Oracle® Identity Management

Concepts and Deployment Planning Guide

10*g* (9.0.4) for Windows or UNIX

Part No. B10660-01

September 2003

ORACLE®

Oracle Identity Management Concepts and Deployment Planning Guide 10*g* (9.0.4) for Windows or UNIX

Part No. B10660-01

Contents

1 Introduction to Identity Management

2 Oracle Identity Management Concepts and Architecture

3 Oracle Identity Management Deployment Planning

4 Oracle Identity Management Administration and Usage

5 Integrating with Other Identity Management Solutions

6 Integrating Enterprise Applications

A Oracle Internet Directory Default Settings

Index

List of Figures

Send Us Your Comments

Oracle Identity Management Concepts and Deployment Planning Guide 10g (9.0.4) for Windows or UNIX

Part No. B10660-01

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) 506-7227   Attn: Server Technologies Documentation Manager
- Postal service:
  Oracle Corporation
  Server Technologies Documentation
  500 Oracle Parkway, Mailstop 4op11
  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.

x

Preface

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

This preface contains these topics:

Intended Audience

Structure

Related Documents

Conventions

Documentation Accessibility

Intended Audience

This document is intended for the following audience:

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

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 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.

Chapter 6, "Integrating Enterprise Applications"
This chapter discusses integrating enterprise applications with Oracle Identity Management.

Appendix A, "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 manuals:

- *Oracle Application Server 10g Administrator's Guide*
- *Oracle Application Server 10g Security Guide*
- *Oracle Application Server 10g High Availability Guide*
- *Oracle Application Server 10g 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*

Conventions

The following conventions are used in this manual:

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.	*Oracle9i 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 executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as 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 open 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 U`old_release`.SQL where `old_release` refers to the release you installed prior to upgrading.

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 Corporation 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 Corporation does not own or control. Oracle Corporation neither evaluates nor makes any representations regarding the accessibility of these Web sites.

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 various components in an identity management system manage the security life cycle for network entities in an organization, and most commonly refers to the management of an organization's application users. Steps in the security lifecycle include account creation, suspension, privilege modification, and account deletion.

The network entities managed can include devices, processes, applications, or anything else that interacts in a networked environment. Entities managed by an identity management process can also include users outside of an organization, such as customers, trading partners, or Web services.

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 leverage the existing infrastructure to provision user accounts and privileges

- Improve the user experience by allowing rapid application access to new users

- Improve security and usability by centrally managing user passwords and security credentials and customizing applications to leverage centralized authorization and policy information

Identity Management System Components

A complete identity management system includes the following components:

- A scalable, secure, and standards-complaint 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 runtime 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. Security and user interface models that can support various requirements are critical.

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

Figure 1–1   Overview of an Identity Management System
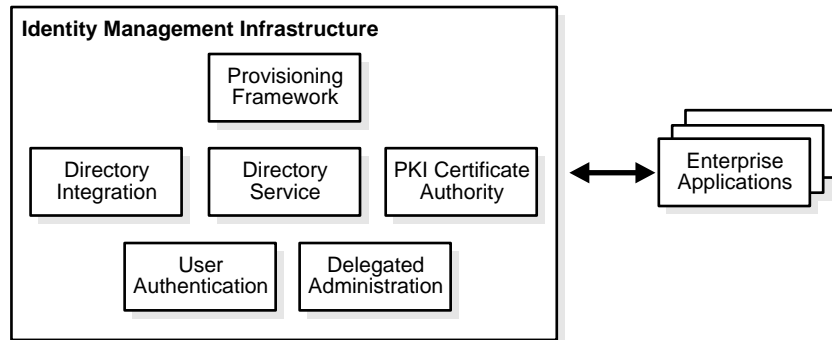
Oracle Identity Management Overview

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 Oracle9*i* Database Server 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 Oracle9*i* Database Server

- **Oracle Directory Integration and Provisioning**: A component of Oracle Internet Directory that enables you to:

  - Synchronize data between Oracle Internet Directory and other connected directories

  - Send notifications to target applications to reflect changes to a user's status or information

  - Develop and deploy your own connectivity agents

- **Oracle Delegated Administration Services**: A component of Oracle Internet Directory that provides trusted proxy-based administration of directory information by users and application administrators

- **Oracle Application Server Single Sign-On** (OracleAS Single Sign-On): Provides single sign-on access to Oracle and third-party Web applications

- **Oracle Application Server Certificate Authority** (OCA): Issues, revokes, renews, and publishes X.509v3 certificates to support PKI-based strong authentication methods

Many different applications, including Oracle E-Business Suite and Oracle Collaboration Suite, can leverage the Oracle Identity Management infrastructure, as shown in Figure 1–2.

Figure 1–2   Oracle Identity Management
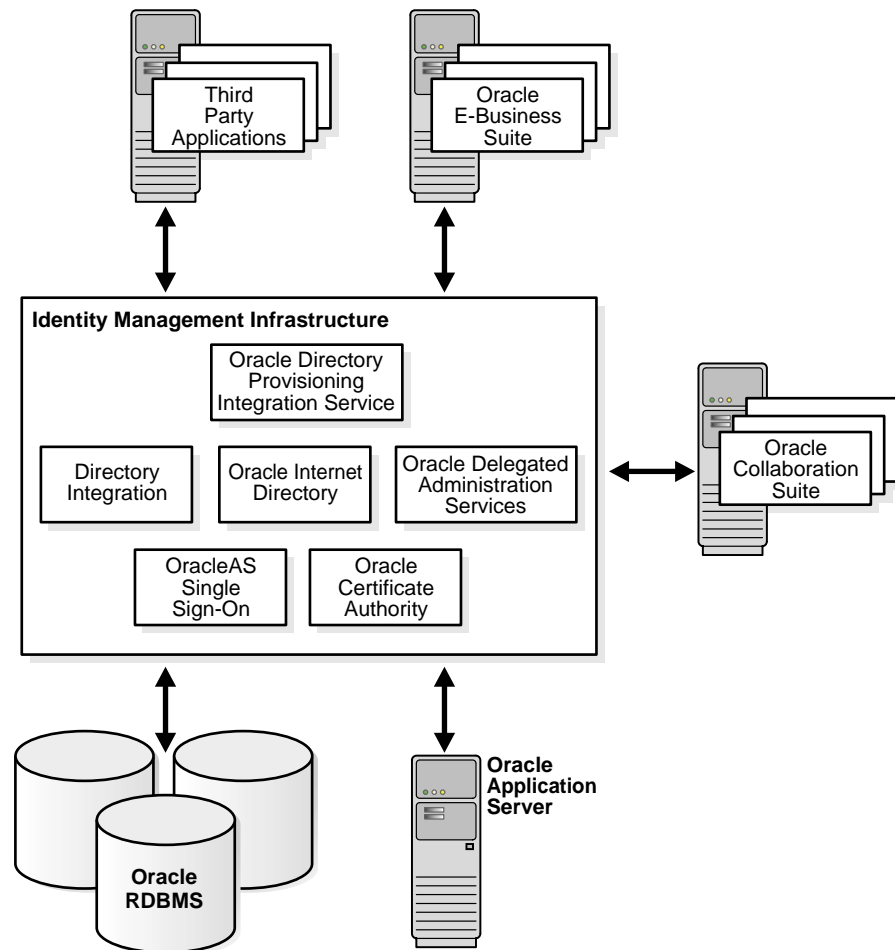
While Oracle Identity Management is designed to provide an enterprise infrastructure for Oracle products, it can also serve as a general purpose identity management solution for user-written and third-party enterprise applications.

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 serves as a shared infrastructure for all Oracle products and technology stacks, including Oracle Application Server, Oracle9*i* Database Server, Oracle E-Business Suite, and Oracle Collaboration Suite. Accordingly, it is secure, reliable, and scalable, consistent with the core strengths of Oracle products and technologies.

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

- Oracle Identity Management provides a secure, efficient, and reliable way to leverage 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

  - Using Oracle Directory Integration and Provisioning, Oracle Identity Management leverages current investment in planning and deployment of a third-party enterprise directory. This provides the means 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, identity, and account provisioning 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 the means to integrate with the service and extend 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 serve as an enterprise-wide foundation for identity management, to support other Oracle products as well as third-party vendor products deployed in the customer environment.

Oracle Identity Management offers lower ownership costs by streamlining the process of both user and account provisioning for all Oracle and third-party products. It also offers high levels of security, scalability, and functional richness. By supporting industry standards in all relevant interfaces, Oracle Identity Management can be customized and extended for use in many disparate 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 and 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

Following is a list of some important identity management terms and concepts and their definitions:

- **Account Provisioning**: The process of creating an account for a given application and network identity, and managing the account's entitlements to allow and control its access to the resources managed by the application

- **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. OCA is another type of assertion service, because the X.509v3 certificates it generates are indeed assertions about a network entity'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 network entity. A network entity can have many different accounts that it uses to access various applications in the network. These accounts can be identified by these applications by different attributes of this entity. For example, a user can be known in the e-mail service by his or her e-mail ID, whereas that same user can be known in the human resource application by his or her 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 network entity. The information can be used by the identity management infrastructure itself to determine administrative privileges.

- **Identity Database**: A specialized database service designed to hold and manage identity information

- **Identity Management Policies**: Policies affecting the management of identities in an enterprise which includes naming policies and security policies

- **Identity Management 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

- **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 other services that the entities access.

- **Identity Provisioning**: The act of establishing the identity of a network entity and the necessary credentials to facilitate authentication of the identity

- **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.

- **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.

These terms are used to describe the identity management concepts included in the next section.

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 blueprint for administrators of a typical application integrated with Oracle Identity Management. It provides a framework for understanding the roles of the various Oracle Identity Management components and services, and provides a basis for understanding how to engineer secure application deployments in an enterprise environment.

