Oracle® Identity Management

Concepts and Deployment Planning Guide

10*g* Release 2 (10.1.2)

Part No. B14084-01

December 2004

Oracle Identity Management Concepts and Deployment Planning Guide 10*g* Release 2 (10.1.2)

Part No. B14084-01

Primary Authors: Ellen Desmond, Richard Strohm

Contributors: Tridip Bhattacharya, Kamelendu Biswas, Daria Hutchinson, Ganesh Kirti, Ashish Kolli, Stephen Lee, Michael Mesaros, Deborah Owens, Santhisree Ragipati, David Saslav, Daniel Shih, Saurabh Shirvastava, Richard Smith, Uppili Srinivasan

Contents

4 Oracle Identity Management Administration and Usage

5 Integrating with Other Identity Management Solutions

A Deploying Oracle Identity Management with Multimaster Replication

List of Figures

Send Us Your Comments

Oracle Identity Management Concepts and Deployment Planning Guide 10*g* Release 2 (10.1.2)

Part No. B14084-01

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: appserverdocs_us@oracle.com
- FAX: (650) 506-7375. Attn: Oracle Application Server Documentation Manager
- Postal service:

  Oracle Corporation
  Oracle Application Server Documentation
  500 Oracle Parkway, Mailstop 1op6
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.

Preface

Oracle Identity Management Concepts and Deployment Planning Guide describes concepts pertaining to identity management and provides deployment planning information for administrators and application developers.

This preface contains these topics:

Intended Audience

This document is intended for the following audience:

- Identity management administrators
- Oracle application administrators
- Enterprise application developers

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. 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 additional information, visit the Oracle Accessibility Program Web site at

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

Accessibility of Code Examples in Documentation

JAWS, a Windows screen reader, 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, JAWS 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.

Structure

The *Oracle Identity Management Concepts and Deployment Planning Guide* provides the conceptual framework required to understand and deploy the Oracle Identity Management infrastructure in an enterprise. Details on how to deploy and administer specific components of the Oracle Identity Management infrastructure are covered in their respective administrator's guides.

This document contains the following chapters:

Chapter 1, "Introduction to Identity Management"

This chapter introduces identity management and describes why it is needed in an enterprise.

Chapter 2, "Oracle Identity Management Concepts and Architecture"

This chapter discusses Oracle Identity Management concepts and architecture.

Chapter 3, "Oracle Identity Management Deployment Planning"

This chapter discusses Oracle Identity Management deployment.

Chapter 4, "Oracle Identity Management Administration and Usage"

This chapter discusses Oracle Identity Management administration and usage.

Chapter 5, "Integrating with Other Identity Management Solutions"

This chapter discusses integrating Oracle Identity Management with other identity management solutions.

Appendix A, "Deploying Oracle Identity Management with Multimaster Replication"

This appendix describes how to install Oracle Identity Management with Multimaster Replication.

Appendix B, "Deploying Oracle Identity Management with Fan-Out Replication"

This appendix describes how to install Oracle Identity Management with Fan-Out Replication.

Appendix C, "Oracle Internet Directory Default Settings"

This appendix discusses the defaults available upon installation of Oracle Internet Directory.

Related Documents

For more information, see the following guides:

- *Oracle Application Server Administrator's Guide*
- *Oracle Application Server Security Guide*
- *Oracle Application Server High Availability Guide*

- *Oracle Application Server Installation Guide*
- *Oracle Application Server Certificate Authority Administrator's Guide*
- *Oracle Application Server Single Sign-On Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Identity Management Guide to Delegated Administration*
- *Oracle Identity Management Integration Guide*

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle Database Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.
UPPERCASE monospace (fixed-width) font	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a NUMBER column. You can back up the database by using the BACKUP command. Query the TABLE_NAME column in the USER_TABLES data dictionary view. Use the DBMS_STATS.GENERATE_STATS procedure.
lowercase monospace (fixed-width) font	Lowercase monospace typeface indicates executable programs, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names and connect identifiers, user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. *Note:* Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter sqlplus to start SQL*Plus. The password is specified in the orapwd file. Back up the datafiles and control files in the /disk1/oracle/dbs directory. The department_id, department_name, and location_id columns are in the hr.departments table. Set the QUERY_REWRITE_ENABLED initialization parameter to true. Connect as oe user. The JRepUtil class implements these methods.

Convention	Meaning	Example
lowercase italic monospace (fixed-width) font	Lowercase italic monospace font represents placeholders or variables.	You can specify the *parallel_clause*. Run *old_release*.SQL where *old_release* refers to the release you installed prior to upgrading.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[ ]	Anything enclosed in brackets is optional.	DECIMAL (*digits* [, *precision*])
{ }	Braces are used for grouping items.	{ENABLE | DISABLE}
|	A vertical bar represents a choice of two options.	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]

...	Ellipsis points mean repetition in syntax descriptions.
	In addition, ellipsis points can mean an omission in code examples or text.
		CREATE TABLE ... AS *subquery*;
		SELECT *col1*, *col2*, ... , *coln* FROM employees;

Other symbols	You must use symbols other than brackets ([ ]), braces ({ }), vertical bars (|), and ellipsis points (...) exactly as shown.	acctbal NUMBER(11,2);
		acct CONSTANT NUMBER(4) := 3;

Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	CONNECT SYSTEM/*system_password* DB_NAME = *database_name*

UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. Because these terms are not case sensitive, you can use them in either UPPERCASE or lowercase.	SELECT last_name, employee_id FROM employees;
		SELECT * FROM USER_TABLES;
		DROP TABLE hr.employees;

lowercase	Lowercase typeface indicates user-defined programmatic elements, such as names of tables, columns, or files.
	Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.
		SELECT last_name, employee_id FROM employees;
		sqlplus hr/hr
		CREATE USER mjones IDENTIFIED BY ty3MU9;

1

Introduction to Identity Management

This chapter introduces identity management, describes components of an identity management system, and provides an overview and objectives of Oracle Identity Management.

This chapter contains the following topics:

- What Is Identity Management?
- Identity Management System Components
- Oracle Identity Management Overview
- Oracle Identity Management Objectives

What Is Identity Management?

Identity management is the process by which user identities are defined and managed in an enterprise environment. Specifically, identity management describes the process by which:

- User identities are provisioned and coordinated.
- Application provisioning is automated.
- User roles, privileges, and credentials are managed.
- Administrators delegate responsibility.
- Administrators deploy applications easily and securely.
- Users self-manage their preferences and passwords.
- Users have single sign-on access.

Steps in the security lifecycle include account creation, suspension, privilege modification, and account deletion.

An identity management system can include users outside an enterprise, such as customers, trading partners, or Web services, as well as users inside an organization. In addition, an identity management system can manage network entities other than users, such as devices, processes, and applications.

By using an identity management system, an enterprise can:

- Reduce administration costs through centralized account management and automated tasks
- Accelerate application deployment by enabling new applications to use the existing infrastructure to provision user accounts and privileges

- Reduce the time it takes to give new users access to applications
- Improve security and usability by centrally managing user passwords and security credentials

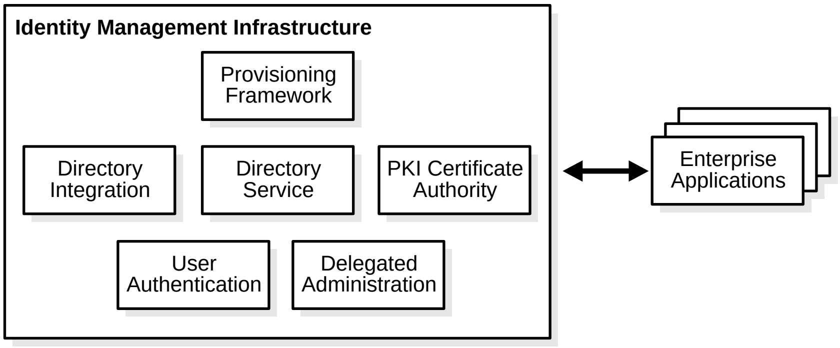
Identity Management System Components

A complete identity management system includes the following components:

- A scalable, secure, and standards-compliant directory service for storing and managing user information.
- A provisioning framework that can either be linked to the enterprise provisioning system, such as a human resources application, or operated in standalone mode.
- A directory integration platform that enables the enterprise to connect the identity management directory to legacy or application-specific directories.
- A system to create and manage public key infrastructure (PKI) certificates.
- A run time model for user authentication.
- A delegated administration model and application that enables the administrator of the identity management system to selectively delegate access rights to an administrator of an individual application or directly to a user.

Figure 1–1 shows an overview of an identity management system.

Figure 1–1 Overview of an Identity Management System



Oracle Identity Management Overview

Oracle Identity Management is an integrated infrastructure that provides distributed security to Oracle products. Oracle Identity Management is included with Oracle Application Server, as well as Oracle Database and Oracle Collaboration Suite.

The Oracle Identity Management infrastructure includes the following components:

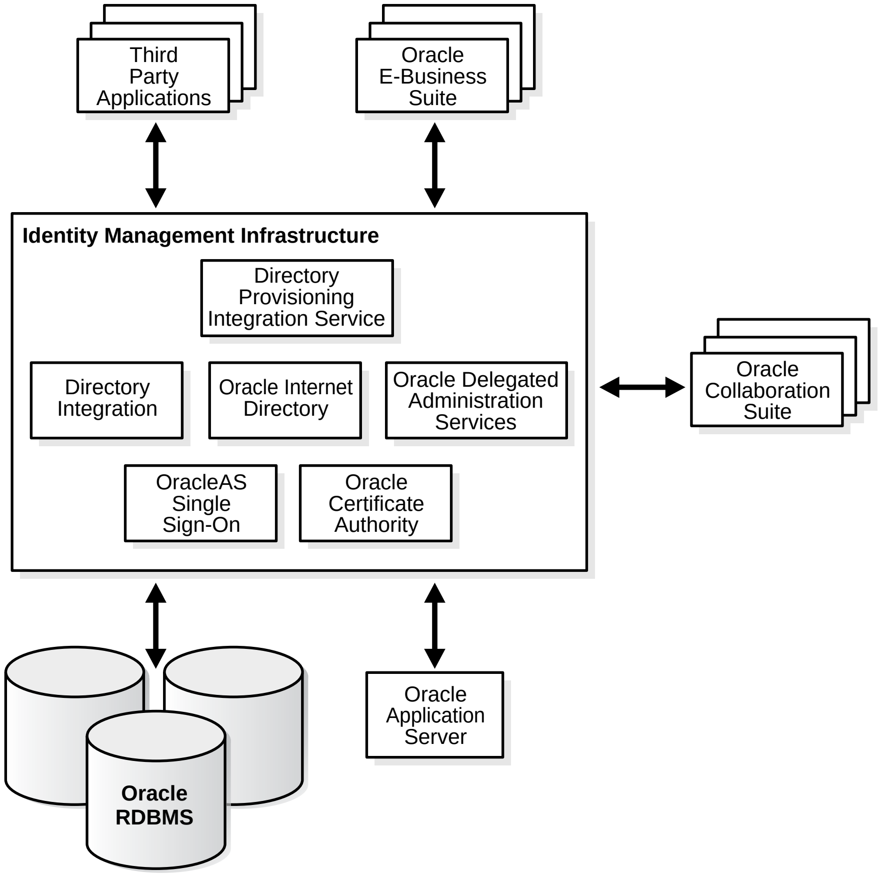
- Oracle Internet Directory: A scalable, robust LDAP V3-compliant directory service implemented on the Oracle Database
- Oracle Directory Integration and Provisioning Platform: A component of Oracle Internet Directory that consists of two parts:
  - Directory Provisioning Integration Service, which notifies to target applications of changes to a user’s status or information
  - Directory Integration, which enables:

  - * Synchronization of data between Oracle Internet Directory and other connected directories
  - * Development and deployment of custom connectivity agents

- Oracle Application Server Certificate Authority: A component that issues, revokes, renews, and publishes X.509v3 certificates to support PKI-based strong authentication methods
- Oracle Application Server Single Sign-On (OracleAS Single Sign-On): A component that provides single sign-on access to Oracle and third-party Web applications
- Oracle Delegated Administration Services: A component of Oracle Internet Directory that provides trusted proxy-based administration of directory information by users and application administrators

Many different applications, including third-party applications, Oracle E-Business Suite, Oracle Application Server, Oracle Database and Oracle Collaboration Suite, can use the Oracle Identity Management infrastructure, as shown in Figure 1–2.

Figure 1–2 Oracle Identity Management


Third Party Applications
Oracle E-Business Suite
Identity Management Infrastructure
Directory Provisioning Integration Service
Directory Integration
Oracle Internet Directory
Oracle Delegated Administration Services
OracleAS Single Sign-On
Oracle Certificate Authority
Oracle Collaboration Suite
Oracle RDBMS
Oracle Application Server

While Oracle Identity Management provides an enterprise infrastructure for Oracle products, it can also be a general-purpose identity management solution for custom and third-party enterprise applications.

In addition, third-party application vendors certify with Oracle Identity Management infrastructure to ensure proper operation.

Oracle Identity Management Objectives

Oracle Identity Management is designed to meet three key architectural objectives:

- Oracle Identity Management is a shared infrastructure for all Oracle products and technology stacks, including Oracle Application Server, Oracle Database, Oracle E-Business Suite, and Oracle Collaboration Suite.

  Oracle Identity Management provides a consistent security model among all Oracle products and technology stacks. Oracle Identity Management infrastructure is planned for and deployed once, to support any current or future deployment of Oracle products.

- Oracle Identity Management provides a secure, efficient, and reliable way to use and extend your investment in an existing third-party identity management infrastructure.

  - Within a third-party identity management environment, Oracle Identity Management provides a single consistent point of integration for the entire Oracle technology stack, eliminating the need to configure and manage integration of various individual Oracle products with the third-party environment
  - By using Oracle Directory Integration and Provisioning, Oracle Identity Management takes advantage of the investment made in planning and deployment of a third-party enterprise directory. This provides a way to map and inherit major considerations such as directory naming, directory tree structure, schema extensions, access control, and security policies. Established procedures in an existing framework for user enrollment can be seamlessly incorporated into the corresponding operations of Oracle Identity Management.
  - If a third-party authentication service is in use, OracleAS Single Sign-On provides a way to integrate with the service and provide a seamless single sign-on experience to users accessing the Oracle environment. Certified interoperability solutions exist for leading third-party authentication platforms, and well-defined interfaces are available for implementing similar solutions for any new product.

- The Oracle Identity Management infrastructure can be an enterprise-wide foundation for identity management, to support other Oracle products and third-party products deployed in the enterprise.

  Oracle Identity Management can lower ownership costs by streamlining the maintenance of account information for all Oracle and third-party products. It also offers high levels of security and scalability, and provides numerous features. By supporting industry standards in all relevant interfaces, Oracle Identity Management can be customized and used in many different application environments.

2

Oracle Identity Management Concepts and Architecture

This chapter introduces concepts that deployment planners must understand to effectively deploy identity management. It provides an overview of the Oracle Identity Management architecture, the provisioning lifecycle of applications and users in the Oracle environment, and presents the terms that are commonly used to describe identity management.

This chapter contains the following sections:

- Identity Management Terminology
- Identity Management Concepts
- Identity Management Integration with Oracle Products

Identity Management Terminology

The following list defines some important identity management terms and concepts:

- **Authentication**: The process of verifying the identity claimed by an entity based on its credentials.
- **Authorization**: The process of establishing a specific entitlement that is consistent with authorization policies.
- **Authorization policies**: Declarations that define entitlements of a security principal and any constraints related to that entitlement.
- **Centralized assertion services**: Part of the identity management infrastructure that generates identity assertions. OracleAS Single Sign-On is an example of an assertion service that generates identity assertions. OracleAS Certificate Authority is another type of assertion service, because the X.509v3 certificates it generates are assertions about a security principal’s identity and its entitlements.
- **Entitlements**: The actions an entity in a network is allowed to perform and the resources to which it is allowed access.
- **Identity**: The set of attributes that uniquely identifies a security principal. A security principal can have many different accounts that it uses to access various applications in the network. These accounts can be identified by these applications using different attributes of this entity. For example, a user can be known in the e-mail service by an e-mail ID, whereas that same user can be known in the human resource application by an employee number. The global set of such attributes constitutes the identity of the entity.

- **Identity administration**: The act of managing information associated with the identity of a security principal. The information can be used by the identity management infrastructure itself to determine administrative privileges.
- **Identity management policies**: Policies affecting the management of identities in an enterprise which includes naming policies and security policies.
- **Identity policy assertion services**: A process that generates verifiable assertions about the identity of an entity or its authorizations. Network entities present these assertions to services the entities access.
- **Metadata repository**: An Oracle database used to hold metadata, including identity information.
- **Policy decision services**: A process that interprets any applicable entitlement policies associated with the resources to which applications secure and control access. Some applications rely on decision services that are embedded in the application itself, while others depend on centralized decision services.
- **Provisioning**: Notification of applications whenever changes are applied to Oracle Internet Directory.
- **Realm**: A collection of identities and associated policies which is typically used when enterprises want to isolate user populations and enforce different identity management policies for each population.
- **Security principals**: The subjects of authorization policies, such as users, user groups, and roles. A security principal can be a human or any application entity with an identity in the network and credentials to assert the identity.

Identity Management Concepts

This section describes the fundamental concepts of identity management and contains the following topics:

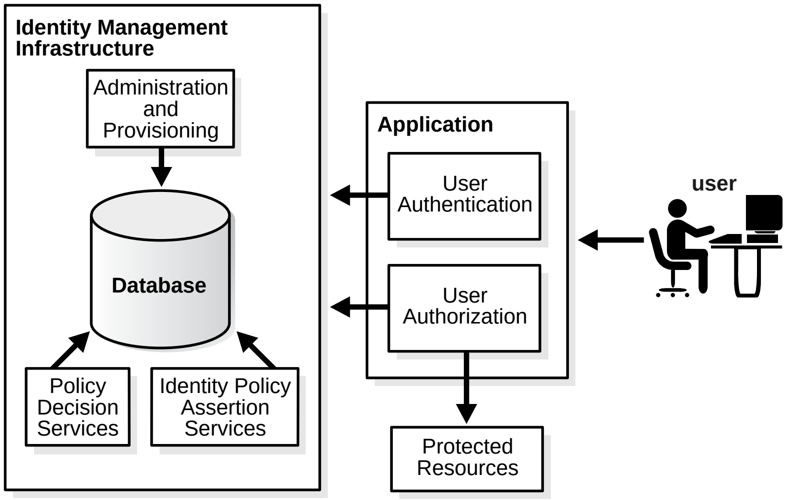
- Integrating Application Security with Identity Management
- Identity and Application Provisioning Lifecycle
- Administrative Delegation

Integrating Application Security with Identity Management

This section provides a framework for understanding the roles of various Oracle Identity Management components and services, and provides a basis for understanding how to create secure application deployments in an enterprise environment.

The application integration model is shown in Figure 2–1.

Figure 2–1 Application Integration Model



In this model, the following essential services are performed by the identity management infrastructure:

- **Administration and provisioning**: Provides administration and provisioning services for the identities managed by the identity management infrastructure. In Oracle Identity Management, these services are performed using tools such as Oracle Delegated Administration Services and Oracle Directory Integration and Provisioning.
- **Policy decision services**: Oracle Internet Directory performs policy decision services for the identity management infrastructure itself.
- **Identity policy assertion services**: In Oracle Identity Management these services are performed by OracleAS Single Sign-On and OracleAS Certificate Authority

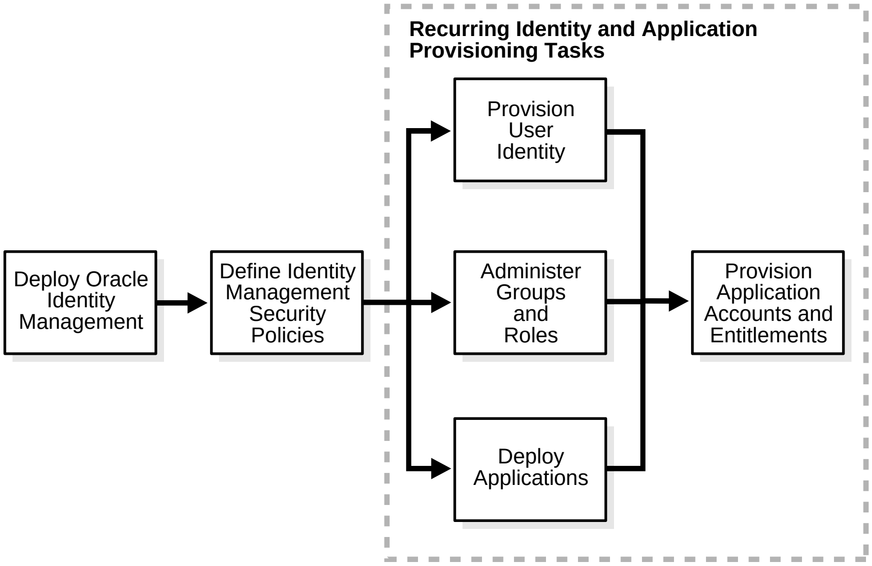
Applications deployed against the identity management infrastructure interact with the infrastructure in the following ways:

- **User authentication**: When a user accesses an application, it validates the user credentials using the services provided by the identity management infrastructure. The authentication and the associated communication to the application is accomplished with the identity policy assertion services. For example, in the case of the Oracle Identity Management infrastructure, this would be validation of the credential, in the form of an encrypted browser cookie, by OracleAS Single Sign-On.
- **User authorization**: Once authenticated, the application must also check if the user has sufficient privileges over resources protected by the application. This check is performed by the application based on identity information managed in the identity management infrastructure. For example, a Java2 Enterprise Edition application uses Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider (OracleAS JAAS Provider) to access user and role information in the Oracle Identity Management infrastructure, after authentication.

