHostedPaymentTerm`, `orclIsEnabled`, `orclIsVisible`, `orclMaidenName`, `orclPassword`, `orclPasswordHint`, `orclPasswordHintAnswer`, `orclPasswordVerifier`, `orclPKCS12Hint`, `orclSAMAccountName`, `orclSearchFilter`, `orclSubscriberFullName`, `orclSubscriberType`, `orclTimeZone`, `orclUIAccessibilityMode`, `orclVersion`, `orclWirelessAccountNumber`, `orclWorkflowNotificationPref`, `userPKCS12`

Object Classes

`orclSubscriber`, `orclUserV2`

Password Policy Schema Elements

This section lists the attributes and object classes that pertain to password policy configuration.

Attributes

`cn`, `displayName`, `orclPwdAllowHashCompare`, `orclPwdAlphaNumeric`, `orclPwdEncryptionEnable`, `orclPwdIllegalValues`, `orclPwdIPLockout`, `orclPwdIPLockoutDuration`, `orclPwdIPMaxFailure`, `orclPwdPolicyEnable`, `pwdAllowUserChange`, `pwdCheckSyntax`, `pwdExpireWarning`, `pwdFailureCountInterval`, `pwdGraceLoginLimit`, `pwdInHistory`, `pwdLockout`, `pwdLockoutDuration`, `pwdMaxAge`, `pwdMaxFailure`, `pwdMinAge`, `pwdMinLength`, `pwdMustChange`, `pwdSafeModify`

Object Classes

`pwdpolicy`

Password Verifier Schema Elements

This section lists the attributes and object classes that pertain to password verifiers.

Attributes

`cn`, `displayName`, `orclAppId`, `orclPwdVerifierParams`, `owner`

Object Classes

`orclPwdVerifierProfile`

Object Class Reference

This chapter contains reference information about the object classes used for Oracle Identity Management. It contains the following topics:

- [Standard LDAP Object Classes](#)
- [Oracle Identity Management Object Class Reference](#)

For a list of object classes grouped by functional categories, see "[Overview of Oracle Identity Management Schema Elements](#)" on page 6-7.

Standard LDAP Object Classes

Oracle Internet Directory supports the following standard LDAP object classes as defined in the Internet Engineering Task Force (IETF) Requests for Comments (RFC) specifications.

Details of RFC specifications can be found on the IETF Web site at: <http://www.ietf.org>.

Table 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

Table 7-1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
domain	RFC 1274
domainRelatedObject	RFC 1274
dsa	RFC 1274
extensibleObject	RFC 2252
friendlyCountry	RFC 1274
groupOfNames	RFC 2256
groupOfUniqueNames	RFC 2256
ieee802Device	RFC 2307
inetOrgPerson	RFC 2798
ipHost	RFC 2307
ipNetwork	RFC 2307
ipProtocol	RFC 2307
ipService	RFC 2307
javaContainer	RFC 2713
javaMarshaledObject	RFC 2713
javaNamingReference	RFC 2713
javaObject	RFC 2713
javaSerializedObject	RFC 2713
labeledURIObject	RFC 2079
locality	RFC 2256
mailRecipient	RFC 2256
newPilotPerson	RFC 2377
nisDomainObject	RFC 2307
nisKeyObject	RFC 2307
nisMap	RFC 2307
nisNetgroup	RFC 2307
nisObject	RFC 2307
oldQualityLabelledData	RFC 2307
oncRpc	RFC 2307
organization	RFC 2256
organizationalPerson	RFC 2256
organizationalRole	RFC 2256
organizationalUnit	RFC 2256
person	RFC 2256
pilotDSA	RFC 2256
pilotObject	RFC 2256
pilotOrganization	RFC 2256

Table 7–1 (Cont.) Standard LDAP Object Classes Used By Oracle Internet Directory

Object Class Name	Specification
posixAccount	RFC 2307
posixGroup	RFC 2307
referral	RFC 3296
residentialPerson	RFC 2256
room	RFC 1274
shadowAccount	RFC 2307
simpleSecurityObject	RFC 1274
strongAuthenticationUser	RFC 2256

Oracle Identity Management Object Class Reference

This section contains an alphabetical listing of the Oracle Identity Management object classes. These are the object classes used to create entries pertaining to Oracle Internet Directory, Oracle Directory Integration 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.

duaConfigProfile

Description

Configuration profile for a directory user agent (DUA). A DUA is software that accesses the LDAP directory service on behalf of the directory user. The directory user may be a person or another software element.

Object ID

1.3.6.1.4.1.11.1.3.1.2.4

Superior Object Class

[top](#)

Object Class Type

88

Required Attributes

[cn](#), [objectClass](#)

Allowed Attributes

[attributeMap](#), [authenticationMethod](#), [bindTimeLimit](#), [credentialLevel](#), [defaultSearchBase](#), [defaultSearchScope](#), [defaultServerList](#), [followReferrals](#), [objectClassMap](#), [preferredServerList](#), [profileTTL](#), [serviceAuthenticationMethod](#), [serviceCredentialLevel](#), [serviceSearchDescriptor](#)

orclADGroup

Description

Contains Microsoft Active Directory group attributes, which are used to synchronize Active Directory group objects with Oracle Internet Directory group objects in an Oracle Directory Integration 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](#)

orclADUser

Description

Contains Microsoft Active Directory user attributes, which are used to synchronize Active Directory user objects with Oracle Internet Directory user objects in an Oracle Directory Integration 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](#)

orclApplicationEntity

Description

Defines an application entity.

Object ID

2.16.840.1.113894.1.2.55

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes

N/A

Allowed Attributes

[authPassword](#), [description](#), [labeledURI](#), [orclAppFullName](#), [orclApplicationAddress](#), [orclApplicationCommonName](#), [orclCategory](#), [orclDBSchemaIdentifier](#), [orclPasswordVerifier](#), [orclResourceIdentifier](#), [orclTrustedApplicationGroup](#), [orclVersion](#), [protocolInformation](#), [seeAlso](#), [userCertificate;binary](#), [userPassword](#), [userPKCS12](#)

orclAppSpecificUserInfo**Description**

An auxiliary object class for an application entity that defines user information.

Object ID

2.16.840.1.13894.8.2.420

Superior Object Class[top](#)**Object Class Type**

Auxilliary

Required Attributes[orclOwnerGUID](#)**Allowed Attributes**

N/A

orclAppUserEntry**Description**

The user associated with an application entity.

Object ID

2.16.840.1.13894.8.2.423

Superior Object Class[top](#)

Object Class Type

Structural

Required Attributes

[orclOwnerGUID](#)

Allowed Attributes

N/A

orclAuditOC

Description

Generic audit log attributes that can be used in a server audit log entry.

Object ID

2.16.840.1.113894.1.2.18

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[orclAuditMessage](#), [orclEventTime](#), [orclEventType](#), [orclSequence](#)

Allowed Attributes

[orclAuditAttribute](#), [orclOpResult](#), [orclUserDN](#)

orclCertIdMapping

Description

Oracle Internet Directory public key infrastructure (PKI) structural object class for mapping attributes in a client certificate to entries in Oracle Internet Directory.

Object ID

2.16.840.1.113894.1.2.130

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[description](#), [orclCertExtensionAttribute](#), [orclCertExtensionOID](#),
[orclCertMappingAttribute](#)

orclChangeSubscriber**Description**

Status information for an Oracle Directory Integration 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](#)

orclCommonAttributes**Description**

Oracle Context configuration attributes.

Object ID

2.16.840.1.113894.7.2.1004

Superior Object Class

[orclContainer](#)

Object Class Type

Structural

Required Attributes

N/A

Allowed Attributes

[orclCommonAutoRegEnabled](#), [orclCommonContextMap](#),
[orclCommonDefaultUserCreateBase](#), [orclCommonGroupCreateBase](#),
[orclCommonNamingAttribute](#), [orclCommonNicknameAttribute](#),
[orclCommonSASLRealm](#), [orclCommonUserSearchBase](#), [orclVersion](#)

orclCommonAttributesV2

Description

Oracle Context configuration attributes.

Object ID

2.16.840.1.113894.1.2.51

Superior Object Class

[top](#)

Object Class Type

88

Required Attributes

N/A

Allowed Attributes

[orclDefaultSubscriber](#), [orclSubscriberNickNameAttribute](#), [orclSubscriberSearchBase](#), [orclUserObjectClasses](#)

orclConfigSet

Description

Configuration set entry for a server instance.

Object ID

2.16.840.1.113894.1.2.2

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[description](#), [seeAlso](#)

orclContainer

Description

Container object for an Oracle Context.

Object ID

2.16.840.1.113894.7.2.2

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[cn](#)**Allowed Attributes**[orclVersion](#), [orclServiceType](#)**orclDASAppContainer****Description**

Container object for a Oracle Delegated Administration Services application.

Object ID

2.16.840.1.113894.1.2.61

Superior Object Class[top](#)**Object Class Type**

Auxilliary

Required Attributes

N/A

Allowed Attributes[orclDASURLBase](#)**orclDASAttrCategory****Description**

Oracle Delegated Administration Services attribute categories.

Object ID

2.16.840.1.113894.1.2.59

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[cn](#), [displayName](#), [orclDASAttrDispOrder](#), [orclDASAttrName](#)

orclDASConfigAttr

Description

Oracle Delegated Administration Services configuration attributes.

Object ID

2.16.840.1.113894.1.2.56

Superior Object Class

[top](#)

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[displayName](#), [orclDASAdminModifiable](#), [orclDASIsMandatory](#), [orclDASIsPersonal](#), [orclDASLOV](#), [orclDASSearchable](#), [orclDASSearchColIndex](#), [orclDASSearchFilter](#), [orclDASSelfModifiable](#), [orclDASUIType](#), [orclDASValidatePwdReset](#), [orclDASViewable](#)

orclDASConfigPublicGroup

Description

Oracle Delegated Administration Services public group configuration attributes.

Object ID

2.16.840.1.113894.1.2.60

Superior Object Class

[top](#)

Object Class Type

Auxilliary

Required Attributes

[cn](#)

Allowed Attributes

[orclDASIsEnabled](#), [orclDASPublicGroupDNs](#)

orclDASLOVVal

Description

Oracle Delegated Administration Services list of values.

Object ID

2.16.840.1.113894.1.1.919

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[cn](#), [displayName](#)**Allowed Attributes**

N/A

orcidASOperationURL**Description**

Oracle Delegated Administration Services URL.

Object ID

2.16.840.1.113894.1.2.54

Superior Object Class[top](#)**Object Class Type**

Auxilliary

Required Attributes

N/A

Allowed Attributes[cn](#), [description](#), [orcidASURL](#)**orcidASSubscriberContainer****Description**

Oracle Delegated Administration Services subscriber container object.

Object ID

2.16.840.1.113894.1.2.66

Superior Object Class

N/A

Object Class Type

Structural

Required Attributes

N/A

Allowed Attributes

[orclDASEnableProductLogo](#), [orclDASEnableSubscriberLogo](#), [orclDASSearchSizeLimit](#)

orclIDMapping

Description

Auxilliary object class defining the attributes that hold information about directory operations to be performed for mapping.

Object ID

2.16.840.1.113894.1.2.131

Superior Object Class

[top](#)

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclMappedDN](#), [orclSearchBaseDN](#), [orclSearchFilter](#), [orclSearchScope](#)

orclDSAConfig

Description

Configuration attributes for Oracle Internet Directory server.

Object ID

2.16.840.1.113894.1.2.70

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclAnonymousBindsFlag](#), [orclCatalogEntryDN](#), [orclCryptoScheme](#), [orclDebugFlag](#), [orclDebugForceFlush](#), [orclDebugOp](#), [orclDIPRepository](#), [orclEcacheEnabled](#), [orclEcacheMaxEntries](#), [orclEcacheMaxEntSize](#), [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](#)

orclDynamicGroup

Description

Attributes that are used to create dynamic groups. A dynamic group is one whose membership, rather than being maintained in a list, is computed on the fly, based on rules and assertions you specify.

Object ID

2.16.840.1.113894.1.2.190

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[labeledURI](#), [mail](#), [orclConnectByAttribute](#) , [orclConnectBySearchBase](#),
[orclConnectByStartingValue](#)

orclEventLog

Description

Object class used for audit logging of server events.

Object ID

2.16.840.1.113894.1.2.17

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

orclEvents

Description

Object class used for audit logging of events.

Object ID

2.16.840.1.113894.1.2.19

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclEventType](#)

orclGeneralStats

Description

Statistical information for Oracle Internet Directory server operations.

Object ID

2.16.840.1.113894.1.2.30

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclOpAbandoned](#), [orclOpCompleted](#), [orclOpInitiated](#), [orclOpPending](#), [orclOpTimedOut](#), [orclQueueDepth](#)

orclGroup

Description

Additional optional attributes for a group.

Object ID

2.16.840.1.113894.1.2.53

Superior Object Class[top](#)**Object Class Type**

Auxilliary

Required Attributes

N/A

Allowed Attributes[displayName](#), [mail](#), [orclGlobalID](#), [orclIsVisible](#)**orclHealthStats****Description**

Statistical information for Oracle Internet Directory server performance.

Object ID

2.16.840.1.113894.1.2.27

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes[orclActiveThreads](#), [orclEcacheHitRatio](#), [orclEcacheNumEntries](#), [orclEcacheSize](#), [orclIdleConn](#), [orclIdleThreads](#), [orclInitialServerMemSize](#), [orclOpenConn](#), [orclQueueDepth](#), [orclQueueLatency](#), [orclReadWaitThreads](#), [orclServerAvgMemGrowth](#), [orclTcpConnToClose](#), [orclTcpConnToShutDown](#), [orclTotFreePhyMem](#), [orclWriteWaitThreads](#)**orclIndexOC****Description**

Configuration of the indexed attributes for the Oracle Internet Directory server.

Object ID

2.16.840.1.113894.1.2.15

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclIndexedAttribute](#)

orclLDAPInstance

Description

Configuration attributes for an Oracle Internet Directory server instance.

Object ID

2.16.840.1.113894.1.2.13

Superior Object Class

[top](#), [orclLDAPSubConfig](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclConfigSetNumber](#), [orclHostname](#)

Allowed Attributes

[description](#), [seeAlso](#)

orclLDAPSubConfig

Description

Configuration attributes for Oracle Internet Directory server.

Object ID

2.16.840.1.113894.1.2.3

Superior Object Class

[top](#), [orclConfigSet](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclMaxCC](#), [orclNonSSLPort](#), [orclSASLAuthenticationMode](#), [orclSASLCipherChoice](#), [orclSASLMechanism](#), [orclServerProcs](#), [orclSSLAAuthentication](#), [orclSSLCipherSuite](#), [orclSSLEnable](#), [orclSSLPort](#), [orclSSLVersion](#), [orclSSLWalletURL](#)

orclNTUser

Description

Contains Microsoft NT user attributes, which are used to synchronize NT user objects with Oracle Internet Directory user objects in an Oracle Directory Integration 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](#)

orclODIPApplicationCommonConfig

Description

Oracle Directory Integration and Provisioning configuration attributes.

Object ID

2.16.840.1.13894.8.2.421

Superior Object Class

[top](#)

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclApplicationType](#)

orclODIPAppSubscription

Description

Application subscription attributes for Oracle Directory Integration 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](#)

orclODIPEventContainer

Description

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](#)

orclODIPIntegrationProfile

Description

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](#)

orclODIPObject**Description**

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](#)

orclODIPPlugin**Description**

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](#)

orclODIPPluginContainer

Description

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](#)

orclODIPProvEventDefn

Description

Defines a provisioning event.

Object ID

2.16.840.1.113894.8.2.413

Superior Object Class

N/A

Object Class Type

88

Required Attributes

N/A

Allowed Attributes

[cn](#), [orclODIPEventFilter](#), [orclODIPObjectEvents](#), [orclODIPObjectName](#), [orclODIPObjectSyncBase](#), [orclODIPProvEventRule](#), [orclStatus](#)

orclODIPProvEventTypeConfig

Description

Configuration attributes for a provisioning event type.

Object ID

2.16.840.1.113894.8.2.500

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[orclODIPProvEventObjectType](#)**Allowed Attributes**[orclODIPProvEventCriteria](#), [orclODIPProvEventLDAPChangeType](#)

orclODIPProvInterfaceDetails

Description

Provisioning interface details.

Object ID

2.16.840.1.113894.8.2.16

Superior Object Class[top](#)**Object Class Type**

Auxilliary

Required Attributes[orclODIPProfileInterfaceType](#), [orclODIPProfileProvSubscriptionMode](#)**Allowed Attributes**[orclODIPProfileStatusUpdate](#), [orclODIPProvInterfaceFilter](#),
[orclODIPProvInterfaceProcessor](#)

orclODIPProvisioningIntegrationInBoundProfileV2

Description

Configuration for an Oracle Directory Integration 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](#)

orclODIPProvisioningIntegrationOutBoundProfile

Description

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 10g.

Object ID

2.16.840.1.113894.8.2.404

Superior Object Class

[top](#), [orclChangeSubscriber](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclODIPProvisioningAppGUID](#), [orclODIPProvisioningEventSubscription](#)

Allowed Attributes

[orclODIPProfileProvSubscriptionMode](#), [orclODIPProfileLastProcessingTime](#),
[orclODIPProfileLastSuccessfulProcessingTime](#), [orclODIPProfileProcessingErrors](#),
[orclODIPProfileProcessingStatus](#), [orclStatus](#), [orclVersion](#)

orclODIPProvisioningIntegrationOutBoundProfileV2

Description

Configuration for an Oracle Directory Integration 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](#)

orclODIPProvisioningIntegrationProfile

Description

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 10g.