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

Figure 2–1   Application Integration Model
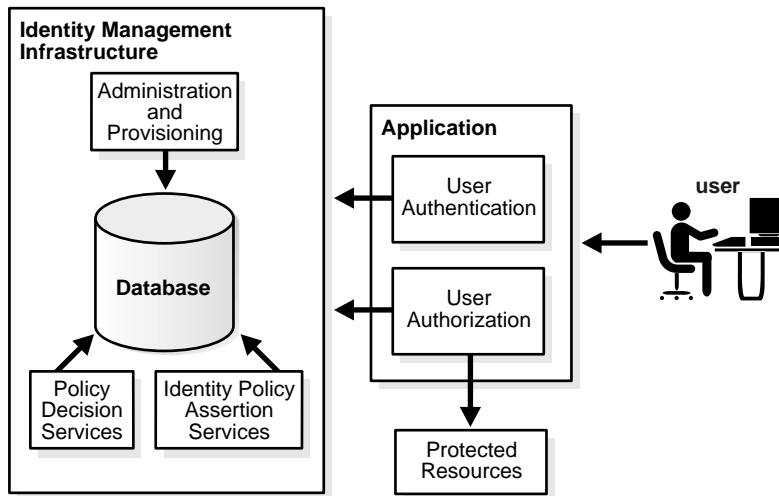
In this model, the following essential services are performed by the identity management infrastructure:

- **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**: Although these services are typically performed by the application, such as OracleAS Portal, in Oracle Identity Management, 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 Oracle Application Server 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 is performed by the application based on identity information managed in the identity management infrastructure. For example, a J2EE application uses Oracle Application Server Java Authentication and Authorization Service (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 Life Cycle
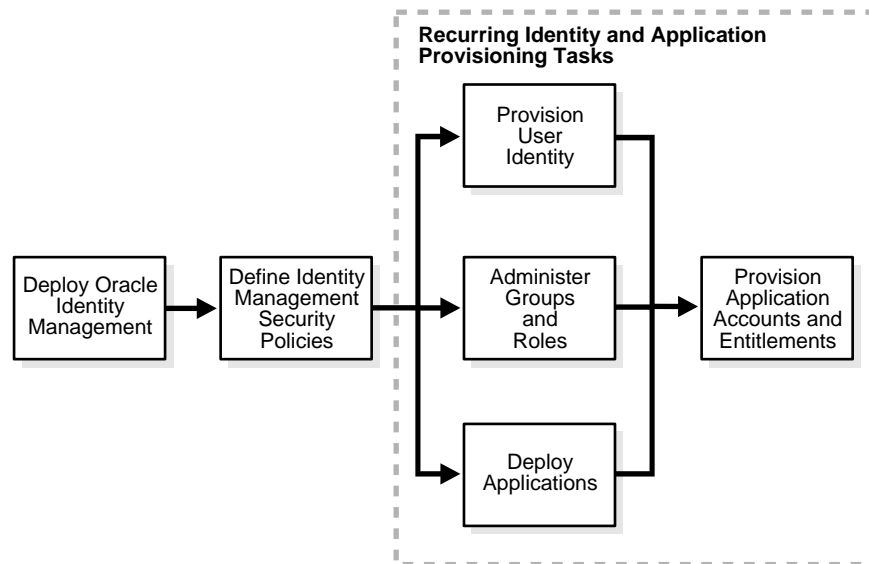
Following is a description of the provisioning flow shown in Figure 2–2:

1. The first step is the deployment of the Oracle Identity Management infrastructure using the product's installation and configuration tools.

2. The next step is to define the identity management security policies. These policies determine what data users and applications can access. They are codified as access control lists (ACLs) in Oracle Internet Directory, and are typically managed using Oracle Directory Manager.

3. The following three activities typically take place on an ongoing basis. Each of these activities can happen in parallel, and in no particular order.

   - User identities are provisioned in Oracle Internet Directory. These identities can come from multiple sources, including human resources applications, user administration tools (such as the Oracle Internet Directory Self-Service Console), through synchronization with other directories, or through directory 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 account provisioning. This can be performed manually using application administration tools or in an automated fashion through provisioning integration.

Administrative Delegation

Oracle Identity Management requires a centralized repository for the enterprise users, groups, and services. Business requirements, however, make it difficult to manage a centralized store 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 various administrators, and satisfy the different security requirements, the identity management system needs delegated administration.

With delegated administration, the management of the 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, Oracle9*i* Database Server, Oracle E-Business Suite, and Oracle Collaboration Suite—supports a security model that is appropriate for its design. Nevertheless, they all employ 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
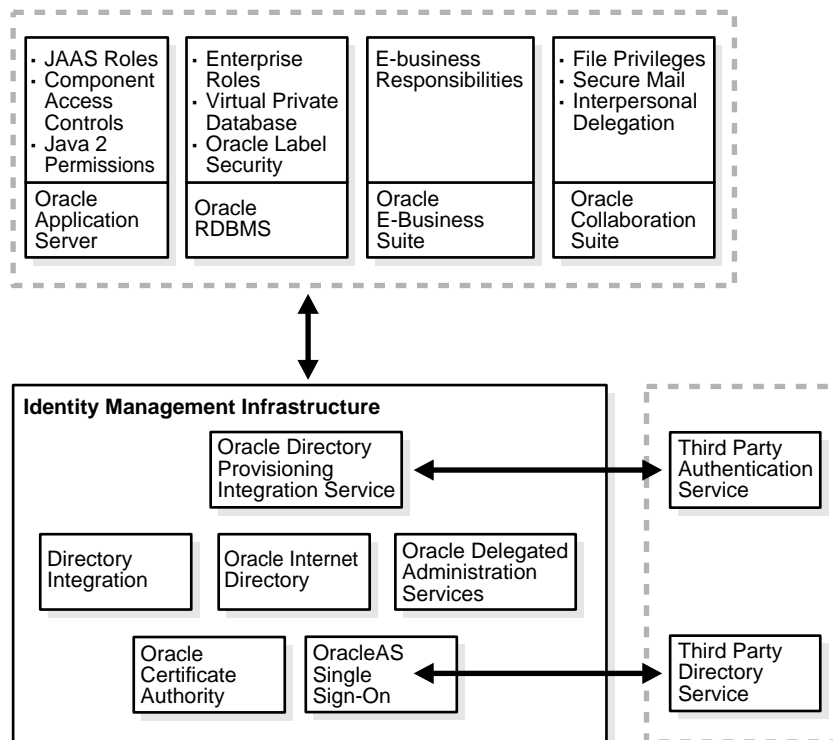
Oracle Application Server supports a J2EE compliant security service called Java Authentication and Authorization Service (JAAS). JAAS can be configured to utilize users and roles defined in Oracle Internet Directory.

Similarly, the database security capabilities—Enterprise User and Oracle Label Security—provide the means to leverage 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.

The Oracle E-Business Suite and Oracle Collaboration Suite application stacks are layered over the Oracle9*i* Database Server and Oracle Application Server platforms, providing a level of indirect integration with the Oracle Identity Management infrastructure. In addition, these products have independent features that rely upon 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 leverage Oracle Directory Integration and Provisioning to automatically provision and de-provision user accounts and privileges. Oracle Delegated Administration Services is employed extensively for self-service management of user preferences and personal contacts. Also, the security management interfaces of these products leverage the user and group management building blocks called service units.

3

Oracle Identity Management Deployment Planning

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

This chapter contains the following sections:

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

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 you should follow when planning an identity management deployment.

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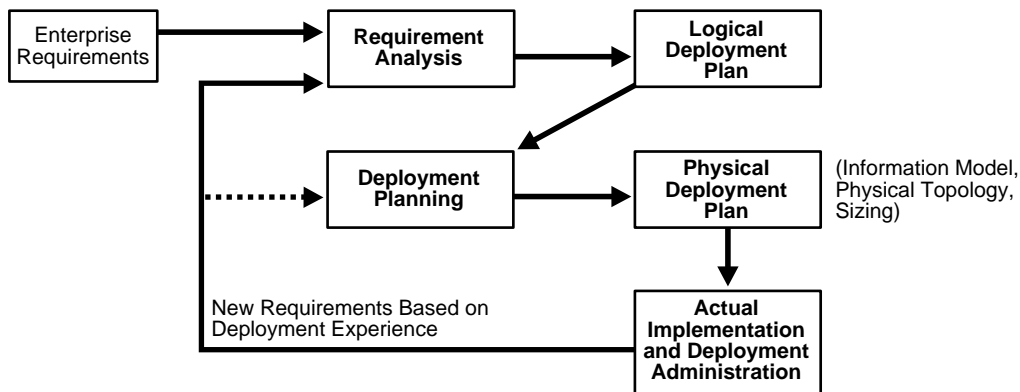
As shown in Figure 3–1, the deployment planning process is iterative. Based on the initial requirements, you perform high-level planning to create a logical deployment plan, and you use the logical deployment plan to perform detailed deployment planning and create the physical deployment plan for the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

Requirement Analysis

This section describes some of the typical enterprise requirements that must be analyzed when planning an Oracle Identity Management deployment. The requirements include process issues, functionality requirements, and high availability concerns. At the end of this analysis phase, you will decide on a high level logical deployment plan for the Oracle Identity Management infrastructure.

This section contains the following topics:

- High-Level Enterprise Requirements
- Translating Requirements into a Logical Deployment Plan
- Summary of Requirement Analysis

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 a small Oracle deployment, 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 the sharing of services across a variety of Oracle and third-party applications, and typically create a central group,

comprised of application, network, and security administrators, to be 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.

Oracle Internet Directory and OracleAS Single Sign-On provides basic identity management services and Oracle Delegated Administration Services is the primary means for user password self-service. Given these considerations, plan on implementing Oracle Internet Directory, OracleAS Single Sign-On, and Oracle Delegated Administration Services

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

Even if you are not using third-party directories, you should still consider deploying Oracle Directory Integration and Provisioning services because many Oracle products, such as OracleAS Portal and Oracle Collaboration Suite, leverage 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 leverage 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 smaller Oracle installation and pre-production environments, application administrators can install minimal instances of the Oracle Identity Management infrastructure to support their Oracle applications.

> **See Also:** *Oracle Application Server 10g Administrator's Guide* for guidelines of such installations

Finally, many organizations already have in place, or have plans to deploy, other identity management components. Oracle Identity Management is designed to leverage other enterprise identity management solutions as well as any applications you already have for provisioning and administering your enterprise environments.

Any Oracle components requiring identity management are supported by an Oracle Identity Management instance, which 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. An enterprise 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. The location and contents of the user entries in the overall directory information tree (DIT) must be planned prior to deploying Oracle Internet Directory and other identity management infrastructure components.

In application service provider (ASP) deployments where centralized identity management is required, different identity management realms must be created for the ASP administrators, as well as the users of each of the ASP customers (subscribers).

Considering Centralized Security Management Requirements

With the growth of e-business and enterprise applications, IT organizations need to consider how to reuse user profile information. Also, they have to provide access to

a growing number of users, both inside and outside the corporation, without diminishing security or exposing sensitive information. The administration of multiple versions of user identities across multiple applications makes the task even more daunting. A central identity management infrastructure should therefore be considered 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 enterprise application deployment requirements:

- **Type of users that the application serves**: It may be necessary for enterprise applications, such as OracleAS Portal, to be internet accessible for external (internet) users, such as business partners, in addition to internal (intranet) users. As a result, consider whether to use one Oracle Internet Directory to represent the user identities, or a separate Oracle Internet Directory to represent each group of user identities.

- **Application load requirements**: Application load and availability requirements indicate the high availability deployment requirements of the identity management infrastructure

- **ASP requirements**: Apart from the identity management deployment, consider the application-mandated requirements for ASP deployments

Considering Administrative Autonomy Requirements

- **Departmental autonomy for deployment of new applications**: For many large enterprises, it may be necessary to facilitate 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**: An important consideration in identity management planning is the security policies for all the employees of a given business. It should be possible to manage the identity of the users according to common privileges defined by the security policies of the enterprise. Consider the administration models for managing the identity, roles, policies, and groups to suit the enterprise requirements.