Identity and Application Provisioning Lifecycle

This section provides an overview of the user identity and application provisioning flow in the Oracle environment.

Figure 2–2 Identity and Application Provisioning Flow


Recurring Identity and Application Provisioning Tasks
Deploy Oracle Identity Management
Define Identity Management Security Policies
Provision User Identity
Administer Groups and Roles
Deploy Applications
Provision Application Accounts and Entitlements

The following describes the provisioning flow shown in Figure 2–2:

1. Deploy the Oracle Identity Management infrastructure using the product's installation and configuration tools.
2. Define the identity management security policies. These policies determine what data users and applications can access. They are stored as access control lists (ACLs) in Oracle Internet Directory, and are typically managed using Oracle Directory Manager.
3. The following activities typically take place on an ongoing basis. Each activity can happen in parallel, and in no particular order.
   - User identities are provisioned in Oracle Internet Directory. These identities can come from multiple sources: human resources applications, user administration tools (such as the Oracle Internet Directory Self-Service Console), synchronization with other directories, or bulk loading tools.
   - Groups and roles are administered in Oracle Internet Directory. Groups and group memberships can be defined in a number of ways, such as through the Oracle Internet Directory Self-Service Console or through synchronization with another directory service.
   - Application instances are deployed against the Oracle Identity Management infrastructure. This typically involves an identity management infrastructure administrator first granting access to the application administrator using the Oracle Internet Directory administration tools. The application administrator uses application installation and configuration tools to create the required directory objects and entries to support the application.
4. User identities, groups and roles, and applications are associated through the process of application provisioning. This can be performed manually using application administration tools or automatically through provisioning integration.

Administrative Delegation

Oracle Identity Management requires a central repository for enterprise users, groups, and services. Business requirements, however, make it difficult to manage a central repository with a centralized set of administrators.

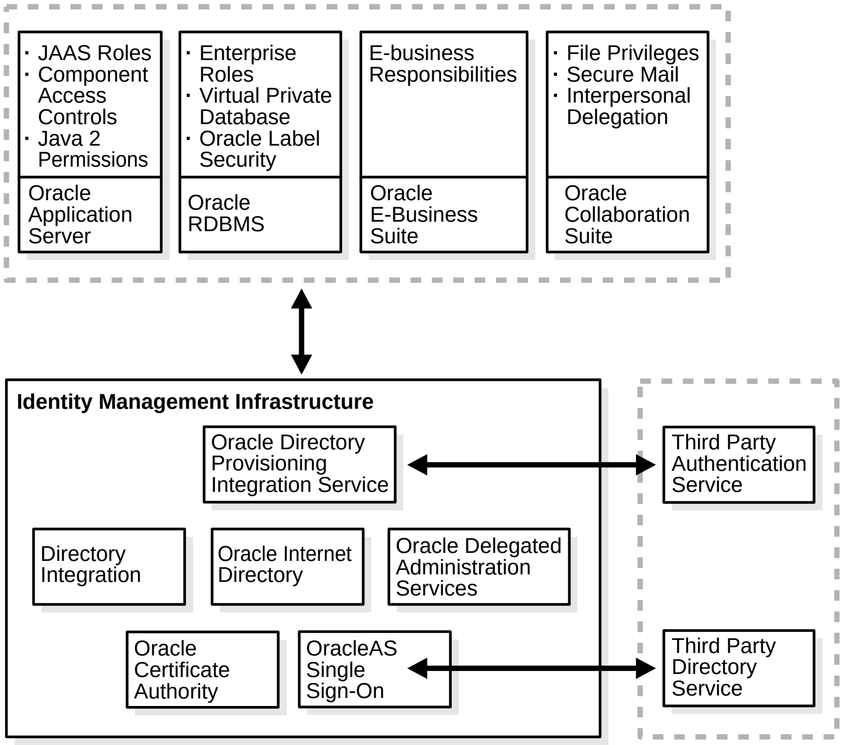
For example, in a business, the administrator of enterprise user management might be different from that of the e-mail service; the administrator of financials may need full control over the privileges of its users; and the OracleAS Portal administrator may need full control over the Web pages for a specific user or a specific group. To meet the needs of these administrators and satisfy their different security requirements, the identity management system needs delegated administration.

With delegated administration, the management of data inside the identity management system can be distributed to many different administrators depending upon their security requirements. This combination of centralized repository and delegated privileges results in a secure and scalable administration in the identity management infrastructure.

Identity Management Integration with Oracle Products

Each of the Oracle technology stacks—Oracle Application Server, Oracle Database, Oracle E-Business Suite, and Oracle Collaboration Suite—supports a security model appropriate for its design. Nevertheless, they all use the Oracle Identity Management infrastructure to implement their respective security models and capabilities, as shown in Figure 2–3.

Figure 2–3 Identity Management Integration with Oracle Products


· JAAS Roles
· Component Access Controls
· Java 2 Permissions
Oracle Application Server
· Enterprise Roles
· Virtual Private Database
· Oracle Label Security
Oracle RDBMS
E-business Responsibilities
Oracle E-Business Suite
· File Privileges
· Secure Mail
· Interpersonal Delegation
Oracle Collaboration Suite
Identity Management Infrastructure
Oracle Directory Provisioning Integration Service
Directory Integration
Oracle Internet Directory
Oracle Delegated Administration Services
Oracle Certificate Authority
OracleAS Single Sign-On
Third Party Authentication Service
Third Party Directory Service

Oracle Application Server supports a J2EE compliant security service called Java Authentication and Authorization Service (JAAS). JAAS can be configured to use the users and roles defined in Oracle Internet Directory.

Similarly, the metadata repository security capabilities—enterprise user and Oracle Label Security—provide a way to take advantage of users and roles defined in Oracle Internet Directory. Both of these platforms facilitate the applications developed using the platforms' respective native security capabilities to transparently leverage the underlying identity management infrastructure.

Oracle E-Business Suite and Oracle Collaboration Suite application stacks are layered over Oracle Database and Oracle Application Server, providing indirect integration with the Oracle Identity Management infrastructure. In addition, these products have independent features that rely on Oracle Identity Management. For example, Oracle Collaboration Suite components, such as Oracle Email and Oracle Voicemail & Fax, use Oracle Internet Directory to manage component-specific user preferences, personal contacts, and address books.

These Oracle technology stacks also use Oracle Directory Integration and Provisioning to automatically provision and de-provision user accounts and privileges. Oracle Delegated Administration Services is used extensively for self-service management of user preferences and personal contacts. In addition, the security management interfaces of these products use the user and group management building blocks called service units.

3

Oracle Identity Management Deployment Planning

This chapter describes the planning methods for deploying Oracle Identity Management services.

This chapter contains the following sections:

- Identity Management Deployment Planning Process
- Requirement Analysis for Identity Management Deployment
- Detailed Deployment Planning for Identity Management

Identity Management Deployment Planning Process

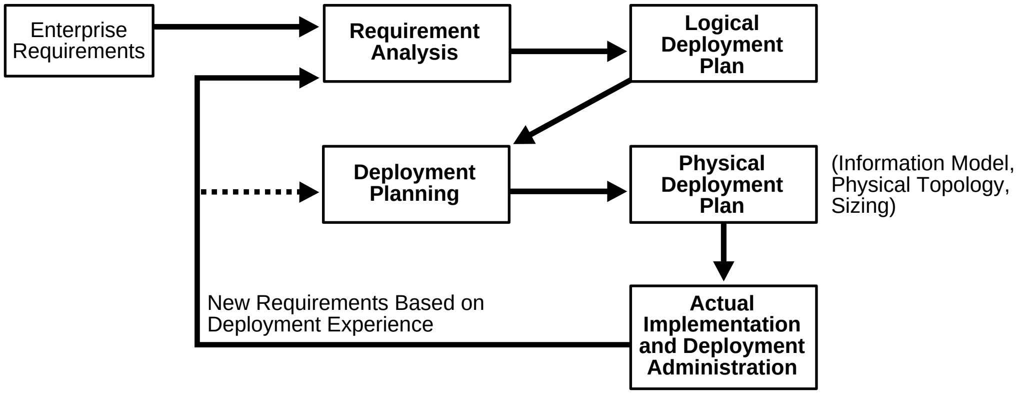
Successful deployment and use of products depend on a well-planned identity management infrastructure.

This section outlines the deployment planning process for the Oracle Identity Management infrastructure, as follows:

- A requirement analysis and high-level deployment considerations are presented along with some logical deployment plans that highlight these considerations.
- Detailed deployment planning considerations are presented.

Figure 3–1 illustrates the process to follow when planning an identity management deployment.

Figure 3–1 The Deployment Planning Process


Enterprise Requirements
Requirement Analysis
Logical Deployment Plan
Deployment Planning
Physical Deployment Plan
(Information Model, Physical Topology, Sizing)
Actual Implementation and Deployment Administration
New Requirements Based on Deployment Experience

As shown in Figure 3–1, the deployment planning process is iterative. Based on the initial requirements, you perform high-level planning to create a logical deployment plan, and you use the logical deployment plan to perform detailed deployment planning and create the physical deployment plan for the actual implementation. If new requirements emerge after implementation, you repeat the analysis, planning, and deployment process.

Requirement Analysis for Identity Management Deployment

This section describes some of the typical enterprise requirements you must analyze when planning an Oracle Identity Management deployment. The requirements include process issues, functionality requirements, and high availability concerns. It also describes various logical deployment plans that can help you select the optimal logical architecture of the Oracle Identity Management infrastructure. Some of the main requirements that drive the logical deployment decision are enterprise integration, administrative controls, and application deployment requirements.

At the end of the requirement analysis process, you select a high-level, logical architecture for the Oracle Identity Management deployment consisting of one or more logical identity management infrastructures. This is the basis for the detailed deployment planning that is outlined in the next section.

This section contains the following topics:

- High-Level Enterprise Requirements
- Transforming Requirements into a Logical Deployment Plan

High-Level Enterprise Requirements

This section describes high-level requirements and contains the following topics:

- Deciding Who Will Plan and Deploy the Oracle Identity Management Infrastructure
- Deciding Which Components of Oracle Identity Management to Deploy
- Considering Information Model Requirements
- Considering Centralized Security Management Requirements
- Considering Enterprise Application Requirements
- Considering Administrative Autonomy Requirements
- Considering Security Isolation Requirements
- Considering Third-Party Identity Management Integration Requirements
- Considering High Availability, Scalability, and Performance Requirements

Deciding Who Will Plan and Deploy the Oracle Identity Management Infrastructure

For small deployments, application administrators are typically responsible for planning, deploying, and administering Oracle Identity Management.

Large deployments can take advantage of the centralized services provided by an identity management infrastructure, such as sharing services across a variety of Oracle and third-party applications, and create a central group, that consists of application, network, and security administrators responsible for these services. This group typically performs the following tasks:

- Designing the identity management system deployment

- Defining security policies for the shared infrastructure
- Managing and administrating the deployment
- Monitoring processes and log files
- Monitoring performance and machine loads
- Implementing data backup strategies and restoring data in the event of failures

Deciding Which Components of Oracle Identity Management to Deploy

The components that comprise Oracle Identity Management centralize many administration tasks.

Plan on implementing Oracle Internet Directory, OracleAS Single Sign-On, and Oracle Delegated Administration Services. Oracle Internet Directory and OracleAS Single Sign-On provide basic identity management services, and Oracle Delegated Administration Services is the primary means for user password self-maintenance.

Deploy Oracle Directory Integration and Provisioning if you are integrating with other third-party directories. The directory integration platform is configured with specific directory synchronization profiles that enable synchronization with supported third-party directories.

If you are not using third-party directories, you should consider deploying Oracle Directory Integration and Provisioning services because many Oracle products, such as Oracle Application Server Portal and Oracle Collaboration Suite, use its provisioning integration features.

If you are deploying a public key infrastructure (PKI), you can use Oracle Application Server Certificate Authority to issue and manage certificates. If you have already deployed a third-party PKI, you can configure the rest of the Oracle Identity Management infrastructure and other Oracle products to use the existing certificate authority.

Additionally, some Oracle products require deployment of some Oracle Identity Management infrastructure components to support user administration.

> **Note:** Specific information about the dependencies of individual Oracle products on the various Oracle Identity Management components are described in their respective administrator's guides.

In small installations of Oracle products and in preproduction environments, application administrators can install minimal instances of the Oracle Identity Management infrastructure to support their Oracle applications.

> **See Also:** *Oracle Application Server Administrator's Guide* for installation guidelines

Many enterprises have, or have plans to deploy, other identity management components. Oracle Identity Management is designed to use other enterprise identity management solutions and any applications you already have for provisioning and administering your enterprise environments.

Oracle components that use identity management, such as Oracle Application Server, Oracle Database, and Oracle Collaboration Suite, are supported by an Oracle Identity Management instance. This instance works with your deployed infrastructure components to provide transparent user management and Web single sign-on across both environments.

Considering Information Model Requirements

The Oracle Identity Management infrastructure uses Oracle Internet Directory as the repository for storing all user identities. A user can have access to multiple applications in the enterprise. Typically, however, there should be only one entry in Oracle Internet Directory representing any particular user's identity. You must plan the location and contents of the user entries in the directory information tree (DIT) before deploying Oracle Internet Directory and other identity management infrastructure components.

In application service provider (ASP) deployments where centralized identity management is required, you must create different identity management realms for the ASP administrators and for the users of each of the ASP customers (subscribers).

Considering Centralized Security Management Requirements

With the growth of e-business and enterprise applications, IT departments need to consider how to reuse user profile information and provide access to a growing number of users, both inside and outside the enterprise, without diminishing security or exposing sensitive information. The administration of multiple versions of user identities across multiple applications makes their task difficult Consider deploying a central identity management infrastructure to enable features such as centralized account creation and management, single password and credential management, and single sign-on to Web applications.

Considering Enterprise Application Requirements

Typically, an identity management infrastructure is shared across an assortment of Oracle and other enterprise applications. Therefore, it is important to consider the following deployment requirements:

- **Types of users**: It may be necessary for enterprise applications, such as OracleAS Portal, to be available to external (Internet) users, such as business partners, in addition to internal (intranet) users. As a result, you must determine if one Oracle Internet Directory for all identities or a separate Oracle Internet Directory for each group of identities is appropriate.
- **Application load requirements**: Application load and availability requirements determine how available the identity management infrastructure must be. If applications must be highly available, so must the identity management infrastructure on which they depend.
- **ASP requirements**: Apart from the identity management deployment, consider the requirements mandated by the application. For example, an ASP deployment might require administrative delegation.

Considering Administrative Autonomy Requirements

- **Departmental autonomy for deployment of new applications**: Large enterprises may require administrative autonomy for applications within independent departmental units. In such a case, it may be necessary to have a separate departmental application repository that contains some enterprise data, along with application-specific data, while maintaining a centralized identity management infrastructure.
- **Administrative autonomy for managing common identity information**: Security policies are important considerations when planning identity management.

Consider the administration models for managing the identity, roles, policies, and groups to meet the enterprise requirements. It should be possible to manage the identity of the users according to common privileges defined by the security policies of the enterprise.

- **Administrative autonomy for individual applications deployed against the identity management infrastructure**: An enterprise may have a different administrator responsible for each enterprise application. For example, the administrator of enterprise user management might be different from that of the e-mail service; the administrator of financials might need full control over the privileges of its users; and the OracleAS Portal administrator may need full control over the Web pages for a specific user or a specific group. In addition, you must define which users need access to which resources and at what level of security. To meet the needs of the administrators, and to satisfy the different security requirements, you need to consider the administrative controls requirements.

Considering Security Isolation Requirements

There may be enterprise applications deployed, such as OracleAS Portal, that must be available to both internal users and external users. You must ensure that corporate intranet resources are isolated from external users, and that intranet applications are protected from denial of service attacks aimed at the extranet portal. In such deployments, security separation may be necessary between the internal and external identity management infrastructures.

Due to organizational constraints and high-level executive mandates, it may be necessary to deploy separate identity management infrastructures for different environments to maintain a clear separation between environments and provide protection from one environment to another. Sometimes, it may also be necessary to isolate some data changes to one environment or to delay their propagation.

Note: These are primarily high-level considerations and not derived from any actual throughput or capacity calculations, which are typically addressed by tuning and sizing in the next stage of planning.

Considering Third-Party Identity Management Integration Requirements

Consider the following integration functions if an enterprise has a third-party identity management infrastructure in place:

- **Windows integration**: If an enterprise is using Microsoft Windows components, such as Active Directory and Kerberos authentication, consider the integration required for the identity management components. Examples of integration functions are synchronizing user information with Oracle Internet Directory, and integrating OracleAS Single Sign-On authentication.
- **User account management**: User account management refers to the process by which new users are added to and deleted from enterprise systems. New user accounts can potentially be created from a number of different sources, such as human resource (HR) systems, customer relationship management (CRM) systems, and network administration environments. When a new user is created in one system, automated provisioning creates the required user account *profiles* in other enterprise applications.

  If an enterprise has deployed enterprise applications such as HR and CRM, consider using the user provisioning integration features with the identity management system. The user provisioning can still be done from the different sources.

- **Directory services**: If an enterprise has deployed an LDAP directory, such as iPlanet, consider synchronizing the LDAP server with Oracle Internet Directory to provide centralized user administration.
- **Runtime security service integration**: If it is necessary for users to access applications integrated with Oracle Internet Directory and a third-party or Web authentication application, consider integration requirements that provide OracleAS Single Sign-On access to Web applications with a single digital identity.

Considering High Availability, Scalability, and Performance Requirements

Identity management infrastructures contain several components, and each has availability considerations. A high availability solution must be able to detect and recover from software failures of any of the processes associated with identity management. Components must be deployed to meet the availability requirements of the whole application.

Based upon application usage and user traffic, performance requirements must be considered. Deployment configurations must be planned so that the deployment can be scaled for increased user traffic as applications are deployed.

"Planning the Physical Network Topologies" on page 3-20 lists accepted physical topologies that implement the requirements, such as high availability, scalability, and performance.

Transforming Requirements into a Logical Deployment Plan

This section discusses commonly-used logical deployment models that can help you select a logical deployment plan. By matching your requirements to one or more of these models, you can derive a logical deployment plan.

This section contains the following topics:

- Model of Deploying a Central Identity Management System - Standard Enterprise Model
- Model for Internal and External Users
- Model of Providing Administrative Autonomy for Departmental Applications
- Model of Integrating Oracle Identity Management in a Windows Environment
- Deploying Central Identity Management Infrastructure in Application Service Provider Hosting Environments

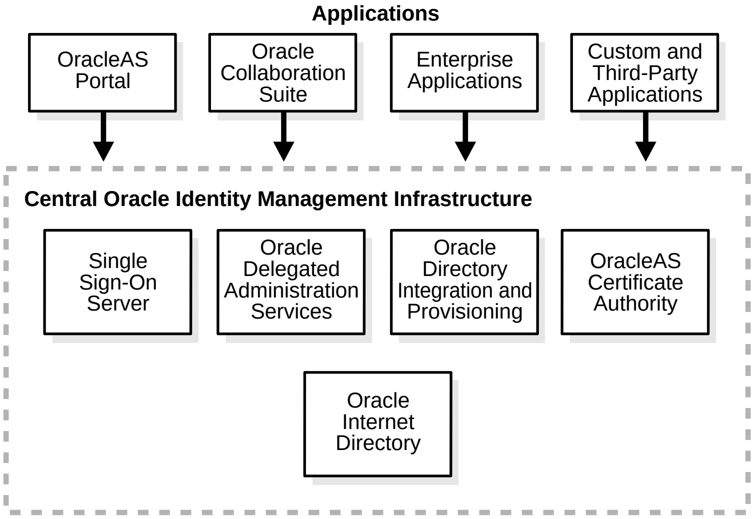
Model of Deploying a Central Identity Management System - Standard Enterprise Model

In a standard enterprise model, such as the one shown in Figure 3–2, a group within an organization manages and deploys a single centralized identity management infrastructure. As instances of enterprise applications are deployed, they use the centralized infrastructure. A centralized security model allows applications to install against a central infrastructure but with controlled privileges. This model makes deployment and administration of new applications much easier and improves application usability by enabling certain features, such as centralized account creation and management, single password and credential management, and single sign-on to Web applications. The information model is the same for all the users in this deployment.