Object ID

2.16.840.1.113894.8.2.400

Superior Object Class

[top](#), [orclODIPIntegrationProfile](#), [orclChangeSubscriber](#)

Object Class Type

Structural

Required Attributes

[orclODIPProvisioningAppName](#), [orclODIPProvisioningAppGUID](#), [orclODIPProvisioningOrgName](#), [orclODIPProvisioningOrgGUID](#), [orclODIPProvisioningEventSubscription](#)

Allowed Attributes

N/A

orclODIPProvisioningIntegrationProfileV2

Description

Configuration for an Oracle Directory Integration 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

orclODIPProfile

Description

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

orclODIPSchemaDetails

Description

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](#)

orclODIPServerConfig**Description**

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](#)

orclODISConfig**Description**

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](#)

orclODIServer

Description

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](#)

orclODISInstance

Description

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](#)

orclPerfStats

Description

Oracle Internet Directory Server Manageability performance statistics.

Object ID

2.16.840.1.113894.1.2.26

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclACLResultsLatency](#), [orclAttrACLEvalLatency](#), [orclBERgenLatency](#), [orclDBLatency](#), [orclDIMEonlyLatency](#), [orclEntryACLEvalLatency](#), [orclFilterACLEvalLatency](#), [orclFrontLatency](#), [orclGenObjLatency](#), [orclGetNearACLLatency](#), [orclOpLatency](#), [orclSQLexefetchLatency](#), [orclSQLGenReusedParsed](#)

orclPKICRL**Description**

Oracle Application Server Certificate Authority certificate revocation list (CRL).

Object ID

2.16.840.1.113894.2.2.300.1

Superior Object Class[crlDistributionPoint](#) (RFC 2256)**Object Class Type**

Structural

Required Attributes[cn](#)**Allowed Attributes**[orclPKINextUpdate](#), [x509issuer](#)**orclPKIVaMecCI****Description**

Used by Oracle Application Server Certificate Authority.

Object ID

2.16.840.1.113894.2.2.300.2

Superior Object Class[orclContainer](#)**Object Class Type**

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclPKIVaMecAttr](#)

orclPluginConfig

Description

Configuration attributes for Oracle Internet Directory plug-ins.

Object ID

2.16.840.1.113894.1.2.90

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclPluginLDAPOperation](#), [orclPluginName](#), [orclPluginType](#)

Allowed Attributes

[orclPluginAttributeList](#), [orclPluginCheckEntryExist](#), [orclPluginEnable](#), [orclPluginEntryProperties](#), [orclPluginIsReplace](#), [orclPluginKind](#), [orclPluginRequestGroup](#), [orclPluginRequestNegGroup](#), [orclPluginResultCode](#), [orclPluginSASLCallBack](#), [orclPluginSearchNotFound](#), [orclPluginShareLibLocation](#), [orclPluginSubscriberDNList](#), [orclPluginTiming](#), [orclPluginVersion](#)

orclPluginContainer

Description

Container object for Oracle Internet Directory plug-ins.

Object ID

2.16.840.1.113894.1.2.92

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclPluginPort](#)

orclPluginUser

Description

Configuration attributes for Oracle Internet Directory plug-ins.

Object ID

2.16.840.1.113894.1.2.91

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [userPassword](#)

Allowed Attributes

[description](#)

orclPurgeConfig

Description

Configuration attributes for Oracle Internet Directory garbage collectors. Oracle Internet Directory provides several predefined garbage collectors that, together, clean up all unwanted data in the directory server.

Object ID

2.16.840.1.113894.1.2.150

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclPurgeBase](#)

Allowed Attributes

[orclPurgeDebug](#), [orclPurgeEnable](#), [orclPurgeFileLoc](#), [orclPurgeFileName](#), [orclPurgeFilter](#), [orclPurgeInterval](#), [orclPurgeNow](#), [orclPurgePackage](#), [orclPurgeStart](#), [orclPurgeTargetAge](#), [orclPurgeTranSize](#)

orclPwdVerifierPolicy

Description

A password verifier policy entry associates a password policy with an application.

Object ID

2.16.840.1.113894.1.2.42

Superior Object Class

[pwdpolicy](#)

Object Class Type

Auxilliary

Required Attributes

[orclAppId](#)

Allowed Attributes

N/A

orclPwdVerifierProfile

Description

Oracle Internet Directory and other Oracle components both store the user password in the user entry, but use different attributes. A password verifier profile entry associates the correct user password attribute with a component or application.

Object ID

2.16.840.1.113894.1.2.41

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclAppId](#)

Allowed Attributes

[displayName](#), [orclPwdVerifierParams](#), [owner](#)

orclReplAgreementEntry

Description

Configuration attributes for replication.

Object ID

2.16.840.1.113894.1.2.8

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes[orclAgreementId](#), [orclReplicationProtocol](#), [orclUpdateSchedule](#)**Allowed Attributes**[orclDirReplGroupDSAs](#), [orclExcludedAttributes](#), [orclExcludedNamingContexts](#), [orclHIQSchedule](#), [orclIncludedNamingContexts](#), [orclLastAppliedChangeNumber](#), [orclLDAPConnKeepALive](#), [orclReplicaDN](#)**orclReplicaSubentry****Description**

Configuration attributes for replication.

Object ID

2.16.840.1.113894.1.2.151

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[orclReplicaID](#)**Allowed Attributes**[orclPilotMode](#), [orclReplicaSecondaryURI](#), [orclReplicaState](#), [orclReplicaType](#), [orclReplicaURI](#), [orclReplicaVersion](#), [pilotStartTime](#), [seeAlso](#)**orclReplInstance****Description**

Configuration attributes for an Oracle Directory Replication server instance.

Object ID

2.16.840.1.113894.1.2.14

Superior Object Class[top](#), [orclReplSubConfig](#)**Object Class Type**

Structural

Required Attributes[cn](#), [orclConfigSetNumber](#), [orclHostname](#)

Allowed Attributes

[description](#), [seeAlso](#)

orclReplNameCtxConfig

Description

Configuration attributes for replication naming contexts.

Object ID

2.16.840.1.113894.1.2.104

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclIncludedNamingContexts](#)

Allowed Attributes

[orclExcludedAttributes](#), [orclExcludedNamingContexts](#)

orclReplSubConfig

Description

Directory Replication server configuration attributes.

Object ID

2.16.840.1.113894.1.2.4

Superior Object Class

[top](#), [orclConfigSet](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[orclChangeLogLife](#), [orclChangeRetryCount](#), [orclDirReplGroupAgreement](#),
[orclPurgeSchedule](#), [orclThreadsPerSupplier](#)

orclResourceDescriptor

Description

Configuration attributes for a resource.

Object ID

2.16.840.1.113894.1.2.65

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[orclResourceName](#)**Allowed Attributes**[description](#), [displayName](#), [orclFlexAttribute1](#), [orclFlexAttribute2](#), [orclFlexAttribute3](#), [orclOwnerGUID](#), [orclPasswordAttribute](#), [orclResourceTypeName](#), [orclResourceViewers](#), [orclUserIDAttribute](#), [orclUserModifiable](#)

orclResourceType

Description

Configuration attributes for resource types.

Object ID

2.16.840.1.113894.1.2.63

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[orclResourceTypeName](#)**Allowed Attributes**[description](#), [javaClassName](#), [orclConnectionFormat](#), [orclFlexAttribute1](#), [orclFlexAttribute2](#), [orclFlexAttribute3](#), [orclPasswordAttribute](#), [orclUserIDAttribute](#)

orclRootContext

Description

Configuration of the Oracle Context.

Object ID

2.16.840.1.113894.7.2.1006

Superior Object Class[top](#)

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[description](#)

orclSchemaVersion

Description

Configuration of the Oracle Context.

Object ID

2.16.840.1.113894.7.2.6

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclProductVersion](#)

Allowed Attributes

N/A

orclSecRefreshEvents

Description

Oracle Internet Directory Server Manageability attributes for security refresh events.

Object ID

2.16.840.1.113894.1.2.28

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclAuditMessage](#), [orclEventType](#), [orclOpResult](#), [orclUserDN](#)

orclService

Description

Configuration attributes for a service.

Object ID

2.16.840.1.113894.7.2.1001

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#)

Allowed Attributes

[description](#), [orclNetDescName](#), [orclNetDescString](#), [orclOracleHome](#), [orclServiceType](#), [orclSID](#), [orclSystemName](#), [orclVersion](#)

orclServiceInstance

Description

Configuration attributes for a service instance.

Object ID

2.16.840.1.113894.1.2.191

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

[cn](#), [orclServiceType](#)

Allowed Attributes

[description](#), [displayName](#), [labeledURI](#), [orclAssocDB](#), [orclAssocInstance](#), [orclEnabled](#), [orclFlexAttribute1](#), [orclMasterNode](#), [orclNetDescName](#), [orclNetDescString](#), [orclOracleHome](#), [orclServiceSubType](#), [orclSID](#), [orclSystemName](#), [orclVersion](#)

orclServiceInstanceReference

Description

Reference for a service instance.

Object ID

2.16.840.1.113894.1.2.200

Superior Object Class

N/A

Object Class Type

Structural

Required Attributes

N/A

Allowed Attributes

[cn](#), [description](#), [orclServiceInstanceLocation](#), [orclServiceSubscriptionLocation](#), [seeAlso](#)

orclServiceRecipient

Description

Additional attributes for a service recipient.

Object ID

2.16.840.1.113894.1.2.68

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclActiveEndDate](#), [orclActiveStartdate](#), [orclIsEnabled](#)

orclServiceSubscriptionDetail

Description

Service subscription detail.

Object ID

2.16.840.1.113894.1.2.201

Superior Object Class

[orclReferenceObject](#)

Object Class Type

Structural

Required Attributes

N/A

Allowed Attributes[orclActiveEndDate](#), [orclActiveStartdate](#), [orclIsEnabled](#)**orclServiceSuite****Description**

Configuration for a suite of services.

Object ID

2.16.840.1.113894.1.2.193

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[cn](#), [orclSuiteType](#)**Allowed Attributes**[description](#), [displayName](#), [orclEnabled](#), [orclFlexAttribute1](#), [orclServiceMember](#), [orclVersion](#)**orclSM****Description**

Oracle Internet Directory Server Manageability statistics.

Object ID

2.16.840.1.113894.1.2.25

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[orclSequence](#)**Allowed Attributes**[orclEventTime](#), [orclHostname](#), [orclLDAPInstanceID](#), [orclLDAPPProcessID](#), [orclSMSpec](#)

orclSubscriber

Description

Subscriber info for a user entry.

Object ID

2.16.840.1.113894.1.2.58

Superior Object Class

[top](#)

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[c](#), [jpegPhoto](#), [orclContact](#), [orclHostedCreditCardExpireDate](#), [orclHostedCreditCardNumber](#), [orclHostedCreditCardType](#), [orclHostedDunsNumber](#), [orclHostedPaymentTerm](#), [orclSubscriberFullName](#), [orclSubscriberType](#), [orclVersion](#)

orclSysResourceEvents

Description

Error log entry for Oracle Internet Directory server.

Object ID

2.16.840.1.113894.1.2.29

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclDBConnCreationFailed](#), [orclDNSUnavailable](#), [orclEventType](#), [orclFDIncreaseError](#), [orclMaxFDLimitReached](#), [orclMaxProcessLimitReached](#), [orclMemAllocError](#), [orclNWCongested](#), [orclNwUnavailable](#), [orclORA28error](#), [orclORA3113error](#), [orclORA3114error](#), [orclThreadSpawnFailed](#)

orclTraceConfig

Description

Configuration for Oracle Internet Directory Server Manageability.

Object ID

2.16.840.1.113894.1.2.31

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes

N/A

Allowed Attributes[orclTraceDimesionLevel](#), [orclTraceFileLocation](#), [orclTraceFileSize](#), [orclTraceLevel](#), [orclTraceMode](#)**orclUniqueConfig****Description**

Configuration for attributes that must have unique values for each entry that meets the specified requirements.

Object ID

2.16.840.1.113894.1.2.103

Superior Object Class[orclCommonAttributes](#)**Object Class Type**

Structural

Required Attributes[orclUniqueAttrName](#)**Allowed Attributes**[orclUniqueEnable](#), [orclUniqueObjectClass](#), [orclUniqueScope](#), [orclUniqueSubtree](#)**orclUserStats****Description**

Oracle Internet Directory Server Manageability statistics for users.

Object ID

2.16.840.1.113894.1.2.32

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

N/A

Allowed Attributes

[orclACLResultsLatency](#), [orclAttrACLEvalLatency](#), [orclBERgenLatency](#), [orclDBLatency](#), [orclDIMEonlyLatency](#), [orclEntryACLEvalLatency](#), [orclFilterACLEvalLatency](#), [orclFrontLatency](#), [orclGenObjLatency](#), [orclGetNearACLLatency](#), [orclIpAddress](#), [orclOpAbandoned](#), [orclOpCompleted](#), [orclOpenConn](#), [orclOpFailed](#), [orclOpInitiated](#), [orclOpLatency](#), [orclOpPending](#), [orclOpSucceeded](#), [orclOpTimedOut](#), [orclSQLexeFetchLatency](#), [orclSQLGenReusedParsed](#), [orclUserDN](#)

orclUserV2**Description**

Optional attributes for user entries.

Object ID

2.16.840.1.113894.1.2.52

Superior Object Class[top](#)**Object Class Type**

88

Required Attributes

N/A

Allowed Attributes

[authPassword](#), [c](#), [krbPrincipalName](#), [middleName](#), [orclActiveEndDate](#), [orclActiveStartDate](#), [orclDateOfBirth](#), [orclDefaultProfileGroup](#), [orclDisplayPersonalInfo](#), [orclGender](#), [orclHireDate](#), [orclIsEnabled](#), [orclIsVisible](#), [orclMaidenName](#), [orclPassword](#), [orclPasswordHint](#), [orclPasswordHintAnswer](#), [orclPasswordVerifier](#), [orclPKCS12Hint](#), [orclSAMAccountName](#), [orclSearchFilter](#), [orclTimeZone](#), [orclUIAccessibilityMode](#), [orclWirelessAccountNumber](#), [orclWorkflowNotificationPref](#), [userPKCS12](#)

pwdpolicy**Description**

Defines password policy information for a set of users in a given DIT. It contains attributes that define the password policy information for the entire directory.

Object ID

1.3.6.1.4.1.42.2.27.8.2.1

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[cn](#)**Allowed Attributes**

[displayName](#), [orclPwdAllowHashCompare](#), [orclPwdAlphaNumeric](#), [orclPwdEncryptionEnable](#), [orclPwdIllegalValues](#), [orclPwdIPLockout](#), [orclPwdIPLockoutDuration](#), [orclPwdIPMaxFailure](#), [orclPwdPolicyEnable](#), [pwdAllowUserChange](#), [pwdCheckSyntax](#), [pwdExpireWarning](#), [pwdFailureCountInterval](#), [pwdGraceLoginLimit](#), [pwdInHistory](#), [pwdLockout](#), [pwdLockoutDuration](#), [pwdMaxAge](#), [pwdMaxFailure](#), [pwdMinAge](#), [pwdMinLength](#), [pwdMustChange](#), [pwdSafeModify](#)

subentry**Description**

Oracle Internet Directory DIT configuration for subentries.

Object ID

2.5.17.0

Superior Object Class[top](#)**Object Class Type**

Structural

Required Attributes[cn](#)**Allowed Attributes**

N/A

subregistry**Description**

Oracle Internet Directory DIT configuration.

Object ID

2.16.840.1.113894.1.2.12

Superior Object Class[top](#)

Object Class Type

Auxilliary

Required Attributes

[cn](#)

Allowed Attributes

N/A

subschema

Description

Oracle Internet Directory schema elements.

Object ID

2.5.20.1

Superior Object Class

N/A

Object Class Type

Auxilliary

Required Attributes

attributetypes, objectclasses

Allowed Attributes

contentRules, ldapSyntaxes, matchingRules

tombstone

Description

Garbage collector to clean up entries marked as deleted.

Object ID

2.16.840.1.113894.1.2.24

Superior Object Class

[top](#)

Object Class Type

Structural

Required Attributes

N/A

Allowed Attributes

[ref](#)

top**Description**

Contains common and operational attributes used by various objects in Oracle Internet Directory.

Object ID

2.5.6.0

Superior Object Class

N/A

Object Class Type

Abstract

Required Attributes

[objectClass](#)

Allowed Attributes

[authPassword](#), [createTimestamp](#), [creatorsName](#), [modifiersName](#), [modifyTimestamp](#), [orclACI](#), [orclEntryLevelACI](#), [orclGUID](#), [orclNormDN](#), [orclObjectGUID](#), [orclPwAccountUnlock](#), [orclPwIPAccountLockedTime](#), [orclPwIPFailureTime](#), [orclRevPw](#), [orclUnsyncRevPw](#), [pwdAccountLockedTime](#), [pwdChangedTime](#), [pwdExpirationWarned](#), [pwdFailureTime](#), [pwdGraceUseTime](#), [pwdHistory](#)

Attribute Reference

This chapter contains reference information about the LDAP attributes used for Oracle Identity Management. It contains the following topics:

- [Standard LDAP Attributes](#)
- [Oracle Identity Management Attribute Reference](#)

For a list of attributes grouped by functional categories, see "[Overview of Oracle Identity Management Schema Elements](#)" on page 6-7.