- **Administrative autonomy for individual applications deployed against the identity management infrastructure**: 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. Also, one must define which users need access to which resources and at what level of security. To meet the needs of these various administrators, and to satisfy the different security requirements, consider the administrative controls requirements.

Considering Security Isolation Requirements

There may be enterprise applications deployed, such as OracleAS Portal, that are required to be accessible by both employees and non-employees. Even though the application is shared by both internal and external users, it is important to ensure that corporate intranet resources are completely isolated from non-employees, and that intranet applications are protected from potential denial of service attacks aimed at the extranet portal. In such deployments, security separation may be necessary between the enterprise and non-enterprise identity management infrastructures.

Due to organizational constraints and high-level executive mandates, it may be necessary to consider deploying separate identity management infrastructures for different environments in order to maintain a clear demarcation 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.[1]

Considering Third-Party Identity Management Integration Requirements

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

- **Windows integration**: If an enterprise is using Microsoft Windows infrastructure 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 the Oracle Internet Directory, and integrating OracleAS Single Sign-On authentication.

---

[1] 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.

■ **User provisioning**: User provisioning refers to the process by which new users are added to and deleted from the various enterprise systems. New user provisioning can potentially be done 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 user provisioning creates the required user account *profiles* in other enterprise applications.

If an enterprise has deployed enterprise applications such as HR and CRM, consider the user provisioning integration functionality 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**: In deployments where it is necessary for application users to access a combination of applications integrated with Oracle Identity Management, in addition to applications integrated with a third-party directory and 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 that work together to provide the services. For the identity management infrastructure to provide all essential services, all of the required components must be available. Any high availability solution must be able to detect and recover from any software failures of any of the processes associated with the identity management components. As high availability requirements depict the deployment configurations, these requirements should be considered as part of the deployment planning.

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

"Planning the Physical Network Topologies" on page 3-30 lists canonical physical topologies that implement the requirements, such as high availability, scalability, and performance.

Translating 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 of Serving Internal and External Users

- Model of Providing Administrative Autonomy for Departmental Applications

- Model of Integrating Oracle Identity Management in a Windows Environment

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 single centralized identity management infrastructure is deployed and administered by a central group within an organization. As instances of enterprise applications are deployed, they leverage 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 across an assortment of 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
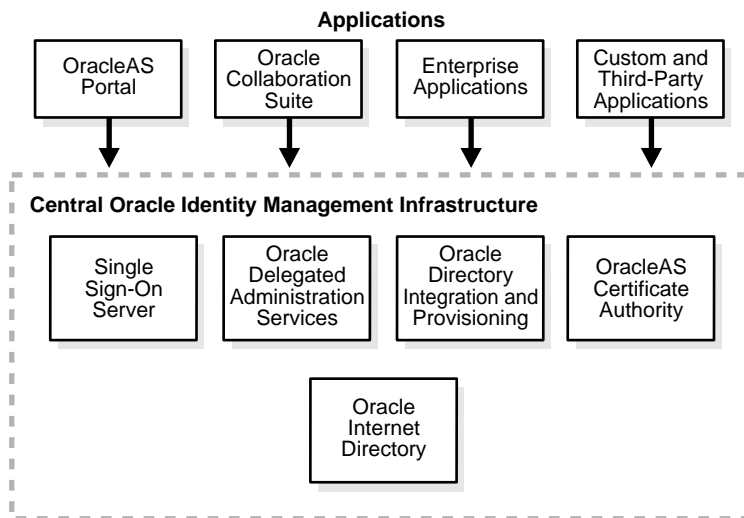
Model of Serving Internal and External Users

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

The following two 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 user information is modeled 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
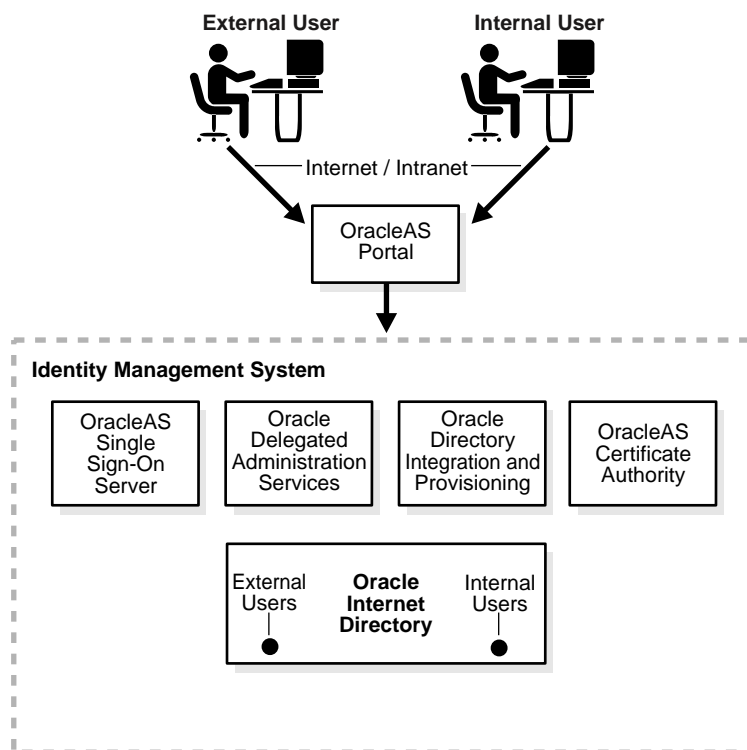
Example B: Using two identity management infrastructures—security isolation

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 demarcation between internal and external user repositories. There is added availability if internal resources are not exposed to the external traffic.

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 non-sensitive profile information is synchronized with the enterprise directory, however intranet application identities and associated metadata are not replicated. Non-employee 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. The information model should be the same in both the 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:** Employees 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: Provides the security environment isolation between groups of applications that require isolation among them, such as extranet and intranet environments

- Accessibility: Applications are accessible to internal and external users and are served by 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
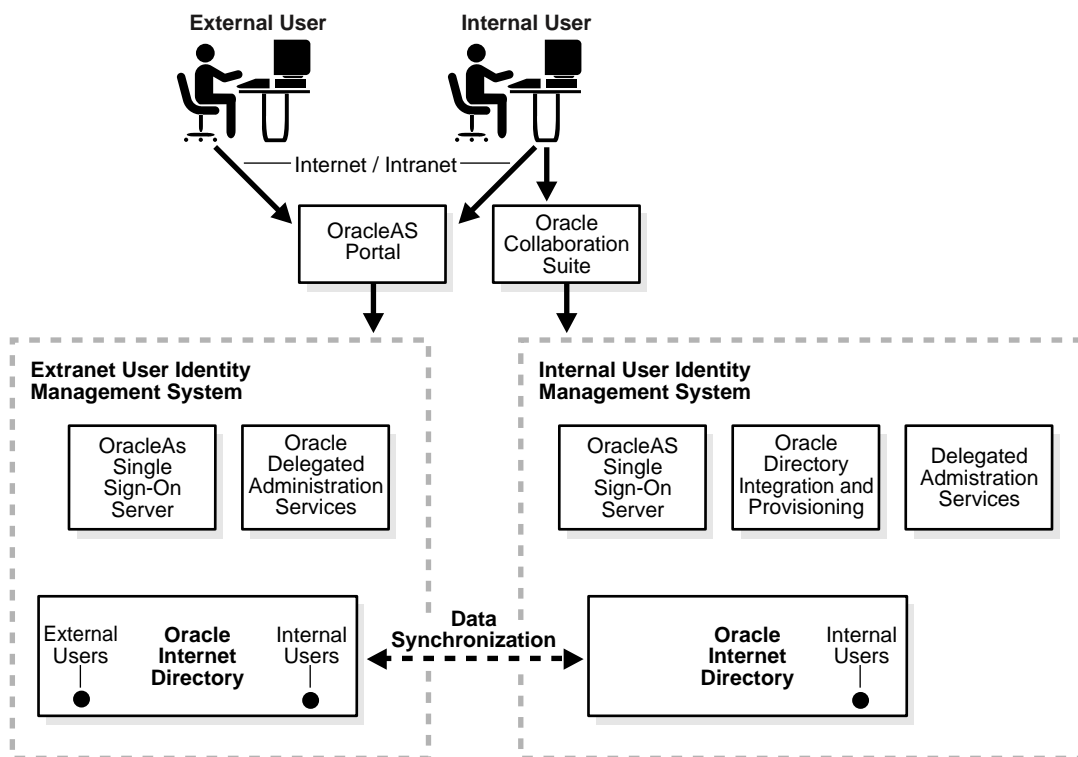
Model of Providing Administrative Autonomy for Departmental Applications

For many large enterprises, it may be necessary to facilitate 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 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 the departmental autonomy for maintaining the application data, as shown in Figure 3–5. A centralized singler 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 against a separate departmental Oracle Internet Directory server, but they use a central identity management service for authentication. Departmentally, 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 experience across all applications

Figure 3–5 Central Single Sign-on and Departmental Autonomy
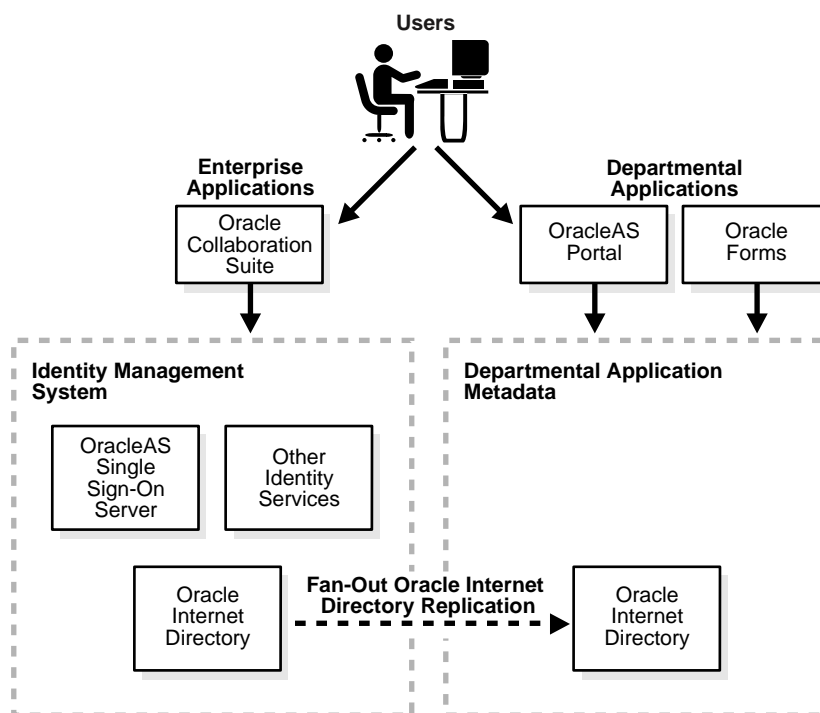
Example B: Departmental identity management system

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 against a separate departmental Oracle Internet Directory and OracleAS Single Sign-On service. Departmentally, local administrators manage the departmental applications.