This type of deployment implements the following:

- Central administration through a single, enterprise-wide console to create enterprise identities and manage shared properties
- A shared identity management infrastructure for Oracle and other enterprise applications
- Administrative controls to delegate the administration of the applications

Figure 3–2 Central Identity Management Infrastructure


Applications
OracleAS Portal
Oracle Collaboration Suite
Enterprise Applications
Custom and Third-Party Applications
Central Oracle Identity Management Infrastructure
Single Sign-On Server
Oracle Delegated Administration Services
Oracle Directory Integration and Provisioning
OracleAS Certificate Authority
Oracle Internet Directory

Model for Internal and External Users

An enterprise application, such as OracleAS Portal, must be available to internal and external users. As a result, enterprise applications must maintain profile and privilege information for internal and external identities. While this integration is optimal, it is also important to ensure intranet resources are isolated from external users and intranet applications are protected from denial of service attacks aimed at the extranet portal.

The following examples illustrate access to internal and external users. Each provides the security environment isolation between groups of applications that require isolation among them, such as extranet and intranet environments.

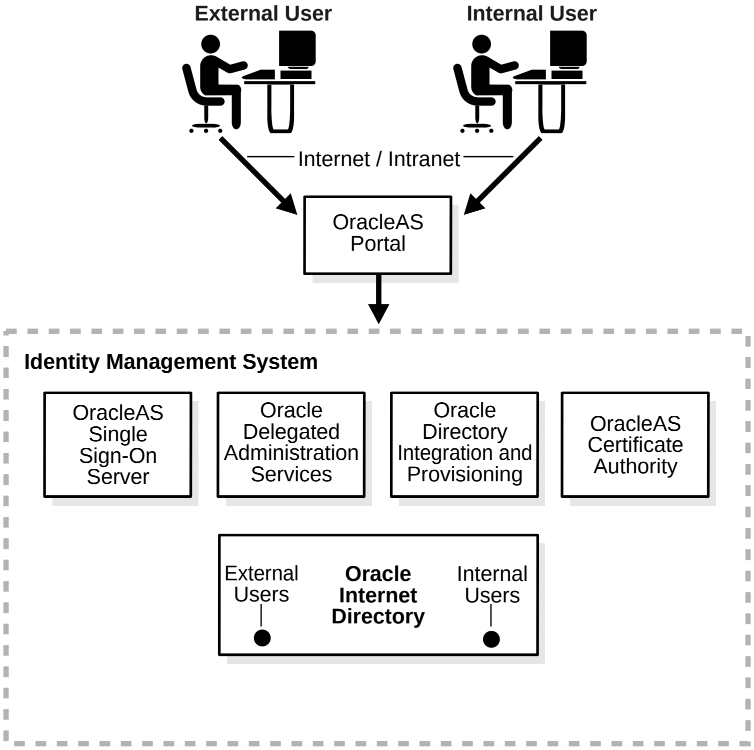
Example A: Using one identity management infrastructure

A single logical Oracle Internet Directory, as shown in Figure 3–3, is used to store internal and external user profiles, and the user information is configured the same for both internal and external users. A different subtree is used to store user profiles for both types of users within the same logical Oracle Internet Directory. The password policies can be the same for both types of users.

This type of deployment implements the following:

- Application deployment that provides access to internal and external users
- Central services and administration

Figure 3–3 Using One Identity Management Infrastructure


External User
Internal User
Internet / Intranet
OracleAS Portal
Identity Management System
OracleAS Single Sign-On Server
Oracle Delegated Administration Services
Oracle Directory Integration and Provisioning
OracleAS Certificate Authority
External Users
Oracle Internet Directory
Internal Users

Example B: Using two identity management infrastructures—security isolation

This example uses two identity management infrastructures: one each for users accessing the applications from inside and outside the enterprise network, as shown in Figure 3–4. In this type of deployment, there is a clear boundary between internal and external user repositories. More resources are available to internal users if external users are restricted.

There are many deployment measures necessary to achieve the isolation described in this example. Isolating the directory service for an extranet portal is a key measure. Only an employee's identity and nonsensitive profile information is synchronized with the enterprise directory; however intranet application identities and associated metadata are not replicated. External user identities (self-registered or otherwise), extranet portal-specific user profiles, preferences, and identities and roles of applications attached to the extranet portal are represented within its dedicated directory but are not replicated to the enterprise directory. It is best if the information model is the same in both logical Oracle Internet Directory instances.

DNS-based routing can be used to route the users to different identity management infrastructures for single sign-on authentication.

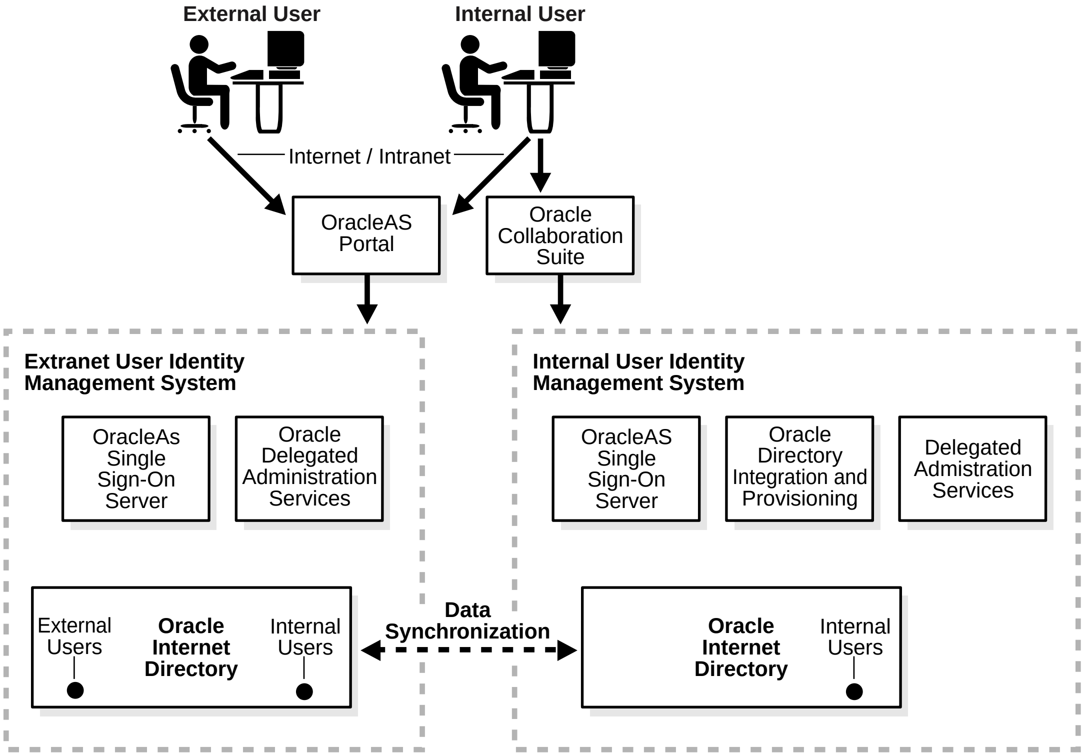
> **Note:** External users accessing applications within the intranet will have single sign-on access across the extranet portal and other internally deployed applications, such as Oracle Collaboration Suite.

This type of deployment implements the following:

- Security isolation: Boundaries among groups of applications that require isolation, such as extranet and intranet environments, are provided

- Access: Internal and external users can access applications by using two identity management infrastructures.
- Data synchronization: Application-required data is synchronized between the two identity management infrastructures.
- Availability: A separate identity management infrastructure is available for internal and external users.

Figure 3–4 Using Two Identity Management Infrastructures


External User
Internal User
Internet / Intranet
OracleAS Portal
Oracle Collaboration Suite
Extranet User Identity Management System
OracleAs Single Sign-On Server
Oracle Delegated Administration Services
External Users
Oracle Internet Directory
Internal Users
Data Synchronization
Internal User Identity Management System
OracleAS Single Sign-On Server
Oracle Directory Integration and Provisioning
Delegated Admistration Services
Oracle Internet Directory
Internal Users

Model of Providing Administrative Autonomy for Departmental Applications

For many large enterprises, it may be necessary to have administrative autonomy for applications within independent departmental units. This type of deployment provides administrative autonomy for applications managed independently within departmental networks and organizational units.

In this type of deployment, fan-out replicas serve as a local infrastructure for autonomously managed applications. The fan-out replica is a replicated Oracle Internet Directory that is configured with one-way replication from the central replica but is configured to be editable for local applications to be deployed, provisioned, and managed directly against the local infrastructure. Any resulting local information will not be replicated back to the central replicas.

Example A: Central single sign-on and departmental autonomy for applications

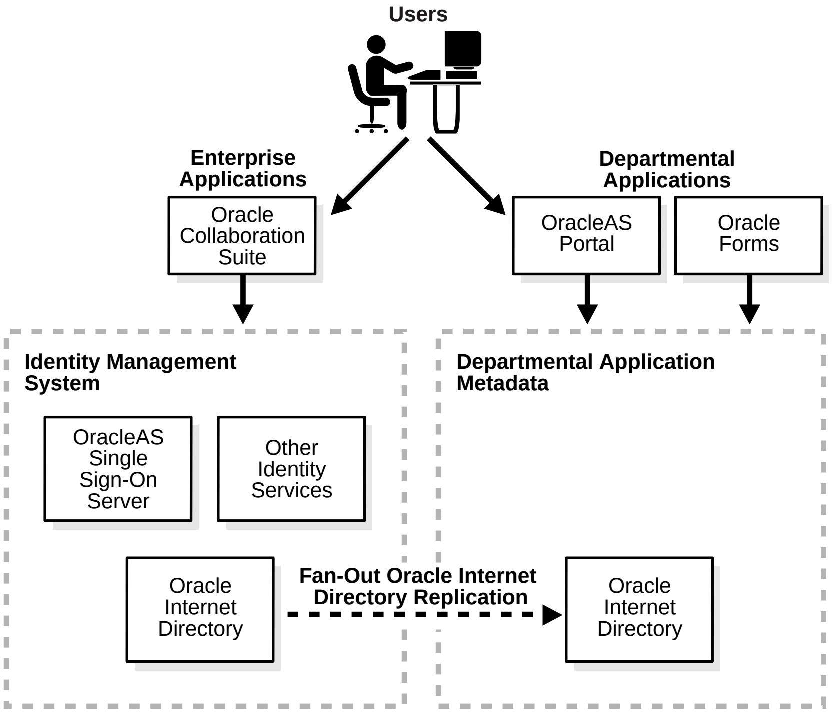
This example provides a central single sign-on and user password management service across the enterprise while providing departmental autonomy for maintaining the application data, as shown in Figure 3–5. A centralized single sign-on is used for user authentication, so applications can link to different Oracle Internet Directory instances depending upon whether they use the central Oracle Internet Directory or a departmental Oracle Internet Directory.

Applications, such as OracleAS Portal, are installed to use a separate departmental Oracle Internet Directory server, but they use a central identity management service for authentication. Local administrators manage the departmental applications.

This type of deployment implements the following:

- Administrative autonomy for applications within the department
- Centralized identity management infrastructure
- Unified login and logout across all applications

Figure 3–5 Central Single Sign-on and Departmental Autonomy


Users
Enterprise Applications
Oracle Collaboration Suite
Departmental Applications
OracleAS Portal
Oracle Forms
Identity Management System
OracleAS Single Sign-On Server
Other Identity Services
Oracle Internet Directory
Departmental Application Metadata
Fan-Out Oracle Internet Directory Replication
Oracle Internet Directory

Example B: Departmental identity management system

This example provides a separate authentication service for each department while still using a central identity management service for enterprise applications, as shown in Figure 3–6.

Applications, such as OracleAS Portal, are installed to use a separate departmental Oracle Internet Directory and OracleAS Single Sign-On service. Local administrators manage the departmental applications.

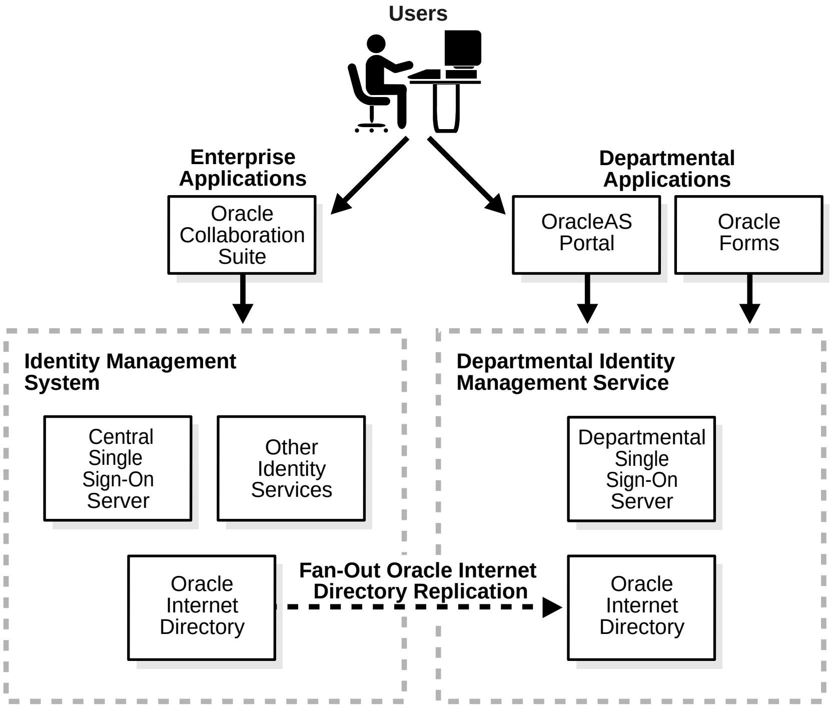
In this model, the user gets the unified login and logout experience for applications within each department, only. This model is useful as a failover plan if the central service suffers a catastrophic outage. Fan-out Oracle Internet Directory replication is used to replicate the enterprise user and password policy information from the central Oracle Internet Directory to the departmental Oracle Internet Directory.

This type of deployment implements the following:

- Administrative autonomy for applications within the department
- A separate identity management infrastructure for departmental autonomy

- Continuous availability of departmental applications regardless of any failures in the central identity management infrastructure

Figure 3–6 Departmental Identity Management Infrastructure


Users
Enterprise Applications
Oracle Collaboration Suite
Departmental Applications
OracleAS Portal
Oracle Forms
Identity Management System
Central Single Sign-On Server
Other Identity Services
Oracle Internet Directory
Fan-Out Oracle Internet Directory Replication
Departmental Identity Management Service
Departmental Single Sign-On Server
Oracle Internet Directory

Model of Integrating Oracle Identity Management in a Windows Environment

This deployment describes enterprise application integration between the Oracle Identity Management system and an existing enterprise application, such as Oracle Human Resources, and third-party LDAP servers, such as Microsoft Active Directory.

Example A: Integrating with enterprise provisioning

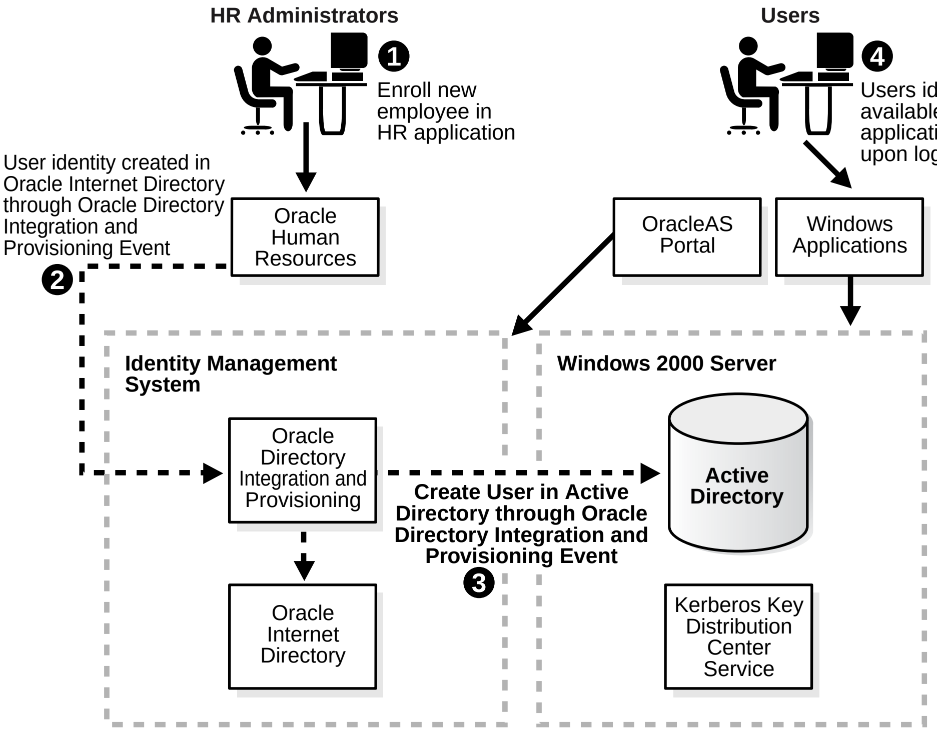
In this example, user provisioning is initially triggered by the enterprise application. Using Oracle Directory Synchronization Service, the user identity is created in Oracle Internet Directory and Active Directory, as shown in Figure 3–7.

Once the user identity is created in Oracle Internet Directory, OracleAS Single Sign-On authenticates users, and applications that are Oracle Internet Directory-enabled will have access to the user data. Similarly, Windows applications will have access to the user data created in Active Directory.

This type of deployment implements the following:

- Identity management system integration with an enterprise user provisioning system, where user provisioning is triggered by the enterprise application and user profile data is synchronized from the application to Oracle Internet Directory
- Integration with a third-party directory (in this example, Active Directory synchronization)
- As the user accounts are synchronized in both Oracle Internet Directory and Active Directory, users will have access to applications enabled for both Oracle Internet Directory and Active Directory

Figure 3–7 Identity Management Infrastructure Integration with Enterprise Provisioning


HR Administrators
1
Enroll new employee in HR application
User identity created in Oracle Internet Directory through Oracle Directory Integration and Provisioning Event
2
Oracle Human Resources
Users
4
Users identity available to applications upon login
OracleAS Portal
Windows Applications
Identity Management System
Oracle Directory Integration and Provisioning
Oracle Internet Directory
Create User in Active Directory through Oracle Directory Integration and Provisioning Event
3
Windows 2000 Server
Active Directory
Kerberos Key Distribution Center Service

Example B: Integrating with Windows user provisioning

If an enterprise has deployed Active Directory as a corporate directory for managing user and network resources, the Oracle Identity Management infrastructure can be integrated with an existing Active Directory, as shown in Figure 3–8.

In this example, user provisioning is initially done in the Windows environment. Windows administrators can use Windows tools to provision user accounts in the system. Synchronizing newly-created user account data in Active Directory with Oracle Internet Directory occurs using Oracle Directory Synchronization Service. Active Directory domain user data is synchronized in a default realm of Oracle Internet Directory. If there are multiple Active Directory domains in an enterprise deployment, they are configured for enterprise use of Oracle Internet Directory for Oracle Application Server by using multiple subtrees in one realm.

Once the user account is synchronized with Oracle Internet Directory, enterprise applications can access user profiles, and users can log in to the applications through a central OracleAS Single Sign-On.

