

Oracle Directory Services: Administration

Volume I • Student Guide

D46306GC10

Edition 1.0

March 2007

D49565

ORACLE®

Authors

David Loo
Vishal Parashar

Technical Contributors and Reviewers

Olfat Aly
Vasuki Ashok
Don Biasotti
Maria Billings
Ellen Desmond
Jim Garm
Don Gosselin
Buddhika Kottahachchi
Robert La Vallie
Russ Lowenthal
Karl Miller
Nagavalli Pataballa
Gayathri Rajagopal
Shankar Raman
Holger Dindler Rasmussen
Mohit Singh
Jerry Smith
Olaf Stullich
Mark Wilcox
Dr. Volker Zell

Publishers

Veena Narasimhan
Sujatha Nagendra

Copyright © 2007, Oracle. All rights reserved.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

Trademark Notice

Oracle, TimesTen, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Preface

O Oracle Directory Services: Administration Course Overview

Objectives O-2

Course Agenda O-3

1 Introduction to Identity Management

Objectives 1-2

Identity Management: Overview 1-3

Benefits of Identity Management 1-4

Identity Management: Terminology 1-5

Functional View of Identity Management Suites 1-7

Directory Services 1-8

Identity Administration 1-9

Access Management 1-10

Provisioning 1-11

Federation 1-12

Web Services Security 1-13

Oracle Identity Management Solution 1-14

Product Functionality Matrix 1-16

Oracle Internet Directory 1-17

Oracle Virtual Directory 1-18

Oracle Access Manager 1-19

Oracle Identity Manager 1-20

Oracle Identity Federation 1-21

Oracle Enterprise Single Sign-On Suite 1-22

Oracle Web Services Manager 1-23

Complete Picture: Oracle Identity Management 1-24

Summary 1-26

2 Installing Oracle Internet Directory

Objectives 2-2

Deployment Planning 2-3

System Requirements for Windows 2-5

Requirements: Environment and User 2-6

Installation Stages 2-7
Installer: Stage 1 of 16 Welcome 2-8
Installer: Stage 2 of 16 Specify File Locations 2-9
Installer: Stage 3 of 16 Select a Product to Install 2-10
Installer: Stage 4 of 16 Select Installation Type 2-11
Installer: Stage 5 of 16 Confirm Pre-installation Requirements 2-12
Installer: Stage 6 of 16 Select Configuration Options 2-13
Installer: Stage 7 of 16 Specify Port Configuration Options 2-14
Installer: Stage 8 of 16 Specify Namespace in Internet Directory 2-15
Installer: Stage 9 of 16 Specify OCA Distinguished Name 2-16
Installer: Stage 10 of 16 Specify OCA Key Length 2-17
Installer: Stage 11 of 16 Specify OCA Administrator's Password 2-18
Installer: Stage 12 of 16 Specify Database Configuration Options 2-19
Installer: Stage 13 of 16 Specify Database Schema Passwords 2-20
Installer: Stage 14 of 16 Specify Instance Name and `ias_admin` Password 2-21
Installer: Stage 15 of 16 Summary 2-22
Installer: Stage 16 of 16 Installation 2-23
Postinstallation Steps 2-24
Setting Environment Variables After Installation for Windows 2-25
Launching the OracleAS Control Console 2-26
Reviewing Port Numbers 2-27
Summary 2-28
Practice 2 Overview: Installing Oracle Internet Directory 2-29

3 Directory and LDAP Concepts for Oracle Internet Directory

Objectives 3-2
What Is a Directory? 3-3
Directory Versus OLTP Database 3-5
Lightweight Directory Access Protocol 3-7
Directory Information Tree 3-8
Root Directory Specific Entry 3-10
Directory Schemas 3-11
LDAP Functions: Connection 3-12
LDAP Functions: Retrieval 3-14
LDAP Functions: Update 3-15
LDAP Functions: Extended Operations 3-16
LDAP Data Interchange Format Files 3-17
LDIF Directives 3-18
Oracle Internet Directory 3-20
OID Architecture: Overview 3-21
OID Node Architecture Components 3-22