In this model, the user gets the unified login and logout experience for applications within each department, only. However, 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
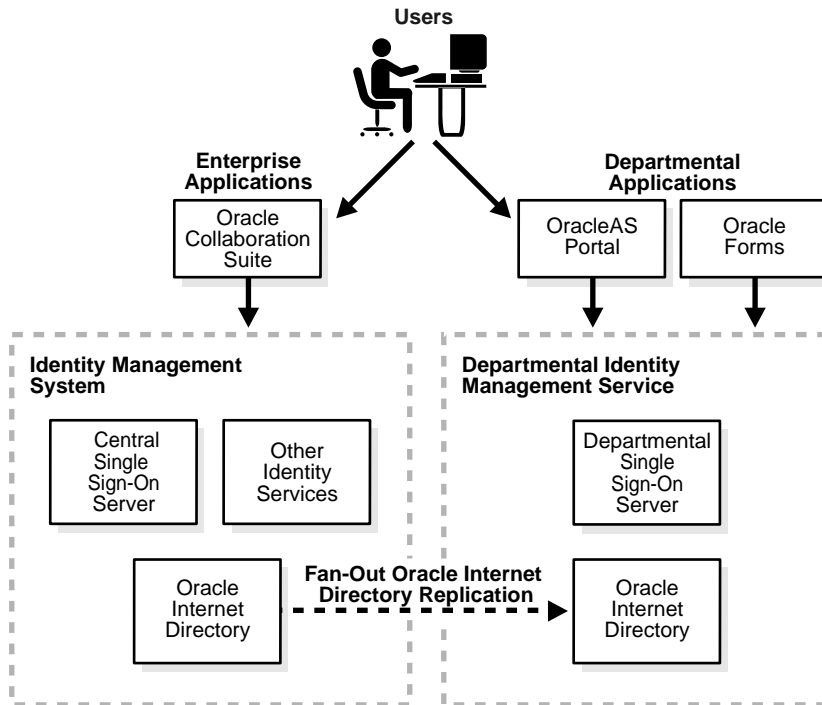
Model of Integrating Oracle Identity Management in a Windows Environment

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 account footprint 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
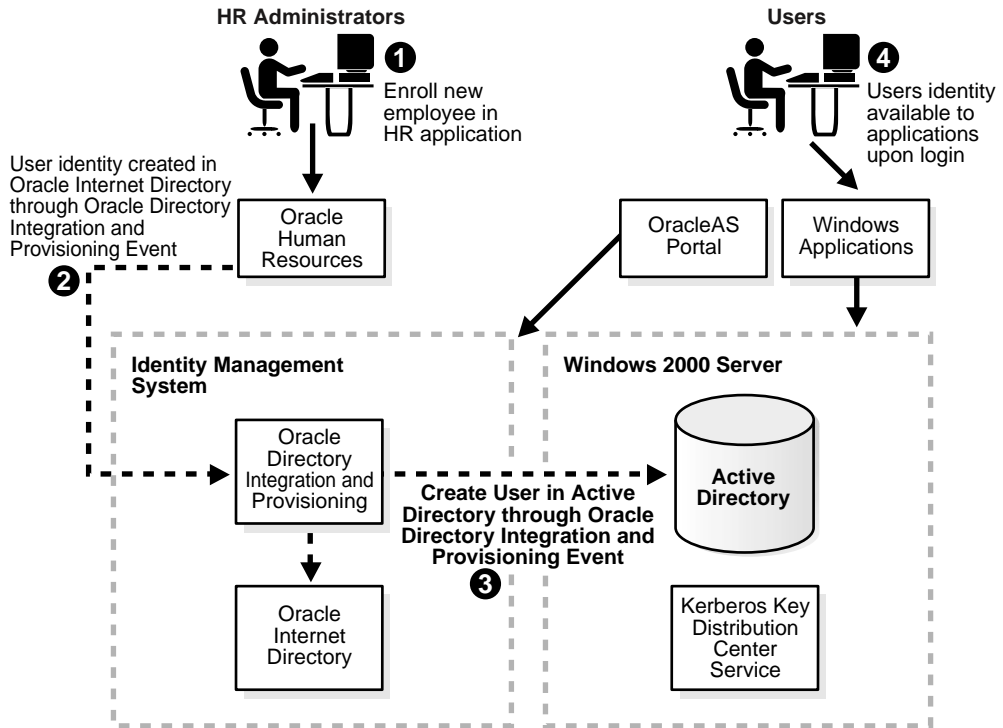
Example B: Integrating with Windows user provisioning

If an enterprise has deployed Windows 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 under a default realm in Oracle Internet Directory. If there are multiple Active Directory domains in an enterprise deployment, they are modeled 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 they successfully log in to a Kerberos-enabled Windows desktop. In cases where Windows Kerberos authentication is not possible, the 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
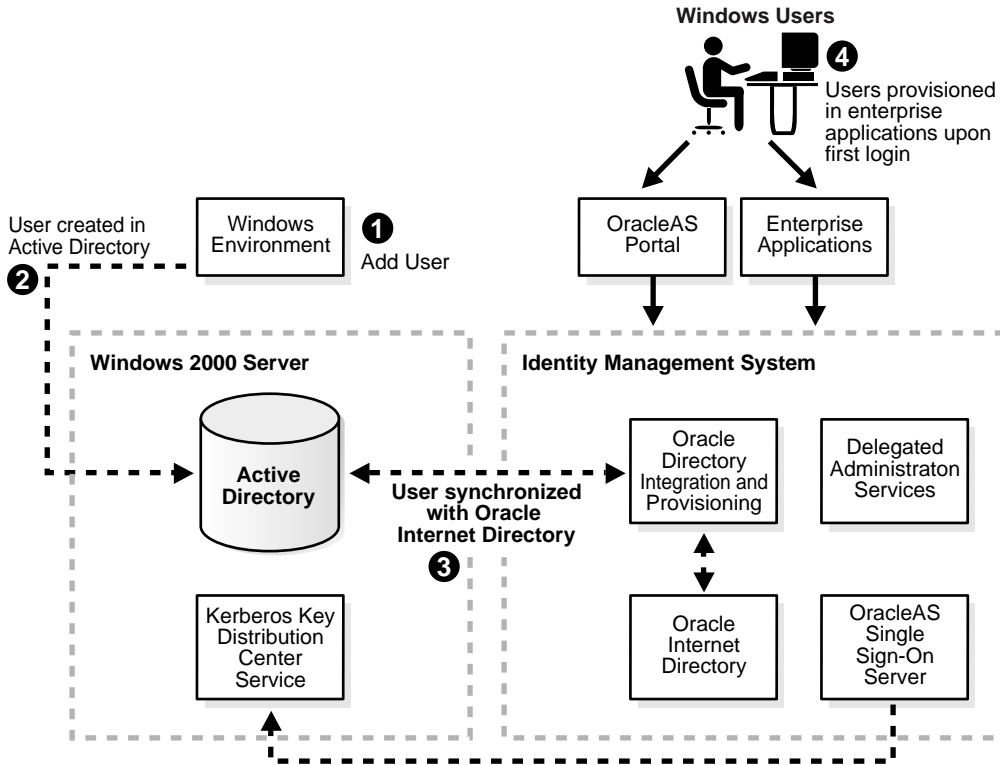
Deploying Central Identity Management Infrastructure in Application Service Provider Hosting Environments

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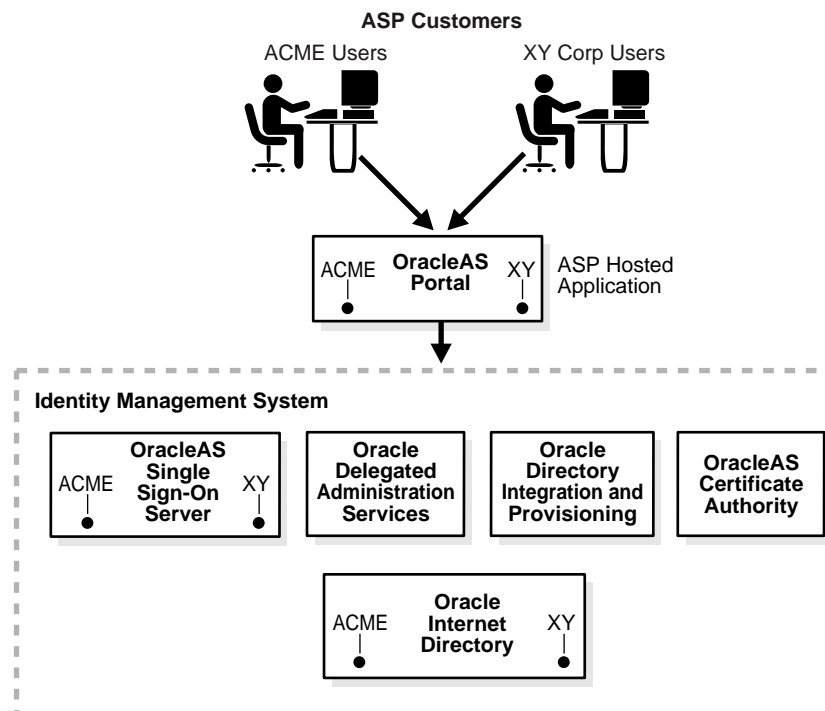
As shown in Figure 3–9, the ASP users, defined in the default identity management realm, manage various applications hosted for the subscribers. Each subscriber has an associated identity management realm where the ASP manages its users, groups, and associated policies.

Summary of Requirement Analysis

This section outlined a number of requirements and considerations that a typical enterprise deployment should consider as part of the high level planning exercise. It also described 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 serves as the basis for the detailed deployment planning that is outlined in the next section.

