

Oracle Identity Governance 11g R2: Essentials

Duration: 5 Days

What you will learn

This Oracle Identity Governance 11g R2: Essentials training teaches essential concepts associated with Oracle Identity Manager (OIM), one product of the Oracle Identity Governance Suite for 11g R2 PS3. Discover the importance, benefits, terminology, and functional aspects of Identity Management.

Learn To: Create, load, and manage organizations, roles, and users, including dynamic organizations and parametric roles. Incorporate Role Lifecycle Management, role consolidation, and role analytics into role management workflows. Import and use predefined OIM connectors and create draft versions of user profiles and requests. Use requests to automate the provisioning of users.

Reconcile user data between OIM, and trusted and non-trusted external resources. Manage OIM security and self-service capabilities through admin roles.

Access OIM reports using Oracle BI Publisher.

Configure and perform certification activities to review periodically the access granted to users.

Build identity audit (IDA) workflows that OIM uses to detect segregation of duties violations.

Migrate an OIM configuration and customization from test to production environments.

Customize the OIM web-based UI.

Benefits to You

You'll develop the knowledge and skills to secure your organization's critical applications and sensitive data to lower operational costs. Learn how to manage the entire user identity life cycle across all enterprise resources.

Create & Manage Roles & Users

Learn how three new PS3 features, Role Lifecycle Management, Role Consolidation, and Role Analytics, fit seamlessly into role management workflows. Explore predefined connectors in the OIM Connector Pack, ways to transfer connectors from one environment to another, and two tools used to import and export connectors: Manage Connector and Deployment Manager.

Implement Provisioning & Reconciliation Workflows

Implement provisioning workflows to create user accounts in external resources-manually and automatically. You'll then deploy these approval workflows as SOA composites to use them as part of a request. Then, explore two new features of requests: the request access catalog and the request cart. See how authoritative and account reconciliation is used to identify new or modified user accounts on trusted sources or target resources and transfer this information into OIM.

Develop Security Expertise

You'll learn about admin roles, examine types of admin roles available in OIM, and see how by managing these roles,

you can perform authorization and authentication in OIM. You'll also become familiar with self-service capabilities, while seeing the role policies and rules play in restricting a user's self-service capabilities in OIM.

Explore Certification and Auditing

Next, you'll develop the skills to use certification to review user access privileges and entitlements to ensure users do not have unauthorized privileges. You'll configure certification workflows so reviewers can certify (approve) or revoke (reject) privileges. You'll then explore the new Identity Audit (IDA) module for PS3, including how to use IDA to detect segregation of duties violations in OIM.

Dive into Web GUI Customization

Finally, taking this course will help you understand how to customize the Web-based UI of OIM. You'll learn how to change the console logo, add a link that redirects the user to a certain URL, and provide custom, descriptive information for entitlements associated with an application instance. Entitlement descriptions help requesters, approvers, and certifiers better understand the functionality associated with the entitlements so you can choose which entitlements to include in the request cart.

Audience

Administrator
Business Analysts
End Users
Functional Implementer
Process Developer
Sales Consultants
Support Engineer
Technical Administrator

Related Training

Required Prerequisites

A general comprehension of Oracle WebLogic Server and Oracle Database.

A high-level understanding of SOA, BPEL and JDeveloper

Oracle WebLogic Server 11g: Administration Essentials

Suggested Prerequisites

A general comprehension of LDAP concepts

A good familiarity with a Linux-based environment

Oracle Identity Manager 11.1.2.3: New Features and Enhancements

Course Objectives

The four solutions-based, functional areas of Oracle Identity Management: Access Management, Identity Governance, Directory Services, and Mobile Security

The role that OIM plays in both Identity Governance and Oracle Identity Management

The tiers of the OIM architecture

How to launch OIM and use the new Identity Self Service Console

How to create and manage organizations, roles, and users

How to use the Bulk Load Utility to load users, roles, and role assignments into OIM

How to incorporate Role Lifecycle Management, role analytics, and role consolidation into role management workflows

How to customize and save searches

How to provision users to resources through request-level and operation-level approval workflows

How to provision users to disconnected resources

How to manage security and self-service capabilities in OIM through admin roles

How to access operational, historical, exception, and entitlement reports in OIM using Oracle BI Publisher

How to configure and perform certification activities to review periodically the access granted to users

How to build identity audit (IDA) workflows that OIM uses to detect segregation of duties violations

How to migrate an OIM configuration and customization from test to production environments

How to customize the OIM web-based UI

Course Topics

Introducing Oracle Identity Governance 11g R2 PS3

Receive a product overview

Manage users, user entities, and resources

Handle reconciliation workflows

Manage security, reports, and tools

Deploy configurations

Customize Oracle Identity Manager

Understanding Identity Management and Identity Governance

Discuss identity management

Explain Oracle Identity Management

Describe the four solutions-based, functional areas of Oracle Identity Management: Access Management, Identity Governance, Directory Services, and Mobile Security