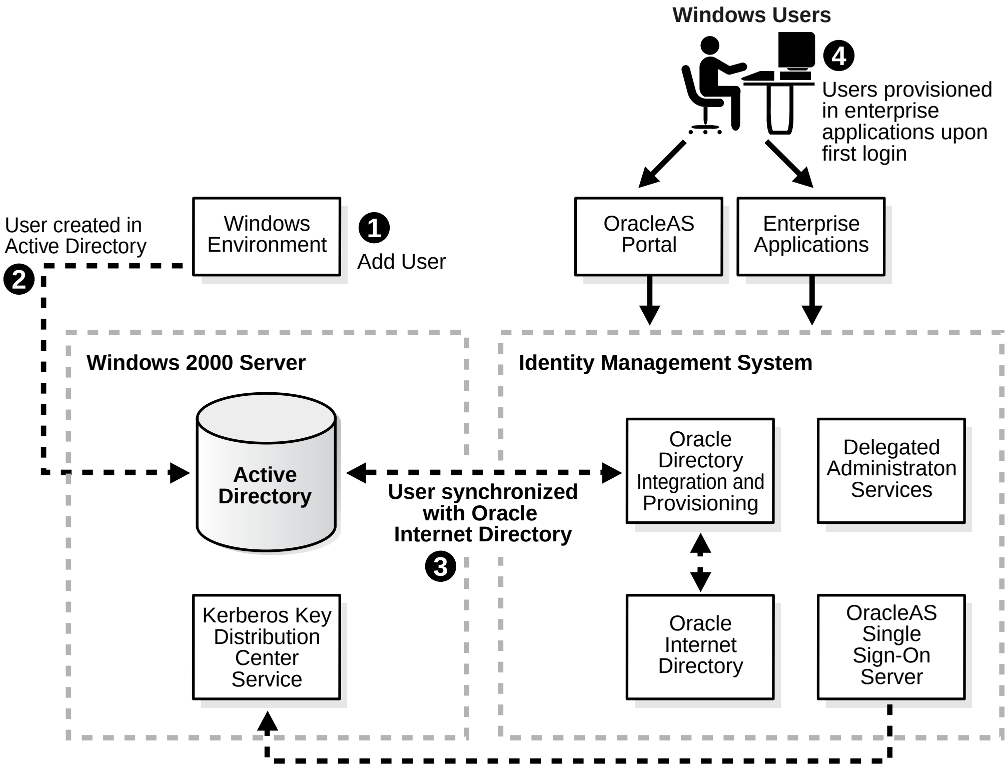
Also, OracleAS Single Sign-On supports Windows native authentication using the Windows Kerberos-based protocol. This feature enables users who have been issued a valid Kerberos ticket in the Windows environment to log in to their Web applications without having to provide a username and password. With this support, a Windows user can automatically log in to a portal application after the user successfully logs in to a Kerberos-enabled Windows desktop. In cases where Windows Kerberos authentication is not possible, Oracle Internet Directory external authentication plug-in authenticates users to Active Directory.

This type of deployment implements the following:

- Seamless integration of the Oracle Identity Management system with an existing Windows system

- Integration with a third-party directory
- Integration with Windows Kerberos authentication for single sign-on with partner applications
- Seamless access for Windows users to the Oracle Identity Management infrastructure-enabled enterprise applications

Figure 3–8 Identity Management Infrastructure Integration with Windows User Provisioning


Windows Users
4
Users provisioned in enterprise applications upon first login
User created in Active Directory
2
Windows Environment
1
Add User
OracleAS Portal
Enterprise Applications
Windows 2000 Server
Identity Management System
Active Directory
User synchronized with Oracle Internet Directory
3
Oracle Directory Integration and Provisioning
Delegated Administraton Services
Kerberos Key Distribution Center Service
Oracle Internet Directory
OracleAS Single Sign-On Server

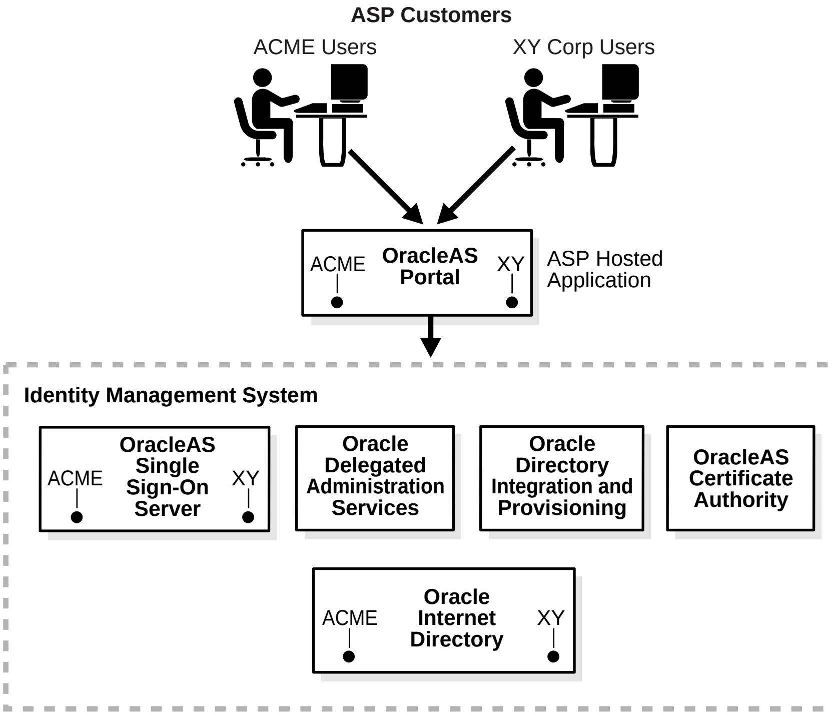
Deploying Central Identity Management Infrastructure in Application Service Provider Hosting Environments

In ASP deployments, different identity management realms must be created for the different namespaces of user populations. ASP administrators manage applications hosted for their customers, or subscribers, or both. Each subscriber has an associated identity management realm where the ASP manages its users, groups, and associated policies. Note that this deployment uses only one identity management infrastructure for all ASP identity management services by using a separate realm for each ASP subscriber.

Apart from using multiple realms in Oracle Internet Directory, the multiple realm feature should be enabled in OracleAS Single Sign-On and applications such as OracleAS Portal and Oracle Collaboration Suite.

Figure 3–9 illustrates a hosted deployment with two companies, Acme and XY Corporation.

Figure 3–9 Multiple Identity Management Realms in a Hosted Deployment


ASP Customers
ACME Users
XY Corp Users
ACME
OracleAS Portal
XY
ASP Hosted Application
Identity Management System
ACME
OracleAS Single Sign-On Server
XY
Oracle Delegated Administration Services
Oracle Directory Integration and Provisioning
OracleAS Certificate Authority
ACME
Oracle Internet Directory
XY

As shown in Figure 3–9, the ASP users, defined in the default identity management realm, manage various applications hosted for the subscribers. Each subscriber has an associated identity management realm where the ASP manages its users, groups, and associated policies.

Detailed Deployment Planning for Identity Management

Once the logical architecture of the Oracle Identity Management deployment has been decided, the next step is deciding the additional details of the deployment. These include the specifics of the directory information model and details of the physical topologies.

This section describes the details of planning the directory information tree (DIT) and lists a number of different physical topologies that meet high availability and performance requirements.

At the end of detailed deployment planning, you should have selected the DIT and physical topology that best meets your requirements. The finalized physical network topology can include a combination of one or more physical topologies listed in this section.

After you have selected the physical topologies, refer to the Oracle Identity Management installation documentation and component-specific administrator's guides for installation and advanced configuration information.

Deployment planning is an iterative process that should be flexible enough to meet the changing needs of an enterprise. In addition to the actual implementation, identity management deployments should establish well-defined processes to monitor the health and performance of the identity management infrastructure and to take corrective actions when necessary.

See Also: "Related Documents" in the Preface.

This section contains the following topics:

- Planning the Logical Organization of Directory Information
- Planning the Physical Network Topologies

Planning the Logical Organization of Directory Information

Directory information is organized in a directory information tree (DIT). This section describes the details of defining the DIT. Deployment planners should review their objectives and identify the configuration that best meets their needs and use that configuration as a deployment planning guide.

This section contains the following topics:

- Sample Directory Information Tree
- Planning the Overall Directory Information Tree Structure
- Planning User and Group Naming and Containment
- Planning the Identity Management Realm

Sample Directory Information Tree

Because the directory can potentially be used by several applications, both Oracle and third-party, the naming attributes used in the relative distinguished names constituting the overall DIT structure should be restricted to well-known attributes. The following attributes are generally well-known among most directory enabled applications:

- **c**: Name of a country
- **cn**: Common name
- **dc**: Component of a DNS domain name
- **l**: Name of a locality, such as a city, county, or other geographic region
- **o**: Name of an organization
- **ou**: Name of an organizational unit
- **st**: Name of a state or province

Figure 3–10 Oracle Internet Directory Information Tree

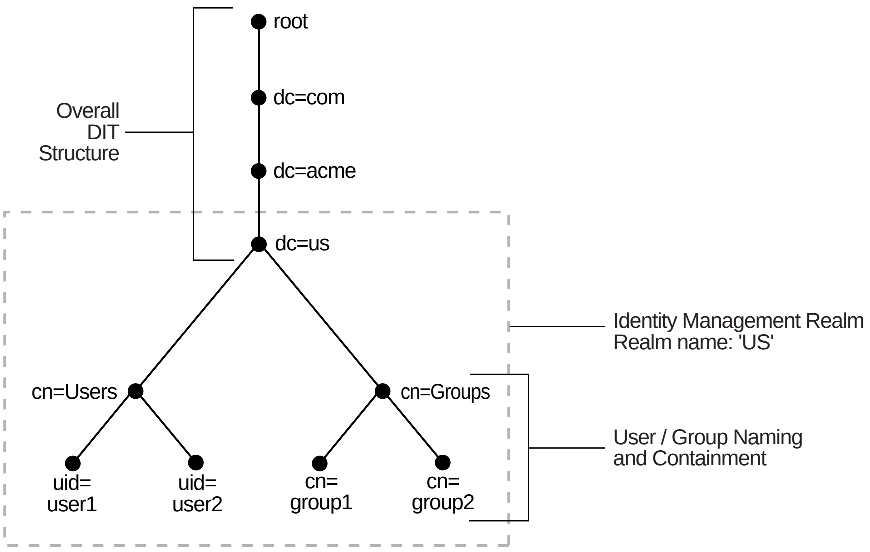


Figure 3–10 illustrates a DIT for a hypothetical company called Acme, which makes the following decisions with respect to the logical organization of the directory information in its U.S. deployment:

- A domain name-based scheme is used to represent the overall DIT hierarchy. Because the identity management infrastructure is being deployed in the U.S., the DIT chosen to represent all information is `dc=us,dc=acme,dc=com`.
- All users are represented in a container called `cn=users`. Within this container, all users are represented at the same level. (There is no organization-based hierarchy.) In addition, the `uid` attribute is chosen as the unique identifier for all users.
- All enterprise groups are represented in a container called `cn=groups`. Within this container, all enterprise groups are represented at the same level, and the naming attribute for all group entries is `cn`.
- The container `dc=us` is chosen as the root of the identity management realm, which is named US. The deployment expects to enforce similar security policies for all users in the US realm.

Because Oracle Internet Directory is a shared repository for the entire identity management infrastructure, a well-planned DIT benefits the enterprise in the following ways:

- It enables the Oracle Identity Management infrastructure to enforce security policies that are aligned with the deployment requirements.
- It helps implement a more efficient physical deployment of the directory service.
- In cases where the enterprise has already invested in a directory service, it enables the enterprise to quickly set up synchronization with Oracle Internet Directory.

For more information about LDAP attributes, see *Oracle Internet Directory Administrator's Guide.*

Planning the Overall Directory Information Tree Structure

The objective of this task is to design the basic DIT hierarchy that all identity management-integrated applications in the enterprise will use, so that:

- The directory organization facilitates effective access control. If you are planning to implement either full or partial replication, proper boundaries and policies for directory replication can only be enforced if the DIT design reflects the separation.
- If the enterprise will be integrated with a third-party directory server, try to align the DIT design of Oracle Internet Directory with the existing DIT to simplify the necessary synchronization process. This consideration is also beneficial to current deployments of Oracle Internet Directory, where future plans of deploying other directories, such as Active Directory, are required for the operation of software from other vendors. In this case, choosing a DIT design for Oracle Internet Directory that is consistent with the preferred DIT design of the planned deployment of a third-party directory will make the synchronization tasks more manageable.
- In a single enterprise scenario, choosing a DIT design that aligns with the domain name of the enterprise is sufficient. For example, if Oracle Internet Directory is being set up in a company that owns the domain name `acme.com`, a directory structure such as `dc=acme,dc=com` is recommended. Use of departmental or organization level domain components, such as `engineering` in `engineering.acme.com`, is not recommended. Most corporations undergo frequent divisional restructuring and reorganization. It is important to insulate the corporate directory from organizational changes as much as possible.
- If an enterprise has deployed an X.500 directory service and has no other third-party LDAP directories in production, the enterprise may benefit by choosing a country-based DIT design. For example, a DIT design with the root of `o=acme,c=US` might be more suitable for an enterprise that already has X.500 directory service.

Planning User and Group Naming and Containment

Most of the design considerations that are applicable to the overall DIT design are also applicable to the naming and containment of users and groups. However, there are additional considerations you must be aware of when configuring users and groups in Oracle Internet Directory.

Considerations for User Identities

Oracle Identity Management infrastructure uses Oracle Internet Directory as the repository for all user identities. Even though a user might have account access to multiple applications in the enterprise, there is only one entry in Oracle Internet Directory representing a particular user's identity. The location and contents of these entries in the overall DIT must be planned by the enterprise before deploying Oracle Internet Directory and other infrastructure components.

Consider the following when planning user identities:

- Similar to planning the overall directory structure, avoid organizing users based on current departmental affiliations and hierarchy. Instead, record a user’s organizational information as an attribute of the user’s directory entry.
- There are no performance benefits to organizing the users in a hierarchy based on the organizational affiliations or management chain, and you should therefore keep the DIT containing users as flat as possible.
- If the deployment has different user populations, each maintained and managed by different organizations, dividing the users into containers based on these administrative boundaries is recommended to simplify the setting of access controls and also helps in cases where replication is needed

- The default attribute for uniquely identifying users is `cn` or `CommonName`. Because the typical values of `CommonName` are the full name of the person, guaranteeing uniqueness for these values is difficult. If possible choose an alternative attribute that uniquely identifies a user, such as the `uid` attribute or the `mail` attribute.
- Typically, most enterprises have a human resources department that establishes rules for assigning unique names and numbers for employees. When choosing a unique naming component for directory entries, you should take advantage of this administrative infrastructure and use its policies.
- All user entries created in the directory should belong to the object class `inetOrgPerson` and `orclUserV2`.
- If the enterprise is using a third-party directory, or is planning to deploy one in the future, align the user naming and directory containment with the one commonly used in the third-party directory to simplify the synchronization and subsequent administration of the distributed directories

Considerations for Group Identities

Some applications that are integrated with the Oracle Identity Management infrastructure can also base their authorizations on enterprise-wide groups created by the deployment in Oracle Internet Directory. As with user identities, the location and content of the group identities should be carefully planned.

Considerations for planning group identities are as follows:

- There are no performance benefits to organizing the enterprise groups in a hierarchy based on the organizational affiliations or ownership. Keep the DIT containing groups as flat as possible to facilitate easy discovery of groups by all applications and to foster sharing of these groups across applications.
- Separate users and groups in the DIT so that different management policies can be applied to each set of entries.
- The attribute used to uniquely identify a group should be `cn` or `CommonName`.
- Oracle recommends that all group entries in the directory belong to the following object classes: `groupOfUniqueNames` and `orclGroup`. The former object class is an internet standard for representing groups. The latter can be used to take advantage of the self-service console to manage groups.
- Instead of creating new directory access controls for each enterprise-wide group, consider using the owner attribute of the group to list which user or users owns this group and then create an access control policy at a higher level that grants all users listed in the owner attribute special privileges, such as modify and delete.
- Consider populating the `description` attribute with text descriptions to make it easy for users to understand the purpose of the group.
- Consider populating the `displayName` attribute from the `orclGroup` object class so that Oracle Delegated Administration Services units and the self-service console can display a more readable name for the group.
- If the deployment has different sets of groups, each maintained and managed by different organizations with different administrative policies, dividing the groups into containers based on these administrative boundaries is recommended to simplify the setting of access controls, and to help in cases where replication is needed.
- If the enterprise is using a third-party directory, or planning to deploy one in the future, align the group naming and directory containment with the one commonly

used by the third-party directory to simplify the synchronization and subsequent administration of the distributed directories

Planning the Identity Management Realm

The preceding sections described guidelines for structuring the overall DIT and the placement of users and groups. Because the implementation of these guidelines can lead to a variety of deployment configurations, you should capture the deployment intent in metadata in the directory itself. This metadata enables Oracle software, and other third-party software that relies on the Oracle Identity Management infrastructure, to understand the deployment intent and successfully function in customized environments.

The identity management realm in Oracle Internet Directory captures this deployment intent and also enables the deployment to set identity management policies relevant to the enterprise users and groups.

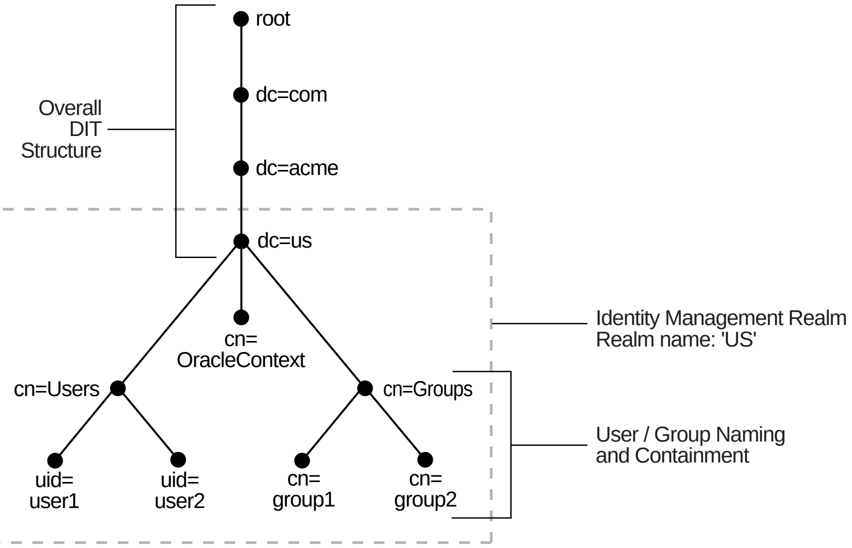
> **See Also:** "Identity Management Terminology" on page 2-1 for more information about identity management realms

After you have selected the overall DIT and the placement of users and groups, identify the directory entry that will serve as the root of the identity management realm in Oracle Internet Directory. This entry helps determine the scope of the identity management policies defined in the identity management realm (by default, the scope is the entire directory subtree under the root of the identity management realm). Under this entry, a special entry called `OracleContext` is created which contains the following:

- The deployment specific DIT design (including user and group naming and placement)
- The identity management policies associated with this realm
- Additional realm-specific information private to Oracle applications

Figure 3–11 illustrates a deployment for the Acme company that uses a domain name-based DIT structure.

Figure 3–11 Identity Management Realm



In this case, the container `dc=us,dc=acme,dc=com` is the directory entry chosen as the root of the identity management realm. The `cn=OracleContext` container holds the *realm-specific* policies, including the user and group naming and containment policies.

A new identity management realm is created whose root is `dc=us`. The scope of the identity management realm, by default, is restricted to the entire directory subtree under the root, and its name is `us`.

Consider the following when planning for the identity management realm in Oracle Internet Directory:

- The security needs of the enterprise dictate the choice of the identity management realm root. Typically, most enterprises require only one identity management realm in Oracle Internet Directory.
- If an enterprise is using a third-party directory, or planning to deploy one in the future, align the choice of the identity management realm root with the DIT design of the third-party directory to simplify the synchronization and subsequent administration of the distributed directories.
- Use Oracle Internet Directory administrative interfaces to set up and administer an identity management realm in Oracle Internet Directory, including Oracle Internet Directory Configuration Assistant, Oracle Internet Directory Self-Service Console, and other command-line tools.
- Once the identity management realm is set up, plan on updating the directory naming and containment policies to reflect the customizations made by the deployment. This update must happen prior to installing and using other Oracle applications that use the Oracle Identity Management infrastructure.

See Also:

- *Oracle Internet Directory Administrator's Guide* for more information on customizing identity management realms
- Appendix C, "Oracle Internet Directory Default Settings" for information model defaults

Planning the Physical Network Topologies

Physical topology choices for the identity management infrastructure are influenced by many requirements; the most common of which are high availability and scalability.

High availability describes the ability of a system to continue processing and functioning for a very high percentage of time. High availability can be implemented by reducing any single points-of-failure and using redundant components. Similarly, coupling multiple identity management component instances with a load balancer can provide a highly available environment.

This section describes several physical topologies you could use for high availability and scalability, and highlights the benefits of each deployment example. You should review your objectives and identify the configuration that most closely matches your enterprise's requirements.