Detailed Deployment Planning

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 contains the following topics:

- Planning the Logical Organization of Directory Information
- Planning the Physical Network Topologies
- Summary of Detailed Deployment Planning

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 serves their needs and use it as a deployment planning guide.
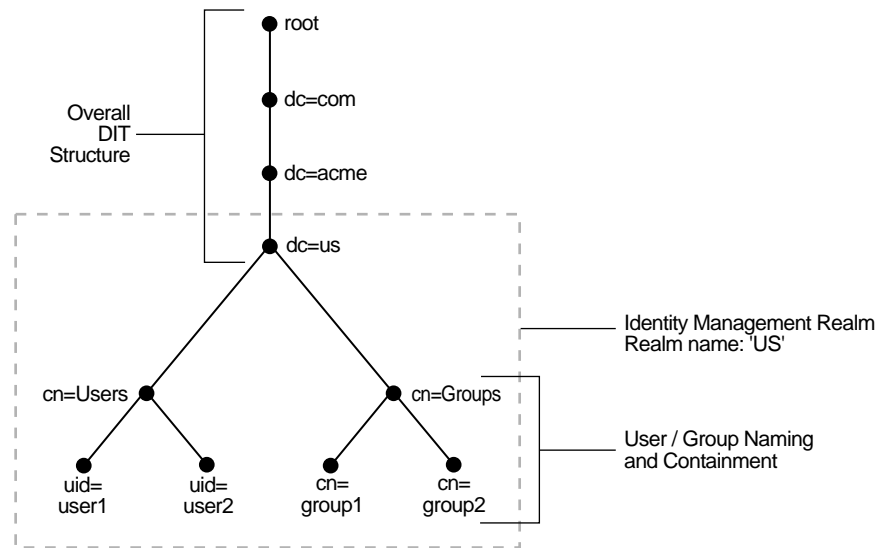
Figure 3–10   Oracle Internet Directory Information Tree

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. Since 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 serves as 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 facilitates the implementation of 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

This section contains the following topics:

- Planning the Overall Directory Information Tree Structure

- Planning User and Group Naming and Containment

- Planning the Identity Management Realm

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 is integrating 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 much more manageable.

- In a single enterprise scenario, choosing a DIT design that aligns with the DNS 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.

- If an enterprise has deployed an X.500 directory service and has no other third-party LDAP directories in production, it 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.

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`: The name of a country
- `dc`: A component of a DNS domain name
- `l`: The name of a locality, such as a city, county, or other geographic region
- `o`: The name of an organization
- `ou`: The name of an organizational unit
- `st`: The name of a state or province

A common mistake in DIT design is to try to reflect either the corporate divisional structure or organizational structure. Usually, this is not recommended because most corporations undergo frequent divisional restructuring and reorganization. It is important to insulate the corporate directory from organizational changes as much as possible.

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 modeling 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 any particular user's identity. The location and contents of these entries in the overall DIT must be planned by the enterprise prior to 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, subdividing the users into containers based on these administrative boundaries is recommended to simplify the setting of access controls and also help 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 problematic. Instead, you should 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 exploit this administrative infrastructure and use its policies.

- All user entries created in the directory should belong to the following object classes: `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 that are created by the deployment in Oracle Internet Directory. Like 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 Corporation 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 leverage 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, subdividing 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 an infinite number 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.
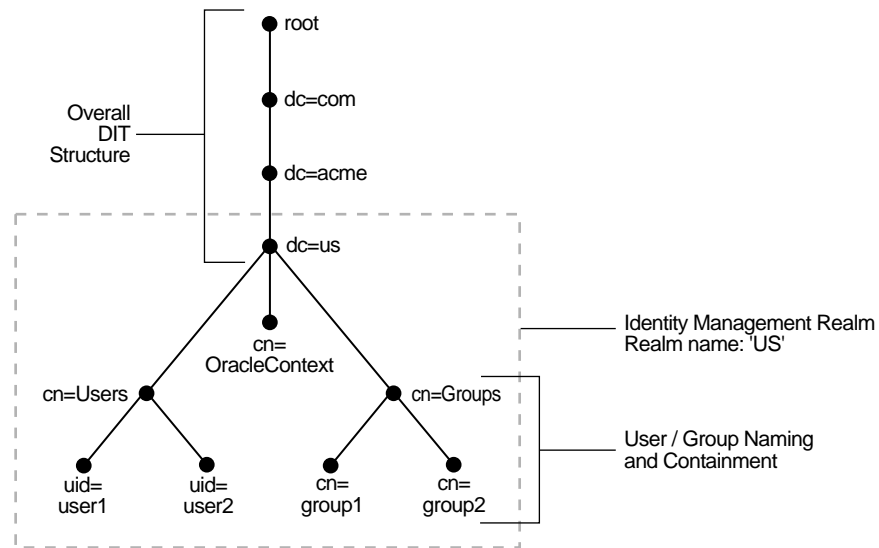
The identity management realm in Oracle Internet Directory captures this deployment intent and also enables the deployment to set identity management policies relevant to the enterprise users and groups.

> **See Also:** "Identity Management Terminology" on page 2-2 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 only require 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 a few 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 A, "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. There are options, such as Oracle Application Server Active Failover Cluster (Active Failover Cluster), available for individual identity management infrastructures to achieve 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 the canonical physical topologies of an identity management infrastructure 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.

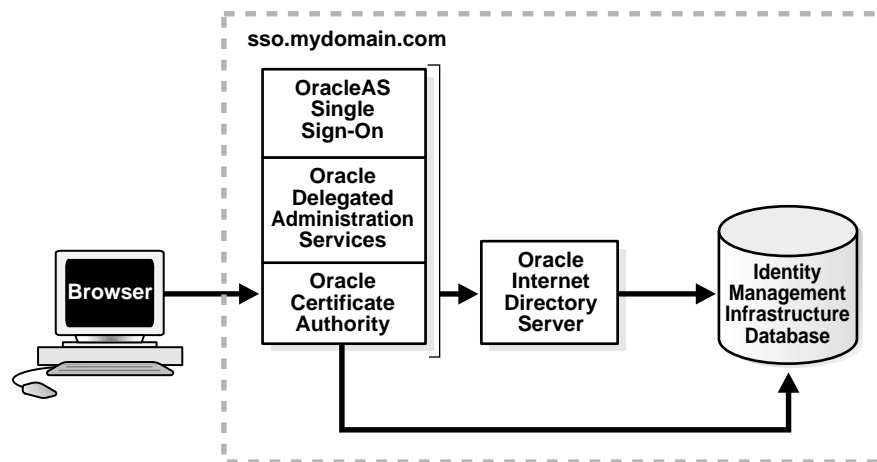This section contains the following topics:

- 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
- Identity Management Infrastructure Deployment on Active Failover Cluster

- Replicated Identity Management Infrastructures
- Application Deployments in Replicated Directory Environments
- Geographically Distributed Identity Management Infrastructure Deployment
- Disaster Recovery Deployment for Identity Management Infrastructure

Identity Management Infrastructure Default Deployment

A default installation of the Oracle Application Server infrastructure consists of installing 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

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 can specify that the entire OracleAS Single Sign-On server not be exposed to the public network. In this case, the deployment is split to deploy the Oracle Application Server infrastructure middle

tier in the DMZ, and Oracle Internet Directory and its underlying database within the intranet firewall, as shown in Figure 3–13.

Since 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 provides security isolation between the infrastructure middle tier and Oracle Internet Directory and its underlying database.

Network level encryption should be provided between the Oracle Application Server Certificate Authority middle tier and the Oracle Application Server Certificate Authority repository to provide 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
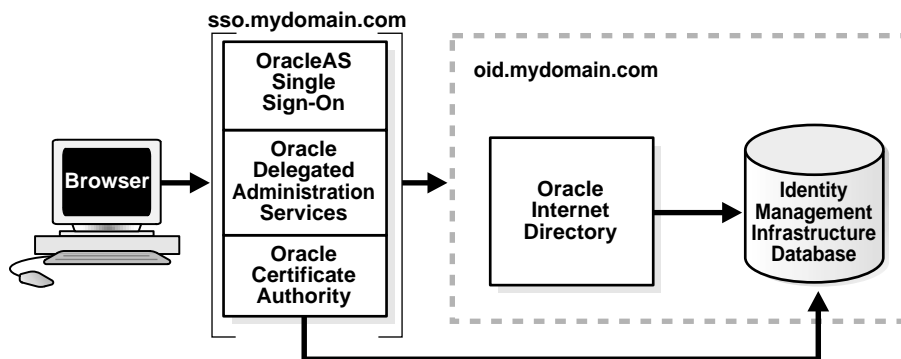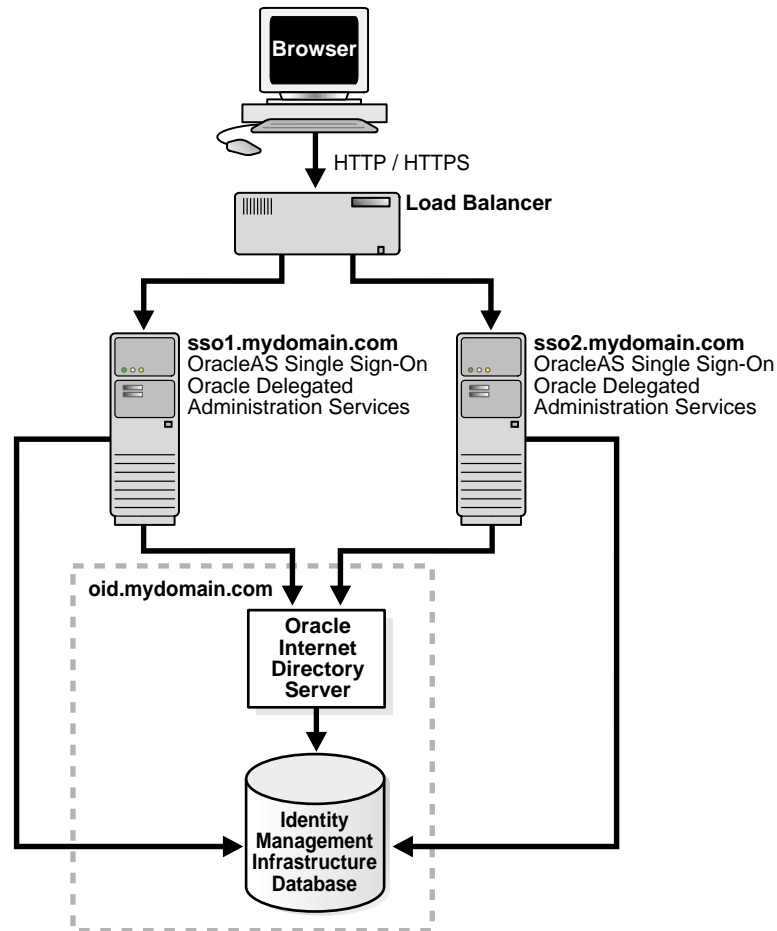

Identity Management Infrastructure Deployment Using Multiple Middle Tiers

For highly available deployment requirements, multiple OracleAS Single Sign-On and Oracle Delegated Administration Services middle tiers can be deployed 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 3–14, provides increased scalability by adding more infrastructure middle tiers.

Figure 3–14 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. Examples of such failures are a system panic or node crash.