OID Server Instance Architecture 3-24
Summary 3-25
Practice 3 Overview: Examining Directory Information in OID 3-26

4 Oracle Internet Directory: Directory Server Administration

Objectives 4-2
Server Administration Tools 4-3
Oracle Directory Manager 4-5
Oracle Application Server Start Sequence 4-6
Oracle Identity Management Stop Sequence 4-7
Options for Starting or Stopping Oracle Identity Management Instances 4-8
Options for Starting or Stopping EM Control Consoles 4-10
Options for Starting or Stopping Oracle Identity Management Components 4-11
Starting and Stopping Log Loader, DSA, and DCM-Daemon 4-12
Changing Password for OID Administrator 4-13
Changing Password for Metadata Repository 4-14
Configuration Sets: Overview 4-15
Managing Configuration Sets 4-16
OID Debug Logging: Overview 4-17
Configuring OID Logging Using Oracle Directory Manager 4-19
Configuring OID Logging Using Command-Line Tools 4-20
Monitoring OID Servers 4-21
Summary 4-22
Practice 4 Overview: Administering an Oracle Internet Directory Server 4-23

5 Oracle Internet Directory: Directory Data Administration

Objectives 5-2
Lesson Agenda 5-3
Managing Entries with Oracle Directory Manager 5-4
Managing Entries with LDAP Command-Line Tools 5-5
Using the `ldapadd` Command 5-6
Using the `ldapaddmt` Command 5-8
Using the `ldapbind` Command 5-9
Using the `ldapcompare` Command 5-10
Using the `ldapdelete` Command 5-11
Using the `ldapmoddn` Command 5-12
Using the `ldapmodify` Command 5-13
Using the `ldapmodifymt` Command 5-16
Using the `ldapsearch` Command 5-17
Lesson Agenda 5-19

- Managing Data with Bulk Tools 5-20
- Using the `bulkload` Command 5-21
- Using the `ldifwrite` Command 5-23
- Using the `bulkmodify` Command 5-25
- Using the `bulkdelete` Command 5-27
- Using the `catalog` Command 5-28
- Lesson Agenda 5-29
- Backing Up and Restoring with LDIF Files 5-30
- Backing Up and Restoring of Metadata Repository 5-31
- Summary 5-32
- Practice 5 Overview: Administering an Oracle Internet Directory Server 5-33

6 Oracle Internet Directory: Directory Schema Administration

- Objectives 6-2
- Mechanisms for Data Integrity 6-3
- Attribute Uniqueness Constraints 6-4
- Attribute Uniqueness Constraint: Example 6-5
- Multiple Attribute Uniqueness Constraints 6-6
- Storage of Attribute Uniqueness Constraints 6-7
- Managing Attribute Uniqueness Constraints 6-8
- Directory Schemas 6-9
- Example Object Class: `inetOrgPerson` 6-10
- Example Attribute: `telephoneNumber` 6-11
- Storage of Directory Schemas 6-12
- Managing Directory Schema Objects 6-13
- Adding Object Classes 6-14
- Adding Attributes to Object Classes 6-15
- Adding Attributes 6-16
- Referential Integrity 6-17
- Summary 6-18
- Practice 6 Overview: Administering an Oracle Internet Directory Server 6-19

7 Oracle Internet Directory: Directory Security

- Objectives 7-2
- Managing Special Users 7-3
- Password Storage in OID 7-5
- Password Policies 7-6
- Creating Password Policies 7-7
- Applying Password Policies 7-10
- Password Verifiers 7-11