This section contains the following topics:

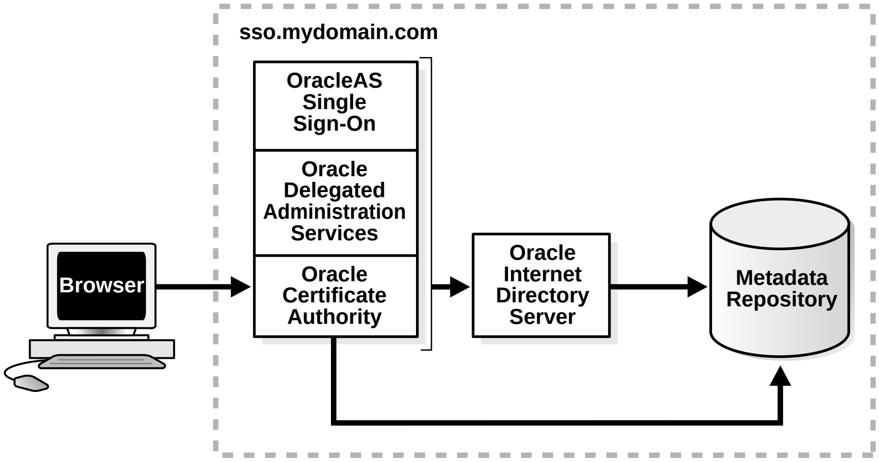
- Identity Management Infrastructure Default Deployment
- Identity Management Infrastructure Deployment in a DMZ Network
- Identity Management Infrastructure Deployment Using Multiple Middle Tiers

- Identity Management Infrastructure Deployment Using Cold Failover Cluster Solution
- Replicated Identity Management Infrastructures
- Fan-out Replication Deployment
- Application Deployments in Replicated Directory Environments
- Geographically Distributed Identity Management Infrastructure Deployment
- Disaster Recovery Deployment for Identity Management Infrastructure
- Oracle Application Server Certificate Authority Recommended Deployment

Identity Management Infrastructure Default Deployment

In a default installation of the Oracle Application Server infrastructure, you install all infrastructure components on the same system, including OracleAS Single Sign-On, Oracle Application Server Certificate Authority, and Oracle Delegated Administration Services, as shown in Figure 3–12.

Figure 3–12 OracleAS Single Sign-On and Oracle Delegated Administration Services Default Deployment


sso.mydomain.com
OracleAS Single Sign-On
Oracle Delegated Administration Services
Oracle Certificate Authority
Browser
Oracle Internet Directory Server
Metadata Repository

This deployment is simple and automatically configures OracleAS Single Sign-On, Oracle Application Server Certificate Authority, and Oracle Delegated Administration Services as part of the repository and Oracle Internet Directory. This deployment is adequate for setting up a quick development or testing environment.

Identity Management Infrastructure Deployment in a DMZ Network

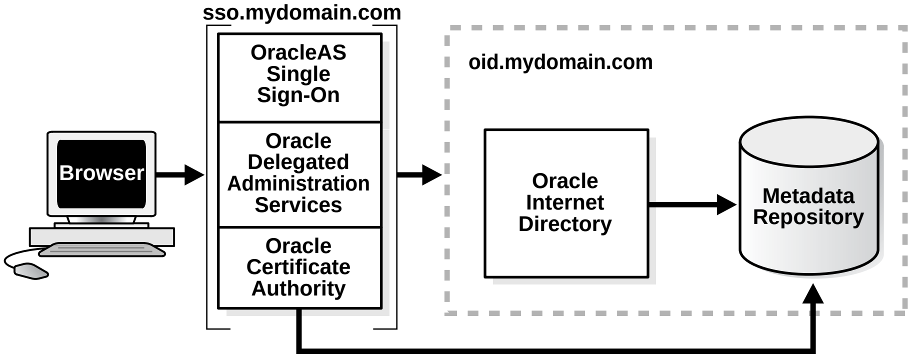
In production deployments, security policies might specify that the entire OracleAS Single Sign-On server not be exposed to the public network. One way to do this is to deploy the Oracle Application Server infrastructure middle tier in the DMZ, and Oracle Internet Directory and its underlying metadata repository within the intranet firewall, as shown in Figure 3–13.

Because Oracle Delegated Administration Services and Oracle Application Server Certificate Authority are middle tier components, the considerations are the same as they are for the OracleAS Single Sign-On middle tier.

This deployment isolates between the infrastructure middle tier from Oracle Internet Directory and its underlying metadata repository.

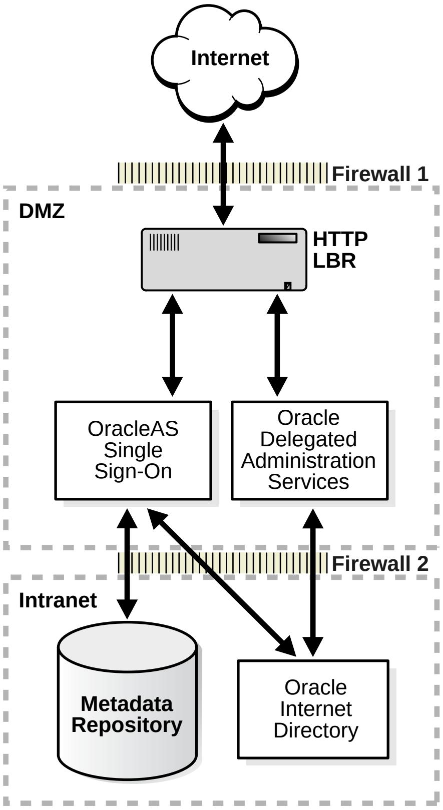
You must provide network level encryption between the Oracle Application Server Certificate Authority middle tier and the Oracle Application Server Certificate Authority repository to ensure security isolation between the Oracle Application Server Certificate Authority middle tier and repository.

Figure 3–13 OracleAS Single Sign-On, Oracle Delegated Administration Services Deployment, and Oracle Application Server Certificate Authority in a DMZ


sso.mydomain.com
OracleAS Single Sign-On
Oracle Delegated Administration Services
Oracle Certificate Authority
Browser
oid.mydomain.com
Oracle Internet Directory
Metadata Repository

The high-level deployment topology in Figure 3–14 shows an Oracle Application Server installation that allows Oracle Internet Directory and its underlying metadata repository to be available in the intranet zone while Web-enabled components are placed in the DMZ. Internet Web traffic is routed to the HTTP load balancer that routes traffic to the Web-enabled components. This deployment configuration provides enhanced security because Oracle Internet Directory and its metadata repository are separated from Internet traffic by firewalls.

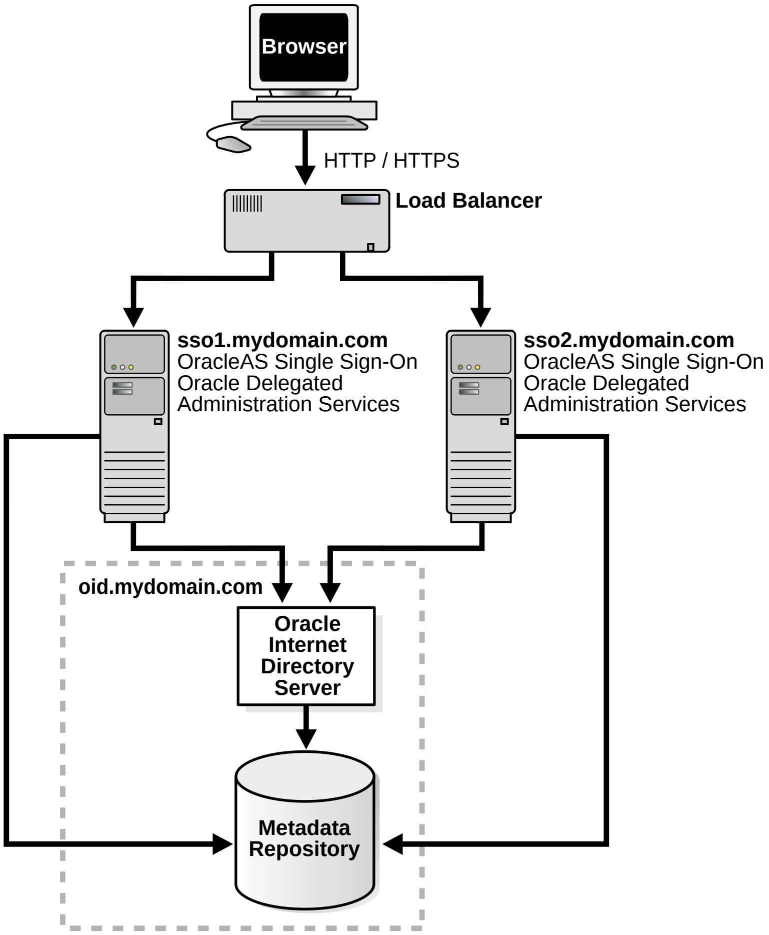
Figure 3–14 OracleAS Single Sign-On, Oracle Delegated Administration Services Deployment, and HTTP Load Balancer in a DMZ



Identity Management Infrastructure Deployment Using Multiple Middle Tiers

If you require a highly available deployment, you can deploy multiple OracleAS Single Sign-On and Oracle Delegated Administration Services middle tiers to handle the load and support the failover process. Even though multiple OracleAS Single Sign-On middle tiers are deployed, they use the same Oracle Internet Directory server. This deployment, shown in Figure 3–15, provides increased scalability by adding more infrastructure middle tiers.

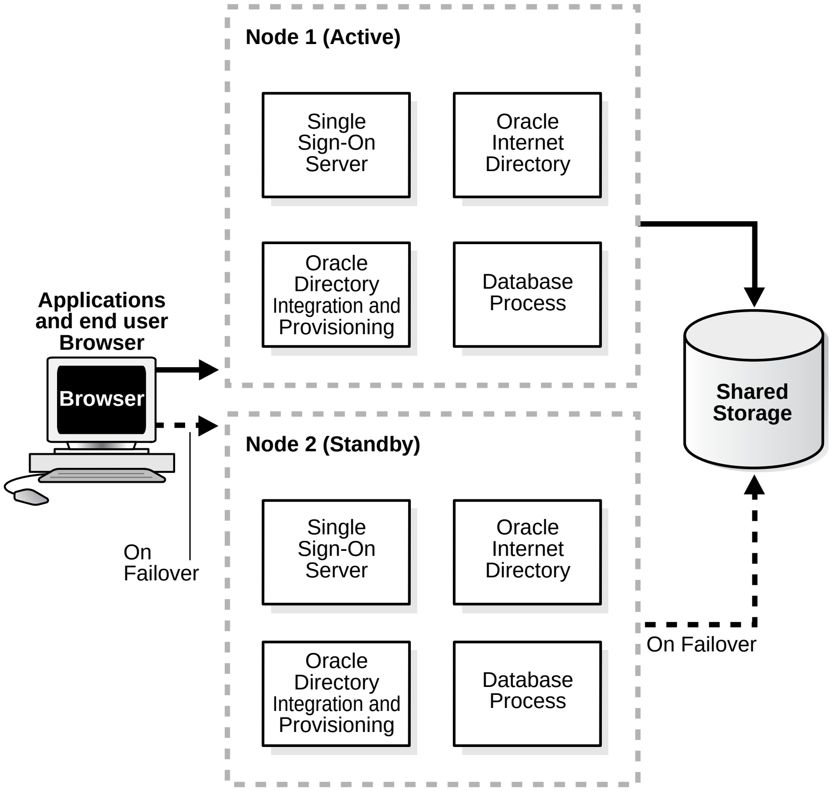
Figure 3–15 Multiple OracleAS Single Sign-On and Oracle Delegated Administration Services Middle Tiers with one Oracle Internet Directory Server



Identity Management Infrastructure Deployment Using Cold Failover Cluster Solution

Cold failover deployment is an intrasite, high availability solution that provides protection from local hardware and software failures.

Figure 3–16 Oracle Internet Directory Deployment Using Cold Failover


Node 1 (Active)
Single Sign-On Server
Oracle Internet Directory
Oracle Directory Integration and Provisioning
Database Process
Applications and end user Browser
Browser
On Failover
Shared Storage
Node 2 (Standby)
Single Sign-On Server
Oracle Internet Directory
Oracle Directory Integration and Provisioning
Database Process
On Failover

In this deployment, you use a two node hardware-based cluster to achieve high availability. As shown in Figure 3–16, the two nodes are attached to a shared storage disk. You only need to install one Oracle Identity Management infrastructure, as long as it is on a shared storage disk that can be accessed by both physical nodes. A virtual logical IP address is active on Node 1, so Node 1 is the primary (active) node and Node 2 is the secondary node.

If Node 1 fails, the logical IP address is moved to Node 2. All the infrastructure processes are then started on Node 2. The application processes accessing the identity management infrastructure will experience a temporary loss of service as the logical IP address and the shared storage are moved over, and the metadata repository, its database listener, and all other processes are started.

The cold failover solution provides high availability with some loss of service during the failover.

Replicated Identity Management Infrastructures

You could deploy replication-enabled Oracle Identity Management in different configurations, depending on your deployment requirements. For example, deploying two or more multimaster replication nodes in different locations provides distributed identity management. Deploying the same configuration in a single location could provide rolling upgrade support.

For highly available deployment requirements, multiple OracleAS Single Sign-On middle tiers can be deployed to bear the load and support failover access. Oracle Internet Directory servers can be set up as replicas to provide the highly available Oracle Internet Directory server for middle tier access, as shown in Figure 3–17.

This deployment should be planned before installing the Oracle Application Server infrastructure. The planning includes providing the URLs for the OracleAS Single Sign-On and Oracle Internet Directory servers and setting up the load balancer for both the infrastructure middle tier and Oracle Internet Directory.

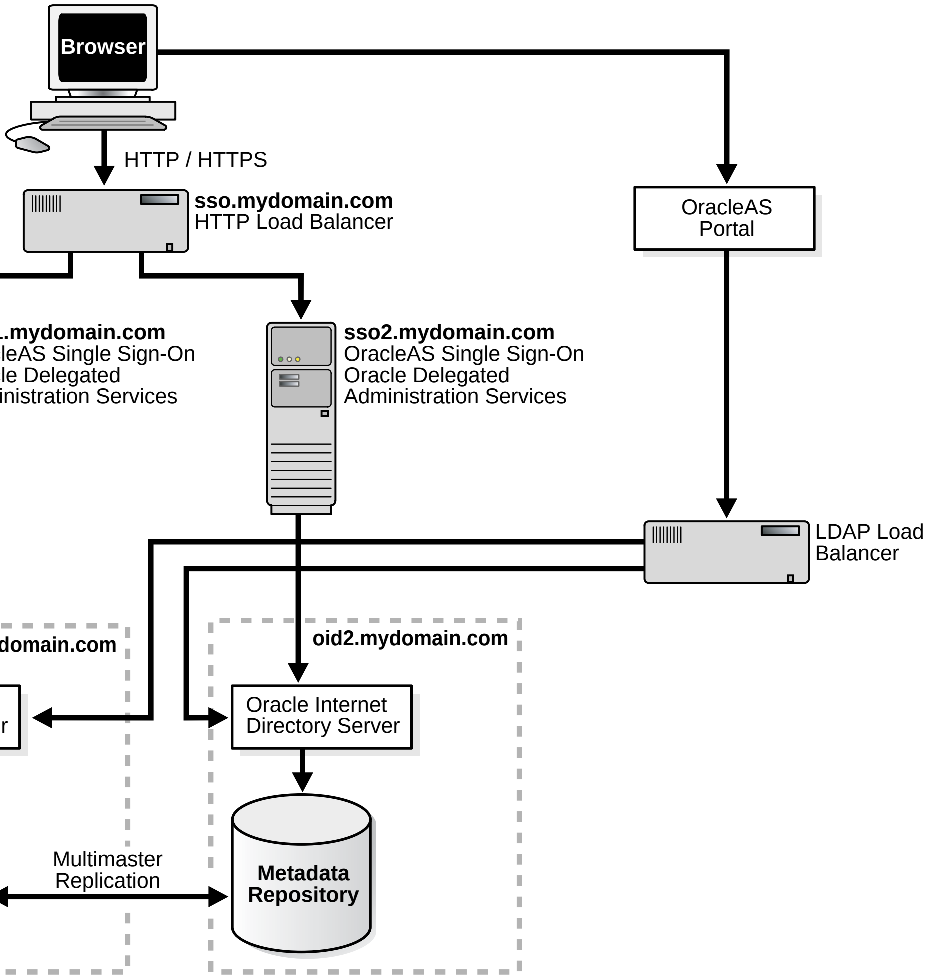
The load balancer for Oracle Internet Directory should be configured with persistent routing and to use failover. The load balancer should not be configured to load balance requests.

This deployment provides high availability and failover for both the Oracle Internet Directory server and the OracleAS Single Sign-On middle tier.

Oracle Internet Directory multimaster replication provides the following benefits:

- **No single point-of-failure**: Multiple identical replicas prevent the directory service from becoming a single point-of-failure for applications on the network.
- **Transparent failover**: Achieved by placing load balancers or routing elements in front of the network of replicas. These elements are configured so that if an Oracle Internet Directory node becomes unavailable, the applications transparently fail over to other nodes in the network.
- **Load balance**: Achieved by using load balancers to distribute application and user access requests among Oracle Internet Directory nodes in the replication network so that no one node is overloaded, leading to performance degradation.

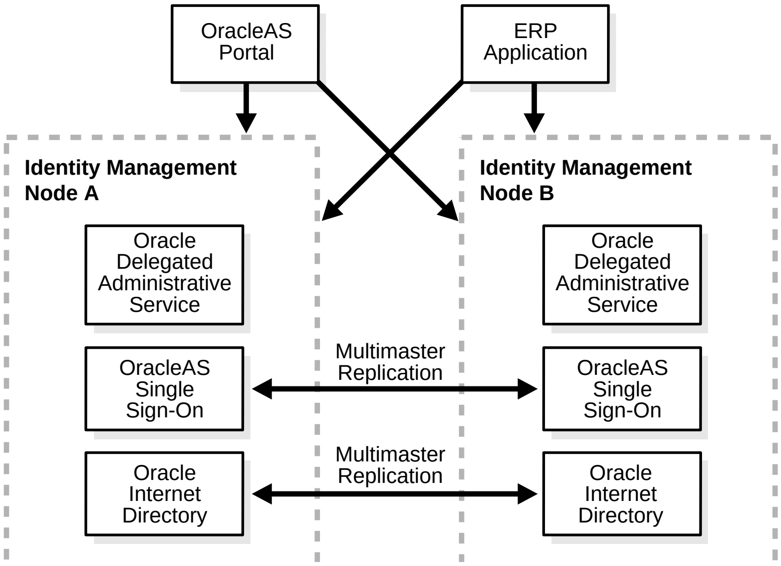
Figure 3–17 Multiple OracleAS Single Sign-On and Oracle Delegated Administration Services Middle Tiers Within a Replicated Oracle Internet Directory Network



- **Rolling upgrade support**: In an enterprise organization, critical business applications require an identity management system to provide service without interruption. However, you might need to make a system unavailable for some time to perform maintenance work, such as patching or upgrading. You can solve this problem by deploying multimaster replication in Oracle Identity Management. This configuration enables you to take replica Node B out of the replication group for maintenance while other nodes handle business application requests. After your maintenance work is completed, you put Node B back online to handle application requests. Node B then retrieves changes from Node A that occurred while Node B was offline. Other nodes can be upgraded or patched by repeating this procedure.

  In Figure 3–18, Oracle Identity Management Node A provides service to OracleAS Portal and Oracle Collaboration Suite applications while Node B is offline for maintenance. When the maintenance process is complete for Node B, Node A can be taken offline for maintenance while applications work with upgraded Node B.

Figure 3–18 Rolling Upgrade Support with Multimaster Replication

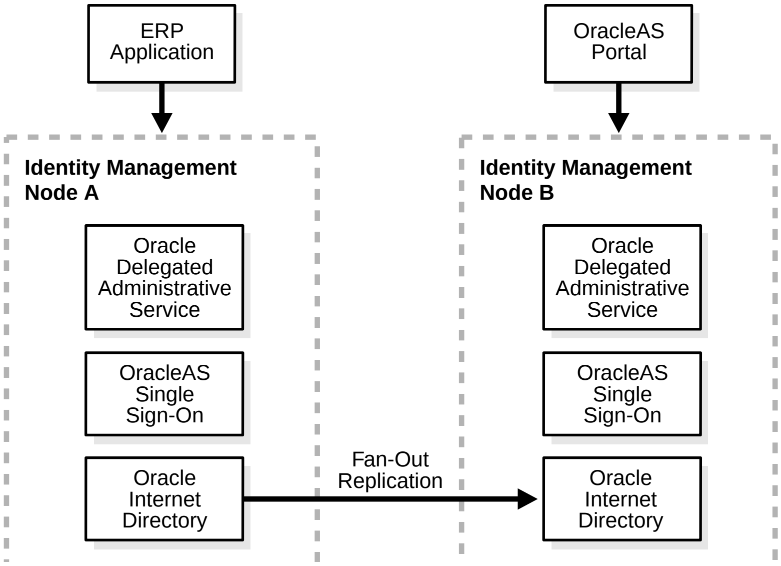

OracleAS Portal
ERP Application
Identity Management Node A
Identity Management Node B
Oracle Delegated Administrative Service
Oracle Delegated Administrative Service
OracleAS Single Sign-On
Multimaster Replication
OracleAS Single Sign-On
Oracle Internet Directory
Multimaster Replication
Oracle Internet Directory

Fan-out Replication Deployment

Oracle Identity Management supports fan-out replication. In this configuration, changes to the master replica are propagated to the fan-out replica. Changes to the fan-out replica, however, are local, and do not propagate back to the master replica. Propagation from the master to the fan-out replica can include either the entire DIT or a subset of the DIT. The latter is known as a partial replica.

In Figure 3–19, Identity Management Node B is a fan-out replica of Node A. Data from Node A is replicated one way to the fan-out node, Node B. The identity management system on Node A provides service to the ERP application. Fan-out Node B is provides service to Oracle Portal.

