Oracle Access Manager 11g R2: Administration Essentials

Duration: 5 Days

What you will learn
This course teaches you to install, configure and implement a real life deployment of Oracle Access Manager 11g R2(11.1.2.0).

Learn To:
Install and Configure Oracle Access Manager 11g R2.
Configure Servers, Data Sources and Agents.
Set up Policy Configuration(shared components and application domain).
Manage sign-on, sign-off, and sessions.
Set up Auditing, Logging and Troubleshooting OAM 11g R2.
Use Access SDK, Extensibility APIs and Integrate with RSA Authentication Manager 7.x.

Key Concepts
This course teaches you key concepts like installing, configuring and registering Webgates, creating authentication and authorization policies to protect resources, understanding session management and single sign on.

Troubleshooting & Diagnosing
Learn to troubleshoot, diagnose and monitor the OAM deployment environment. Explore the Oracle Fusion Middleware Audit Framework, a centralized audit framework to the OAM and other Fusion Middleware component products.

Course Wrap-Up
Finally, expert instructors will teach you how to generate reports and audit for OAM deployments. Briefly review custom authentication plugins and using OAM SDK (Software Developer Kit) to understand the APIs. You'll also understand how to use them to extend the default functionality of the product.

Audience
Sales Consultants
Security Administrators
Support Engineer
Technical Administrator
Technical Consultant
Web Administrator

Related Training
Suggested Prerequisites
General Security Concepts

Oracle WebLogic Server 11g: Administration Essentials
Working knowledge of Identity and Access Management products

**Course Objectives**

Install and configure Oracle Access Manager (OAM 11g)

Configure servers, data sources, and agents

Set up policy configuration (shared components and application domain)

Manage sign-on, sign-off, and sessions

Explain and set up auditing and logging for OAM 11g

Troubleshoot OAM 11g

Provide overview of Mobile SSO integration and Social identity login

Configure and explain WLS, identity assertion, OAM assertion provider, and WLS authenticator

Setup SSL communication between webgates and OAM server

Explain all new features in OAM 11g R2

Use access SDK, extensibility APIs and integrate with RSA Authentication manager 7.x

**Course Topics**

**Overview of Access Manager**

Explain the salient features of Oracle Access Manager

Explain the key products that comprise the Oracle Access Management Suite

Explain the functional areas for each of the Oracle Access Management products

Explain Oracle Access Manager overall architecture

Explain Oracle Access Manager run-time architecture

Identify key Oracle Access Manager 11g R2 new features

OIF enhancements to the OAM admin console to support SP functionality

SAML attributes can be configured for OAM policy, SAML attribute can be used by OAAM risk analysis

**Installation and Configuration**

Describe basic concepts of Oracle WebLogic Server

Explain key definitions and terminologies

Describe the prerequisites for installing Oracle Access Manager

Install Oracle WebLogic Server (WLS)

Configure seeded database schemas by using the Repository Creation Utility

Install and configure Oracle Access Manager

Perform post-installation validation checks

Perform an uninstallation

**System Configuration: Servers, Datasources and Agents**
Policy Configuration: Shared Components and Application Domains

Explain Access Control - Authentication and Authorization
Authentication Modules and Schemes
Understanding Policy Objects and Policy Model
Two-factor/Multi-factor authentication
Complex LDAP AuthZ and Response Filters
Resource matching and Excluded resources
Authorization expressions
LDAP search Filter support

SSO and Session Management
OAM single sign-on and single logout
Sessions life cycle, caching and cookies
Configuring single sign-on and single logout
Customizing the ECC login and logout pages
Customizing user defined error msgs
Implementations of custom login pages for DCC
Impersonation
Errors codes, information and password policy validation errors

Using Oracle Access Manager With WebLogic Applications
Protecting WLS applications with OAM
Identity assertion providers
OAM authenticator

Auditing and Logging
Fusion Middleware audit framework
Audit output options
Configure audit settings
Audited events and recorded data
Generating audit reports
Configuring logging settings
Locating and examining logging output
Locating log files from other servers

Troubleshooting and Management
Work with Access Tester
Identifying connectivity issues between agents and servers (impact of load balancers and firewalls)
Understand OAM specific WLST commands
Work with Oracle Enterprise Manager Fusion Middleware Control
Explain EM FMW Control integration
Server processes and charts
Topology viewer
Farm and domain

Access SDK, Extensibility APIs and Third Party Integration
Using ASDK 11g R2 to create access client
Compatibility between ASDK 10g and ASDK 11g
Overview of custom authentication plugins and their life cycle
Using extensibility APIs to create Custom Authentication plugins
Development methodology - Decision point vs Hard coded
Multifactor authentication
Brief primer of APIs
Integrating OAM 11g R2 with RSA Authentication manager 7.x