How Password Verification Works	7-13
Location of Password Verifiers	7-14
Attributes Storing Password Verifiers	7-15
Password Verifier Authentication Model	7-17
Managing Password Verifier Profiles	7-18
Creating Oracle Wallet for SSL	7-20
Configuring OID for SSL	7-21
Configuring OID Security Audits	7-23
Structure of Audit Log Entries	7-25
Managing Audit Log Entries	7-26
Summary	7-27
Practice 7 Overview: Implementing Oracle Internet Directory Security	7-28
8 Oracle Directory Integration Platform: Synchronization Concepts	
Objectives	8-2
Oracle Directory Integration Platform: Overview	8-3
Oracle Directory Integration Platform: Installation	8-5
Synchronization Service: Overview	8-6
Default Integration Profiles	8-8
Oracle Directory Integration Server: Run-Time Functionality	8-9
Registering the Oracle Directory Integration Server	8-10
Sequence of Oracle Directory Integration Server Events	8-12
Monitoring DIP Using Application Server Control	8-14
Starting the Oracle Directory Integration Server	8-15
Stopping the Oracle Directory Integration Server	8-17
Setting the Debug Level	8-19
Viewing Oracle Directory Integration Platform Information	8-21
Integration Profile Authentication	8-24
Access Control for DIP Server and Profiles	8-25
Connectors	8-27
Directory Synchronization Profiles	8-29
Synchronization Agent	8-31
Summary	8-32
9 Oracle Directory Integration Platform: Synchronization Services Administration	
Objectives	9-2
Synchronization Process	9-3
Registering Connectors to Oracle Internet Directory	9-5
Mapping Rules and Formats	9-10
Mapping Rule Format	9-12

- Domain Rules 9-15
- Attribute Rules 9-17
- Creating a New Mapping File 9-18
- Matching Filters 9-20
- Location and File Names 9-22
- Registering Profiles by Using ODM 9-24
- Deregistering a Profile Using ODM 9-25
- Using Directory Integration Assistant (`dipassistant`) 9-26
- Creating and Modifying Directory Synchronization Profile 9-28
- Creating, Modifying, Deleting and Viewing Directory Synchronization Profile 9-29
- Bootstrapping Data into OID 9-30
- Synchronization with Relational Database Tables 9-32
- Troubleshooting Oracle Directory Integration Platform 9-35
- Summary 9-41

10 Integrating with Sun Java System Directory Server

- Objectives 10-2
- Supported Third-Party Directories and Servers 10-3
- Integration Planning: OID as central enterprise directory 10-4
- Integration Planning: Third-party directory as central enterprise directory 10-5
- Integration Planning: Custom schema extensions 10-6
- Integration Planning: Password storage 10-7
- Integration Planning: Structure of DIT 10-9
- Integration Planning: Login name attribute 10-11
- Integration Planning: Set user/group search base 10-12
- Limitation of Third-Party Directory Integration 10-13
- Checklist Before Setting Up OID–Sun Java Directory Server Integration 10-14
- Creating Basic Synchronization Using Express Configuration 10-15
- Assumptions for Using Express Configuration 10-16
- Integrating OID–Sun Directory Using Express Configuration 10-17
- Integrating OID–Sun Directory Using Custom Configuration 10-19
- Integrating OID–Sun Directory Using Custom Configuration: Configuring the realms 10-20
- Integrating OID–Sun Directory Using Custom Configuration: Customize ACLs 10-21
- Integrating OID–Sun Directory Using Custom Configuration: Customize attribute mapping 10-23
- Integrating OID–Sun Directory Using Custom Configuration: Synchronize Deletions 10-24
- Integrating OID–Sun Directory Using Custom Configuration: Synchronize passwords 10-25
- Integrating OID–Sun Directory Using Custom Configuration: Using SSL 10-26

Integrating OID–Sun Directory Using Custom Configuration: External Authentication
plugin 10-27
Postconfiguration Tasks 10-30
Summary 10-31

11 Integrating with Microsoft Active Directory

Objectives 11-2
Checklist Before Setting Up OID and AD Integration 11-3
Creating Basic Synchronization Using Express Configuration 11-5
Assumptions for Using Express Configuration 11-6
Integrating OID–AD Using Express Configuration 11-7
Running Express Configuration Using Oracle Directory Integration Server
Administration Tool 11-10
Synchronizing from AD to OID 11-11
OID Schema Elements for AD 11-13
Integrating OID and AD Directory Using Advanced Configuration 11-14
Customizing the Search Filter to Retrieve Information from AD 11-15
Customizing Attribute Mappings 11-16
Customizing with Multiple AD Domains 11-17
Synchronizing Deletions from AD 11-19
Synchronizing Passwords 11-20
Microsoft Active Directory Forest 11-21
Foreign Security Principals 11-23
Resolving Foreign Security Principal References 11-25
Switching to a New AD Domain Controller Within the Same Domain 11-28
Summary 11-31