Figure 3–19 Fan-out Replication Deployment


ERP Application
OracleAS Portal
Identity Management Node A
Identity Management Node B
Oracle Delegated Administrative Service
Oracle Delegated Administrative Service
OracleAS Single Sign-On
OracleAS Single Sign-On
Oracle Internet Directory
Fan-Out Replication
Oracle Internet Directory

Fan-out replication in Oracle Identity Management addresses the following business requirements in an enterprise organization:

- **Security isolation**: An enterprise application, such as Oracle Portal, is required to be available to both internal and external users. As a result, enterprise applications must maintain profile and privilege information for both employee (internal) and other (external) identities. While this integration is optimal, it is also important to ensure corporate intranet resources are completely isolated from external users and intranet applications are protected from denial of service attacks aimed at the extranet portal. This can be achieved by setting up the master management node that delivers security information for the internal users and a fan-out identity management replica that is responsible for external users. At the same time internal users can also access the portal deployed using the fan-out replica.
- **Management and administrative isolation**: This example provides a central single sign-on and user password management service across the enterprise while providing the departmental autonomy for maintaining the application data. A centralized single sign-on is used for user authentication, while applications can link to different Oracle Internet Directory instances depending upon whether they use the central Oracle Internet Directory or a departmental Oracle Internet Directory.

  Applications, such as OracleAS Portal, are installed to use a separate departmental Oracle Internet Directory server, but they use a central identity management service for authentication. Local administrators manage the departmental applications.

  This type of deployment implements the following:

  - Administrative autonomy for applications within the department
  - Centralized identity management infrastructure
  - Unified login and logout across all applications
- **Performance isolation**: In an enterprise organization, directory enabled applications needs to access enterprise directory data. While it is necessary for all applications to access directory data, some overloaded applications may put an unexpected heavy load in the directory. This may lead to a service outage for all applications due to directory service unavailability. To address this problem, fan-out replica could be deployed and applications can be configured to access a particular directory instance to isolate the directory service load.
- **Application maintenance and upgrade isolation**: Departmental administrators in an enterprise organization can install Oracle applications such as OracleAS Portal using the departmental fan-out replica node to address local departmental need. While these departmental applications can use enterprise users security information, they can administer these applications and corresponding directory data independently. In addition, departmental administrator can upgrade applications associated with the fan-out directory node independently.

  Fan-out replicas can be further customized to support sophisticated deployment requirements of an enterprise such as:

  - Replicate a subset of data from the master.
  - Configure plug-ins at the fan-out replica to propagate some data modification back to the master.

  For example, an enterprise might want to allow password modification at fan-out but then have them synchronize back to the master replica.

Application Deployments in Replicated Directory Environments

Directory replication is an asynchronous mechanism, so the directory nodes in the network are loosely consistent. The directory replication mechanism guarantees that when changes are made on any node in the network, all other nodes will eventually converge and become consistent within an acceptable time interval. This, however, does not guarantee that all nodes will be identical at all times.

As a consequence of the loose coupling among replicas, different applications connected to different physical directory servers in the replication network can encounter temporary inconsistencies among their directory views. Such temporary inconsistencies do not adversely impact the application users and are generally acceptable. But, there are scenarios in which this could impact users. For example, upon password reset, if the resulting changes are not reflected immediately in the directory server to which OracleAS Single Sign-On is connected, it is bound to confuse or inconvenience the user.

In addition to the temporary inconsistency due to asynchronous replication, conflicting changes can occur in a multimaster network where different changes are made simultaneously to the same piece of information on different directory nodes. When that happens, Oracle Internet Directory replication is capable of bringing convergence among the various nodes using a process of reconciliation called *conflict resolution*.

To avoid these problems, it is important to adhere to appropriate best practices when deploying applications to use a replicated directory network. Following are guidelines that an administrator should consider while deploying directory-enabled applications in a replicated directory environment:

1. Primary replicas should be designated for each major category of directory data in the enterprise.

   a. Typical categories for primary replicas are user entries and common user attributes; user passwords and other authentication credentials; user groups and distribution lists; user profiles, preferences, and roles associated with key application suites.

   b. Designating a primary replica does not mean a single-master environment. There are actually many master nodes, but different ones designated for provisioning different categories of directory data. Upon directory or network failure, provisioning applications, like any other applications, can temporarily fail over to alternate masters.

   c. This deployment practice combines the flexibility of a multimaster network with the tighter data consistency of single master configurations.

      – Data recovery for any given category of data becomes more manageable because it does not involve reconciliation among multiple masters.

      – Services sensitive to changes to specific attributes, such as authentication services on passwords, can rely on the associated primary replica for the most up-to-date values.

2. Middle tier and back-end server components of applications should be deployed to use specific directory server instances in the replication network.

   a. Uniform load balancing and distribution is not acceptable and not recommended for application middle tier and back-end components. For example, if consecutive logon operations of an OracleAS Single Sign-On server were routed to different Oracle Internet Directory servers, authentication policies such as logon retry limit could not be enforced effectively.

  b. Uniform load distribution is acceptable only for operations that are not critical, such as address book lookups.

3. Middle tier and back-end server components of related applications should be deployed to share directory server instances. Different groups of applications can share different directory instances.

   This practice ensures that related applications are not affected by the temporary inconsistency between the different directory servers upon which they rely. For example, OracleAS Single Sign-On and the Helpdesk application used for resetting a password should share the same Oracle Internet Directory instance. Otherwise, users could reset the password and find that they are unable to sign on because the OracleAS Single Sign-On server is connected to a different Oracle Internet Directory server from where the password changes were made.

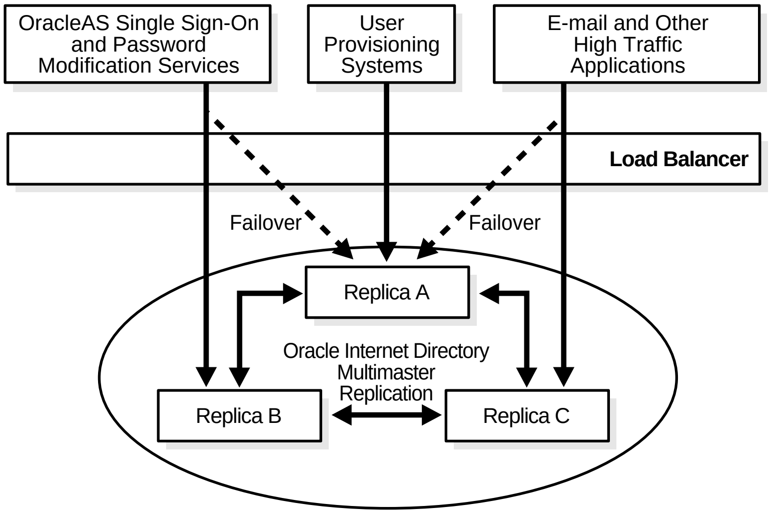
4. Any bulk provisioning of data in a directory should be performed only when the directory network and all the nodes in the directory network are in a healthy state.

   a. When there is an outage in any part of the directory network or when there is an excessive backlog of changes waiting to be replicated or reconciled, continuing with any bulk provisioning would further aggravate the problems and might lead to more pervasive loss of data and service.

   b. Replication environment health monitoring and diagnosis must be performed on a regular basis. Oracle Internet Directory includes tools that support these operations.

Considering the previous guidelines, Figure 3–20 shows an example of enterprise applications configured in a replicated directory environment. In this deployment, OracleAS Single Sign-On and other password modification services, such as Oracle Delegated Administration Services, are configured to use Replica B as the primary Oracle Internet Directory server and Replica A as the temporary failover server. Similarly, e-mail and other high-traffic applications are configured to use Replica C as the primary server and Replica A as the failover server.

Figure 3–20 Enterprise Applications Configured in a Replicated Environment


OracleAS Single Sign-On and Password Modification Services
User Provisioning Systems
E-mail and Other High Traffic Applications
Load Balancer
Failover
Failover
Replica A
Oracle Internet Directory Multimaster Replication
Replica B
Replica C

Geographically Distributed Identity Management Infrastructure Deployment

Enterprises with geographically distributed operational branches want to set up multiple OracleAS Single Sign-On instances distributed across the different geographic locations to authenticate users locally. This deployment, shown in Figure 3–21, reduces the network round trips for authentication and provides faster access to applications. OracleAS Single Sign-On server data is replicated globally across all geographic branches, which enables an employee who travels to any remote business location to be authenticated locally.

For enterprises with applications deployed in multiple geographic locations, it is important to physically distribute the Oracle Internet Directory replicas in at least two regions. Such a configuration prevents regional availability problems (due to network failures or natural disasters) from turning into global service outages for dependent applications.

Even though Oracle Internet Directory and the metadata repository are set up in replication, each OracleAS Single Sign-On site uses its own Oracle Internet Directory and metadata repository located at the local site.

If replicated OracleAS Single Sign-On sites are distributed over a wide area network (WAN), local DNS servers should be configured to route user requests to the closest geographic site.

In case a database failure is detected at one site, Oracle Internet Directory and OracleAS Single Sign-On servers are reconfigured to point to a metadata repository at another site. In case an OracleAS Single Sign-On middle tier failure is detected, the network is reconfigured to route traffic to a remote middle tier.

Figure 3–21 Geographically Distributed Deployment

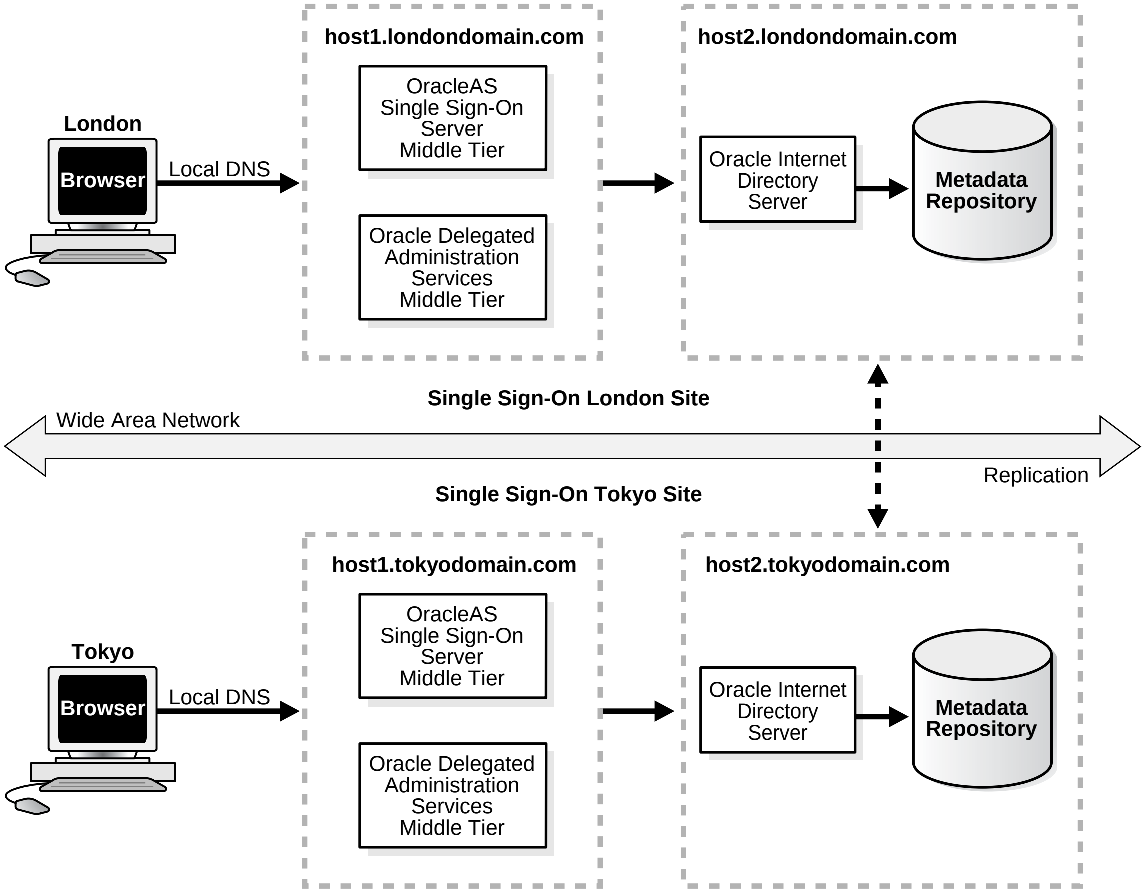
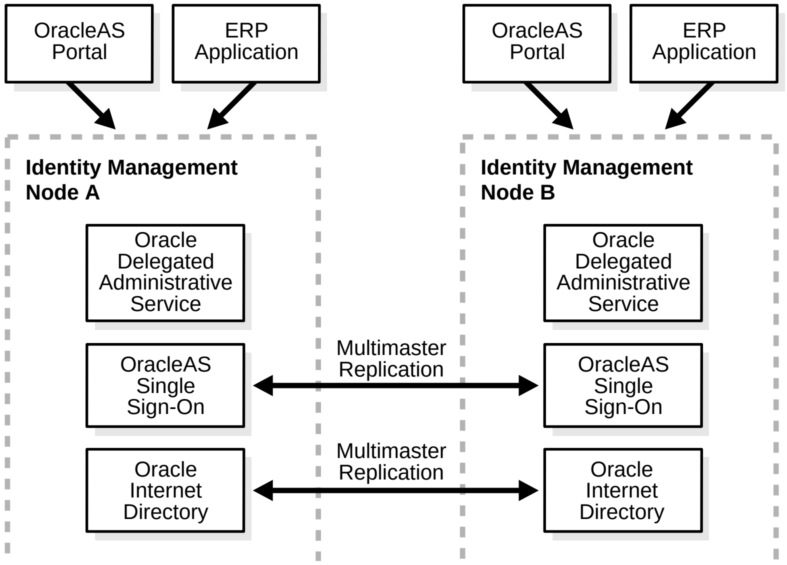

host1.londondomain.com
host2.londondomain.com
London
Browser
Local DNS
OracleAS Single Sign-On Server Middle Tier
Oracle Delegated Administration Services Middle Tier
Oracle Internet Directory Server
Metadata Repository
Single Sign-On London Site
Wide Area Network
Replication
Single Sign-On Tokyo Site
host1.tokyodomain.com
host2.tokyodomain.com
Tokyo
Browser
Local DNS
OracleAS Single Sign-On Server Middle Tier
Oracle Delegated Administration Services Middle Tier
Oracle Internet Directory Server
Metadata Repository

Figure 3–22 provides another example of a geographically distributed deployment. Identity management Node A and Node B are located in different places. Applications such as OracleAS Portal and ERP applications located near Node A are using services provided by the local identity management system. Similarly, applications located near Node B are using services provided by the local identity management system. The nodes replicate Oracle Internet Directory andOracle Application Server Single Sign-On data.

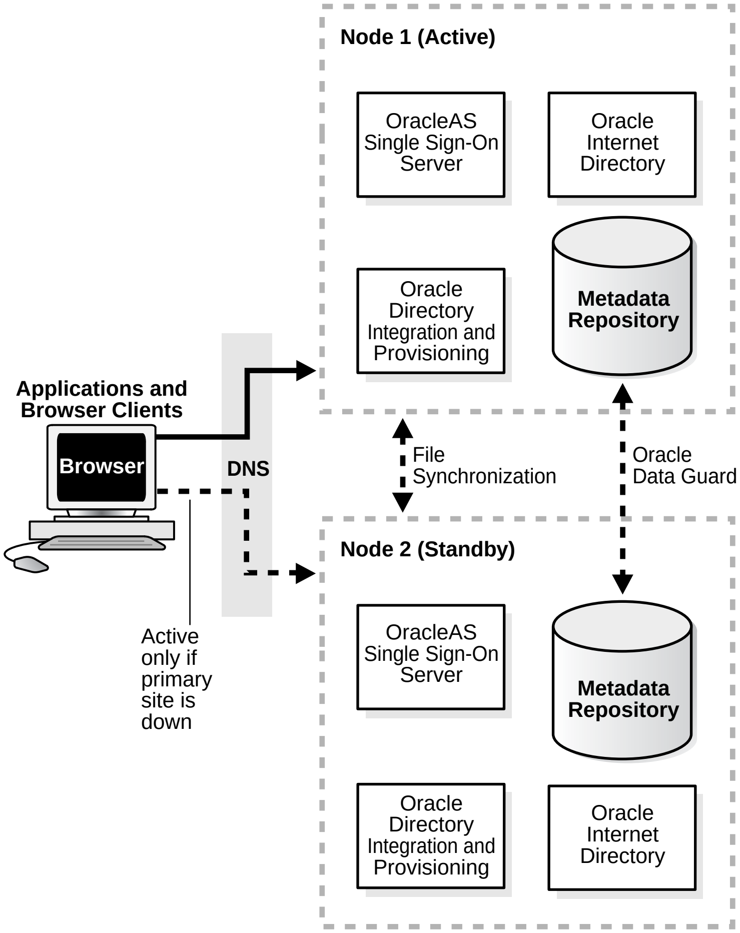
Figure 3–22 Distributed Deployment Support with Multimaster Replication


OracleAS Portal
ERP Application
OracleAS Portal
ERP Application
Identity Management Node A
Identity Management Node B
Oracle Delegated Administrative Service
Oracle Delegated Administrative Service
Multimaster Replication
OracleAS Single Sign-On
OracleAS Single Sign-On
Multimaster Replication
Oracle Internet Directory
Oracle Internet Directory

Disaster Recovery Deployment for Identity Management Infrastructure

Disaster recovery refers to how a system recovers from catastrophic site failures. Examples of catastrophic failures include earthquakes, tornadoes, floods, and fire. In simple terms, disaster recovery involves replicating an entire site, including the metadata repository and configuration files, in addition to replacing hardware or subcomponents. The most stringent requirement is to keep the services running despite a disaster. This deployment also protects the identity management infrastructure from site failures or media failures, which result in damage to, or loss of, data.

Figure 3–23 Oracle Internet Directory Deployment Using Oracle Application Server Guard


Node 1 (Active)
OracleAS Single Sign-On Server
Oracle Internet Directory
Oracle Directory Integration and Provisioning
Metadata Repository
Applications and Browser Clients
Browser
DNS
File Synchronization
Oracle Data Guard
Node 2 (Standby)
Active only if primary site is down
OracleAS Single Sign-On Server
Metadata Repository
Oracle Directory Integration and Provisioning
Oracle Internet Directory

Identical software, such as a single instance of the identity management infrastructure, can be run in multiple data centers with Oracle Application Server Guard to protect against data center disaster. Oracle Application Server Guard also provides single-instance directory data recovery and transparent failover.

As shown in Figure 3–23, Oracle Application Server Guard is configured to maintain a physical standby identity management infrastructure that is synchronized with the primary Oracle Identity Management infrastructure. Oracle Internet Directory and other Oracle Internet Directory components are started on the primary identity management infrastructure metadata repository node.

During disaster recovery, the standby becomes the primary node, the virtual host name is moved to the standby, and the identity management processes are then started on the standby node.

Oracle Application Server Certificate Authority Recommended Deployment

In production deployments, Oracle recommends deploying Oracle Application Server Certificate Authority on a separate system with its own repository. Other components of the Oracle Identity Management infrastructure can use any of the configurations described in this chapter.

The Oracle Application Server Certificate Authority system should be secured with all known mechanisms, in addition to the following guidelines:

- Physical access to the Oracle Application Server Certificate Authority system should be strictly controlled.
- The operating system should be hardened and user accounts on the system should be limited.
- The metadata repository for Oracle Application Server Certificate Authority should be secured with database securing guidelines.
- Oracle Application Server should be secured.
- Turn on metadata repository database auditing.

Follow other guidelines to improve the security of the system, such as physical security and network security.

4

Oracle Identity Management Administration and Usage

This chapter describes how to administer and use the Oracle Identity Management infrastructure, including administering users with Oracle Delegated Administration Services, as well as considerations for administering the infrastructure itself.

Considerations for supporting Oracle and third-party application deployments with the Oracle Identity Management infrastructure are also described.

This chapter contains the following topics:

- Administering Oracle Identity Management Infrastructure
- Delegating Oracle Identity Management Administration

Administering Oracle Identity Management Infrastructure

After a successful deployment, there are a number administrative tasks involved in managing the Oracle Identity Management infrastructure, including routine monitoring, managing individual components of, and managing enterprise data within the Oracle Identity Management infrastructure.

This section contains the following topics:

- Routine Monitoring of the Oracle Identity Management Infrastructure
- Managing Individual Oracle Identity Management Components
- Managing Enterprise Data in the Oracle Identity Management Infrastructure

Routine Monitoring of the Oracle Identity Management Infrastructure

Table 4–1 describes the various tasks, tools, and references necessary to perform routine monitoring of the Oracle Identity Management infrastructure.