Examine the role that Oracle Identity Manager plays in both Identity Governance and Oracle Identity Management

Describe the tiers of the Oracle Identity Manager architecture

Launching Oracle Identity Manager

Compare Oracle WebLogic Server, Oracle Identity Manager Server, and SOA Server

Discuss the Oracle Identity Manager interfaces: self-service interfaces, administrative interface, Design Console, and SC

Identify the differences among the consoles available from Oracle Identity Manager and Oracle SOA

Understanding Organizations, Roles, and Users

Explain users, roles, and organizations

Compare parent and child organizations and roles

Compare types of Oracle Identity Manager users

Discuss Oracle Identity Manager user membership in organizations and roles

Describe dynamic organizations and parametric roles

Discuss Role Lifecycle Management (LCM) and role analytics

Explain the Bulk Load Utility and discuss its benefits

Discuss customized search results

Installing and Configuring Predefined Connectors

Identify an Oracle Identity Manager connector

List the connectors in the Oracle Identity Manager Connector Pack

Describe the ways to transfer connectors from one environment to another

Explain the advantages of and best practices for transferring connectors

Identify two tools used to import and export connectors: Manage Connector and Deployment Manager

Explain how the Manage Connector tool is used to import connectors for external resources

Configure a connector to make it operable

Understanding Application Instances

Identify an Oracle Identity Manager application instance

Describe how application instances relate to connector objects

Provide examples of application instances

Identify entitlements for application instances

Discuss complex entitlements for application instances

Describe and manage sandboxes

Describe how to create an application instance

Manage entitlements for application instances

Using the Access Request Catalog

Identify the Request Access Catalog

Describe the business challenges solved by the Request Access Catalog

Understand the concepts and terminology associated with the Request Access Catalog

Describe how to manage the Catalog

Understanding Policy-Based Provisioning

Identify and compare resources and Oracle Identity Manager connectors

Describe how connectors are used to assign resources to users

Discuss two ways to provision a resource to an Oracle Identity Manager user: through policies (user membership rules and

Discuss autoprovisioning

Understanding Advanced Request Functionality

Explain the types of requests that you can create and manage

Compare single requests and bulk requests

Discuss how to create draft versions of requests

Describe the two types of approval workflows associated with requests: request-level and operational-level approval workflows

Explain the stages of a request throughout a request's life cycle for both single and bulk requests

Discuss the role that users, entities, approval workflows, email notifications, and SOA composites play in requests
Deploy SOA composites
Associate approval rules with, and complete, request-level and operational-level approval workflows

Understanding Application Instances for Disconnected Resources

Identify application instances
Describe disconnected resources
Create and manage application instances for disconnected resources

Understanding Reconciliation

Identify and compare two types of reconciliation associated with Oracle Identity Manager: authoritative and account reconciliation
Discuss three reconciliation events that Oracle Identity Manager can perform with a resource
Compare primary and non-primary user accounts
Discuss the role that reconciliation plays in designating user accounts as primary accounts
Identify scheduled tasks
Discuss the role that scheduled tasks have with authoritative reconciliation and account reconciliation
Explain how to implement authoritative reconciliation and account reconciliation workflows
Identify access policy harvesting, and discuss the role that access policy harvesting plays in a reconciliation workflow

Understanding Oracle Identity Manager Security

Compare authorization and authentication
Identify administrative roles
Examine types of administrative roles available in Oracle Identity Manager
Manage administrative roles
Describe self service capabilities
Discuss the role that policies and rules play in restricting a user's self-service capabilities in Oracle Identity Manager

Managing Reports

Identify and compare types of reports that an administrator can create for Oracle Identity Manager organizations, roles, and users
List different reports available with Oracle Identity Manager
Identify Oracle Business Intelligence (BI) Publisher, the reporting tool for Oracle Identity Manager

Understanding Identity Certifications

Describe identity certification and attestation
Identify the business drivers for certification
Configure certification in Oracle Identity Manager
Create and manage certification definitions
Explain how risk summaries are calculated
Describe closed-loop remediation and remediation tracking
Describe event listeners
Describe and configure multi-phased reviews for user certifications

Understanding Identity Audit (IDA)

Describe Identity Audit (IDA)
Compare two IDA types: preventative and detective
Discuss IDA concepts
Enable IDA in Oracle Identity Manager
Manage four IDA components: rules, policies, scan definitions, and policy violations

Transferring Oracle Identity Manager Configurations

Identify the Deployment Manager and the sandbox
List the objects that you can import or export by using the Deployment Manager

Discuss the advantages and best practices of using the Deployment Manager
List other operations that you can perform with sandboxes

Customizing the Oracle Identity Manager UI

Discuss three approaches for customizing the Oracle Identity Manager web-based UI

Identify Web Composer

Describe Expression Language (EL)

Examine the role EL plays in web customization

Customize the Oracle Identity Manager UI by changing the Oracle Identity Manager console logo, providing links in Oracl