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

Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
co	RFC 1274
crossCertificatePair	RFC 2256
dc	RFC 2247
deltaRevocationList	RFC 2256
departmentNumber	RFC 2798
description	RFC 2256
destinationIndicator	RFC 2256
displayName	RFC 2798
dITRedirect	RFC 1274
dmdName	RFC 2256
dNSRecord	RFC 1274
drink	RFC 1274
dSAQuality	RFC 1274
employeeNumber	RFC 2798
employeeType	RFC 2798
facsimileTelephoneNumber	RFC 2256
gecos	RFC 2307
gidNumber	RFC 2307
givenName	RFC 2798
homeDirectory	RFC 2307
homePhone	RFC 1274
homePostalAddress	RFC 1274
host	RFC 1274
initials	RFC 2256
internationalISDNNumber	RFC 2256
ipHostNumber	RFC 2307
ipNetmaskNumber	RFC 2307
ipNetworkNumber	RFC 2307
ipProtocolNumber	RFC 2307
ipServicePort	RFC 2307
ipServiceProtocol	RFC 2307
javaClassName	RFC 2713
javaClassNames	RFC 2307
javaCodebase	RFC 2307
javaDoc	RFC 2307
javaFactory	RFC 2307
javaReferenceAddress	RFC 2713

Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
javaSerializedData	RFC 2713
janetMailbox	RFC 1274
jpegPhoto	RFC 1488
knowledgeInformation	RFC 2256
l	RFC 2256
labeledURI	RFC 2079
lastModifiedBy	RFC 1274
lastModifiedTime	RFC 1274
loginShell	RFC 2307
macAddress	RFC 2307
mail	RFC 2798
mailAlternateAddress	RFC 2256
mailHost	RFC 2256
mailPreferenceOption	RFC 1274
mailRoutingAddress	RFC 2256
manager	RFC 1274
member	RFC 2256
memberNisNetgroup	RFC 2307
memberUid	RFC 2307
mobile	RFC 1274
nisDomain	RFC 2307
nisMapEntry	RFC 2307
nisMapName	RFC 2307
nisNetgroupTriple	RFC 2307
nisPublicKey	RFC 2307
nisSecretKey	RFC 2307
o	RFC 2256
oncRpcNumber	RFC 2307
organizationalStatus	RFC 1274
otherMailbox	RFC 1274
ou	RFC 2256
owner	RFC 2256
pager	RFC 1274
personalSignature	RFC 1274
personalTitle	RFC 1274
photo	RFC 1274
physicalDeliveryOfficeName	RFC 2256

Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
postalAddress	RFC 2256
postalCode	RFC 2256
postOfficeBox	RFC 2256
preferredDeliveryMethod	RFC 2256
preferredDeliveryMethod	RFC 2377
preferredLanguage	RFC 2798
presentationAddress	RFC 2256
protocolInformation	RFC 2256
ref	RFC 3296
registeredAddress	RFC 2256
roleOccupant	RFC 2256
roomNumber	RFC 1274
searchGuide	RFC 2256
secretary	RFC 1274
seeAlso	RFC 2256
serialNumber	RFC 2256
shadowExpire	RFC 2307
shadowFlag	RFC 2307
shadowInactive	RFC 2307
shadowLastChange	RFC 2307
shadowMax	RFC 2307
shadowMin	RFC 2307
shadowWarning	RFC 2307
sn	RFC 2256
st	RFC 2256
street	RFC 2256
subtreeMaximumQuality	RFC 1274
subtreeMinimumQuality	RFC 1274
supportedApplicationContext	RFC 2256
telephoneNumber	RFC 2256
teletexTerminalIdentifier	RFC 2256
telexNumber	RFC 2256
textEncodedORaddress	RFC 2377
title	RFC 2256
uid	RFC 2253
uidNumber	RFC 2307
uniqueIdentifier	RFC 1274

Table 8–1 (Cont.) Standard LDAP Attributes Used By Oracle Internet Directory

Attribute Name	Specification
uniqueMember	RFC 2256
userCertificate;binary	RFC 2256
userClass	RFC 1274
userPassword	RFC 2256
userPKCS12	RFC 2798
userSMIMECertificate	RFC 2798
x121Address	RFC 2256
x500UniqueIdentifier	RFC 2256

Oracle Identity Management Attribute Reference

This section contains an alphabetical listing of the Oracle Identity Management attributes. These are the attributes used in entries pertaining to Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, and Oracle Single Sign-On.

Note: Oracle Fusion Middleware 11g Release 1 (11.1.1) does not include Oracle Single Sign-On or Oracle Delegated Administration Services. Oracle Internet Directory 11g Release 1 (11.1.1), 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

attributeMap

Description

Attribute mappings used by the POSIX naming directory user agent (DUA).

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.9

attributeTypes

Description

Attribute types supported by the directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.3 (Attribute Type Description)

Matching Rule

objectIdentifierFirstComponentMatch

Object ID

2.5.21.5

Other

Directory operational attribute.

authenticationMethod**Description**

Identifies the type of authentication method used to contact the directory server agent (DSA).

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.6

Other

Single-valued attribute.

authPassword**Description**

Attribute for storing a password to an Oracle component when that password is the same as that used to authenticate the user to the directory, namely, [userPassword](#). The value in this attribute is synchronized with that in the [userPassword](#) attribute.

Several different applications can require the user to enter the same clear text password used for the directory, but each application may hash it with a different algorithm. In this case, the same clear text password can become the source of several different password verifiers.

This attribute is multivalued and can contain all the other verifiers that different applications use for this user's clear text password. If the `userpassword` attribute is modified, then the `authpassword` values for all applications are regenerated.

Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

1.3.6.1.4.1.4203.1.3.4

bindTimeLimit**Description**

Maximum time in seconds a POSIX directory user agent (DUA) should allow for a search to complete.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.11.1.3.1.1.4

Other

Single-valued attribute.

c**Description**

Specifies the country associated with a user's address.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.5.4.6

Other

Single-valued attribute.

changestatus**Description**

The last change number transported by the replication server.

Syntax

DN

Matching Rule

DistinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.22

cn**Description**

The common name (nickname) attribute which contains the name of an object. If the object corresponds to a user, it is typically the user's full name. A cn (common name) isn't unique, whereas a dn (distinguished name) is unique.

For example, if ABC corp employs two people with the name John Smith, one in HR and one in 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, o=ABC
```

Where ou= organizational unit, and o=organization

Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule

caseIgnoreMatch

Object ID

2.5.4.3

contentRules**Description**

Specifies the permissible content of entries of a particular structural object class through the identification of an optional set of auxiliary object classes, mandatory, optional, and precluded attributes.

Syntax

1.3.6.1.4.1.1466.115.121.1.16 (DIT Content Rule Description)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1004

createTimestamp**Description**

The time that the entry was created.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rules

generalizedTimeMatch

Object ID

2.5.18.1

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

creatorsName**Description**

The DN of the entity (such as a user or an application) that created the entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.5.18.3

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

credentialLevel**Description**

Identifies the type of credentials a POSIX directory user agent (DUA) should use when binding to the directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.10

Other

Single-valued attribute.

defaultSearchBase

Description

The default base DN used by a POSIX directory user agent (DUA).

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

1.3.6.1.4.1.11.1.3.1.1.1

Other

Single-valued attribute.

defaultSearchScope

Description

User defined search scope used by a POSIX directory user agent (DUA).

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

N/A

Object ID

1.3.6.1.4.1.11.1.3.1.1.12

Other

Single-valued attribute.

defaultServerList

Description

The IP addresses of the default servers that a directory user agent (DUA) should use in a space separated list. After the servers in [preferredServerList](#) are tried, those default servers on the client's subnet are tried, followed by the remaining default servers, until a connection is made. At least one server must be specified in either [preferredServerList](#) or [defaultServerList](#). This attribute has no default value.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.0

Other

Single-valued attribute.

description**Description**

An optional description for the entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{1024} (Directory String, 1024 character maximum)

Matching Rule

caseIgnoreMatch

Object ID

2.5.4.13

displayName**Description**

The preferred name used when displaying the entry in the GUI tools.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113730.3.1.241

Other

Single-valued attribute.

followReferrals**Description**

Tells a POSIX directory user agent (DUA) if it should follow referrals returned by a directory server agent (DSA) search result.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseIgnoreIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.5

Other

Single-valued attribute.

javaClassName

Description

Fully qualified name of a distinguished Java class or interface.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseExactMatch

Object ID

1.3.6.1.4.1.42.2.27.4.1.6

Other

Single-valued attribute.

jpegPhoto

Description

A photograph file in JPEG format.

Syntax

1.3.6.1.4.1.1466.115.121.1.28 (Binary)

Matching Rule

octetStringMatch

Object ID

0.9.2342.19200300.100.1.60

krbPrincipalName

Description

Contains the Kerberos principal name.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

1.3.18.0.2.4.1091

Other

Single-valued attribute.

labeledURI**Description**

Uniform Resource Locator (URL).

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseExactIA5Match

Object ID

1.3.6.1.4.1.250.1.57

ldapSyntaxes**Description**

Identifies the LDAP syntaxes implemented in the directory schema.

Syntax

1.3.6.1.4.1.1466.115.121.1.54 (LDAP Syntax Description)

Matching Rule

objectIdentifierFirstComponentMatch

Object ID

1.3.6.1.4.1.1466.101.120.16

Other

Directory operational attribute.

mail**Description**

This attribute is defined in RFC 1274. Identifies a user's primary e-mail address (the e-mail address retrieved and displayed by "white-pages" lookup applications).

For example: mail: user.name@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

matchingRules

Description

Identifies the matching rules implemented in the directory schema.

Syntax

1.3.6.1.4.1.1466.115.121.1.30 (Matching Rule Description)

Matching Rule

objectIdentifierFirstComponentMatch

Object ID

2.5.21.4

Other

Directory operational attribute.

middleName

Description

A user's middle name.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

1.3.6.1.4.1.1466.101.120.34

modifiersName

Description

The DN of the entity (such as a user or application) that last updated the entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.5.18.4

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

modifyTimestamp**Description**

The time the entry was last modified.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.5.18.2

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

namingContexts**Description**

Top-level DNs for the naming contexts contained in this server. You must have 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.

objectClass

Description

The list of object classes from which this object class is derived.

Syntax

1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

Matching Rule

objectIdentifierMatch

Object ID

2.5.4.0

objectClasses

Description

Defines the object classes which are in force within a subschema.

Syntax

1.3.6.1.4.1.1466.115.121.1.37 (Object Class Description)

Matching Rule

objectIdentifierFirstComponentMatch

Object ID

2.5.21.6

Other

Directory operational attribute.

objectClassMap

Description

A mapping from an object class defined by a directory user agent (DUA) to an object class in an alternative schema used in the directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

N/A

Object ID

1.3.6.1.4.1.11.1.3.1.1.11

orclACI

Description

Access control instructions are stored in the directory as attributes of entries. The `orclACI` attribute is an operational attribute; it is available for use on every entry in the directory, regardless of whether it is defined for the object class of the entry. It is used by the directory server to evaluate what rights are granted or denied when it receives an LDAP request from a client.

Syntax

1.3.6.1.4.1.1466.115.121.1.1 (Access Control Item)

Matching Rule

accessDirectiveMatch

Object ID

2.16.840.1.113894.1.1.42

orclACLResultsLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.129

Other

Single-valued attribute.

orclActivateReplication

Description

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

orclActiveConn

Description

Specifies the number of active connections to the Oracle Internet Directory server, including client LDAP connections and database connections.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.150

Other

Single-valued attribute.

orclActiveEndDate

Description

Specifies the date and time beyond which a user account is no longer active and beyond which the user is not allowed to authenticate.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.339

Other

Single-valued attribute.

orclActiveStartdate

Description

Specifies the date and time that a user account is active and the user is allowed to authenticate. If not specified, then the user is considered active immediately.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.330

Other

Single-valued attribute.

orclActiveThreads**Description**

Specifies the number of active threads on the Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.140

Other

Single-valued attribute.

orclAgreementId**Description**

Naming attribute for the replication agreement entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.26

Other

Single-valued attribute.

orclagreementtype**Description**

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

orclAnonymousBindsFlag

Description

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.

orclAppFullName

Description

The full name of an application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.320

orclAppId

Description

The unique identifier of an application entry associated with a password verifier.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 characters maximum)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.207

Other

Single-valued attribute.

orclApplicationAddress**Description**

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

orclApplicationCommonName**Description**

The common name (cn) of the application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.319

orclApplicationType**Description**

Identifies the application type, such as 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.

orclAssocDB

Description

Identifies the associated Oracle Database instance with the application or service.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1007

orclAssocAsInstance

Description

Identifies the associated Oracle Application Server instance with the application or service.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1006

orclAttrACLEvalLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.138

Other

Single-valued attribute.

orclAudCustEvents**Description**

A comma-separated list of events and category names to be audited. Custom events are only applicable when `orclAudFilterPreset` is `Custom`.

Examples include:

```
Authentication.SUCCESESONLY,  
Authorization(Permission -eq 'CSFPerfmission')
```

Syntax

IA5 String

Matching Rule

caseExactIAI5Match

Object ID

2.16.840.1.113894.1.1.373

orclAudFilterPreset**Description**

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

orclAuditAttribute**Description**

Identifies the audit attribute.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.58

orclAuditMessage

Description

Stores an audit message.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.59

orclAudSplUsers

Description

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

orclBERgenLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.139

Other

Single-valued attribute.

orclCatalogEntryDN**Description**

Contains the DN of the catalog entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.50

Other

Single-valued attribute.

orclCategory**Description**

Identifies the business category of a service or an application entity

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.317

orclCertExtensionAttribute**Description**

Holds the OID of a field within an extension field of the client certificate.

Syntax

1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

Matching Rule

objectIdentifierMatch

Object ID

2.16.840.1.113894.1.1.711

Other

Single-valued attribute.

orclCertExtensionOID

Description

Holds the extension field OID of the client certificate.

Syntax

1.3.6.1.4.1.1466.115.121.1.38 (Object Identifier)

Matching Rule

objectIdentifierMatch

Object ID

2.16.840.1.113894.1.1.709

Other

Single-valued attribute.

orclCertificateHash

Description

This is a special catalog attribute used for certificate matching. The value of this attribute is computed by calculating a hash of the user certificate when it is added to Oracle Internet Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

2.16.840.1.113894.1.1.184

Other

Single-valued attribute.

Not user modifiable.

orclCertificateMatch

Description

This is a special catalog attribute used for certificate matching. The value of this attribute contains the correct matching value to use for a user certificate based on the [orclPKIMatchingRule](#) setting.

Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule

octetStringMatch

Object ID

2.16.840.1.113894.1.1.183

Other

Single-valued attribute.

Not user modifiable.

orclCertMappingAttribute

Description

Holds the standard field `OID` of the client certificate.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.708

Other

Single-valued attribute.

orclChangeLogLife

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.806

Other

Single-valued attribute.

DSA operational attribute.

orclChangeRetryCount

Description

The number of processing retry attempts for a replication change-entry before being moved to the human intervention queue. The value for this parameter must be equal to or greater than 1 (one).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.23

Other

Single-valued attribute.

DSA operational attribute.

orclCommonAutoRegEnabled

Description

Specifies if auto-registration is enabled or disabled. Allowed values are 0 (disabled) or 1 (enabled).

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.567

Other

Single-valued attribute.

orclCommonContextMap

Description

Stores the common context map.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.904

Other

Single-valued attribute.

orclCommonDefaultUserCreateBase

Description

Identifies the default user creation base where users are created.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.908

Other

Single-valued attribute.

orclCommonGroupCreateBase

Description

Identifies the group creation base under which Oracle Delegated Administration Services creates groups

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.903

orclCommonNamingAttribute

Description

Specifies the name of the attribute that is used as an RDN component when creating a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.900

orclCommonNicknameAttribute

Description

Specifies the name of the attribute that uniquely identifies users.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.7

Other

Single-valued attribute.

orclCommonSASLRealm

Description

Identifies the common SASL realm. This attribute contains a string value specifying a subset of related entries under a subscriber realm.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.20

Other

Single-valued attribute.

orclCommonUserSearchBase

Description

Identifies the branch that contains user entries.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.7.1.10

orclCommonVerifierEnable

Description

If this attribute is enabled then the common verifier will be used for all related applications. If this attribute is disabled then each application must setup their own verifier profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.214

Other

Single-valued attribute.

orclConfigSetNumber

Description

The configuration parameters for each Oracle Internet Directory server instance are stored in an entry called a configuration set entry (configset). This attribute specifies a number of a configset entry, which can be referenced when starting an Oracle Internet Directory server instance. The number of the default configset entry is 0 (zero).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.40

Other

Single-valued attribute.

orclconflresolution

Description

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

orclConnectByAttribute

Description

The attribute type name that you want to use as the filter for a dynamic group query—for example, `manager`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1001

Other

Single-valued attribute.

orclConnectBySearchBase

Description

A naming context in the DIT that you want to use as the base for a dynamic group query—for example, `l=us, dc=mycompany, dc=com`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1003

Other

Single-valued attribute.

orclConnectByStartingValue**Description**

For a dynamic group query, this specifies the DN of the attribute you specified in the [orclConnectByAttribute](#) attribute—for example, `Anne Smith`.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.1002

Other

Single-valued attribute.

orclConnectionFormat**Description**

Specifies the format used to construct the connect string associated with a resource.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.354

Other

Single-valued attribute.

orclContact**Description**

Identifies a contact person for an organization or an application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.332

Other

Single-valued attribute.

orclCryptoScheme

Description

The hash algorithm used to encrypt passwords that are stored in the directory. Options are: MD4, MD5, No encryption, SHA, SSHA, or UNIX Crypt. The default is MD4.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 characters maximum)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.68

Other

Single-valued attribute.

orclDASAdminModifiable

Description

Specifies whether or not administration of this entry is available through Oracle Delegated Administration Services.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.324

Other

Single-valued attribute.

orclDASAttrDispOrder

Description

Specifies the display order of an attribute in Oracle Delegated Administration Services.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.341

orciDASAttrName**Description**

Specifies the name of an attribute to show in Oracle Delegated Administration Services.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.340

orciDASEnableProductLogo**Description**

Specifies whether or not to display a product logo on the Identity Management Realm Configuration window of Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.362

Other

Single-valued attribute.

orciDASEnableSubscriberLogo**Description**

Specifies whether or not to display a realm logo on the Identity Management Realm Configuration window of Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.361

Other

Single-valued attribute.

orcidASIsEnabled

Description

Specifies whether or not an attribute is enabled for Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.344

Other

Single-valued attribute.

orcidASIsMandatory

Description

Specifies whether or not an attribute is mandatory for Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.321

Other

Single-valued attribute.

orclDASIsPersonal

Description

Specifies whether or not an attribute is personal information to be supplied by a user in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.326

Other

Single-valued attribute.

orclDASLOV

Description

The list of values to display to users in the UI when the `orclDASUIType=Predefined List`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.328

orclDASPublicGroupDNs

Description

Specifies the DN's 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

orcidASSearchable

Description

Specifies whether or 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.

orcidASSearchColIndex

Description

Indicates the position in the DAS search result table column, if present.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.902

Other

Single-valued attribute.

orcidASSearchFilter

Description

Specifies whether the attribute is searchable through Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.325

Other

Single-valued attribute.

orcidASSearchSizeLimit**Description**

The maximum number of entries to return in a Oracle Delegated Administration Services search.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.363

Other

Single-valued attribute.

orcidASSelfModifiable**Description**

Specifies whether or not an attribute is modifiable by the user in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.322

Other

Single-valued attribute.

orcidASUIType**Description**

Specifies the UI field type for an attribute when displayed in Oracle Delegated Administration Services. Options are:

- Single Line Text
- Multi Line Text
- Predefined List

- Date
- Browse and Select
- Number

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.327

Other

Single-valued attribute.

orcidASURL

Description

The corresponding URL of an Oracle Delegated Administration Services unit.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.310

orcidASURLBase

Description

This holds the URL base in install area for Oracle Delegated Administration Services.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.345

orcidASValidatePwdReset

Description

Specifies whether or not this attribute can be used for password reset validation purposes in Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.905

Other

Single-valued attribute.

orcidASViewable

Description

Specifies whether or not this attribute is viewable through Oracle Delegated Administration Services. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.323

Other

Single-valued attribute.

orcldataprivacymode

Description

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

orclDateOfBirth

Description

Specifies the date on which a user was born.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.307

Other

Single-valued attribute.

orclDBConnCreationFailed

Description

Indicates a connection failure to the database in an error log entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.155

Other

Single-valued attribute.

orclDBLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.130

Other

Single-valued attribute.

orciDBSchemalIdentifier**Description**

DN of the DB registration entry in OID that an application entity uses.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.347

orciDBType**Description**

The type of database used. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.5

Other

Single-valued attribute.

orciDebugFlag**Description**

The debug level associated with a server instance. The default for 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.

orclDebugForceFlush

Description

Specifies whether debug messages are to be written to the log file when a message is logged by the directory server. To enable it, set its value to 1. To disable it set it to 0, which is its default value.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.193

Other

Single-valued attribute.

orcldebuglevel

Description

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

orclDebugOp

Description

To make logging more focused, limits logged information to particular directory server operations by specifying the debug dimension to those operations. Values for operations are:

- 1 - ldapbind
- 2 - ldapunbind
- 4 - ldapadd
- 8 - ldapdelete
- 16 - ldapmodify
- 32 - ldapmodrdn
- 64 - ldapcompare
- 128 - ldapsearch
- 264 - ldapabandon
- 511 - all operations

To log more than one operation, add the values of their dimensions. For example, if you want to trace ldapbind (1), ldapadd (4) and ldapmodify (16) operations, then the value would be 21 ($1 + 4 + 16 = 21$).

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.601

Other

Single-valued attribute.

orclDefaultProfileGroup

Description

Holds the DN of the group to designate the default group for a user, such that a default profile can be built for the user based on this attribute value.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.309

Other

Single-valued attribute.

orclDefaultSubscriber

Description

Identifies the default realm.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.312

orclDIMEonlyLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.131

Other

Single-valued attribute.

orclDIPRepository

Description

Used to determine if the directory is used as the Oracle Directory Integration 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.

orclDirectoryVersion**Description**

The version of Oracle Internet Directory. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.67

Other

Single-valued attribute.

orclDirReplGroupAgreement**Description**

Contains the directory replication group agreement DN.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

N/A

Object ID

2.16.840.1.113894.1.1.25

Other

DSA operational attribute.

orclDirReplGroupDSAs**Description**

For Oracle Database Advanced Replication-based directory replication groups (DRGs), the [orclReplicaID](#) values of all the nodes in the DRG. This list must be identical on all nodes in the group. This attribute is not applicable for LDAP-based replication agreements.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

N/A

Object ID

2.16.840.1.113894.1.1.48

Other

DSA operational attribute.

orclDisplayPersonalInfo

Description

Specifies if the user's personal information should be displayed in white pages queries. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.304

Other

Single-valued attribute.

OrclDispThreads

Description

Number of dispatcher threads per server process.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.613

orclDITRoot

Description

The root of the directory information tree (DIT). This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.7

Other

Single-valued attribute.

orclDNSUnavailable**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.161

Other

Single-valued attribute.

orclEcacheEnabled**Description**

Specifies whether or not entry caching is enabled. The value for enabled is 1; the value for disabled is 0. The default is 1.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.400

Other

Single-valued attribute.

orclEcacheHitRatio

Description

Stores the cache hit ratio.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.170

Other

Single-valued attribute.

orclEcacheMaxEntries

Description

Maximum number of entries that can be present in the entry cache. The default is 25,000.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.402

Other

Single-valued attribute.

orclEcacheMaxEntSize

Description

Stores the maximum size of a cache entry in bytes.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.602

Other

Single-valued attribute.

orclEcacheMaxSize**Description**

Maximum number of bytes of RAM that the entry cache can use. The default is 100 MB.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.401

Other

Single-valued attribute.

orclEcacheNumEntries**Description**

The number of entries currently in the entry cache.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.171

Other

Single-valued attribute.

orclEcacheSize**Description**

The current size of the entry cache.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.172

Other

Single-valued attribute.

orclEnabled

Description

Determines whether an application is enabled or disabled for use.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.1008

Other

Single-valued attribute.

orclEnableGroupCache

Description

Whether or not to cache privilege groups and ACL groups. Using this cache improves the performance of access control evaluation for users.

Use the group cache when a privilege group membership does not change frequently. If a privilege group membership does change frequently, then it is best to turn off the group cache. This is because, in such a case, computing a group cache increases overhead. The default is 1 (enabled). Change to 0 (zero) to disable.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.403

Other

Single-valued attribute.

orclencryptedattributes

Description

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

orclEntryACLEvalLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.136

Other

Single-valued attribute.

orclEntryLevelACI

Description

Specifies the ACI that holds object level ACL.

Syntax

1.3.6.1.4.1.1466.115.121.1.1 (Access Control Item)

Matching Rule

accessDirectiveMatch

Object ID

2.16.840.1.113894.1.1.43

orclEventLevel

Description

Specifies critical events related to security and system resources to be recorded for server manageability statistics. The default value is 0. [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)
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.

orclEventTime

Description

The time that a logged directory event occurred.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.60

orclEventType**Description**

The type of logged directory event.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.57

orclExcludedAttributes**Description**

Specifies an attribute (within the specified naming context) to be excluded from replication. Applies to partial replication only.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

N/A

Object ID

2.16.840.1.113894.1.1.506

Other

DSA operational attribute.

orclExcludedNamingContexts**Description**

For Oracle Database Advanced Replication-based agreements, this attribute specifies one or more subtrees to be excluded from replication.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

N/A

Object ID

2.16.840.1.113894.1.1.47

Other

DSA operational attribute.

orclFDIncreaseError

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.163

Other

Single-valued attribute.

orclFilterACLEvalLatency

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.137

Other

Single-valued attribute.

orclFlexAttribute1

Description

An additional attribute for storing more information about a resource, service, or component.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.355

orclFlexAttribute2**Description**

An additional attribute for storing more information about a resource, service, or component.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.356

orclFlexAttribute3**Description**

An additional attribute for storing more information about a resource, service, or component.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.357

orclFrontLatency**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.128

Other

Single-valued attribute.

orclGender

Description

The gender of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.346

Other

Single-valued attribute.

orclgeneratechangelog

Description

Enables change log generation 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

orclGenObjLatency

Description

Stores the general object latency.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.133

Other

Single-valued attribute.

orclGetNearACLLatency**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.135

Other

Single-valued attribute.

orclGlobalID**Description**

Specifies the attribute that is used to identify the global ID of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.8

Other

Single-valued attribute.

orclGUID**Description**

This is the global unique identifier for an entry within Oracle Internet Directory. The value for this attribute is automatically generated when an entry is created and remains constant, even if an entry is moved.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.37

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

orclGUPassword

Description

Password for the guest user account in Oracle Internet Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.1.1.12

Other

Single-valued attribute.

orclHIQSchedule

Description

The interval, in minutes, at which the directory replication server repeats the change application process.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

N/A

Object ID

2.16.840.1.113894.1.1.98

Other

Single-valued attribute.

DSA operational attribute.

orclHireDate

Description

Specifies the date on which a user was hired by the organization.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.308

Other

Single-valued attribute.

orclHostedCreditCardExpireDate

Description

The credit card expiration date for a subscriber.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.338

Other

Single-valued attribute.

orclHostedCreditCardNumber

Description

The credit card number for a subscriber.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.337

Other

Single-valued attribute.

orclHostedCreditCardType

Description

The credit card type for a subscriber.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.336

Other

Single-valued attribute.

orclHostedDunsNumber

Description

The DUNS number of a business subscriber. DUNS (Data Universal Numbering System) is a unique nine character company identification number issued by Dun and Bradstreet Corporation used to identify a US corporate entity.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.334

Other

Single-valued attribute.

orclHostedPaymentTerm

Description

Payment terms for a subscriber account.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.335

Other

Single-valued attribute.

orclHostname**Description**

The host name of the Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.41

Other

Single-valued attribute.

orclIdleConn**Description**

The number of open connections that are currently inactive. Oracle Internet Directory tracks the idle connections for server manageability statistics.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.151

Other

Single-valued attribute.

orclIdleThreads**Description**

The number of 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.

orclIncludedNamingContexts**Description**

The naming context included in a partial replica. For each naming context object, you can specify only one unique subtree.

In partial replication, except for subtrees listed in the [orclExcludedNamingContexts](#) attribute, all subtrees in the specified included naming context are replicated.

Only LDAP-based replication agreements respect this attribute to define one or more partial replicas. If this attribute contains any values in an 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.

orclIndexedAttribute**Description**

Attributes that are indexed in the Oracle Internet Directory catalog.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.49

orclInitialServerMemSize**Description**

The memory size of the Oracle Internet Directory server at start up.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.147

Other

Single-valued attribute.

orclinmemfiltprocess**Description**

Search filters to be processed in memory.

Syntax

Printable String

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.608

orclInterval**Description**

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

orclIpAddress

Description

The IP address of the Oracle Internet Directory server host.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.186

orclIsEnabled

Description

Whether or not a user or service subscriber is enabled in Oracle Internet Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.316

Other

Single-valued attribute.

orclIsVisible

Description

This attribute is used to determine if users or groups will be visible to applications managed by Oracle Delegated Administration Services, such as 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.

orclLastAppliedChangeNumber

Description

For Oracle Directory Integration and Provisioning export operations, the last change from Oracle Internet Directory that was applied to the connected directory. The default value is 0. If you have used the Oracle Directory Integration 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.

orclLDAPConnKeepALive

Description

For replication, whether or not to keep the LDAP connection to the connected directory alive due to activity. If not set Oracle Internet Directory will drop inactive connections after a period of time. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.822

Other

Single-valued attribute.

orclLDAPConnTimeout

Description

The number of minutes before Oracle Internet Directory times out and drops an inactive connection.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.194

Other

Single-valued attribute.

orciLDAPInstanceID

Description

The instance number of a particular Oracle Internet Directory server instance.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.125

Other

Single-valued attribute.

orciLDAPProcessID

Description

The process ID of a particular Oracle Internet Directory server instance.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.126

Other

Single-valued attribute.

orciMaidenName

Description

The maiden name of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.306

orclMappedDN**Description**

Holds the required information for generating the mapped identity.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.704

Other

Single-valued attribute.

orclMasterNode**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.1010

Other

Single-valued attribute.

orclMatchDnEnabled**Description**

If the base DN of a search request is not found, then the directory server returns the nearest DN that matches the specified base DN. Whether the directory server tries to find the nearest match DN is controlled by this attribute. If set to 1, then match DN

processing is enabled. If set to 0, then match DN processing is disabled. The default is 1.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.404

Other

Single-valued attribute.

orclMaxCC

Description

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.

orclMaxConnInCache

Description

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.

See Also: section "Caching of Connection DNs" of Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory for more information.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.605

Other

Single-valued attribute.

orclMaxFDLimitReached**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.156

Other

Single-valued attribute.

orclmaxfiltsize**Description**

Max size of the filter to be allowed for ldap search operation.

Syntax**Matching Rule****Object ID**

2.16.840.1.113894.1.1.610

OrclMaxLdapConns**Description**

Max LDAP connections per server.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.611

orclmaxlogfiles

Description

Maximum number of log files to keep in rotation.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.615

orclmaxlogfilesize

Description

Maximum size of the log file.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.614

orclMaxProcessLimitReached

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.164

Other

Single-valued attribute.

orclMaxServerRespTime

Description

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

orclMemAllocError

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.162

Other

Single-valued attribute.

orclNetDescName

Description

The DN of an Oracle Net Service description entry. Oracle Net directory naming allows net service names to be stored in and retrieved from Oracle Internet Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.3.1.12

Other

Single-valued attribute.

orclNetDescString

Description

The description string for an Oracle Net Service. For example:

```
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
(HOST = hostname)(PORT =1521))) (CONNECT_DATA = (SID = ORCL)))
```

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.3.1.13

Other

Single-valued attribute.

orclNonSSLPort

Description

The non-SSL LDAP listening port for Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.102

Other

Single-valued attribute.

orclNormDN

Description

Identifies the normalized DN of an entry.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.1000

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

orclNWCongested**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.160

Other

Single-valued attribute.

orclNrwTimeout**Description**

Stores the network read/write time out. When an LDAP client initiates an operation, then does not respond to the server for a configured number of seconds, the server closes the connection. The number of seconds is controlled by the attribute orclnrwtimeout in the DSA configuration entry. The default is 300 seconds.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.603

Other

Single-valued attribute.

orclNwUnavailable

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.159

Other

Single-valued attribute.

orclObjectGUID

Description

Stores Microsoft Active Directory's OBJECTGUID attribute value for users and groups migrated to Oracle Internet Directory from Active Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.901

Other

Single-valued attribute.

orclObjectSID

Description

Stores Microsoft Active Directory's OBJECTSID attribute value for users and groups migrated to Oracle Internet Directory from Active Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.902

Other

Single-valued attribute.

orclODIPAgent**Description**

The DN of a provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.9.1.6

orclODIPAgentConfigInfo**Description**

Any configuration information that you want the connector to store in Oracle Internet Directory. It is passed by the Directory Integration Platform server to the connector at time of connector invocation. The information is stored as an attribute and the Directory Integration Platform server does not have any knowledge of its content. When the connector is scheduled for execution, the value of the attribute is stored in the file, `ORACLE_HOME/ldap/odi/conf/profile_name.cfg` that can be processed by the connector.

Upload the file by using:

```
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 [Chapter 5, "Oracle Directory Integration Platform Tools"](#) and the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management* 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

orclODIPAgentControl

Description

Whether a synchronization profile is enabled or disabled. Valid values are ENABLE or DISABLE. The default is DISABLE.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.3

Other

Single-valued attribute.

orclODIPAgentExeCommand

Description

The executable name and argument list used by the Directory Integration Platform server to invoke a connector. It can be passed as a command-line argument when the connector is invoked. For example, here is a command to invoke the Oracle HR connector:

```
odihragent OracleHRAgent connect=hrdb login=%orclodipConDirAccessAccount  
pass=%orclodipConDirAccessPassword date=%orclODIPLastSuccessfulExecutionTime
```

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.21

Other

Single-valued attribute.

orclODIPAgentHostName

Description

The host name of the Oracle Directory Integration 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.

orclODIPAgentName**Description**

The name of a third-party synchronization profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.1

Other

Single-valued attribute.

orclODIPAgentPassword**Description**

Password that the synchronization profile uses to bind to the directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.4

Other

Single-valued attribute.

orclODIPApplicationName**Description**

The name of an application to which a provisioning subscription belongs.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.9.1.7

orclODIPApplicationsLocation

Description

The DN of the application to which a provisioning subscription belongs.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.918

Other

Single-valued attribute.

orclODIPAttributeMappingRules

Description

Attribute for storing the mapping rules used by a synchronization profile. Store the mapping rules in a file by using the Directory Integration Platform Assistant. See [Chapter 5, "Oracle Directory Integration Platform Tools"](#) and the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management* for more information about mapping rules.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.41

orclODIPBootStrapStatus

Description

The bootstrap status of a synchronization profile (the initial migration of data between a connected directory and Oracle Internet Directory).