12 Windows Native Authentication and Oracle Password Filter

Objectives 12-2
Understanding WNA 12-3
How WNA Works 12-5
Configuring WNA for a Single AD Domain 12-6
Oracle Password Filter for AD: Overview 12-13
How Does Oracle Password Filter Work 12-14
Deploying Oracle Password Filter for AD 12-15
Configuring OID to Run in SSL Server Authentication Mode 12-16
Importing OID Trusted Server Certificate into AD Domain Controller 12-18
Verify SSL Server Authentication Mode Communication Between
OID and AD 12-20

Installing Oracle Password Filter for AD 12-21
Deinstalling Oracle Password Filter for AD 12-25
Summary 12-30

13 Oracle Internet Directory: Server Chaining

Objectives 13-2
Server Chaining: Overview 13-3
Reasons for Server Chaining 13-4
Server Chaining: Capabilities 13-5
Server Chaining: Attribute Mapping 13-6
Server Chaining: Command-Line Configuration 13-7
Server Chaining: Oracle Directory Manager Configuration 13-10
Server Chaining: Debugging 13-11
Summary 13-12
Practice 13 Overview: Configuring Server Chaining 13-13

14 Oracle Internet Directory: Replication Concepts

Objectives 14-2
OID Replication 14-3
Directory Replication Group and Replication Agreement 14-4
Types of Replicas 14-5
Types of Replication: Full Replication 14-6
Types of Replication: Partial Replication 14-7
Types of Directory Replication Groups 14-9
Data Transfer Between Nodes in a DRG 14-10
Single-Master DRG 14-11
Multimaster DRG 14-12
Fan-Out DRG 14-13
Multimaster and Fan-Out DRG 14-14
Replication Configuration Objects in OID 14-15
Replication Architecture 14-18
Supplier Oracle Advanced Replication Process 14-20
Consumer Oracle Advanced Replication Process 14-22
LDAP Replication Process 14-23
LDAP Replication Failover: Case 1 14-25
LDAP Replication Failover: Case 2 14-26
OID Replication Server Conflict Resolution 14-27
Automated Resolution of Conflicts 14-29
Replication Processes 14-30
Adding a New Entry to a Consumer 14-31
Deleting an Entry 14-33

Modifying an Entry	14-35
Modifying a Relative Distinguished Name	14-36
Modifying a Distinguished Name	14-38
Included and Excluded Naming Contexts	14-39
LDAP Replication Filtering Rules	14-40
Sample DIT	14-41
Scenario A: Partial Filtering Rules	14-42
Scenario B: Partial Filtering Rules	14-43
Planning Partial Replication Filtering Rules	14-44
Optimization of Partial Replication Filtering Rules	14-46
Summary	14-47

15 Setting LDAP-Based and ASR-Based OID Replication

Objectives	15-2
Master Definition Site and Remote Master Site	15-3
Rules of ASR-Based Replication	15-4
Installing and Configuring ASR	15-5
Installing OID on the MDS and RMS	15-6
Setting Up OID Advanced Replication for DRG	15-8
Loading Data into OID	15-11
Starting OID and Replication Server	15-12
Testing Directory Replication	15-13
Adding a Node for ASR	15-14
Adding a Replication Node	15-16
Deleting a Node from ASR	15-17
Rules of LDAP-Based Replication	15-18
Installing and Configuring Full One-Way or Two-Way LDAP Replication (Default Setting)	15-19
Installing and Configuring Partial One-Way or Two-Way LDAP Replication	15-20
Configuring LDAP Replication Using Automatic Bootstrapping or <code>ldifwrite/bulkload</code> Manually	15-21
Deleting an LDAP-Based Replica	15-26
Creating, Viewing, Modifying, and Deleting Replica Naming Context Objects	15-27
Human Intervention Queue Manipulation Tool	15-28
OID Comparison and Reconciliation Tool	15-29
Managing OID Replication	15-32
Modifying Configuration Parameters	15-33
Viewing and Modifying a Replica Node	15-35
Viewing and Modifying a Replication Agreement for ASR	15-37
Viewing and Modifying a Replication Agreement for LDAP Replication	15-39
Changing the Replication DN Password	15-41