Figure 3–15   Oracle Internet Directory Deployment Using Cold Failover
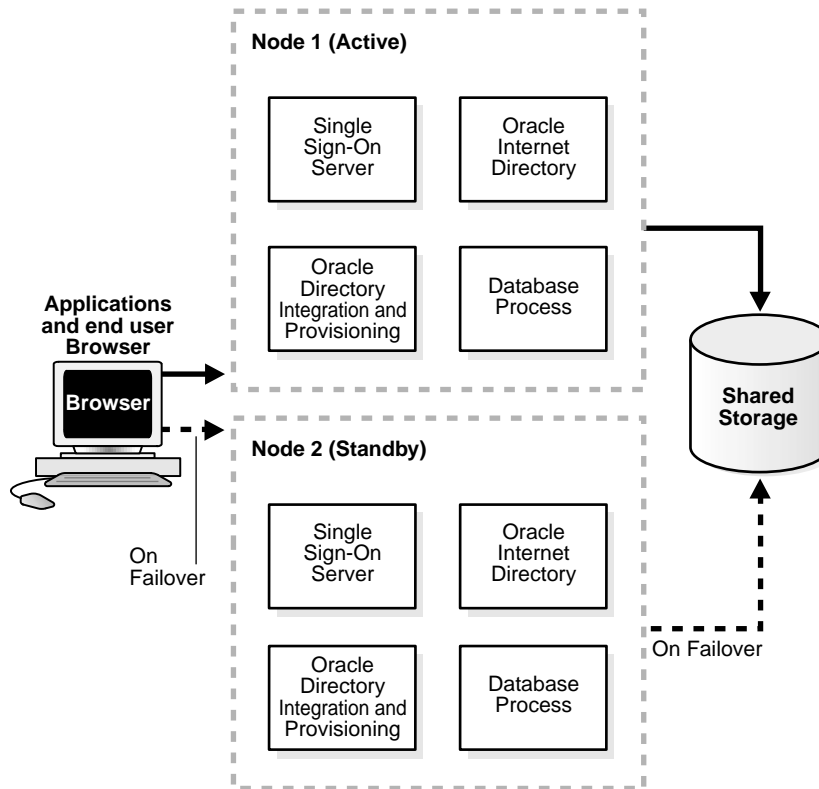
A two node hardware-based cluster is used to achieve high availability. As shown in Figure 3–15, the two nodes are attached to shared storage and a virtual logical IP address is active on one of the physical nodes (Node 1). Hence, Node 1 is the primary or active node. Only one Oracle Identity Management infrastructure is installed on a shared storage disk that can be accessed by both the physical nodes.

If the primary node fails, the logical IP address is moved over to the secondary node. All the infrastructure processes are then started on the secondary node. The application processes accessing the identity management infrastructure will see a temporary loss of service as the logical IP and the shared storage are moved over, and the database, database listener, and all other processes are started.

The cold failover solution provides high availability with some loss of service during the failover.
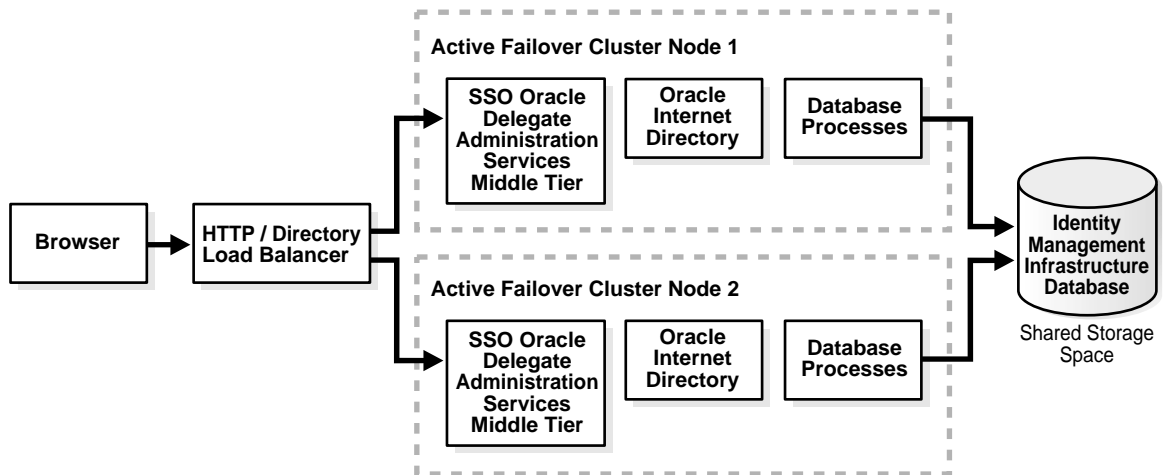
Identity Management Infrastructure Deployment on Active Failover Cluster

Oracle Application Server supports installation of the Oracle Application Server infrastructure on Active Failover Cluster. The default Oracle Application Server infrastructure installation installs all the infrastructure components on one Active Failover Cluster node: OracleAS Single Sign-On (including Oracle Application Server Containers for J2EE and Apache), Oracle Delegated Administration Services, Oracle Internet Directory, and the database, as shown in Figure 3–16.

A load balancer for HTTP and Oracle Internet Directory is used for failover access. OracleAS Single Sign-On provides database failover using JDBC failover support. Oracle Internet Directory can be configured with two types of database failover mechanisms: connection time failover and transparent application failover.

Active Failover Cluster deployment provides the high availability and failover access for the OracleAS Single Sign-On middle tier, Oracle Internet Directory server, and database.

Figure 3–16   OracleAS Single Sign-On and Oracle Delegated Administration Services Deployment on Active Failover Cluster

Replicated Identity Management Infrastructures

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 in replication to provide the highly

available Oracle Internet Directory server for middle tier access, as shown in Figure 3–17.

This deployment should be planned prior to 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 (state full) 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.

Multimaster Oracle Internet Directory replication networks provide 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 front-ending the network of replicas with appropriate load balancers or routing elements that can be configured such that if any Oracle Internet Directory node becomes unavailable, the applications are transparently failed-over to alternative nodes in the network

- **Load balance**: Achieved by employing 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
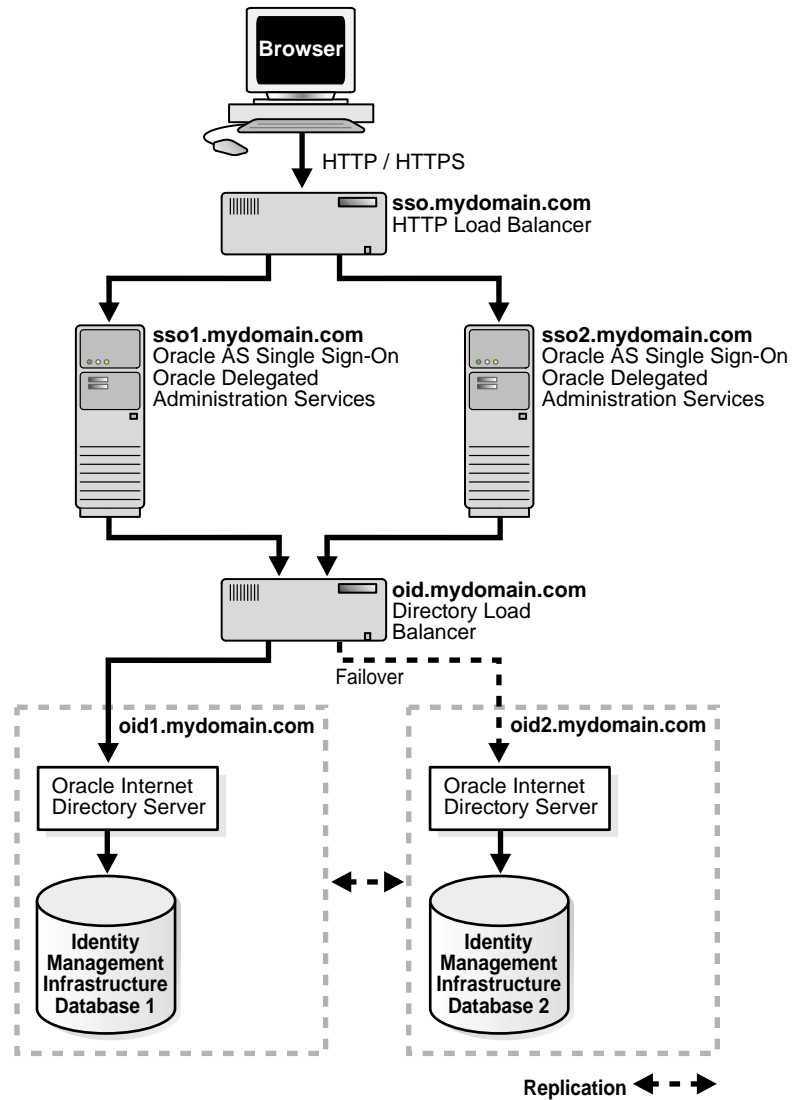
Application Deployments in Replicated Directory Environments

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 in real time.

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 application user experience 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 multi-master 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 against 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 be temporarily failed over to alternate masters.

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

— Data recovery for any given category of data becomes more manageable since 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.

— 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.

— Uniform load distribution is acceptable only for non-critical operations, such as end user 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 would ensure 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 password reset should share the same Oracle Internet Directory instance. Otherwise, a user could reset the password and find that he or she is unable to sign on because the OracleAS Single Sign-On server is connected to a different Oracle Internet Directory server from where the password change was 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.

— When there is an outage in any part of the directory network or when there is 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

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

Considering the above guidelines, Figure 3–18 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 primary and Replica A as the failover server.