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.101

Other

Single-valued attribute.

orclODIPCommand**Description**

The command to invoke a provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.9.1.5

orclODIPConDirAccessAccount**Description**

Valid user account in the connected directory to be used by the connector for synchronization. The value is specific to the connected directory with which you are integrating. For instance, for the SunONE synchronization connector, it is the valid bind DN in the SunONE Directory Server. For the Human Resources Connector, it is a valid user identifier in the Oracle Human Resources database. For other connectors, it can be passed as a command-line argument when the connector is invoked.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.22

Other

Single-valued attribute.

orclODIPConDirAccessPassword

Description

Password to be used by the user specified in the [orclODIPConDirAccessAccount](#) attribute to connect to the connected directory. The value is specific to the third-party directory with which you are integrating. For instance, for the SunONE synchronization connector, it is the valid bind password in the SunONE Directory Server. For the Human Resources Agent, it is the Oracle Human Resources database password.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.23

orclODIPConDirLastAppliedChgNum

Description

For Oracle Directory Integration and Provisioning import operations, the last change from the connected directory that was applied to Oracle Internet Directory. The default value is 0. If you have used the Directory Integration Platform Assistant to bootstrap the connected directory, then this value is set automatically. See [Chapter 5, "Oracle Directory Integration Platform Tools"](#) and the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management* for more information about the bootstrap operation. This is valid only in the import profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.65

Other

Single-valued attribute.

orclODIPConDirMatchingFilter

Description

This attribute specifies the filter to apply to the third-party directory change log. It is used in the Oracle Directory Integration 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

orclODIPConDirURL**Description**

Connection string required to connect to the third-party connected directory. This value refers to the host name and port number as *host:port:[sslmode]*.

To connect by using SSL, enter *host:port:1*.

Make sure the certificate to connect to the directory is stored in the wallet, the location of which is specified in the file *odi.properties*.

Note: To connect to SunONE Directory Server by using SSL, the server certificate needs to be loaded into the wallet.

See Also: The chapter on Oracle Wallet Manager in *Oracle 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.

orclODIPConfigDNs**Description**

Stores the DN's of integration profiles for a particular configuration set in Oracle Directory Integration Platform.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.72

orclODIPConfigRefreshFlag

Description

Stores a flag which indicates whether any integration profiles have been added, deleted, or modified. Used in association with a configuration set.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.71

Other

Single-valued attribute.

orclODIPDbConnectInfo

Description

The connection string for the database of a provisioning profile subscriber. The format of the string is `host:port:sid:username:password`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.9.1.2

orclODIPEncryptedAttrKey

Description

Stores a key which is used to encrypt and decrypt sensitive data that is transmitted by the Oracle directory integration platform server to other applications.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.215

Other

Single-valued attribute.

orclODIPEventFilter**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.433

orclODIPEventSubscriptions**Description**

Store configuration information for events to which a provisioned-integrated application subscribes.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubStringsMatch

Object ID

2.16.840.1.113894.9.1.1

orclODIPFilterAttrCriteria**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.605

Other

Single-valued attribute.

orclODIPInstancesLocation**Description**

Identifies the location in the directory that stores information about instances of the Oracle directory integration platform server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.913

Other

Single-valued attribute.

orclODIPInstanceStatus**Description**

Stores a flag that indicates whether an instance of the Oracle directory integration platform server should continue running or shut down. This flag provides a means of communication between the OID Monitor, OID Control, and the Oracle directory integration platform server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.76

Other

Single-valued attribute.

orclODIInterfaceType

Description

The data format or protocol used in synchronization with a third-party directory. Supported values are:

- LDIF—Import or export from a LDIF File.
- Tagged—Import or export from a tagged file—a proprietary format supported by the Oracle Directory Integration Platform server, similar to LDIF format.
- LDAP—Import from or export to an LDAP-compliant directory.
- DB —Import from or export to an Oracle Database directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.28

Other

Single-valued attribute.

orclODIPLastExecutionTime

Description

Status attribute set to the last time the integration profile was executed by the Oracle Directory Integration 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.

orclODIPLastSuccessfulExecutionTime

Description

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.

orclODIPMustAttrCriteria

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.603

Other

Single-valued attribute.

orclODIPObjectCriteria

Description

Used in an object definition to identify and classify a particular type of object.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.602

orclODIObjectDefnLocation

Description

Identifies the location of the various object definitions used by the Oracle directory integration platform server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.917

Other

Single-valued attribute.

orclODIObjectEvents

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.432

orclODIObjectName

Description

Used in an object definition to store the name of an object.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.601

Other

Single-valued attribute.

orclODIPObjectSyncBase

Description

The search base in the directory for an object associated with an Oracle Directory Integration 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

orclODIPOIDMatchingFilter

Description

In export profiles, this attribute specifies the filter to apply to the Oracle Internet Directory change log container. It is used in the export profile. It must be set in the export profile when both the import and export integration profiles are enabled, as in the following example:

```
Modifiersname !=orclodipagentname=iPlanetImport,cn=subscriber profile,cn=changelog  
subscriber,cn=oracle internet directory
```

This prevents the same change from being exchanged between the two directories indefinitely.

In import profiles, this attribute specifies a key for mapping entries between Oracle Internet Directory and the connected directory. This is useful when the DN cannot be used as the key.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.43

orclODIPOperationMode

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.430

orclODIPOptAttrCriteria**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.604

Other

Single-valued attribute.

orclODIPPluginAddInfo**Description**

Additional information that may be needed by an Oracle Directory Integration 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.

orclODIPPluginConfigInfo**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.261

Other

Single-valued attribute.

orclODIPPluginEvents

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.265

orclODIPPluginExecData

Description

The Oracle Directory Integration 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

orclODIPPluginExecName

Description

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.

orclODIPProfileDataLocation**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.914

Other

Single-valued attribute.

orclODIPProfileDebugLevel**Description**

The debugging level for an Oracle Directory Integration 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.

orclODIPProfileExecGroupID**Description**

Associates a group number with a particular provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.250

Other

Single-valued attribute.

orclODIPProfileInterfaceAdditionalInformation

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.223

orclODIPProfileInterfaceConnectInformation

Description

Contains information that is used by the Oracle directory integration platform server on how to connect to a provisioning-integrated application for event propagation.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.222

Other

Single-valued attribute.

orclODIPProfileInterfaceName

Description

Contains a provisioning-integrated application's interface name, which is used by the Oracle directory integration platform server for event propagation. The value assigned to this attribute depends on the interface type.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.220

Other

Single-valued attribute.

orclODIPProfileInterfaceType**Description**

Specifies the type of interface to which events will be propagated by the Oracle directory integration platform server. Valid values for this attribute are PLSQL or JAVA.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.221

Other

Single-valued attribute.

orclODIPProfileInterfaceVersion**Description**

Specifies the provisioning profile version to which events will be propagated by the Oracle directory integration platform server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.224

Other

Single-valued attribute.

orclODIPProfileLastAppliedAppEventID

Description

Contains the number of the last event that was generated by a provisioning-integration application and updated in Oracle Internet Directory by the Oracle directory integration platform server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.234

Other

Single-valued attribute.

orclODIPProfileLastProcessingTime

Description

The last time the Oracle Directory Integration 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.

orclODIPProfileLastSuccessfulProcessingTime

Description

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.

orclODIPProfileMaxErrors**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.214

Other

Single-valued attribute.

orclODIPProfileMaxEventsPerInvocation**Description**

Specifies the maximum number of events that the Oracle directory integration platform server packages and sends to an application during one invocation of a provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.212

Other

Single-valued attribute.

orclODIPProfileMaxEventsPerSchedule**Description**

Specifies the maximum number of events that the Oracle directory integration platform server sends to an application during one execution of a provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.213

Other

Single-valued attribute.

orclODIPProfileMaxRetries

Description

The maximum number of times an Oracle Directory Integration 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.

orclODIPProfileName

Description

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.

orclODIPProfileProcessingErrors

Description

Contains errors raised during event propagation by the Oracle directory integration platform server for a particular provisioning-integrated application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.231

orclODIPProfileProcessingStatus

Description

Contains the Oracle directory integration platform server's event propagation status for a particular provisioning-integrated application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.230

Other

Single-valued attribute.

orclODIPProfileProvSubscriptionMode

Description

The subscription mode for a provisioning profile: INBOUND, OUTBOUND, or BOTH.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.408

orclODIPProfileSchedule

Description

The number of seconds between executions of an Oracle Directory Integration 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.

orclODIPProfileStatusUpdate

Description

Indicates whether the Oracle directory integration platform server should perform a provisioning profile status update while propagating events to a provisioning-integrated application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.610

Other

Single-valued attribute.

orclODIPProvEventCriteria

Description

Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to identify a particular type of event.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.503

orclODIPProvEventLDAPChangeType**Description**

Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to indicate what type of operation in LDAP (add, modify, delete) can cause some type of event.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.502

orclODIPProvEventObjectType**Description**

Used with version 2.0 provisioning profiles to convert a change in Oracle Internet Directory to an event before propagating it to a provisioning-integrated application. This attribute is used to indicate the type of object (i.e whether it is a USER or a GROUP and so forth) based on other qualifying criteria.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.501

Other

Single-valued attribute.

orclODIPProvEventRule**Description**

Stores the XML-based rule definitions used by the Oracle directory integration platform server to convert changes in Oracle Internet Directory into events before propagating them to a provisioning-integrated application.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.607

Other

Single-valued attribute.

orclODIPProvEventRuleDTD

Description

Stores the XML DTD for event rule definitions used by the Oracle directory integration platform server to understand and parse event rule definitions.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.606

Other

Single-valued attribute.

orclODIPProvInterfaceFilter

Description

Used with version 3.0 provisioning profiles to identify and classify an object based on the entry's object class. This attribute is used in the object definitions stored in Oracle Internet Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.609

orclODIPProvInterfaceProcessor

Description

Used by the Oracle directory integration platform server to identify the Java classes to use for reading and writing events from and to provisioning-integration applications and for processing event propagation results. The default configurations in this attribute should not be changed.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.608

Other

Single-valued attribute.

orclODIPProvisioningAppGUID

Description

The global unique identifier for the application entry associated with a provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.402

Other

Single-valued attribute.

orclODIPProvisioningAppName

Description

The distinguished name (DN) of the application to which the provisioning subscription belongs. The combination of the application name and organization name uniquely identifies a provisioning profile, for example, Email.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.401

Other

Single-valued attribute.

orclODIPProvisioningEventMappingRules**Description**

The event mapping rule maps the object type received from the application (using an optional filter condition) to a domain in Oracle Internet Directory. An inbound provisioning profile can have multiple mapping rules defined.

The following example shows a sample mapping rule value. The rule shows that a user object (USER) whose locality attribute equals US (l=US) should be mapped to the domain l=US, cn=users, dc=company, dc=com.

```
USER:l=US:l=US,cn=users,dc=company,dc=com
```

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.406

orclODIPProvisioningEventPermittedOperations**Description**

Defines the types of events that the application is allowed to send to the Oracle Directory Integration 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

orclODIPProvisioningEventSubscription**Description**

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

orclODIPProvisioningOrgGUID**Description**

The global unique identifier for the organization entry associated with a provisioning profile.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.404

Other

Single-valued attribute.

orclODIPProvisioningOrgName**Description**

The distinguished name (DN) of the organization to which the provisioning subscription belongs, for example `dc=company,dc=com`. The combination of the

application DN and organization DN uniquely identifies a provisioning profile. Defaults value is the DN of the default identity management realm.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.403

Other

Single-valued attribute.

orclODIPProvProfileLocation

Description

Contains the DN of the directory container that stores provisioning profiles.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.916

Other

Single-valued attribute.

orclODIPRootLocation

Description

Refers to the root location in the directory tree where the Oracle Directory Integration Platform configuration is stored.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.912

Other

Single-valued attribute.

orclODIPSchedulingInterval

Description

Time interval in seconds after which a connected directory is synchronized with Oracle Internet Directory. The default is 600.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.6

Other

Single-valued attribute.

orclODIPSchemaVersion

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.911

Other

Single-valued attribute.

orclODIPSearchCountLimit

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.511

Other

Single-valued attribute.

orclODIPSearchTimeLimit

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.512

Other

Single-valued attribute.

orclODIPServerCommitSize

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.515

Other

Single-valued attribute.

orclODIPServerConfigLocation

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.919

Other

Single-valued attribute.

orclODIPServerDebugLevel**Description**

The number that corresponds to the debugging level for the Oracle Directory Integration 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.

orclODIPServerRefreshIntvl**Description**

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

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.514

Other

Single-valued attribute.

orclODIPServerSSLMode**Description**

The number of the corresponding SSL mode. The default is 0. The modes are as follows:

- 0 — SSL is not used.

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

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.513

Other

Single-valued attribute.

orclODIPServerWalletLoc

Description

The complete path and file name of the Oracle Directory Integration 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.

orclODIPSynchronizationErrors

Description

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

orclODIPSynchronizationMode

Description

Direction of synchronization between Oracle Internet Directory and the connected directory. Allowed values are: IMPORT or EXPORT.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.2

Other

Single-valued attribute.

orclODIPSynchronizationStatus

Description

Status of the last execution of a synchronization profile: SUCCESS or FAILURE. Initially, this attribute has the value YET TO BE EXECUTED.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.63

Other

Single-valued attribute.

orclODIPSyncProfileLocation

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.915

Other

Single-valued attribute.

orclODIPSyncRetryCount

Description

Maximum number of times Oracle Directory Integration 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.

orclOidComponentName

Description

Name of OID component where replication server will be started.

Syntax

Directory String

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.832

orclOidInstanceName

Description

Name of instance where replication server will be started.

Syntax

Directory String

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.830

orclOpAbandoned

Description

Specifies the number of abandoned LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.168

Other

Single-valued attribute.

orclOpCompleted

Description

Specifies the number of completed LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.166

Other

Single-valued attribute.

orclOpenConn

Description

Specifies the number of open connections to the Oracle Internet Directory server, including client LDAP connections and database connections.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.149

Other

Single-valued attribute.

orclOpFailed

Description

Specifies the number of failed LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.190

Other

Single-valued attribute.

orclOpInitiated

Description

Specifies the number of initiated LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.165

Other

Single-valued attribute.

orclOpLatency

Description

Stores operation latency.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.127

Other

Single-valued attribute.

orclOpPending**Description**

Specifies the number of pending LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.167

Other

Single-valued attribute.

orclOpResult**Description**

Stores the operation result.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.64

orclOpSucceeded**Description**

Specifies the number of successful LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.189

Other

Single-valued attribute.

orclOpTimedOut

Description

Specifies the number of LDAP search operations that timed out.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.169

Other

Single-valued attribute.

orcloptracklevel

Description

Security event tracking level.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.180

orcloptrackmaxtotalsize

Description

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

orcloptracknumelemcontainers**Description**

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

orclORA28error**Description**

Specifies the number of ORA-28 errors encountered by Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.182

Other

Single-valued attribute.

orclORA3113error**Description**

Specifies the number of ORA-3113 errors encountered by Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.157

Other

Single-valued attribute.

orclORA3114error

Description

Specifies the number of ORA-3114 errors encountered by Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.158

Other

Single-valued attribute.

orclOracleHome

Description

The *ORACLE_HOME* location of an Oracle service.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

N/A

Object ID

2.16.840.1.113894.7.1.2

Other

Single-valued attribute.

orclOwnerGUID

Description

The global unique identifier of the user who owns an application or resource.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.358

orclPassword**Description**

Identifies an Oracle-specific password for custom authentication schemes like O3Logon for the database server.

Syntax

1.3.6.1.4.1.1466.115.121.1.44 (Printable String)

Matching Rule

caseExactMatch

Object ID

2.16.840.1.113894.7.1.13

orclPasswordAttribute**Description**

Specifies the password value to access the resource.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.353

Other

Single-valued attribute.

orclPasswordHint**Description**

Specifies the password hint to be displayed when users forget their password.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.314

Other

Single-valued attribute.

orclPasswordHintAnswer**Description**

The answer related to the password hint question stored in [orclPasswordHint](#).

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.315

Other

Single-valued attribute.

Note: `orclPasswordHintAnswer` is hashed using the SHA-1 algorithm. The hexadecimal value of this is Base64 encoded.

Oracle Internet Directory hashes the value only if it is provided as plaintext. Prehashed values are not hashed again.

orclPasswordVerifier**Description**

Attribute for storing a password to an Oracle component when that password is different from that used to authenticate the user to the directory, namely, [userPassword](#). The value in this attribute is not synchronized with that in the [userPassword](#) attribute.