Change Log Management 15-42
Modifying the Speed of Directory Replication 15-43
Managing and Monitoring LDAP Replication 15-44
Rules for Replication Failover 15-45
Types of Replication Failover 15-46
Summary 15-47

16 Oracle Virtual Directory: Concepts

Objectives 16-2
Types of Directory Services Solutions 16-3
Obstacles for Traditional Directories 16-4
Benefits of Virtual Directories 16-5
Oracle Virtual Directory: Features 16-7
Oracle Virtual Directory: Data Federation 16-8
Oracle Virtual Directory: Translation 16-9
Oracle Virtual Directory: Directory Security 16-10
Oracle Virtual Directory: High Availability Support 16-12
Oracle Virtual Directory: Custom-Integration APIs 16-13
Summary 16-14

17 Oracle Virtual Directory: Installation and Orientation

Objectives 17-2
OVD System Requirements 17-3
OVD Supported Software 17-4
OVD Installation Stages 17-5
OVD Installer: Install Location 17-6
OVD Installer: Configuration 1 17-7
OVD Installer: Configuration 2 17-8
OVD Installer: Configuration 3 17-9
OVD Installer: Pre-Install Summary and Installing 17-10
OVD Installer: SSL/TLS Config 17-11
OVD Installer: Finished 17-12
OVD Manager System Requirements 17-13
OVD Manager Installation Stages 17-14
OVD Manager Installer: Install Options 17-15
OVD Manager Installer: Pre-Installation Summary and Installing 17-16
OVD Manager: Overview 17-17
OVD Manager: Log Browser View 17-18
OVD Manager: Connection Configuration 17-19

OVD Manager: SSL Configuration to Server 17-20
Summary 17-21
Practice 17 Overview: Installing Oracle Virtual Directory 17-22

18 Oracle Virtual Directory: Basic Adapters

Objectives 18-2
Oracle Virtual Directory Adapters 18-3
LDAP Proxy Adapter 18-4
LDAP Adapter: Initial Configuration 18-5
LDAP Adapter: Configuration 18-7
LDAP Adapter: SSL Configuration 18-10
Database Adapter 18-11
Database Adapter: Functional Limitations 18-12
Database Adapter: Initial Configuration 18-13
Database Adapter: Table Mapping 18-15
Database Adapter: LDAP Object Mapping 18-16
Database Adapter: Configuration 18-18
NT Adapter 18-19
NT Adapter: Configuration 18-20
Local-Store Adapter 18-21
Local-Store Adapter: Initial Configuration 18-22
Local-Store Adapter: Configuration 18-23
Summary 18-25
Practice 18 Overview: Configuring OVD Adapters 18-26

19 Oracle Virtual Directory: Advanced Topics

Objectives 19-2
Join View Adapter 19-3
Join View Adapter: Roles 19-4
Join View Adapter: Join Relationships 19-5
Join View Adapter: Initial Configuration 19-6
Join View Adapter: Configuration 19-7
Routing 19-9
Routing: Configuration 19-10
Plug-Ins and Mappings 19-13
Preinstalled Plug-Ins 19-14
Preinstalled Mappings 19-16
Deploying and Applying Plug-Ins 19-18
Deploying and Applying Mappings 19-19
Summary 19-20
Practice 19 Overview: Completing OVD Practice Configuration 19-21

Appendix A: Practices

Appendix B: Practice Solutions

Index