Table 4–1 Routine Monitoring Tasks

Task	Tools	Additional References
Monitoring the status and performance of the Oracle Internet Directory server	■ Application Server Control ■ LDAP command-line tools	*Oracle Internet Directory Administrator's Guide*
Monitoring the status of Oracle Directory Integration and Provisioning	Application Server Control	*Oracle Identity Management Integration Guide*

Table 4–1 (Cont.) Routine Monitoring Tasks

Task	Tools	Additional References
Monitoring the status of Oracle Delegated Administration Services	Application Server Control	*Oracle Identity Management Guide to Delegated Administration*
Monitoring the status of OracleAS Single Sign-On	Application Server Control	*Oracle Application Server Single Sign-On Administrator's Guide*

Managing Individual Oracle Identity Management Components

Table 4–2 describes the various tasks, tools, and references necessary for managing individual components of Oracle Identity Management.

Table 4–2 Managing Oracle Identity Management Components

Task	Tools	Additional References
Starting and stopping directory services	■ Application Server Control ■ `oidctl` command-line tools	*Oracle Internet Directory Administrator's Guide*
Configuring directory services	Oracle Directory Manager	*Oracle Internet Directory Administrator's Guide*
Starting and stopping Oracle Directory Integration and Provisioning services	■ Application Server Control ■ `oidctl` command-line tools	*Oracle Identity Management Integration Guide*
Configuring Oracle Directory Integration and Provisioning	■ Oracle Directory Manager ■ Oracle Directory Integration Platform Assistant	*Oracle Identity Management Integration Guide*
Starting and stopping Oracle Delegated Administration Services	■ Application Server Control ■ `opmctl` command-line tools	■ *Oracle Identity Management Guide to Delegated Administration* ■ *Oracle Application Server Administrator's Guide*
Configuring Oracle Delegated Administration Services	Oracle Delegated Administration Services Configuration tab	*Oracle Identity Management Guide to Delegated Administration*
Starting and stopping OracleAS Single Sign-On	■ Application Server Control ■ `opmctl` command-line tools	■ *Oracle Application Server Single Sign-On Administrator's Guide* ■ *Oracle Application Server Administrator's Guide*
Registering a partner application with OracleAS Single Sign-On	`ossoreg.jar` registration tool	*Oracle Application Server Single Sign-On Administrator's Guide*

Managing Enterprise Data in the Oracle Identity Management Infrastructure

In addition to monitoring and managing individual components, Table 4–3 describes tasks, tools, and references available to enterprises for managing their data (users, groups, applications, and policies) within the Oracle Identity Management infrastructure.

Table 4–3 Managing Enterprise Data

Task	Tools	Additional References
User management (adding, deleting, and modifying users)	■ Oracle Delegated Administration Services ■ LDAP command-line tools ■ Oracle Directory Manager	*Oracle Internet Directory Administrator's Guide*
Group management (adding, deleting, and modifying groups)	■ Oracle Delegated Administration Services ■ LDAP command-line tools ■ Oracle Directory Manager	*Oracle Internet Directory Administrator's Guide*
Application deployment security management	■ Oracle Delegated Administration Services ■ LDAP command-line tools ■ Oracle Directory Manager	■ *Oracle Internet Directory Administrator's Guide* ■ *Oracle Application Server Administrator's Guide*
Delegation of privileges	■ Oracle Delegated Administration Services ■ LDAP command-line tools ■ Oracle Directory Manager	*Oracle Internet Directory Administrator's Guide*
OracleAS Single Sign-On partner and external applications administration	OracleAS Single Sign-On Administration Application	*Oracle Application Server Single Sign-On Administrator's Guide*

Delegating Oracle Identity Management Administration

The delegation model supported by Oracle Identity Management is customizable to align with the security requirements of the enterprise. The deployment uses the Oracle Identity Management infrastructure to manage enterprise identities, manage enterprise groups and roles, and manage applications that rely on enterprise identities and groups.

This section contains the following topics:

- Delegating User Management
- Delegating Group Management
- Delegating Component Deployment and Administration
- Oracle Internet Directory Delegated Administration Services

Delegating User Management

As shown in Figure 4–1, the final targets for delegation of user management privileges are either Oracle components that use the identity management infrastructure or end users. A privilege can be delegated to either an identity, such as a user or an application, or to a role or group.

In a typical deployment, the Oracle Internet Directory super user creates an identity management realm and identifies a special user in that realm to be the identity management realm administrator. The super user delegates all privileges to the new identity management realm administrator who, in turn, delegates certain privileges required by Oracle components to the Oracle defined roles, such as Oracle Application Server administrators. The Oracle components are granted these roles when they are deployed.

In addition to delegating the necessary privileges to Oracle defined roles, the realm administrator can also define deployment-specific roles, such as help desk administrator, and delegate specific privileges to them. The respective administrators, in turn, grant these roles to the users.

Because most of the user management tasks are self-service oriented, such as changing phone numbers, language preferences, and application specific preferences stored in Oracle Internet Directory, these privileges can be delegated to the users by both the realm administrator and the Oracle application components.

Delegating Group Management

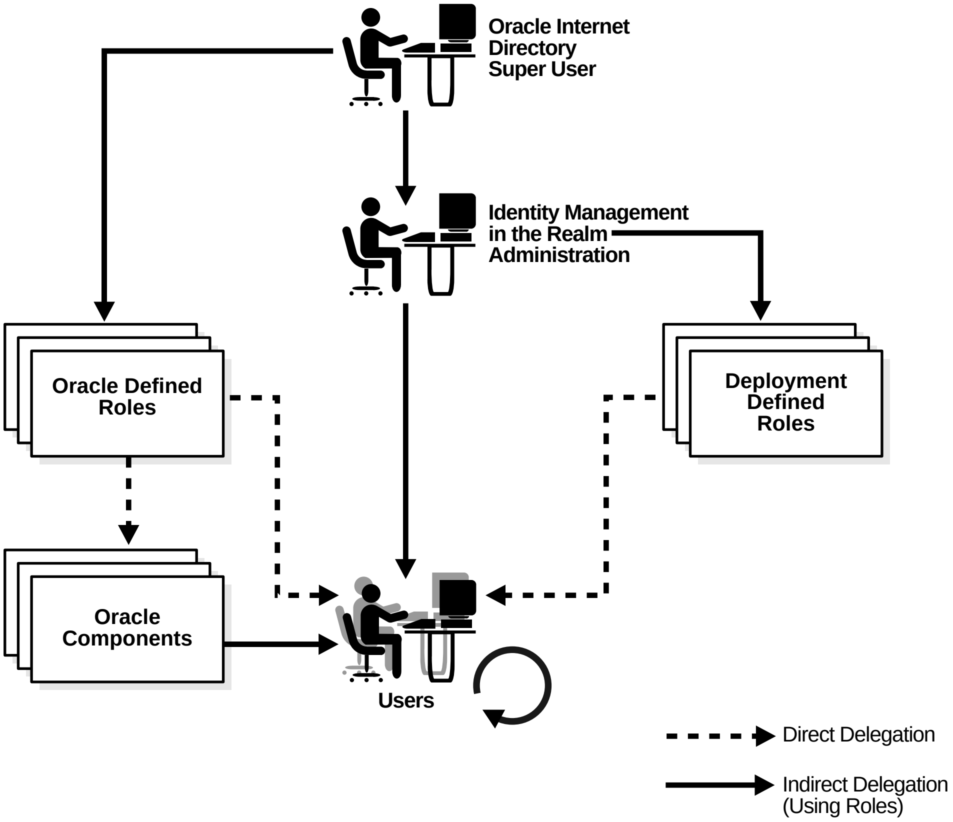
As with delegating user management, the final targets for delegation of group management privileges are either Oracle components that use the identity management infrastructure, or users, as shown in Figure 4–1.

The Oracle Internet Directory super user delegates all group-related privileges within the realm to the identity management realm administrator who, in turn, delegates certain group management privileges required by Oracle components to the Oracle defined roles. The Oracle components are granted these roles when they are deployed.

In addition to delegating the necessary privileges to Oracle defined roles, the realm administrator can also define deployment-specific roles, such as help desk administrator, and delegate specific privileges to them. The respective administrators, in turn, grant these roles to users.

Once a group is created, one or more *owners* of the group can be identified and all subsequent management of the group can be delegated to the owners, who are typically users. These owners can use the self-service console to manage the groups based on the privileges granted to them.

Figure 4–1 Delegating User and Group Management Privileges


Oracle Internet Directory Super User
Identity Management in the Realm Administration
Oracle Defined Roles
Deployment Defined Roles
Oracle Components
Users
Direct Delegation
Indirect Delegation (Using Roles)

Delegating Component Deployment and Administration

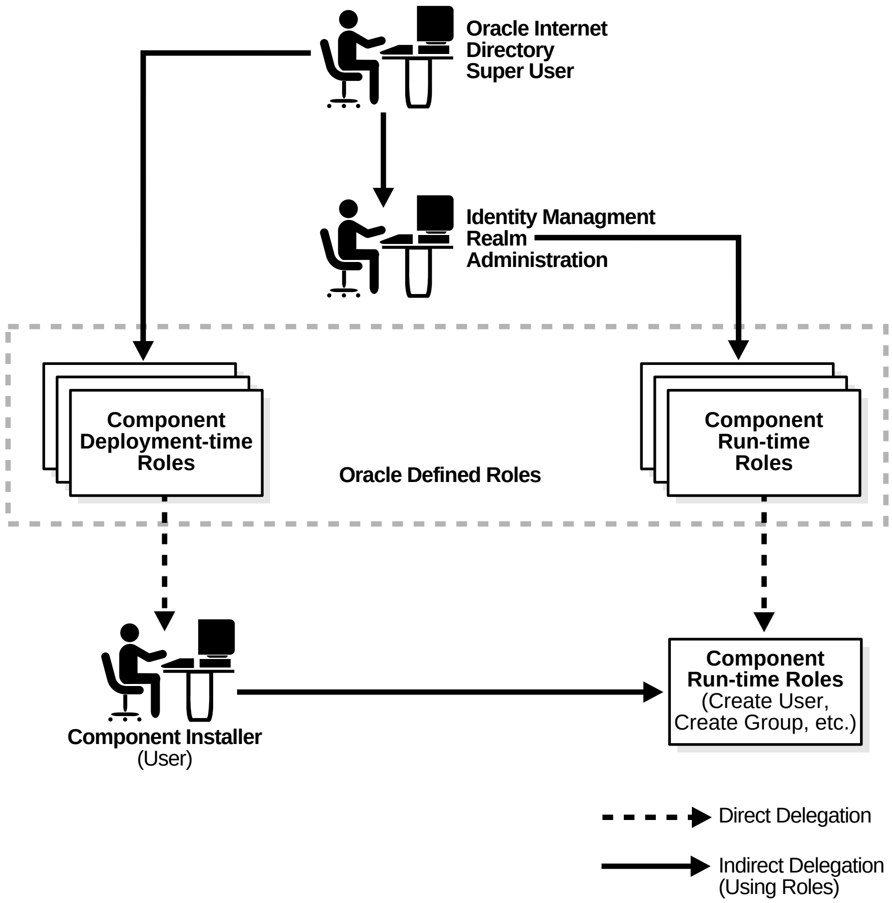
The set of privileges required for Oracle component deployment and administration can be separated into two categories: *deployment-time* privileges and *run-time* privileges.

Deployment-time privileges refer to those privileges that are required to create the appropriate entries inside the directory, and for storing the meta-information in a common repository. By having a centralized repository, the component can be run from multiple nodes without any further administrative steps.

Run-time privileges refer to those privileges that are required to facilitate the run-time interactions of Oracle components within the identity management infrastructure. These include the privileges to view user attributes, add new users, and modify the group membership. For all Oracle components, the component-specific administration tool requires a certain set of privileges to access, or make appropriate entries into, Oracle Internet Directory.

Figure 4–2 illustrates the delegation of deployment-time and run-time privileges in the Oracle Identity Management infrastructure.

Figure 4–2 Delegating Deployment-time and Run-time Privileges


Oracle Internet Directory Super User
Identity Managment Realm Administration
Component Deployment-time Roles
Oracle Defined Roles
Component Run-time Roles
Component Installer (User)
Component Run-time Roles (Create User, Create Group, etc.)
Direct Delegation
Indirect Delegation (Using Roles)

In Figure 4–2, note that the super user grants certain deployment privileges to groups, which, during the deployment process, are granted to certain users for installing specific Oracle components by making them members of those groups. As part of the installation process, the component installer then grants specific run-time privileges to the component.

> **Note:** Even though most Oracle components ship with a preconfigured set of privileges, it is always possible to change the privileges to satisfy specific business requirements.

Oracle Internet Directory Delegated Administration Services

Oracle Delegated Administration Services allows the enterprise to assign administrative responsibilities according to the business requirements. It provides different levels of security policies for different components of the enterprise, such that specific administrators, or sets of administrators, can independently manage access to their resources, and yet not create different silos of security information.

The Oracle Internet Directory-based multi tier delegation architecture supports millions of users in multiple realms, management domains, applications, business units, and geographies. In combination with the centralized repository, Oracle Identity Management enables decentralized administration, and lowers the total cost of ownership.

One of the challenges faced by application designers is being able to invoke the user management and resource management with consistent security and use semantics across applications. For example, if multiple applications need to manage groups, they should not be required to understand the various steps required to implement group management and the directory access control list (ACL) semantics.

The user interfaces for Oracle Identity Management system privileges can be divided into various delegated administration service units (DAS service units), which can then be combined by the application console. For example, if the application console needs to be used to modify a user attribute, it would integrate the link for the appropriate DAS service unit in its console or portal page, without having to create the user interface.

The various DAS service units can also be used to build self-service applications, which can be used to update attributes, such as language preferences and home address. Thus, the DAS service units-based integration approach provides for consistent security semantics, consistent usage model, and reuse of the components.

5

Integrating with Other Identity Management Solutions

This chapter discusses integrating Oracle components with other enterprise identity management solutions.

This chapter contains the following topics:

- Reasons for Identity Management Integration
- Identity Management Integration Tools and Strategies

Reasons for Identity Management Integration

While the Oracle Identity Management infrastructure is an essential component in most Oracle deployments, it is also designed to permit integration with other identity management solutions. Integration of Oracle products around a common infrastructure provides a single point of integration with other enterprise identity management solutions, including:

- Directory services
- User authentication services
- User provisioning applications
- Third-party PKI solutions

Identity management integration allows Oracle users to use existing enterprise infrastructure components in the Oracle environment, which can provide the following benefits:

- **Unified user provisioning**: User provisioning refers to the process by which new users are added and deleted from the various enterprise systems. New user provisioning can be driven by a number of different sources, such as human resource (HR) systems, customer relationship management (CRM) systems, and network administration environments. When a new user is created in one system, automated user provisioning creates the required user account *footprints* in other enterprise applications. An account footprint is the set of application resources required by a user account.
- **Centralized user administration**: Once a user account is created, it must be maintained and administered. Centralized user administration ensures that all application-related information associated with a user, such as passwords, roles, and application preferences, are administered in one place.

- **Runtime security service integration**: Organizations want applications in the enterprise environment to be capable of using a common set of security services for authentication and data privacy.

Delivering these benefits requires tools and strategies for integrating Oracle Identity Management and third-party directory, security, and user administration environments.

> **See Also:** *Oracle Identity Management Integration Guide* and *Oracle Application Server Single Sign-On Administrator's Guide* for information about deploying these integration solutions

Identity Management Integration Tools and Strategies

Oracle Identity Management provides a number of tools for integrating with other identity management environments, including various services and APIs, preconfigured directory connectivity solutions, and standards support, which are briefly described in this section. For additional information on their use, see the appropriate component documentation.

Oracle Directory Integration and Provisioning

Oracle Directory Integration and Provisioning consists of a set of services and interfaces built into Oracle Internet Directory that facilitate the development of synchronization and provisioning solutions between Oracle Internet Directory and other repositories, such as third-party directories (SunONE Directory and Microsoft Active Directory, for example), application user repositories (as might be stored in a flat file, for example), or database tables containing HR information.

Oracle Directory Integration and Provisioning includes a documented API and incorporates available industry standards where they exist, making it possible for Oracle, customers, and third parties to develop and deploy customized synchronization and provisioning solutions. It also facilitates interoperability between Oracle Internet Directory and third-party metadirectory and provisioning solutions.

Oracle Internet Directory Plug-In Architecture

Oracle Internet Directory supports a PL/SQL-based plug-in framework that enables you to include custom routines (Oracle, customer-written, or third-party) that can execute before, during, or after a directory operation. For example, this framework can be used to:

- Validate data before the directory server performs an operation on it
- Perform specified actions after the server performs an operation
- Define custom password policies
- Authenticate users through external credential stores such as NOS directories

> **See Also:** *Oracle Internet Directory Administrator's Guide* for more information

Preconfigured Directory Connectivity Solutions

Oracle Internet Directory includes preconfigured connectivity solutions built on Oracle Directory Integration and Provisioning and the Oracle Internet Directory plug-in architecture, which make it possible to automatically provision users in the Oracle Identity Management space from other systems, and to administer users in the Oracle

Identity Management space from those environments. Preconfigured connectivity solutions include:

- Oracle E-Business Suite
- Oracle Database tables
- SunONE and iPlanet
- Microsoft Active Directory

> **See Also:** *Oracle Identity Management Integration Guide* for more information about preconfigured directory connectivity solutions

OracleAS Single Sign-On Partner APIs

OracleAS Single Sign-On supports a third-party authentication API that allows Oracle Application Server Single Sign-On to obtain user identities from a trusted, third-party authentication mechanism. This feature can be used to allow application users to access Web applications across the two environments, having to log in only once.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for more information

Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider Developer APIs

Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider allows user-written Java applications running in the Oracle J2EE environment to use OracleAS Single Sign-On and Oracle Internet Directory for authentication and identity services.

> **See Also:** *JAAS Provider API Reference* for more information

LDAP Standard Support

Oracle Internet Directory supports the LDAPv3 standard in accordance with the IETF RFC 2251.

> **See Also:** *Oracle Internet Directory Administrator's Guide* for more information about preconfigured directory connectivity solutions

Authentication Standard Support

OracleAS Single Sign-On supports user authentication using Kerberos tickets issued by a Kerberos key distribution center, which allows users who have been issued a valid Kerberos ticket (in, for example, the Windows environment) to log in to their Web applications without having to provide a username and password.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for more information

X.509v3 Certificate Standard Support

Oracle Identity Management issues and uses X.509v3 standard PKI certificates for strong authentication services. Customers with existing X.509v3 certificate authorities can use these certificates in the Oracle environment.

A

Deploying Oracle Identity Management with Multimaster Replication

This Appendix describes how to deploy Oracle Application Server 10*g* Release 2 (10.1.2) Identity Management with multimaster replication in a configuration that includes multiple components.

Before attempting the tasks described in this document, you should become familiar with all components of Oracle Application Server 10*g* Release 2 (10.1.2), including: Oracle Internet Directory, Oracle Application Server Single Sign-On, Oracle Delegated Administration Services, and Oracle Directory Integration and Provisioning. You should also be familiar with replication concepts.

> **See Also:** Replication information in the *Oracle Internet Directory Administrator's Guide* and the *Oracle Application Server Installation Guide*.

Keep the following points in mind when using the commands-line tools mentioned in this document:

- The `ORACLE_HOME`, `MASTER_HOME`, and `REPLICA_HOME` variables designate absolute Oracle home paths.
- Use the appropriate path separator while running the tools. The notation in this appendix is based on the UNIX patch variable notation. For example, the `ldifadd` tool is located in the `$ORACLE_HOME/bin` directory in the UNIX environment. In the Windows environment, this tool is located in the `ORACLE_HOME\bin` directory.
- The `PATH` environment variable should include `ORACLE_HOME\bin`, `ORACLE_HOME\ldap\bin` and `ORACLE_HOME\opmn\bin` directories.
- Include `$ORACLE_HOME/lib` in the appropriate library environment variable. For example, in the Solaris environment, include `$ORACLE_HOME/lib` in the `LD_LIBRARY_PATH` environment variable.

