Course Contents: Oracle Access Manager 11g R2 PS3 – OAM 11.1.2.3

Course Duration - Around 35+ Hours

- **Before you start :**
  1. Hardware Requirements for hands on: 16 GB RAM, **i3 2nd Generation onwards or equivalent Processor**, 70 GB HDD is needed for hands on.
  2. Download the OAM 11.1.2.3 Virtual Box Image (From **Curriculum**), follow the video instruction on how to set it up, ask (Via call or mail) for **one to one support on setup of virtual box image** in case any issue.
  3. OAM 11.1.2.3 Virtual Box Image is a Linux based image having same configuration and software versions as trainer virtual box image.
  4. It's a 100% practical, use case oriented course.
- **Installation Phase :** Understand the Linux pre-requisites, install DB(create and tune), RCU, weblogic using custom JDK, IDM Suite, IAM Suite, OHS, WebGate, OUD and additionally will discuss and understand Oracle Security Solutions Offerings(Identity Governance Suite, Access Management Suite, Directory Services Suite, DB Security, Cloud Security).
- **Configuration and Integration Phase:**
  5. Create IDMDomain (ODSM) and create instances of OID/OVD
  6. Understand OID/OVD(start/stop, logging, troubleshooting)
  7. Extending OID Schema(Attributes, Object classes for OAM)
  8. Understanding need of OVD, Creating adapter of DB in OVD using ODSM console
  9. Create OAM Domain(Admin server, OAM server)
  10. Upgrading OPSS schema
  11. Create DB Security Store for IAM.
  12. Understanding Weblogic Server life cycle and various consoles/interfaces.
- **OAM Administrations topics :**
  1) Overview of Access Management Suite – OAM, OAAM, OIF, eSSO, Social & Mobile.
  2) Create OHS Webserver instance (also understand the WebGates and supported webservers) and verify.
  3) Deploy the webgate to OHS instance and verify.
  4) Modify the webserver configuration file with webgate details and verify.
  5) Register the OHS WebGate Instance with OAM 11g R2 Server (using both RREG tool and from OAM console) and **verify OAM integration with Webserver** (having OAM agent)**.**
  6) Understand WLS Embedded LDAP Directory and Default OAM User Identity (Default and System Store).
  7) **OAM Integration with Directory Server**: Configure OVD (with DB Adapter) as new default and system Identity Store for OAM, will cover OAM Integration with OID, OVD, Active Directory and OUD.
  8) Working with Security Realm, Creating OVD Authenticator and Creating SSO Identity Asserter (Understanding the context).
  9) Deploying Sample Web Application, configuring SSO of the application.
  10) Creating Application Domain, Creating resources, **Creating AuthN Policies** (with LDAP Scheme and Anonymous Scheme), Creating default AuthZ Policy.
  11) Creating Custom Authentication Scheme for customizations.

12) Understand how to **protect and unprotect** the enterprise resources.
13) Working with **authorization policies** – Working on all 4 conditions and rules (Allow, Deny), (with practical use case of each condition) and demonstrating IP Range, Temporal, Identity, Asserted Attribute based Authorization.
14) Integrating **OAM with ADF or J2EE application** (weblogic deployed application) with 7 golden steps.
15) Creating and working with Custom Authentication (AuthN) and Authorization (AuthZ) policies.
16) Explaining the **complete technical flow** of AuthN and AuthZ in OAM (how SSO work, role of each entity).
17) Managing Authentication and Authorization **Responses** in Headers, Cookies and session variables.
18) Demonstrating Single Sign-On, Cookie Management and Session Management.
19) Configuring/developing the **custom SSO login page (Deploying the web application on OAM Server and External Server), Configuration of Logout Page, Error Pages.** (Code will be explained and shared)
20) Understanding the requirement and possibility of creation of **multiple SSO login pages**.
21) Working with Weblogic deployed Applications.
22) Configuring/Working with misc. OAM scenarios - Multi-Browser Scenario, View Cookies During the Login and Logout Process, Constraining the Number of User Sessions, Extending the Session and Idle Timeouts(Global as well as at Application Level)
23) Explaining Authentication Level and its impact on **Multi Factor Authentication**.
24) **Working with x.509**: The digital certificates used in SSO for Second or Multi Factor Authentication: Concept and context, installing **server certificates**, extracting **OAM Keystore password**, installing **CA root certificate in OAM keystore**, installing **client certificate** in Chrome, Firefox and Internet Explorer, protecting/defining resources with 2nd Factor using **X.509 AuthN Policy**, modifying **x.509 AuthN Scheme**, **x.509 AuthN Module** and **observing X.509 AuthN flow end to end**.
25) Configuring and understanding **OAM Auditing** (Changing the auditing from File System to Audit Schema – Creating the Data Source, modifying the Audit MBean property, Audit Level), logging and troubleshooting.
26) **OAM audit reporting in BI Publisher** – 1. OAM Report Templates 2. Report Templates in BI Publisher 3. Creating Data Sources 4. Populating reports with data from OAM Audit Schema. 5. Observing OAM Audit Reports in BI Publisher and further working on reports.
27) Working with **Access Tester** (Used for testing/troubleshooting purposes in OAM)
28) **SSO of OBIEE application** – OBIEE integration with OVD for AuthN/AuthZ by creating **AuthN Provider**, configure OBIEE to use **OHS weblogic directive file for proxy** access of resources, configure OAM **Identity Asserter in OBIEE**, Configure OAM WebGate Agent with predefined protected and unprotected resources of OBIEE, **enable SSO for OBIEE**, test and verify SSO of various OBIEE applications like analytics, BI Search and BI Console.
29) **Cross Domain or Cross network SSO** of Weblogic Deployed Application
30) **ProxyPass and ProxyPassReverse** for Cross Domain SSO of web application deployed on external webserver.
31) **SSL of all end points of OAM SSO Solution** - OHS, SSL of Custom SSO Login Page, OAM, OUD
32) **Integration of OAM 11.1.2.3 with OIM 11.1.2.3 (in Split Domain Configuration) –** Purpose of integration, Configuring the Identity Store, Configuring OAM for Integration, Configuring Oracle HTTP Server to Front-End Resources on OIM, Validation/Verification of integration.
33) **Working on Embedded Credential Collector (ECC) and Detached Credential Collector (DCC):** Understanding default ECC (with webgate creation), Configuring separate **webgate for DCC** in OAM, **Impersonation** and comparison with ECC.

34) **OAM Session Impersonation with use case**
35) **Custom Password Management** in OAM (without OIM integration)
36) Apply latest security bundle patches on OAM stack.

The approach to complete course is 100% practical, all use cases will be demonstrated practically, keeping real time scenarios in mind.