Figure 3–18   Enterprise Applications Configured in a Replicated Environment
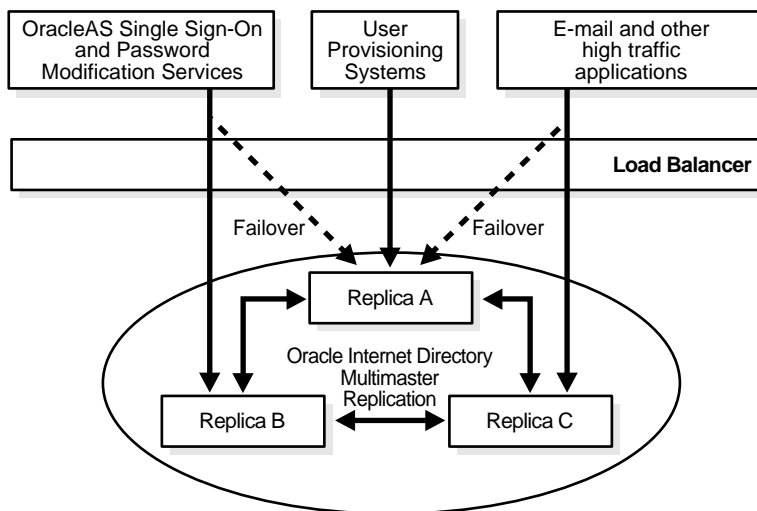
Geographically Distributed Identity Management Infrastructure Deployment

Enterprises with geographically distributed operational branches want to set up multiple OracleAS Single Sign-On instances distributed across the different geographical locations to authenticate users locally. This deployment, shown in Figure 3–19, 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 geographical 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 database are set up in replication, each OracleAS Single Sign-On site uses its own Oracle Internet Directory and database 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, the Oracle Internet Directory and OracleAS Single Sign-On servers are reconfigured to point to a database 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 3–19   Geographically Distributed Deployment
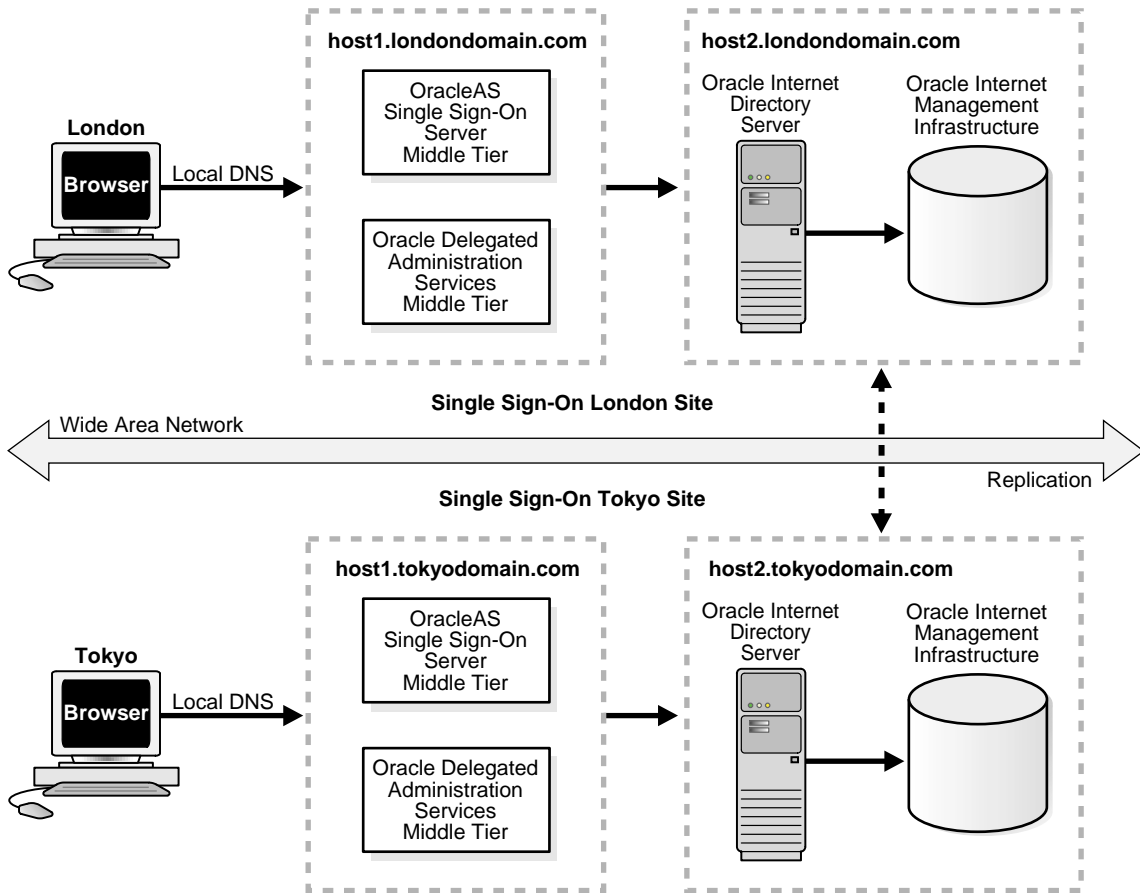
Disaster Recovery Deployment for Identity Management Infrastructure

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
database and configuration files, in addition to replacing hardware or
subcomponents. The most stringent requirement is to keep the services running
despite the 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 3–20 Oracle Internet Directory Deployment Using Oracle Data Guard
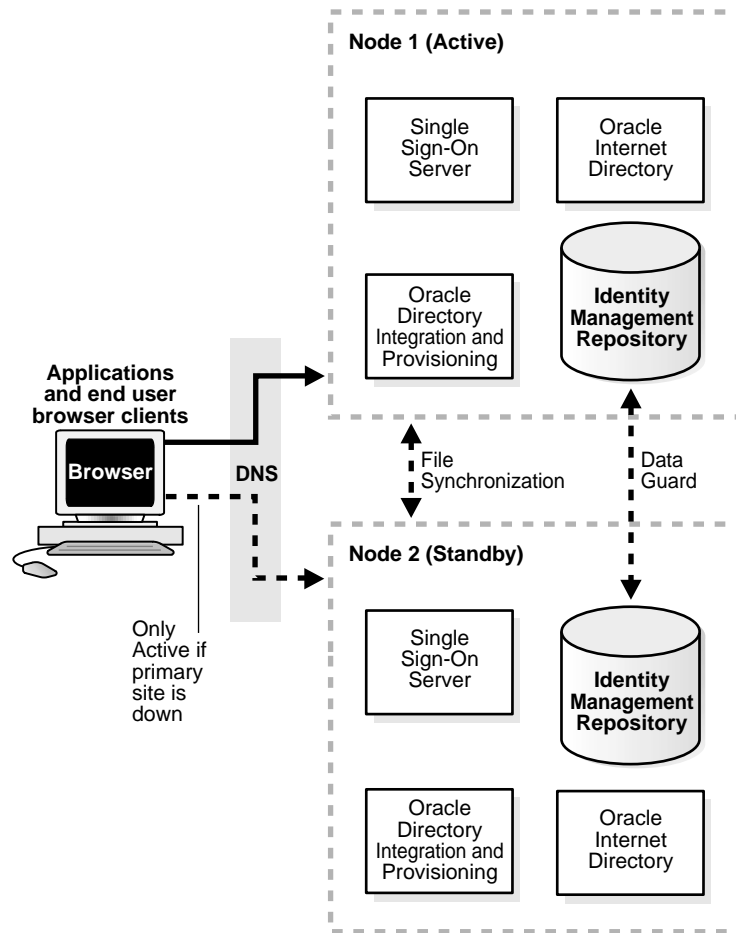
Identical software, such as a single instance of the identity management infrastructure, can be run in multiple data centers with Oracle Data Guard to protect against data center disaster. Oracle Data Guard also provides single-instance directory data recovery and transparent failover.

As shown in Figure 3–20, Oracle Data 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 database node.

During disaster recovery, the standby is switched to become 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 Corporation recommends deploying Oracle Application Server Certificate Authority on a separate host with its own repository. Other components of the Oracle Identity Management infrastructure can use any of the configurations described elsewhere in this document.

The Oracle Application Server Certificate Authority host 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 repository for Oracle Application Server Certificate Authority should be secured with database securing guidelines

- Oracle Application Server should be secured

- Turn on repository database auditing

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

Summary of Detailed Deployment Planning

This section described the details of planning the directory information tree and listed 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 always 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 wherever necessary.

> **See Also:**
>
> - "Related Documents" in the Preface

4

Oracle Identity Management Administration and Usage

This chapter describes how to administer and use the Oracle Identity Management infrastructure, as a whole, including administering users with the 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
- Oracle Identity Management Administration Delegation

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 Infrastucture
- Managing Individual Oracle Identity Management Components
- Managing Enterprise Data in the Oracle Identity Management Infrastructure

Routine Monitoring of the Oracle Identity Management Infrastucture

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	Addtional References
Monitoring the health and performance of the Oracle Internet Directory server	■ Oracle Enterprise Manager Central Console (Central Console) ■ LDAP command line tools	*Oracle Internet Directory Administrator's Guide*
Monitoring the health of Oracle Directory Integration and Provisioning	Central Console	*Oracle Internet Directory Administrator's Guide*
Monitoring the health of Oracle Delegated Administration Services	Central Console	*Oracle Internet Directory Administrator's Guide*
Monitoring the health of OracleAS Single Sign-On	Central Console	*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	■ Central Console ■ `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	■ Central Console ■ `oidctl` command line tools	*Oracle Internet Directory Administrator's Guide*
Configuring Oracle Directory Integration and Provisioning	■ Oracle Directory Manager ■ Directory Integration Platform Assistant	*Oracle Internet Directory Administrator's Guide*
Starting and stopping Oracle Delegated Administration Services	■ Central Console ■ `opmctl` command line tools	■ *Oracle Internet Directory Administrator's Guide* ■ *Oracle Application Server 10g Administrator's Guide*
Configuring Oracle Delegated Administration Services	Oracle Delegated Administration Services Configuration tab	*Oracle Internet Directory Administrator's Guide*
Starting and stopping OracleAS Single Sign-On	■ Central Console ■ `opmctl` command line tools	■ *Oracle Application Server Single Sign-On Administrator's Guide* ■ *Oracle Application Server 10g 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	Additonal 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 10g 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*

Oracle Identity Management Administration Delegation

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.

Since 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 end 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 end 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
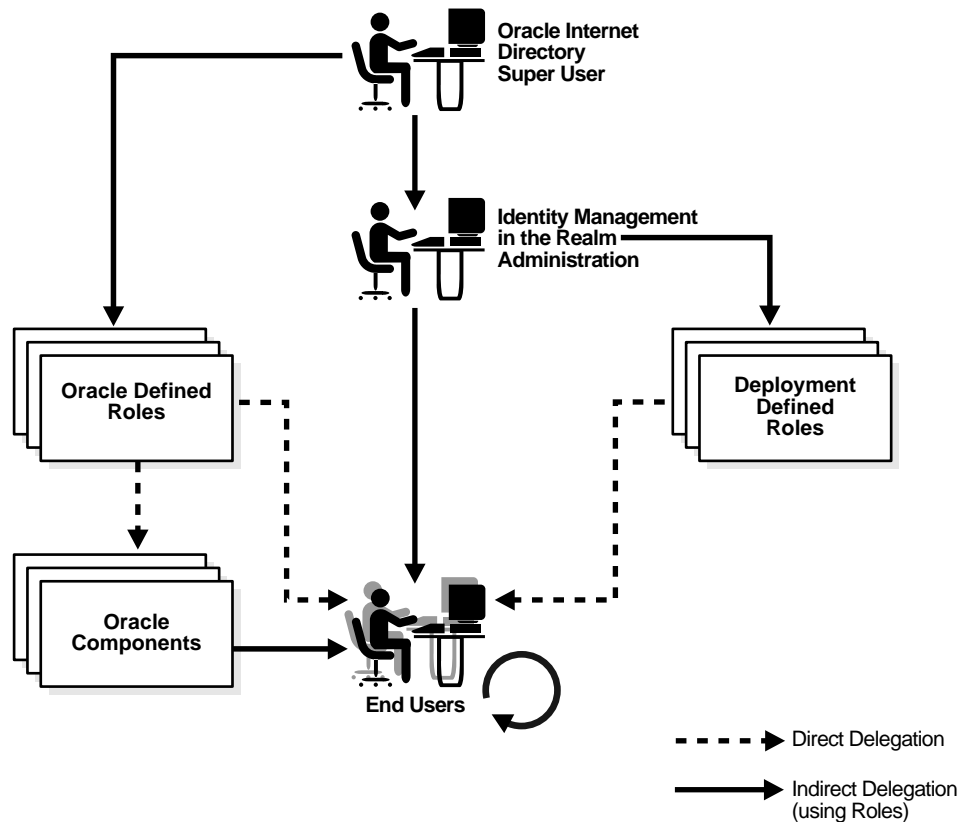
Delegating Component Deployment and Administration