Like [authPassword](#), this attribute is multivalued and can contain all the other verifiers that different applications use for this user's clear text password.

Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

2.16.840.1.113894.1.1.210

orclPilotMode**Description**

Whether to BEGIN or END pilot mode for a replica.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch, equality integermatch

Object ID

2.16.840.1.113894.1.1.824

Other

Single-valued attribute.

orclPKCS12Hint**Description**

Password hint for the user's PKCS12 private key store.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.11

orclPKIMatchingRule**Description**

This is used to specify the matching rule for mapping a user's PKI certificate DN to the user's entry DN in Oracle Internet Directory. The following matching rule values are allowed:

- 0 - Exact match. The PKI certificate DN must match the user entry DN.
- 1 - Certificate search. Check to see if the user has a PKI certificate provisioned into Oracle Internet Directory.
- 2 - A combination of exact match and certificate search. If the exact match fails, then a certificate search is performed.
- 3 - Mapping rule only. Use a mapping rule to map user PKI certificate DNs to Oracle Internet Directory DNs.

- 4 - Try in order: 1 (mapping rule), 2 (certificate search), 3 (exact match).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.703

Other

Single-valued attribute.

orciPKINextUpdate

Description

The universal time when the certificate revocation list (CRL) should be updated.

Syntax

1.3.6.1.4.1.1466.115.121.1.53 (UTC Time)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.2.1.300.1

orciPKIVaMecAttr

Description

Contains the certificate validation mechanism supported. Currently, only validation with crls is supported, hence the value of this attribute will be CRL.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.2.1.300.2

orciPluginAttributeList

Description

A semicolon-separated attribute name list that controls whether the plug-in takes effect. If the target attribute is included in the list, the plug-in is invoked.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.563

Other

Single-valued attribute.

orclPluginCheckEntryExist**Description**

If enabled, then the Plug-in will be invoked when the base entry does not exist. 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.

orclPluginEnable**Description**

Whether or not a plug-in is enabled or disabled. Allowed values are 0 (disabled) or 1 (enabled). The default is 0 (disabled).

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.554

Other

Single-valued attribute.

orclPluginEntryProperties

Description

An LDAP search filter that specifies entry criteria that will cause the plug-in to not be invoked. For example, if the following filter is used, the plug-in will not be invoked if the target entry has `objectclass` equal to `inetorgperson` and `sn` equal to `Cezanne`.

```
(&(objectclass=inetorgperson)(sn=Cezanne))
```

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.568

Other

Single-valued attribute.

orclPluginsReplace

Description

For plug-ins that use WHEN timing only. 0 is disabled (default). 1 is enabled. This attribute can be set to enabled only if the [orclPluginLDAPOperation](#) attribute value is `ldapbind`, `ldapcompare`, or `ldapmodify`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.559

Other

Single-valued attribute.

orclPluginBinaryFlexfield

Description

Custom binary information (Java only)

Syntax

1.3.6.1.4.1.1466.115.121.1.5

Object ID

2.16.840.1.113894.1.1.574

Other

Single-valued attribute.

orclPluginFlexfield**Description**

Custom text information (Java only). To indicate a subtype, specify `orclPluginFlexfield; subtypename`, for example, `orclPluginFlexfield; minPwdLength: 8`

Syntax

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.573

Other

Single-Valued attribute.

orclPluginSecuredFlexfield**Description****Syntax**

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.577

Other

Single-Valued attribute.

orclPluginKind**Description**

The kind of plug-in. PL/SQL is the only allowed value.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.562

Other

Single-valued attribute.

orclPluginLDAPOperation

Description

The LDAP operation that this plug-in supplements. Allowed values are:

- ldapcompare
- ldapmodify
- ldapbind
- ldapadd
- ldapdelete
- ldapsearch

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.557

Other

Single-valued attribute.

orclPluginName

Description

The plug-in package name.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.552

Other

Single-valued attribute.

orclPluginPort**Description**

The port that the plug-in is using.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.566

Other

Single-valued attribute.

orclPluginRequestGroup**Description**

A semicolon-separated group list that controls if the plug-in takes effect. You can use this group to specify who can actually invoke the plug-in. For example, if you specify `orclpluginrequestgroup:cn=security,cn=groups,dc=oracle,dc=com`, when you register the plug-in, then the plug-in will not be invoked unless the ldap request comes from the person who belongs to the group `cn=security,cn=groups,dc=oracle,dc=com`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.564

Other

Single-valued attribute.

orclPluginRequestNegGroup**Description**

A semicolon-separated group list that controls if the plug-in takes effect. You can use this group to specify who cannot invoke the plug-in. For example, if you specify `orclpluginrequestneggroup:cn=security,cn=groups,dc=oracle,dc=com`, when you register the plug-in,

then the plug-in will not be invoked if the ldap request comes from the person who belongs to the group `cn=security,cn=groups,dc=oracle,dc=com`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.571

Other

Single-valued attribute.

orclPluginResultCode

Description

An integer value to specify the LDAP result code. If this value is specified, then the plug-in will be invoked only if the ldap operation is in that result code scenario. This only applies if the value for the [orclPluginTiming](#) attribute is POST.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.565

Other

Single-valued attribute.

orclPluginSASLCallback

Description

Controls the type of bind used when the LDAP_PLUGIN package connects back to the same Oracle Internet Directory server.

- 1= SASL bind (default).
- 0= Simple bind.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.572

Other

Single-valued attribute.

orclPluginSearchNotFound**Description**

This only applies if the value for the [orclPluginTiming](#) attribute is `POST`. Brings in the external entries if the entry is not found in Oracle Internet Directory. Provides additional plug-in invocation checking and ensures that the plug-in will only be invoked when the entry is not present in Oracle Internet Directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.570

Other

Single-valued attribute.

orclPluginShareLibLocation**Description**

File location of the program libraries for the plug-in. If this value is not present, then the Oracle Internet Directory server assumes the plug-in language is PL/SQL.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.556

Other

Single-valued attribute.

orclPluginSubscriberDNList**Description**

A semicolon-separated DN list that controls if the plug-in takes effect. For example:

dc=COM, c=us; dc=us, dc=oracle, dc=com; dc=org, dc=us; o=IMC, c=US

If the target DN of an LDAP operation is included in the list, then the plug-in is invoked.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.561

Other

Single-valued attribute.

orclPluginTiming

Description

Specifies when the plug-in is to be invoked in relation to the LDAP operation it supplements. The following values are allowed:

- PRE
- WHEN
- POST

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.558

Other

Single-valued attribute.

orclPluginType

Description

Valid value is *operational* — Operational plug-ins augment existing LDAP operations. The work they perform depends on whether they execute before, after, or in addition to normal directory server operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.553

Other

Single-valued attribute.

orclPluginVersion**Description**

The supported version number of the plug-in.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.555

Other

Single-valued attribute.

OrclPluginWorkers**Description**

Number of plug-in threads per server process.

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.612

orclPrName**Description**

Stores a process name.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.55

Other

Single-valued attribute.

orclProductVersion

Description

Identifies the product version.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.6

orclPrPassword

Description

Contains a password for the OID proxy user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.56

Other

Single-valued attribute.

orclPurgeBase

Description

The base DN in the directory information tree (DIT) where the garbage collection task is applied. This attribute value is reserved for each garbage collector and it must not be modified. Defaults to the RDN of the garbage collector configuration entry DN.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.805

Other

Single-valued attribute.

orclPurgeDebug**Description**

Flag to enable (1) or disable (0) collection of debugging messages. Default value is 0.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.810

Other

Single-valued attribute.

orclPurgeEnable**Description**

Flag to enable (1) or disable (0) this garbage collector. Default value is 1.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.808

Other

Single-valued attribute.

orclPurgeFileLoc**Description**

Absolute file directory where the garbage collection log file is saved. Default value is . (period - the current directory).

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.812

Other

Single-valued attribute.

orclPurgeFileName

Description

The file name of the garbage collection log file. Default value is `oidgc001.log`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.811

Other

Single-valued attribute.

orclPurgeFilter

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.803

Other

Single-valued attribute.

orclPurgeInterval

Description

Time interval in hours that the garbage collection job is executed again. This can be measured from either the point in time specified in the [orclPurgeStart](#) attribute or from the last time it was run. Default value is 24.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.801

Other

Single-valued attribute.

orclPurgeNow

Description

Every time this attribute is added or modified to a garbage collection entry, then the submitted job is executed immediately.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.809

Other

Single-valued attribute.

orclPurgePackage

Description

Specifies the package name for purging directory objects.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.804

Other

Single-valued attribute.

orclPurgeSchedule

Description

Specifies the schedule for purging directory objects.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integermatch

Object ID

2.16.840.1.113894.1.1.24

Other

Single-valued attribute.

DSA operational attribute.

orclPurgeStart

Description

The time when the garbage collector starts to run. The format is `yyyymmddhhmmss`. Default value is 12:00 a.m. of the day Oracle Internet Directory is installed.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.813

Other

Single-valued attribute.

orclPurgeTargetAge

Description

This attribute enables time-based purging of change log records. Set this to the number of hours after which old change logs will be purged. Time-based purging respects the change status of replication, but not the change status of other consumers. When

time-based purging is enabled, the change log garbage collector purges all change logs that are not needed by replication and that are at least the specified number of hours old.

The default behavior is change number-based purging, meaning this attribute is NULL or set to a value less than zero. Change number-based purging respects the change status of all change log consumers. That is, it does not purge change logs unless they have been consumed by all consumers. In addition, it does not purge change logs until they are 10 days old.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.800

Other

Single-valued attribute.

orclPurgeTranSize

Description

The number of objects to be purged in one commit transaction. The default value is 1000.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.802

Other

Single-valued attribute.

orclPwdAccountUnlock

Description

It allows a user with the appropriate 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.

orclPwAllowHashCompare**Description**

Whether or not to allow password validations by comparing the hash values of encrypted passwords. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.218

Other

Single-valued attribute.

orclPwAlphaNumeric**Description**

Number of numeric characters required in a password. The default value is 1.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.205

Other

Single-valued attribute.

orclPwEncryptionEnable**Description**

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.

orclPwIllegalValues**Description**

Lists the common words and attribute types whose values cannot be used as a valid password. By default, all words are acceptable password values.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{1024} (Directory String, 1024 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.204

orclPwIPAccountLockedTime**Description**

The time when a user account was locked for a specific IP address.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.211

Other

Directory operational attribute.

Not user modifiable.

orclPwIPFailureTime

Description

The time of a password failure.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.212

Other

Directory operational attribute.

Not user modifiable.

orclPwIPLockout

Description

Whether or not 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.

orclPwIPLockoutDuration

Description

The number of seconds you want to enforce account lockout for a specific IP address. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.201

Other

Single-valued attribute.

orclPwIPMaxFailure**Description**

The maximum number of failed logins from a specific IP address after which the account is locked.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.202

Other

Single-valued attribute.

orclPwPolicyEnable**Description**

Whether to enable or disable the password policy. The value can be 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.

orclPwVerifierParams**Description**

This attribute contains the values of different password verifier types, such as:

```
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

orclQueueDepth

Description

Indicates the queue depth.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.144

Other

Single-valued attribute.

orclQueueLatency

Description

Defines the queue latency.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.145

Other

Single-valued attribute.

orclReadWaitThreads

Description

Specifies the number of Oracle Internet Directory server threads waiting to read from the network.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.142

Other

Single-valued attribute.

orclrefreshdgrmems

Description

Refresh 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

orclReplAgreements

Description

The DNs of the replication agreement entries.

Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.105

orcreplautotune

Description

Dynamically vary the number of threads assigned to transport and apply tasks based on load. 0: Off, 1: 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

orclReplicaDN

Description

For LDAP-based replication only. The DN of the consumer replica in the replication agreement.

Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.817

orclReplicaID

Description

Naming attribute for the replica subentry. Its value is unique to each directory server node that is initialized at installation. The value of this attribute, assigned during installation, is unique to each directory node, and matches that of the `orclreplicaID` attribute at the root DSE. You cannot modify this value.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.106

Other

Single-valued attribute.

orclReplicaSecondaryURI**Description**

Contains the set of ldapURI formatted addresses that can be used if the [orclReplicaURI](#) values cannot be used.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseExactIA5Match

Object ID

2.16.840.1.113894.1.1.815

orclReplicaState**Description**

Defines the state of the replica. Possible values are:

- 0 (boot strapping)
- 1 (online)
- 2 (offline)
- 3 (bootstrap in progress)
- 4 (bootstrap in progress, cn=oraclecontext bootstrap has completed)
- 5 (bootstrap completed, failure detected for one or more naming contexts)
- 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.

orclreplicationid

Description

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

orclReplicationProtocol

Description

Defines the replication protocol for change propagation to replica. Values are:

- ODS_ASR_1.0 (Oracle Database Advanced Replication-based protocol)
- ODS_LDAP_1.0 (LDAP-based replication)

You cannot modify this attribute.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.29

Other

Single-valued attribute.

orclReplicationState

Description

Activation state of the replication server. 0-Inactive, 1-Active

Syntax

Integer

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.831

orclReplicaType

Description

Defines the type of replica such as read-only or read/write. Possible values are:

- 0 (Read/Write)
- 1 (Read-Only)

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.816

Other

Single-valued attribute.

orclReplicaURI

Description

Contains information in ldapURI format that can be used to open a connection to this replica.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseExactIA5Match

Object ID

2.16.840.1.113894.1.1.814

Other

Single-valued attribute.

orclReplicaVersion

Description

Oracle Internet Directory version of the replica.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.820

Other

Single-valued attribute.

orclreplmaxworkers

Description

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

orclreplusesasl;digest-md5

Description

Use 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

orclResourceIdentifier

Description

Stores the resource identifier.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.348

orclResourceName

Description

Specifies the name of the resource for which the connection information is being maintained.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.350

orclResourceTypeName

Description

Specifies the name of the resource, for example, database, XMLPDS, JDBCPS.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.351

orclResourceViewers

Description

Lists the users or groups of users who can view a Resource Access Descriptor.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.366

orclRevPwd

Description

Reversible encrypted value of the user password. This attribute is generated only if the attribute value of [orclPwdEncryptionEnable](#) in the password policy entry is set to 1.

This attribute can be queried only by using the SSL one-way and two-way authentication mechanisms. This attribute cannot be queried over non-SSL sessions.

Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

2.16.840.1.113894.1.1.216

Other

Directory operational attribute.

Not user modifiable.

orclrienabled**Description**

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

orclSAMAccountName**Description**

Stores the value of Active Directory's `SAMAccountName` attribute. In Oracle Internet Directory, this attribute is defined as a directory string type. However, in Active Directory this attribute cannot accept any special or non-printable characters. If any entry is added in Oracle Internet Directory with this attribute, it can only contain a simple text string or synchronization from Oracle Internet Directory to Active Directory will fail.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.903

Other

Single-valued attribute.

orclSASLAuthenticationMode**Description**

SASL authentication mode indicates different modes depending on the type of authentication required and the level of security, such as, auth-only, auth-int, or auth-conf.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.700

Other

Single-valued attribute.

orclSASLCipherChoice**Description**

Contains the SASL cipher choice. when the authentication mode is auth-conf, the SASL cipher choices can be 3DES, DES, RC4, RC4-56, or RC4-40.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.702

orclSASLMechanism**Description**

Indicates the different kinds of SASL mechanisms supported in the LDAP server. Currently, OID supports SASL-EXTERNAL and DIGEST-MD5.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.701

orclDumpFlag**Description**

Determines whether to generate or stack file (default value 0) or OS level core file (value 1) in case the OID server crashes.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.407

Other

Single-valued attribute.

orclSearchBaseDN**Description**

Contains search base information to be used when performing the directory query for identity mapping.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.706

Other

Single-valued attribute.

orclSearchFilter**Description**

Contains search filter information to be used when performing the directory query for identity mapping.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.705

Other

Single-valued attribute.

orclSearchScope**Description**

Contains search scope information to be used when performing the directory query for identity mapping.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.707

Other

Single-valued attribute.

orclSecondaryUID**Description**

Indicates the secondary UID of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.360

orclSequence**Description**

Specifies the sequence number for audit log 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

orclServerAvgMemGrowth

Description

Specifies the Oracle Internet Directory server process memory growth as a percentage.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.148

Other

Single-valued attribute.

orclServerMode

Description

Specifies if data can be written to the server. Valid values are:

- r (read-only)
- rw (read/write)
- rm (read-modify, that is, to read and modify, but not to add or delete)

The default value is *rw*.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.51

Other

Single-valued attribute.

orclServerProcs

Description

Number of server processes to start. The default for `configset0` is 1. You cannot use a negative value for this attribute.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.364

Other

Single-valued attribute.

orclServiceInstanceLocation

Description

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.

orclServiceMember

Description

Identifies all the service instances that are members of a logical service entity.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.1005

orclServiceSubscriptionLocation

Description

Specifies the DN where the list of users subscribed to a service is available.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseExactMatch

Object ID

2.16.840.1.113894.1.1.1100

Other

Single-valued attribute

orclServiceSubType

Description

Identifies the sub-types of a Service e.g. IMAP, SMTP are sub-type of an e-mail service.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1009

Other

Single-valued attribute

orclServiceType

Description

Identifies the type of Service e.g. Email, Calendar, and so forth.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.4

Other

Single-valued attribute

orclSID**Description**

Stores the SID.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.5

Other

Single-valued attribute

orclsimplemodchglogattributes**Description**

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

orclSizeLimit**Description**

Maximum number of entries to be returned by a search.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.10

Other

Single-valued attribute

orclSkewedAttribute

Description

Attribute that contains names of attributes which are skewed. A skewed attribute has very different search response times depending on its value. You can uniform the response times for searches for such an attribute by adding it as a value of the orclskewedattribute attribute.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.405

orclSkipRefInSQL

Description

Specifies whether to skip referral in SQL generated for searches. Its default value is 0. Set it to 1 if there are no referral entries in the directory; this will help optimizing search performance.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.410

Other

Single-valued attribute

orclSMSpec

Description

Represents a structural object class that includes common attributes for server manageability object classes.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.185

orclSQLexefetchLatency**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.132

Other

Single-valued attribute

orclSQLGenReusedParsed**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.134

Other

Single-valued attribute

orclSSLAuthentication**Description**

Type of SSL authentication to use for this instance of Oracle Internet Directory server. The default value of 1, specifies no SSL authentication. Different instances can have different values. One-way and two-way SSL authentication requires a wallet. You may use one of the following three values:

- 1 = Neither the client nor the server authenticates itself to the other. No certificates are sent or exchanged. If you selected the SSL Enabled check box on the Credentials tab, and choose this option, then only SSL encryption/decryption will be used.
- 32 = One-way authentication. Only the directory server authenticates itself to the client by sending its certificate to the client.
- 64 = Two-way authentication. Both client and server send certificates to each other.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.13

Other

Single-valued attribute

orclSSLCipherSuite**Description**

A cipher suite is a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth. The following cipher suites are supported:

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

orclSSLEnable**Description**

Flag for enabling or disabling SSL. Use this flag when you use different instances of the same server for either SSL or non-SSL. Allowed values are:

- 0—for non-secure operation only
- 1—for SSL authentication only
- 2— for both non-secure operation and SSL authentication

The default value is 0.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.14

Other

Single-valued attribute

orclsslinteropmode**Description**

Enable SSL interoperability with Oracle applications using legacy no-auth mode. Default Value 1. This allows legacy Oracle components to connect with Oracle Internet Directory. New clients using JSSE (Java Secure Socket Extensions) need an instance with the interopmode disabled (0). With interomode disabled, Oracle Internet Directory is fully compliant with the Sun JDK's SSL support.

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

orclSSLPort

Description

The default SSL default port for the directory server. 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

orclSSLVersion

Description

SSL version. The default value is 3.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.18

Other

Single-valued attribute

orclSSLWalletURL

Description

Sets the location of the Oracle Wallet. You initially set this value when you create the wallet. If you elect to change the location of the Oracle Wallet, you must change this parameter. You must set the wallet location on both the client and the server. For example, on UNIX, you could set this parameter as follows:

```
file:/home/my_dir/my_wallet
```

On Microsoft Windows, you could set this parameter as follows:

```
file:C:\my_dir\my_wallet
```


Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.15

Other

Single-valued attribute

orclStatsDN**Description**

Specifies list of user DNs for which to track LDAP operations.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.187

orclStatsFlag**Description**

Enable or disable the Oracle Internet Directory Server Manageability framework. To enable, set this to 1. To disable, set it to 0.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.197

Other

Single-valued attribute.

orclStatsLevel

Description

Level of statistics collection for users. There is only one valid value in this release, 1. Specifying this value collects the number of bind and compare operations against the directory and the user who performed each one.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.199

Other

Single-valued attribute.

orclStatsOp

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.188

Other

Single-valued attribute.

orclStatsPeriodicity

Description

Time interval in minutes for gathering server manageability statistics. The default value is 60.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.198

Other

Single-valued attribute.

orclStatus**Description**

Depending on the context of the object that it is applied to, like a service, it indicates if the service is available or not.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.9.1.9

orclSUAccountLocked**Description**

Determines whether a 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.

orclSubscriberDisable**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.100

Other

Single-valued attribute.

orclSubscriberFullName

Description

Stores the full name of the configured realm.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.333

Other

Single-valued attribute.

orclSubscriberNickNameAttribute

Description

Stores a name of an attribute that holds the unique identifier of a realm.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.302

Other

Single-valued attribute.

orclSubscriberSearchBase

Description

Specifies the DIT node that contains all realms.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.301

orclSubscriberType**Description**

Defines the type of realm created.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.331

Other

Single-valued attribute.

orclSuffix**Description**

To have the directory server manage part of an LDAP directory, you can specify the highest level parent DNs in the server configuration. These DNs are called suffixes. The server can access all objects in the directory that are below the specified suffix in the directory hierarchy. This attribute is part of the root DSE (DSA-Specific Entry). The root DSE contains a number of attributes that store information about the directory server itself.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{128} (Directory String, 128 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.6

Other

Single-valued attribute.

orclSuiteType

Description

Identifies the type of suite e.g ocs, ebiz, and so forth.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.1011

Other

Single-valued attribute.

orclSULoginFailureCount

Description

The number of failed login attempts for the directory 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.

orclSUName

Description

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.

orclSUPassword**Description**

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.

orclSystemName**Description**

Identifies the host name on which a particular instance of a service is running.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.3

Other

Single-valued attribute.

orclTcpConnToClose**Description**

Specifies the number of clients for which the Oracle Internet Directory server will close TCP connections.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.153

Other

Single-valued attribute.

orclTcpConnToShutDown

Description

Specifies the number of clients for which the Oracle Internet Directory server will shut down TCP connections.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.152

Other

Single-valued attribute.

orclThreadSpawnFailed

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.154

Other

Single-valued attribute.

orclThreadsPerSupplier

Description

Specifies the number of threads per supplier for the Oracle directory replication server.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integermatch

Object ID

2.16.840.1.113894.1.1.31

Other

DSA operational attribute.

orclTimeLimit**Description**

Maximum number of seconds allowed for a search to be completed. The default value is 3600.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.65

Other

Single-valued attribute.

orclTimeZone**Description**

Specifies the time zone applicable for a user location.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.311

orclTimeLimitMode**Description**

Defines the time limit mode.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.406

Other

Single-valued attribute.

orclTotFreePhyMem

Description

Stores the total amount of free system physical memory.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.146

Other

Single-valued attribute.

orclTraceDimesionLevel

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.174

Other

Single-valued attribute.

orclTraceFileLocation

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.176

Other

Single-valued attribute.

orclTraceFileSize

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.177

Other

Single-valued attribute.

orclTraceLevel

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.173

Other

Single-valued attribute.

orclTraceMode

Description

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.175

Other

Single-valued attribute.

orclTrustedApplicationGroup

Description

Identifies the DN of the group that list all the applications that specific application trusts for Service to Service Authentication.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.368

orclUIAccessibilityMode

Description

Set to TRUE to display a user interface that is accessible to people with impaired vision.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

2.16.840.1.113894.1.1.367

Other

Single-valued attribute.

orclUniqueAttrName**Description**

The name of an attribute that you want to be unique. Autoboot uniqueness means that each entry must have a unique value for this attribute type.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.500

Other

Single-valued attribute.

orclUniqueEnable**Description**

Disables or enables attribute uniqueness constraints. Allowed values are 0 (disable) or 1 (enable). The default value is 0.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.508

Other

Single-valued attribute.

orclUniqueObjectClass**Description**

Specifies an object class filter for an attribute uniqueness constraint entry. This means the attribute specified in [orclUniqueAttrName](#) must be unique in an instance of this object class.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.503

Other

Single-valued attribute.

orclUniqueScope

Description

The scope of the attribute uniqueness constrain in the DIT. Allowed values are:

- `base`—Searches the root entry only
- `onelevel`—Searches one level only
- `sub`—Searches the entire directory

The default value is `sub`.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.501

Other

Single-valued attribute.

orclUniqueSubtree

Description

When multiple attribute uniqueness constraints have the same values in [orclUniqueAttrName](#), [orclUniqueScope](#) and [orclUniqueObjectClass](#), but different values in `orcluniquesubtree`, the union of subtree scopes specified by those attribute uniqueness constraints is checked.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.502

Other

Single-valued attribute.

orclUnsyncRevPwd**Description**

This attribute stores a password that is not synchronized with the entry in the userpassword.

Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

2.16.840.1.113894.1.1.217

Other

Directory operational attribute.

Not user modifiable.

orclUpdateSchedule**Description**

Replication update interval for new changes and those being retried. The value is in minutes.

Syntax

1.3.6.1.4.1.1466.115.121.1.27

Matching Rule

integermatch

Object ID

2.16.840.1.113894.1.1.30

Other

Directory operational attribute.

Not user modifiable.

Single-valued attribute.

orclUpgradeInProgress**Description**

Indicates whether rolling upgrade is in progress.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.104

Other

Single-valued attribute.

orclUserDN

Description

The distinguished name (DN) of the user who performed an operation.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.16.840.1.113894.1.1.61

orclUserIDAttribute

Description

Specifies the attribute to use as the user identifier value when accessing the resource.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.16.840.1.113894.1.1.352

Other

Single-valued attribute.

orclUserModifiable

Description

Specifies if the data is modifiable by the user that this resource access descriptor entry is created for.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

1.2.3.4.5.6.1.11

orclUserObjectClasses**Description**

A list of the object classes that comprise a user entity.

Syntax

1.3.6.1.4.1.1466.115.121.1.15

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.329

orclUserPrincipalName**Description**

This is the Kerberos user principal name for Microsoft Active Directory users.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.8.1.904

Other

Single-valued attribute.

orclVersion**Description**

The release version of the Oracle Internet Directory server.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.7.1.1

Other

Single-valued attribute.

orciWirelessAccountNumber

Description

Stores the wireless account number of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.365

Other

Single-valued attribute.

orciWorkflowNotificationPref

Description

Identifies workflow notification preferences for a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

caseIgnoreMatch

Object ID

2.16.840.1.113894.1.1.313

orciWriteWaitThreads

Description

Specifies the number of Oracle Internet Directory server threads waiting to write to the network.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

2.16.840.1.113894.1.1.143

Other

Single-valued attribute.

owner**Description**

Specifies the distinguished name (DN) of some object which has some responsibility for the associated object.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.5.4.32

pilotStartTime**Description**

The time stamp of when pilot mode was started for a replica.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

2.16.840.1.113894.1.1.825

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

preferredServerList**Description**

The IP addresses of the preferred servers that a directory user agent should use in a space separated list. The servers in this list are tried in order before those in the

`defaultServerList` until a successful connection is made. This has no default value. At least one server must be specified in either `preferredServerList` or `defaultServerList`.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (Printable String)

Matching Rule

`caseIgnoreIA5Match`

Object ID

1.3.6.1.4.1.11.1.3.1.1.2

Other

Single-valued attribute.

profileTTL

Description

The time to live before a client directory user agent (DUA) should re-read this configuration profile. The values for `profileTTL` can be zero, to indicate no expiration, or a positive integer combined with one of the following letters to indicate the unit of measure:

d: indicates days

h: indicates hours

m: indicates minutes

s: indicates seconds

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

`integerMatch`

Object ID

1.3.6.1.4.1.11.1.3.1.1.7

Other

Single-valued attribute.

protocolInformation

Description

This attribute is used in conjunction with the `presentationAddress` attribute, to provide additional information to the Open System Interconnection (OSI) network service.

Syntax

1.3.6.1.4.1.1466.115.121.1.42 (Protocol Information)

Matching Rule

protocolInformationMatch

Object ID

2.5.4.48

pwdAccountLockedTime**Description**

The time stamp of when a user's account was locked.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.17

Other

Single-valued attribute.

Directory operational attribute.

No user modification.

pwdAllowUserChange**Description**

Reserved for future use.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.14

Other

Single-valued attribute.

pwdChangedTime

Description

The time stamp indicating when the user's current password was created or modified.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.16

Other

Single-valued attribute.

Directory operational attribute.

No user modification.

pwdCheckSyntax

Description

A value of 1 (default) means passwords are checked for syntax errors. A value of 0 means syntax checking is disabled.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.5

Other

Single-valued attribute.

pwdExpirationWarned

Description

The time stamp when the first password expiration warning was sent to the user.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.18

Other

Directory operational attribute.

No user modification.

pwdExpireWarning

Description

The number of seconds before a password expires that a warning should be sent to the user. The user will see the warning when they attempt to log on during the warning period. If the user does not modify the password before it expires, the user is locked out until the password is changed by the administrator. The default value is 0, which means no warnings are sent.

For this feature to work, the client application must support it.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.7

Other

Single-valued attribute.

pwdFailureCountInterval

Description

The number of seconds after which the password failure times are purged from the user entry. If this attribute is not present, or if it has a value of 0, then failure times are never purged. The default value is 0.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.12

Other

Single-valued attribute.

pwdFailureTime

Description

The time stamp of consecutive failed login attempts by the user.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.19

Other

Directory operational attribute.

No user modification.

pwdGraceLoginLimit

Description

Maximum number of grace logins allowed after a password expires. The default value is 0 (no grace logins allowed). The recommended value is 3.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.8

Other

Single-valued attribute.

pwdGraceLoginTimeLimit

Description

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.

pwdGraceUseTime**Description**

The time stamps of each grace login for a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.24 (Generalized Time)

Matching Rule

generalizedTimeMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.21

Other

Directory operational attribute.

No user modification.

pwdHistory**Description**A history of a user's previous passwords. The number of passwords stored in the history is determined by the [pwdInHistory](#) attribute.**Syntax**

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.20

Other

Single-valued attribute.

Directory operational attribute.

No user modification.

pwdInHistory

Description

Number of previous passwords to be stored in the password history ([pwdHistory](#)). If a user attempts to reuse one of the passwords stored in the history, then the password is rejected. The default value is 0 (no previous passwords stored in the history).

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.4

Other

Single-valued attribute.

pwdLockout

Description

Specification for whether users are locked out of the directory after the number of consecutive failed bind attempts specified by [pwdMaxFailure](#). If the value of this policy attribute is TRUE, then users are locked out. If this attribute is not present, or if the value is FALSE, then users are not locked out and the value of [pwdMaxFailure](#) is ignored. By default, account lockout is enforced.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.9

Other

Single-valued attribute.

pwdLockoutDuration

Description

The number of seconds a user is locked out of the directory if both of the following are true:

- Account lockout is enabled.
- The user has been unable to bind successfully to the directory for at least the number of times specified by [pwdMaxFailure](#).

You can set user lockout for a specific duration, or until the administrator resets the user's password. A default value of 0 (zero) means that the user is locked out forever. A user account stays locked even after the lockout duration has passed unless the user binds with the correct password.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.10

Other

Single-valued attribute.

pwdMaxAge

Description

The maximum number of seconds that a given password is valid. If this attribute is not present, or if the value is 0 (zero), then the password does not expire. By default, the passwords expire in 60 days.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.3

Other

Single-valued attribute.

pwdMaxFailure

Description

The number of consecutive failed bind attempts after which a user account is locked. If this attribute is not present, or if the value is 0 (zero), then the account is not locked due to failed bind attempts, and the value of the password lockout policy is ignored. The default is 4.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.11

Other

Single-valued attribute.

pwdMinAge

Description

This attribute holds the number of seconds that must elapse between modifications to the password. If this attribute is not present, 0 seconds is assumed.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.2

Other

Single-valued attribute.

pwdMinLength

Description

The minimum number of characters required in a password. The default is 5. The value for this attribute must be at least 1.

Syntax

1.3.6.1.4.1.1466.115.121.1.27 (Integer)

Matching Rule

integerMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.6

Other

Single-valued attribute.

pwdMustChange

Description

Indicator of whether users must change their passwords after the first login, or after the password is reset by the administrator. Enabling this option requires users to change their passwords even if user-defined passwords are disabled. By default, users need not change their passwords after reset. Allowed values are 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.

pwdpolicysubentry**Description**

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

pwdReset**Description**

Indicator that the password has been reset and must be changed by the user on first authentication. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.22

Other

Single-valued attribute.

Directory operational attribute.

Not user modifiable.

pwdSafeModify

Description

Indicator of whether user must supply old password with new one when modifying password. By default, the old password is not required. Allowed values are TRUE or FALSE.

Syntax

1.3.6.1.4.1.1466.115.121.1.7 (Boolean)

Matching Rule

booleanMatch

Object ID

1.3.6.1.4.1.42.2.27.8.1.15

Other

Single-valued attribute.

ref

Description

A named reference. Values placed in the attribute must conform to the specification given for the [labeledURI](#) attribute (RFC 2079).

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseExactIA5Match

Object ID

2.16.840.1.113730.3.1.34

Other

DSA operational attribute.

seeAlso

Description

Specifies the distinguished names of other directory objects which may be other aspects (in some sense) of the same real world object.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.5.4.34

serverName**Description**

The name of the server involved in an Oracle Directory Integration 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

serviceAuthenticationMethod**Description**

The authentication method for the service.

Syntax

1.3.6.1.4.1.1466.115.121.1.15 (Directory String)

Matching Rule

N/A

Object ID

1.3.6.1.4.1.11.1.3.1.1.15

serviceCredentialLevel**Description**

The credential level to be used by a service. The default value for all services is NULL. The supported credential levels are `anonymous` or `proxy`.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

N/A

Object ID

1.3.6.1.4.1.11.1.3.1.1.13

serviceSearchDescriptor

Description

Defines how and where an LDAP naming service client should search for information for a particular service. Contains a service name, followed by one or more semicolon-separated base-scope-filters.

Syntax

1.3.6.1.4.1.1466.115.121.1.26 (IA5 String)

Matching Rule

caseExactIA5Match

Object ID

1.3.6.1.4.1.11.1.3.1.1.8

sn

Description

The surname or last name of a user.

Syntax

1.3.6.1.4.1.1466.115.121.1.15{32768} (Directory String, 32768 character maximum)

Matching Rule

caseIgnoreMatch, caseIgnoreSubstringsMatch

Object ID

2.5.4.4

supportedcontrol

Description

List of controls supported by directory server.

Syntax

OID

Object ID

1.3.6.1.4.1.1466.101.120.13

supportedextension

Description

List of extended operation supported

Syntax

OID

Object ID

1.3.6.1.4.1.1466.101.120.7

supportedldapversion**Description**

LDAP versions supported.

Syntax

Integer

Object ID

1.3.6.1.4.1.1466.101.120.15

uniqueMember**Description**

The distinguished name for the member of a group.

Syntax

1.3.6.1.4.1.1466.115.121.1.34 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

2.5.4.50

supportedsaslmmechanisms**Description**

List of SASL mechanism supported.

Syntax

Directory String

Matching Rule**Object ID**

1.3.6.1.4.1.1466.101.120.14

userCertificate;binary**Description**

The user's certificate.

Syntax

1.3.6.1.4.1.1466.115.121.1.8 (Certificate)

Matching Rule

octetStringMatch

Object ID

2.5.4.36

userPassword

Description

The password used to authenticate a user to the directory.

Syntax

1.3.6.1.4.1.1466.115.121.1.44{128} (Printable String, 128 character maximum)

Matching Rule

octetStringMatch

Object ID

2.5.4.35

Other

Single-valued attribute.

userPKCS12

Description

PKCS#12 PFX PDU for exchange of personal identity information.

Syntax

1.3.6.1.4.1.1466.115.121.1.5 (Binary)

Matching Rule

N/A

Object ID

2.16.840.1.113730.3.1.216

x509issuer

Description

The DN of the certificate authority who issued the X.509 certificate revocation list.

Syntax

1.3.6.1.4.1.1466.115.121.1.12 (Distinguished Name)

Matching Rule

distinguishedNameMatch

Object ID

1.3.6.1.4.1.10126.1.5.3.4

Part III

Appendixes

This part contains the following appendix:

- [Appendix A, "LDIF File Format"](#)

LDIF File Format

This appendix provides some general information about creating LDAP Data Interchange Files (LDIF) that can be used by the Oracle Internet Directory command-line tools. LDIF files are specially formatted text files that can be used to exchange data between LDAP directory servers, such as Oracle Internet Directory.

This appendix contains the following topics:

- [General LDIF Formatting Rules](#)
- [LDIF Format for Entries](#)
- [LDIF Format for Adding Schema Elements](#)

General LDIF Formatting Rules

LDIF formats are defined by the Internet Engineering Task Force (IETF) in RFC 2849. Visit the IETF Web site at <http://www.ietf.org/rfc/rfc2849.txt> for more information about LDIF formatting rules. This section explains some general rules for formatting LDIF files.

Line Types and White Space

Each line in an LDIF file must be correctly formatted in order to be read by the Oracle Internet Directory command-line tools. White space and line breaks must be used carefully.

Each line in an LDIF file is terminated with a line feed, which is <LF> on UNIX or <CR><LF> on Windows. In LDIF you can have the following types of lines:

- **Directive Line** - Any line that does not begin with either a SPACE or # (hash). A directive line specifies either some type of data in an entry or an operation to perform.
- **Continuation Line** - A line that begins with a SPACE denotes that the characters following the space are part of the previous line.
- **Blank Line** - Blank lines are used to separate entries and are typically created with the ENTER key.
- **Comment Line** - A comment line begins with a # (hash). Comments are ignored by the Oracle Internet Directory command-line tools.
- **Separator Line** - A line that starts with a - (dash) character is used to end an operation. It denotes that the next line begins a new operation directive.

Unnecessary space characters in the LDIF input file, such as a space at the end of an attribute value, will cause the LDAP operations to fail.

Sequencing of Entries

The sequence of entries in your LDIF file must follow the Directory Information Tree (DIT) from the top down. Parent entries should be listed before their children entries. Any attributes or object classes used in an entry must exist in the schema or be added to the schema before they can be used. Separate entries with a blank line.

Binary Files

Reference binary files, such as photographs, with the absolute address of the file preceded by a / (forward slash).

Non-Printing Characters in Attribute Values

Non-printing characters and tabs are represented in attribute values as base-64 encoding.

LDIF Format for Entries

The standard format for directory entries is as follows:

```
dn: distinguished_name
changetype: add|delete|modify|modrdn|moddn
attribute_type: attribute_value
...
objectClass: object_class_value
...
```

The dn Directive

The `dn` directive defines the distinguished name (DN) of an entry. It is assumed that all lines below a `dn` directive belong to that entry until you add a space in the LDIF file to denote a separate entry. The following example shows a `dn` directive line:

```
dn: cn=Mary Jones,ou=Sales,dc=company,dc=com
```

The changetype Directive

The `changetype` directive defines the operation you want to perform on the entry. The operations that you specify with the `changetype` directive are:

- `add` - See ["LDIF Format for Adding Entries"](#) on page A-3 for syntax and examples.
- `delete` - See ["LDIF Format for Deleting Entries"](#) on page A-3 for syntax and examples.
- `modify` - ["LDIF Format for Modifying Entries"](#) on page A-4 for syntax and examples.
- `modrdn` - See ["LDIF Format for Modifying the RDN of an Entry"](#) on page A-4 for syntax and examples.
- `moddn` - See ["LDIF Format for Modifying the DN of an Entry"](#) on page A-5 for syntax and examples.

If `changetype` directive is omitted, then an `add` operation is assumed if using `bulkload`, `ldapadd` or `ldapaddmt`. A `delete` operation is assumed if using `bulkdelete` or `ldapdelete`. All other operations must specify a `changetype: directive`.

The *attribute_type* Directive

The *attribute_type* directive is used to specify an attribute type name and value pair. The entry will have an *attribute_type* directive for each attribute in the entry. For example, here is an *attribute_type* directive for the attribute type named `cn` where the value is `Mary Smith`.

```
cn: Mary Smith
```

The *objectClass* Directive

The *objectClass* directive is used to specify the object class that is associated with the entry. If an entry uses multiple object classes, then it will have an *objectClass* directive for each object class used. For example, here are the object classes used to define a user entry.

```
objectClass: orclUserV2
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Note that if an object class has required attributes, you must supply a value for those attributes using *attribute_type* directives.

LDIF Format for Adding Entries

The following example shows a file entry for an employee. The first line contains the DN. The second line contains the `changetype: add` directive. The lines that follow begin with the name for an attribute type, followed by the value to be associated with that attribute. Note that the `photo` attribute value begins with a forward slash (`\`) to denote that it is a binary file reference. 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: \${ORACLE_INSTANCE}/empdir/photog/ssmith.jpg
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

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.

```
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.

LDIF Format for Modifying Entries

When modifying an entry, you must supply the DN of the entry followed by the `changetype: modify` directive. Next you must specify the attributes you want to modify using one of the following directives:

- `add: attribute_type` - Specifies the name of an attribute type for which you want to add a value. The next line should then contain the `attribute_type: value` directive for the value you want to add. For example:


```
add: work-phone
work-phone: 510/506-7000
```
- `delete: attribute_type` - Specifies the name of an attribute type for which you want to delete the value. If the attribute is multi-valued, then you should also supply the `attribute_type: value` directive for the specific value you want to delete, otherwise all values for the attribute will be deleted. For example:


```
delete: home-fax
```
- `replace: attribute_type` - Specifies the name of an attribute type for which you want to replace the existing value with a new value. The next line should then contain the `attribute_type: value` directive for the value you want to replace. For example:


```
replace: home-phone
home-phone: 415/697-8899
```

If the attribute is multi-valued then all the current values are replaced with one or more attributes following this directive. If only a single value of a multi-valued attribute needs to be replaced use `delete` then `add`.

If you are making several modifications to an entry, then, between each modification you enter, add a line that contains a hyphen (-) only. For example:

```
dn: cn=Barbara Fritchey,ou=Sales,o=Oracle,c=US
changetype: modify
add: work-phone
work-phone: 650/506-7000
work-phone: 650/506-7001
-
delete: home-fax
-
replace: home-phone
home-phone: 415/697-8899
```

LDIF Format for Modifying the RDN of an Entry

To modify the relative distinguished name (RDN) for an entry, you must supply the DN of the entry followed by the `changetype: modrdn` directive. Next you must specify the new RDN with a `newrdn: directive`, and you can optionally delete or keep the old entry by supplying a `deleteoldrdn: directive`. For example:

```
dn: cn=Sally Smith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: Sally Smith-Jones
# deletes old RDN entry
deleteoldrdn: 1
```

LDIF Format for Modifying the DN of an Entry

To modify the DN for an entry (move the entry to a new node in the DIT), you must supply the DN of the entry followed by the `changetype: moddn` directive. Next you must specify the new parent DN with a `newsuperior:` directive, and you can optionally delete or keep the old entry by supplying a `deleteoldrdn:` directive. For example:

```
dn: cn=Sally Smith,ou=people,dc=example,dc=com
changetype: moddn
newsuperior: ou=expeople,dc=example,dc=com
# keeps old RDN entry
deleteoldrdn: 0
```

LDIF Format for Adding Schema Elements

Attribute types and object classes must be added to the Oracle Internet Directory schema before they can be used in entries.

Example: Adding an Attribute to the Schema

This example adds a new attribute to the schema called `myAttr`. The LDIF file for this operation is:

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 1.2.3.4.5.6.7 NAME 'myAttr' DESC 'New attribute definition'
  EQUALITY caseIgnoreMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

On the first line, enter the DN specifying where this new attribute is to be located. All attributes and object classes are stored in `cn=subschemasubentry`.

The second and third lines show the proper format for adding a new attribute.

The last line is the attribute definition itself. The first part of this is the object identifier number: `1.2.3.4.5.6.7`. It must be unique among all other object classes and attributes. Next is the `NAME` of the attribute. In this case the attribute `NAME` is `myAttr`. It must be surrounded by single quotes. Next is a description of the attribute. Enter whatever description you want between single quotes. At the end of this attribute definition in this example are optional formatting rules to the attribute. In this case we are adding a matching rule of `EQUALITY caseIgnoreMatch` and a `SYNTAX` of `1.3.6.1.4.1.1466.115.121.1.15` (which is the object ID for the syntax of "Directory String").

When you define schema within an LDIF file, insert a white space between the opening parenthesis and the beginning of the text, and between the end of the text and the ending parenthesis.

Example: Adding an Object Class to the Schema

Before you add the object class, all of the attribute types that the object class uses must be in the schema. If there are new attribute types, then define those first in your LDIF file before defining your object class.

The following example adds a new object class named `myObjectClass` to the schema.

```
dn: cn=subschemasubentry
changetype: modify
add: objectClasses
```

```
objectClasses: ( 1.2.3.4.56789.1.0.200 NAME 'myObjectClass'  
  SUP ( top ) STRUCTURAL  
  MUST ( cn )  
  MAY ( myAttr1 $ myAttr2 $ myAttr3 ) )
```

On the first line, enter the DN specifying where this new object class is to be located. All attributes and object classes are stored in `cn=subschemasubentry`.

The second and third lines show the proper format for adding a new object class.

The last line is the object class definition itself. The first part of this is the object identifier number: `1.2.3.4.56789.1.0.200`. It must be unique among all other object classes and attributes. Next is the `NAME` of the object class. In this case the object class name is `myObjectClass`. It must be surrounded by single quotes. Next is the superior (`SUP`) object classes, which in this case is `top`. `STRUCTURAL` denotes the type of object class. `MUST` and `MAY` denote the required and allowed attributes. Separate attribute names with a dollar sign (`$`).

When you define schema within an LDIF file, insert a white space between the opening parenthesis and the beginning of the text, and between the end of the text and the ending parenthesis. If using line breaks for formatting long lines, make sure to add a space at the beginning of a line to denote that it is a continuation of the previous line.

Example: Adding A New Object Class to an Entry

Before you can use a new object class and the attributes it contains, you must update the entry to use the new object class. The following example shows how to add a new object class to an entry. Note that you must define a value for all of the required attributes of the object class.

```
# Add a new AUXILIARY object class to an existing entry  
dn: cn=Robert Smith,ou=people,dc=example,dc=com  
changetype: modify  
# the object class used for binding  
objectclass: inetorgperson  
# objectclass being added  
objectclass: myObjectClass  
# MUST attributes of new object class  
myAttr1: some value  
myAttr2: my value  
myAttr3: a value
```

LDIF Format for Migrating Entries

This section describes how to properly format an LDIF file for use with the Oracle Internet Directory Migration Tool. The migration tool enables you to take LDIF entries output from other directories or applications and convert the data to use the attributes and values found in Oracle Internet Directory entries. You do this by inserting substitution variables for the data elements you want to convert.

See "[ldifmigrator](#)" on page 3-45 for more information about the Oracle Internet Directory Migration Tool.

Substitution Variables for Migration Input Files

Substitution variables are denoted in the LDIF file by the following syntax:

```
%s_variableName%
```

For example, let's say you have the following LDIF formatted entry that was exported from another application. The subtree where user entries are stored, the user nickname

attribute, and the name of the user's organization are different in Oracle Internet Directory than in the original application. For those elements you want to convert, you would add substitution variables to the file as placeholders.

Example:

```
dn: cn=jdoe, %s_UserContainerDN%
sn: Doe
%s_UserNicknameAttribute%: jdoe
objectClass: inetOrgPerson
objectClass: orclUserV2
title: Member of Technical Staff
homePhone: 415-584-5670
homePostalAddress: 234 Lez Drive$ Redwood City$ CA$ 94402
ou: %s_UserOrganization%
```

When you run the Oracle Internet Directory Migration Tool against this file, it will find the variables and either replace them with the values you define on the command-line or look up the correct values in Oracle Internet Directory.

Predefined Substitution Variables

The Oracle Internet Directory Migration Tool recognizes several predefined substitution variables. If running the tool in lookup mode, the values for these variables can be looked up in Oracle Internet Directory. You can use these predefined variables or define variables of your own using the `%s_variableName%` syntax.

Table A-1 Predefined Substitution Variables

Variable Name	Meaning	How OID Migration Tool Determines the Value for This Variable
<code>%s_UserContainerDN%</code>	Distinguished name of the entry under which all users are supposed to be added.	This is assigned the value of the attribute: <code>orclCommonUserSearchBase</code> from the entry <code>cn=Common, cn=Products</code> under the realm-specific Oracle context.
<code>%s_GroupContainerDN%</code>	Distinguished name of the entry under which all public groups are supposed to be added.	This is assigned the value of the attribute: <code>orclCommonGroupSearchBase</code> from the entry <code>cn=Common, cn=Products</code> under the realm-specific Oracle context.
<code>%s_UserNicknameAttribute%</code>	The nickname attribute to be used for user entries in the identity management realm.	This is assigned the value of the attribute: <code>orclCommonNicknameAttribute</code> from the entry <code>cn=Common, cn=Products</code> under the realm-specific Oracle context.
<code>%s_SubscriberDN%</code>	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 <code>orclSubscriberSearchBase</code> and the <code>orclSubscriberNickNameAttr</code> from the entry <code>cn=Common, cn=Products</code> under the root Oracle context.

Table A–1 (Cont.) Predefined Substitution Variables

Variable Name	Meaning	How OID Migration Tool Determines the Value for This Variable
%s_SubscriberOracleContextDN%	Distinguished name of the realm-specific Oracle Context.	First the realm DN is computed as described earlier and then the string <code>cn=OracleContext</code> is pre-pended to it.
%s_RootOracleContextDN%	Distinguished name of the Root Oracle Context.	This is currently hard-coded to <code>cn=OracleContext</code> .
%s_CurrentUserDN%	Distinguished name of the User who is loading the LDIF file. This is sometimes required to bootstrap the creation of groups which require at least one member in them.	The migration tool expects this DN to be specified on the command line as part of the authentication information.

Reconcile Options for Migrated Entries

When migrating entries into Oracle Internet Directory from another application, it is possible that there may be conflicts. For example, a user entry may already be defined in Oracle Internet Directory, or have conflicting values with the migrated data. In this case, the reconcile option will control what LDIF `changetype` directives are performed. There are three modes for reconciliation of migrated data:

- **SAFE** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If any other directive besides the following are specified in the LDIF file, they will not be applied.

```
changetype:add

changetype:modify
  add: attribute_name (adds attribute only if it doesn't exist)
```
- **SAFE-EXTENDED** - This mode only adds new entries that don't exist or appends new attributes to existing entries. If you try to add a new value for existing attributes, then it will add it to the existing set of values. If any other directive besides the following are specified in the LDIF file, they will not be applied.

```
changetype:add

changetype:modify
  add: attribute_name (appends values if attribute exists)
```
- **NORMAL** - This mode applies all directives as intended. The following directives are supported:

```
changetype:add

changetype:delete

changetype:modify
  add: attribute_name
  replace: attribute_name
  delete: attribute_name
```