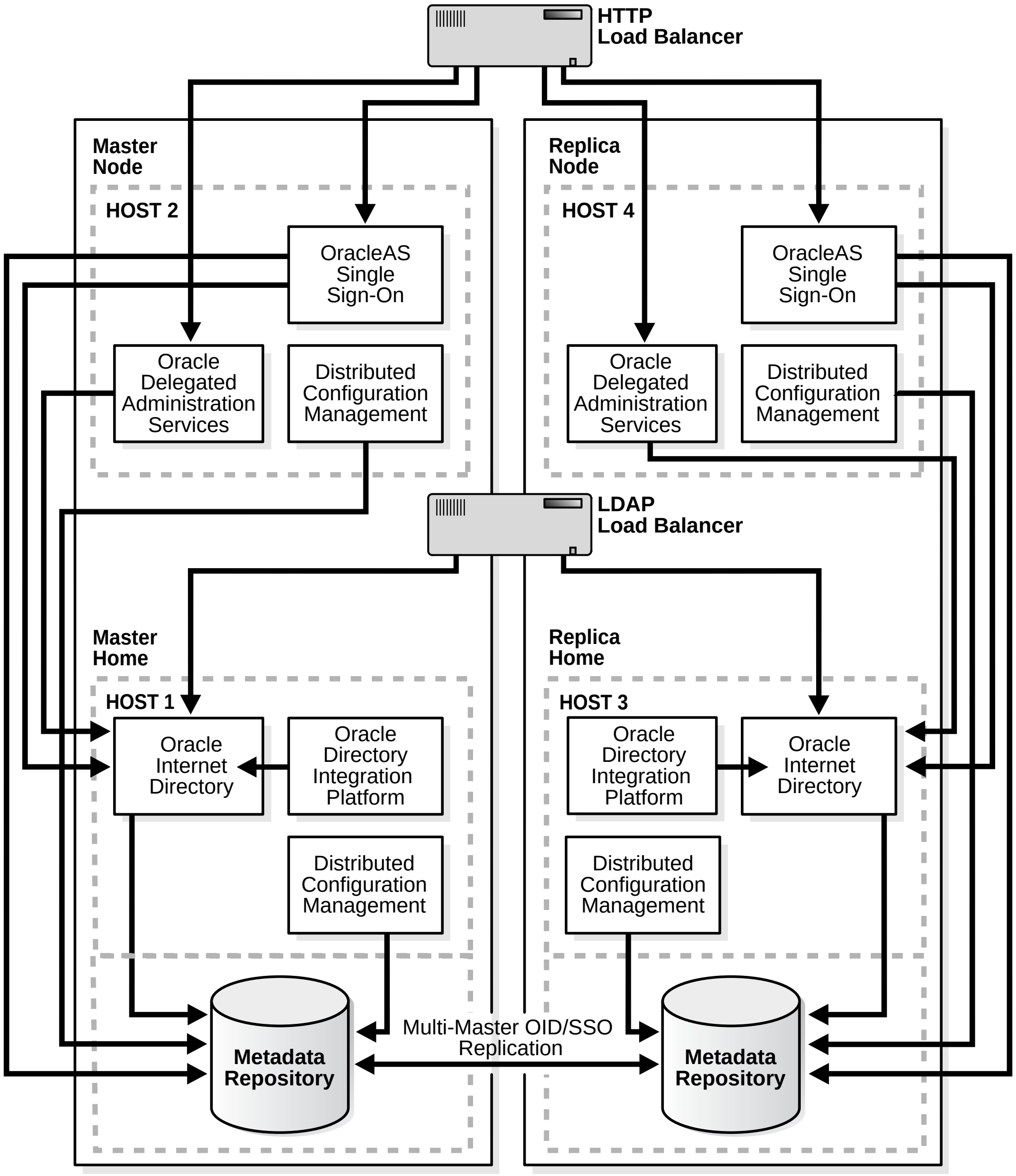
This appendix includes the following sections:

Multimaster Identity Management Replication Configuration

In Figure A–1, The Oracle Identity Management master node includes Host 1 and Host 2. Oracle Identity Management and Metadata Repository, Oracle Internet Directory, and Oracle Directory Integration and Provisioning are installed on Host 1. Oracle Application Server Single Sign-On and Oracle Delegated Administration Services, are installed on Host 2.

Similarly, the Oracle Identity Management replica node includes Host 3 and Host 4. Oracle Identity Management and Metadata Repository, Oracle Internet Directory, and Oracle Directory Integration and Provisioning are installed on Host 3. Oracle Application Server Single Sign-On and Oracle Delegated Administration Services, are installed on Host 4.

Figure A–1 Multimaster Replication Configuration with Two Hosts Per Node



Master Node Installation

Install Oracle Internet Directory and Oracle Directory Integration and Provisioning on the master node as follows:

- Install Oracle Application Server 10*g* Release 2 (10.1.2). Select Oracle Internet Directory, Identity Management and Metadata Repository, and Oracle Directory Integration and Provisioning on Host 1 using MASTER_HOME as the Oracle home.
- Do not install any other Oracle Identity Management components such as Oracle Application Server Single Sign-On, or Oracle Delegated Administration Services

Replica Node Installation

Install and Oracle Internet Directory with Metadata Repository on the replica node as follows:

- Install Oracle Application Server 10*g* Release 2 (10.1.2). Select Oracle Internet Directory, Identity Management and OracleAS Metadata Repository, and Oracle Directory Integration and Provisioning on Host 3 using REPLICA_HOME as the Oracle home. This installation will have only Oracle Internet Directory with Metadata Repository and Oracle Directory Integration and Provisioning. The Replica node Metadata Repository database should have a unique global database name.
- Do not install any other Oracle Identity Management components, such as Oracle Application Server Single Sign-On, and Oracle Delegated Administration Services.

Note: While installing the replica, select **HA** in the advanced configuration screen. Oracle Universal Installer will ask you to choose **Replica** install. When you select that, it will allow you to choose **ASR Replica** or **LDAP Replica**. Select **ASR Replica** and continue.

Multimaster Replication Installation

Use the following procedure to set up replication between the master node and the replica node.

1. Prepare both the master node and the replica node for replication, as described in Task 3, Installing and Configuring a Multimaster Replication Group, in the "Oracle Internet Directory Replication Administration" chapter of *Oracle Internet Directory Administrator’s Guide*.
2. Set up replication by using the following command on both nodes:

   ```
   $MASTER_HOME/bin/remtool -asrsetup
   ```

3. Start up the Oracle Internet Directory replication server at the master node and at the replica node.
4. Verify that the replication setup is correct.

   See Also: Replication information in the *Oracle Internet Directory Administrator’s Guide* and the *Oracle Application Server Installation Guide*.

Installing Oracle Application Server Single Sign-On and Oracle Delegated Administration Services on the Master Node

Install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services, as follows:

1. On Host 2, install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services so that those components use the Metadata Repository and Oracle Internet Directory on the master node. To do that, select Oracle Identity Management (without the Metadata Repository). When prompted for the Oracle Internet Directory information, provide the hostname and port of Host 1.
2. Select the Load Balancer configuration option and provide the load balancer name when prompted.

Repeat this procedure to install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services on additional replicas.

Synchronizing the Single Sign-On Schema Password

To synchronize the Oracle Application Server Single Sign-On schema password, follow Step 2 under "Configuring the Identity Management Database for Replication" in *Oracle Application Server Single Sign-On Administrator's Guide*. This will synchronize Oracle Application Server Single Sign-On schema passwords between the master Metadata Repository database (MDS) and the replica Metadata Repository database (RMS).

After you performed this step on the master node, do it on each replica node.

Note: If you encounter errors, the Metadata Repository might be misconfigured. Either the MDS or RMS might not have the correct database information, as used by Oracle Application Server Single Sign-On.

Installing Oracle Application Server Single Sign-On and Oracle Delegated Administration Services on the Replica Node

Install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services, as follows:

1. On Host 4, install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services so that those components use the Metadata Repository and Oracle Internet Directory on the master node. To do that, select Oracle Identity Management (without the Metadata Repository).
2. Select the Load Balancer configuration option and provide the load balancer name when prompted.
3. Synchronize the `mod_osso` configuration from the master mid-tier, as described in the section on reregistering `mod_osso` for the single sign-on middle tiers, in *Oracle Application Server Single Sign-On Administrator's Guide*.

Repeat this procedure to install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services on additional replicas.

Oracle Directory Integration and Provisioning Event Propagation in a Multimaster Scenario

Oracle Directory Integration and Provisioning supports high availability in an Oracle Internet Directory multimaster replicated scenario, with certain drawbacks. In this high availability scenario, when changes are applied to Oracle Internet Directory on one node, the changes get propagated to the other consumer nodes. The Oracle Directory Integration and Provisioning server running on each node is responsible for event propagation to the configured applications on that node. That is, the applications that have provisioning profiles on that Oracle Internet Directory node will be informed of the changes happening on that Oracle Internet Directory node.

> **See Also:** *Oracle Identity Management Integration Guide*

Adding a Node to a Multimaster Replication Group

To add a replication node to a functioning directory replication group (DRG), follow these steps.

1. First, install the new node.

   Install Oracle Application Server 10*g* Release 2 (10.1.2) Identity Management and Metadata Repository. This installation will have only the Metadata Repository, Oracle Internet Directory and Oracle Directory Integration and Provisioning. The replica node Metadata Repository should have a unique global database name.

   Do not install other Identity Management components such as Oracle Application Server Single Sign-On or Oracle Delegated Administration Services.

2. Prepare the environment for adding a node.

   a. Configure the Oracle Net Services environment as described in Task 3, Installing and Configuring a Multimaster Replication Group, in the "Oracle Internet Directory Replication Administration" chapter of *Oracle Internet Directory Administrator's Guide*.

   b. Stop the directory replication server on all nodes

   c. Identify a sponsor node and switch the sponsor node to read-only mode

      Note: While the sponsor node is in read-only mode, do not make any updates to it. You may, however, update any of the other nodes, but those updates are not replicated immediately. Also, the sponsor node and the MDS can be the same node.

   d. Back up the sponsor node by using `ldifwrite`. Enter the following command:

      ```
      $ORACLE_HOME/bin/ldifwrite -c connect_string  \
              -b "orclagreementid=000001,cn=replication configuration" \
              -f output_ldif_file
      ```

3. Add the node into the replication group.

   a. Perform the Advanced Replication add node setup on the sponsor node by typing:

      ```
      $ORACLE_HOME/ldap/bin/remtool -addnode
      ```

      The Replication Environment Management Tool adds the node to the DRG.

> **Note:** Note: If you encounter errors, then use `remtool -asrverify`. If it reports errors, then rectify them by using `remtool -asrrectify`. Both of those options list all the nodes in the DRG. If the new node is not in the list, then add it by running `remtool -addnode` again.

b. Switch the sponsor node to updatable mode.

c. Start the directory replication server on all nodes except the new node.

d. Stop `oidmon`

e. Load data into the new node, as follows:

First do a check and generate by typing:

```
$ORACLE_HOME/ldap/bin/bulkload.sh \
  -connect <db_connect_string_of_new_node> \
  -check -generate -restore  \
  absolute_path_to_the_ldif_file_generated_by_ldifwrite
```

> **Note:** Verify that the `$ORACLE_HOME/ldap/log/bulkload.log` does not report any errors. It's possible that you might see `Duplicate entry errors` in the log for some of the entries. You can safely ignore this error and proceed with the load.

Now load the data on the target node by typing:

```
$ORACLE_HOME/ldap/bin/bulkload.sh \
  -connect db_connect_string_of_new_node \
  -load -restore  \
  absolute_path_to_the_ldif_file_generated_by_ldifwrite
```

4. Start the directory server on the new node by typing the following command:

```
$ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID
```

5. Start the directory replication server on the new node by typing:

```
$ORACLE_HOME/bin/oidctl connect=db_connect_string_of_new_node \
   server=oidrepld instance=1 \
   flags='-h host_name_of_new_node -p port'  start
```

6. Install a new mid-tier, based on the new replica node.

   a. Synchronize the Oracle Application Server Single Sign-On schema passwords from MDS to the new node as described in "Synchronizing the Single Sign-On Schema Password" on page A-4.

   b. Install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services as described in "Installing Oracle Application Server Single Sign-On and Oracle Delegated Administration Services on the Replica Node" on page A-4.

   c. Configure the HTTP load balancer to distribute incoming traffic to this newly installed node.

Deleting a Node from a Multimaster Replication Group

You can delete a node from a DRG, provided the DRG contains more than two nodes. You might need to do so if the addition of a new node did not fully succeed as a result of system errors. To delete a replication node, perform these steps:

1. Stop the directory replication server on all nodes. To do that, run the following command on each node in the DRG:

   ```
   $ORACLE_HOME/bin/oidctl connect=connect_string server=oidrepld instance=1 stop
   ```

   > **Note:** Note: The instance number may vary.

2. Stop all processes on the node to be deleted.

   a. Stop all processes in the associated mid-tier Oracle home.

      ```
      $ORACLE_HOME/opmn/bin/opmnctl stopall
      ```

   b. On the node to be deleted, stop all Oracle Application Server processes including Oracle Internet Directory Monitor and all directory server instances.

      ```
      $ORACLE_HOME/opmn/bin/opmnctl stopall
      ```

3. Delete the node from the master definition site. From the MDS, run the following command:

   ```
   $ORACLE_HOME/ldap/bin/remtool -delnode
   ```

   > **Note:** If you encounter errors, then use `remtool -asrverify`. If it reports errors, then rectify them by using `remtool -asrrectify`. Both of those options list all nodes in the DRG. If the new node is not in the list, then add it by running `remtool -addnode` again.

4. Start the directory replication server on all nodes by typing the following command:

   ```
   $ORACLE_HOME/bin/oidctl connect=connect_string server=oidrepld \
     instance=1 flags='-h host -p port' start
   ```

5. Decommission the removed node and its associated mid-tier. You can optionally decommission the removed replicated node and associated mid-tier by deinstalling the corresponding Oracle homes.

   > **See Also:** Replication information in the *Oracle Internet Directory Administrator's Guide* and the *Oracle Application Server Installation Guide*.

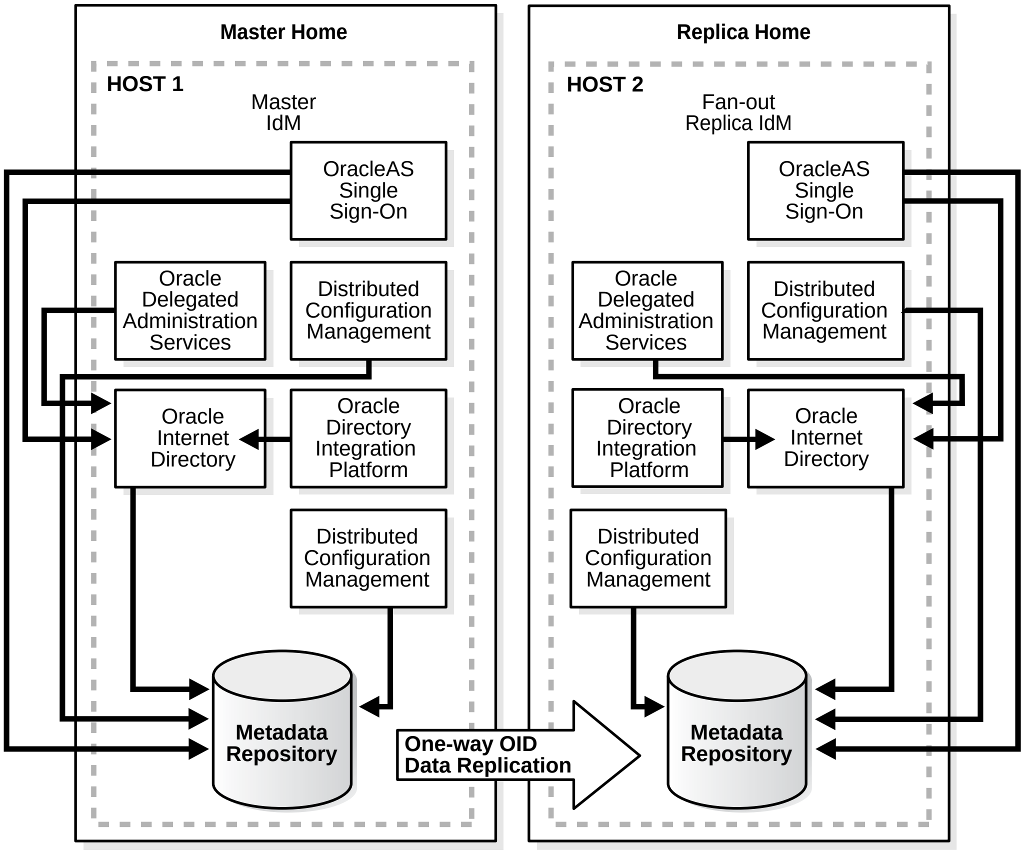
B

Deploying Oracle Identity Management with Fan-Out Replication

In Figure B–1, MASTER Oracle Identity Management node is installed on HOST 1 using default Identity Management install with Metadata Repository, Oracle Internet Directory and Oracle Directory Integration and Provisioning only. In another host, HOST 2, other Identity Management components such as Oracle Application Server Single Sign-On and Oracle Delegated Administration Services are installed.

Similarly, REPLICA Oracle Identity Management node is installed on HOST 3 using default Identity Management install with Metadata Repository, Oracle Internet Directory and Oracle Directory Integration and Provisioning only. In another host, HOST 4, other Identity Management components such as Oracle Application Server Single Sign-On, and Oracle Delegated Administration Services are installed.

Figure B–1 Fan-out Deployment with Oracle Internet Directory, Oracle Directory Integration and Provisioning, Oracle Application Server Single Sign-On, and Oracle Delegated Administration Services on Each Host


Master Home
HOST 1
Master IdM
OracleAS Single Sign-On
Oracle Delegated Administration Services
Distributed Configuration Management
Oracle Internet Directory
Oracle Directory Integration Platform
Distributed Configuration Management
Metadata Repository
One-way OID Data Replication
Replica Home
HOST 2
Fan-out Replica IdM
OracleAS Single Sign-On
Oracle Delegated Administration Services
Distributed Configuration Management
Oracle Directory Integration Platform
Oracle Internet Directory
Distributed Configuration Management
Metadata Repository

Master Node Installation

On the master node, install Oracle Application Server 10*g* Release 2 (10.1.2) Metadata Repository, Oracle Internet Directory, Oracle Application Server Single Sign-On, Oracle Delegated Administration Services and Oracle Directory Integration and Provisioning on Host 1 using MASTER_HOME as the Oracle home.

Replica Node Installation

On the replica node, install Oracle Identity Management and Metadata Repository, Oracle Internet Directory, Oracle Application Server Single Sign-On, Oracle Delegated Administration Services and Oracle Directory Integration and Provisioning on Host 2, using REPLICA_HOME as the Oracle home.

Note: While installing the replica, select **HA** in the advanced configuration screen along with Oracle Application Server Single Sign-On, Oracle Delegated Administration Services, Oracle Directory Integration and Provisioning. Oracle Universal Installer will ask you to choose **Replica** install. When you select **Replica**, Oracle Universal Installer will allow you to choose **ASR Replica** or **LDAP Replica.** Select **LDAP Replica** and continue.

Fan-out Replication Setup

The Oracle Universal Installer automatically configures replication. When the installation is complete, test that everything is working as desired.

C

Oracle Internet Directory Default Settings

This appendix describes the default settings that are available after you install Oracle Internet Directory.

The installation of Oracle Internet Directory creates a default DIT and sets up a default identity management realm using several assumptions about the deployment.

The following is a summary of the operations performed during the Oracle Internet Directory installation:

- A default DIT is created based on the domain name of the system on which Oracle Internet Directory is installed. For example, if Oracle Internet Directory is installed on a machine named `oidhost.us.acme.com`, the default DIT is `dc=us,dc=acme,dc=com`.
- A default identity management realm is created, whose base corresponds to the domain name of the system. Following the preceding example, the root of the default identity management realm is `dc=us,dc=acme,dc=com`.

  Associated with this realm is an entity called *Oracle Context*, that stores all the realm-specific policies and metadata. For example, Oracle Context might be created with the distinguished name `cn=OracleContext,dc=us,dc=acme,dc=com`. This entry, and the nodes under it, serves as the basis for Oracle software to detect realm specific policies and settings.
- Directory structure and naming policies created in the default identity management realm enable Oracle components to locate various identities. Following are the default values for these policies:
  - All users are located in the `cn=users` container under the base of the identity management realm. In this scenario, the distinguished name is `cn=users,dc=us,dc=acme,dc=com`.
  - Any new users created in the identity management realm using the Oracle Identity Management infrastructure are also created under the `cn=users` container.
  - All new users created in the identity management realm using the Oracle Identity Management infrastructure belong to the object classes `orclUserV2` and `inetOrgPerson`.
  - All groups are located in the `cn=groups` container under the base of the identity management realm. In this scenario, the distinguished name is `cn=groups,dc=us,dc=acme,dc=com`.

- A bootstrap user named `cn=orcladmin` is created under the `cn=users` container. In this scenario, the fully-qualified distinguished name of the bootstrap user is `cn=orcladmin,cn=users,dc=us,dc=acme,dc=com`.
- Default authentication policies are created that enable the authentication services to perform appropriate actions, including the default directory password policy (such as password length, number of tries before being locked out, and number of days before password expiration) and additional password verifiers that must be automatically generated when provisioning users.
- Identity management privileges are created and granted to the bootstrap user who can further delegate these authorizations through the Oracle Delegated Administration Services self-service console. Some of these privileges include:
  - Common identity management operational privileges, such as *user creation*, *user profile modification*, and *group creation*
  - Privileges to install new Oracle applications using the identity management infrastructure
  - Privileges to administer Oracle Delegated Administration Services

Index