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 in order 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
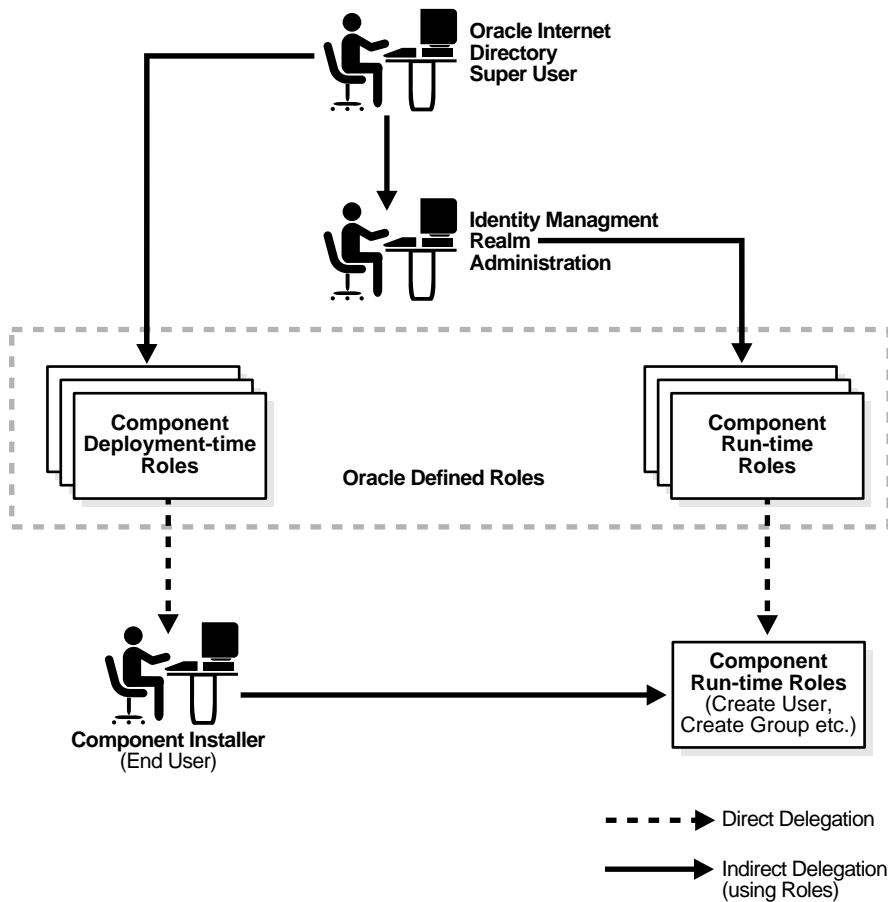
In Figure 4–2, note that the super user grants certain deployment privileges to groups, which, during the deployment process, are granted to certain users for installing specific Oracle components by making them members of those groups. As part of the installation process, the component installer then 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 coarse and fine-grained 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 the 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 the groups, they should not be required to understand the various steps required to implement group management and the directory 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/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:

- Motivations for Integration
- Integration Tools and Strategies

Motivations for 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 leverage 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 potentially be driven 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 user provisioning creates the required user account *footprints* in other enterprise applications.

- **Centralized user administration**: Once a user account is created, it must be maintained and administered. Centralized user administration ensures that all of the 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 to provide their users with a transparent runtime experience. This means that the various applications in the enterprise environment must be capable of leveraging 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 Internet Directory Administrator's Guide* and *Oracle Application Server Single Sign-On Administrator's Guide* for information about deploying these integration solutions

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 Services, 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 Corporation, 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 allows 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 Release 11*i* Human Resources

- Oracle Database Tables

- SunONE and iPlanet Directory Services

- Microsoft Active Directory Services

> **See Also:** *Oracle Internet Directory Administrator's 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 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 Developer APIs

Oracle Application Server Java Authentication and Authorization Service allows user-written Java applications running in the Oracle J2EE environment to leverage 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

> **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.

6

Integrating Enterprise Applications

In addition to serving as a shared infrastructure for all Oracle applications, Oracle Identity Management also provides certain services and programmatic interfaces that facilitate third-party enterprise application development. These interfaces are useful for application developers who need to incorporate identity management into their applications.

This chapter discusses these interfaces and recommends application development best practices in the Oracle Identity Management environment.

The following two types of applications can be integrated with Oracle Identity Management:

- Existing applications already rolled out in the enterprise. The enterprise might have already invested in such applications and would benefit from their integration with the Oracle Identity Management infrastructure.

- New applications being developed by corporate IT departments or ISVs that are based on the Oracle technology stack

This chapter contains the following topics:

- Benefits of Integrating with Oracle Identity Management

- Oracle Identity Management Services Available for Application Integration

- Integrating Existing Applications with Oracle Identity Management

- Integrating New Applications with Oracle Identity Management

Benefits of Integrating with Oracle Identity Management

Enterprise applications integrating with the Oracle Identity Management infrastructure receive the following benefits:

- **Integration facilitates faster application deployment with lower costs**: Deployments (primarily Oracle customers) already using an existing Oracle Identity Management infrastructure can easily deploy the new application. The self-service console of Oracle Delegated Administration Services allows certain aspects of application administration to be delegated to users, which reduces the deployment cost of the application.

- **Seamless integration with Oracle applications**: Since all Oracle applications rely on the Oracle Identity Management infrastructure, integrating natively with it will make the enterprise application more attractive

- **Seamless integration with third-party identity management solutions**: Because Oracle Identity Management infrastructure already has built-in capabilities for integrating with third-party identity management solutions, application developers can leverage this for their applications

Oracle Identity Management Services Available for Application Integration

Custom applications can leverage Oracle Identity Management through a set of documented and supported services and APIs. For example:

- Oracle Internet Directory provides LDAP APIs for C, Java, and PL/SQL, and is compatible with other LDAP SDKs

- Oracle Delegated Administration Services provide a core self-service console that can be customized to support third-party applications. In addition, they provide a number of services for building customized administration interfaces that manipulate directory data.

- Oracle Directory Integration Services facilitate the development and deployment of custom solutions for synchronizing Oracle Internet Directory with third-party directories and other user repositories

- Oracle Provisioning Integration Services provide a mechanism for provisioning third-party applications, as well as a means of integrating the Oracle environment with other provisioning systems

- OracleAS Single Sign-On provides APIs for developing and deploying partner applications that share a single sign-on session with other Oracle Web applications

- JAZN is the Oracle implementation of the Oracle Application Server Java Authentication and Authorization Service standard that allows applications developed for the Web using the Oracle J2EE environment to leverage the identity management infrastructure for authentication and authorization

Integrating Existing Applications with Oracle Identity Management

An enterprise may have already deployed certain applications to perform critical business functions. The Oracle Identity Management infrastructure provides the following services that can be leveraged by the deployment to modify existing applications:

- **Automated User Provisioning**: The deployment can develop a custom provisioning agent that automates the provisioning of users in the existing application in response to provisioning events in the Oracle Identity Management infrastructure. This agent must be developed using the interfaces of the Provisioning Integration Service.

    See Also: *Oracle Internet Directory Administrator's Guide* for more information about developing automated user provisioning

- **User Authentication Services**: If the user interface of the existing application is based on HTTP, integrating it with Oracle HTTP Server and protecting its URL using mod_osso will authenticate all incoming user requests using the OracleAS Single Sign-On service.

- **Centralized User Profile Management**: If the user interface of the existing application is based on HTTP, and it is integrated with OracleAS Single Sign-On for authentication, the application can leverage the self-service console of Oracle Delegated Administration Services to enable centralized user profile management. The self-service console can be customized by the deployment to address the specific needs of the application.

Integrating New Applications with Oracle Identity Management

Application developers can leverage the services provided by the Oracle Identity Management infrastructure more extensively if they are developing a new

application or planning on a new release of an existing application. Application developers should consider the following integration points:

- **User Authentication Services**: The application developer has the following options:

  - If the application is based on J2EE, it can use the services provided by the Oracle Application Server Java Authentication and Authorization Service interface

  - If the application relies on Oracle Application Server Containers for J2EE, it can use the services provided by mod_osso to authenticate users and obtain important information about the user in the HTTP headers

  - If the application is a standalone Web-based application, it can leverage OracleAS Single Sign-On as a partner application using the OracleAS Single Sign-On APIs

  - If the application provides a non-Web-based access interface, it can use the Oracle Internet Directory LDAP APIs (available in C, PL/SQL and Java) to authenticate users

- **Centralized Profile Management**: The application developer has the following options available:

  - The application developer can model application-specific profiles and user preferences as attributes in Oracle Internet Directory

  - If the user interface of the application is based on HTTP, and it is integrated with OracleAS Single Sign-On for authentication, the application can leverage the self-service console of Oracle Delegated Administration Services to enable centralized user profile management. The self-service console can be customized by the deployment to address the specific needs of the application.

  - The application can also retrieve user profiles at runtime using the Oracle Internet Directory LDAP APIs (available in C, PL/SQL and Java)

- **Automated User Provisioning**: Application developers should consider the following options:

  - If the user interface of the application is based on HTTP and it is integrated with OracleAS Single Sign-On for authentication, then the application developer can implement automated user provisioning the first time a user accesses the application

- The application can also be integrated with the Oracle Internet Directory Provisioning Integration Service, which enables it to automatically provision or de-provision user accounts in response to administrative actions, such as adding an identity, modifying the properties of an existing identity, or deleting an existing identity in the Oracle Identity Management infrastructure

A

Oracle Internet Directory Default Settings

This appendix describes the default settings that are available upon installation of 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 all of the operations performed during the Oracle Internet Directory installation:

- A default DIT is created based on the domain name of the machine on which Oracle Internet Directory is installed. For example, if Oracle Internet Directory is being 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 machine. 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. In the example, Oracle Context is 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 are created in the default identity management realm that 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 createdunder 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, lockout, and 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