

**OAM11gR2-AAW: Oracle Access Manager  
11g R2: Advanced Administration Workshop**

Course Code: OAM11gR2-AAW

Duration: 5 days

Instructor-led Training (ILT) | Virtual Instructor-  
led Training (VILT)**OVERVIEW**

This Oracle Access Manager 11g R2: Administration Workshop preparing is intended for heads. When you're OK with introducing, designing, overseeing, investigating, diagnosing and fundamental organization of Oracle Access Manager 11g R2, master Oracle University educators will show you further developed organization points in this course.

**SKILLS COVERED****You will learn how to :**

- Perform organization life-cycle activities including moving from advancement, to testing and creation situations.
- Configure high accessibility for an OAM area.
- Create progressed pre and post validation rules utilizing the versatile verification highlight.
- Configure solid confirmation by broadening OAM with Oracle Adaptive Access Manager.
- Configure Windows Native Authentication ability for Active Directory in a multi-area design.
- Upgrade Oracle Access Manager 11g R1 to Oracle Access Manager 11g R2.
- Provide portable validation with Oracle Mobile and Social administrations.

**WHO SHOULD ATTEND?**

- Administrator

- End User
- Implementer
- Manager
- System Integrator
- Systems Administrator

**PREREQUISITES****Proposed Prerequisite :**

- General Security ideas
- Knowledge of Identity and Access the executives items

**Required Prerequisite :**

- A great strong working information on Oracle Access Manager 11g R2.
- Install, arrange and the executives of Oracle Access Manager 11g R2.
- Diagnostics and investigating of Oracle Access Manager 11g R2.
- A great comprehension of webgates, datasources, have identifiers, LDAP Schemes and modules, application areas inside the setting of OAM 11g R2

**MODULES****Module 1: Upgrade OAM 11g R1 to OAM 11g R2**

- Review policy configuration in the R1 OAM domain
- Upgrade from OAM 11g R1 PS6 to OAM 11g R2 PS3
- Validate policies and operations post-upgrade

**Module 2: Move OAM domain from test to production environment**

- Copy the binaries from the test machine.

- Create the archive of the Oracle Weblogic Server domain configuration, the OHS instance configuration, and the OAM policy data on the test machine
- Create the OAM product metadata repository on the production machine
- Import the metadata and OAM policy data in the production database
- Configure the OAM Domain by using the configuration that you copied from the test machine
- Configure the OHS instance on the production machine using the configuration that you copied from the test machine

### **Module 3: Configure High Availability for OAM domain**

- Create OAM Cluster
- Add the existing OAM Server to the cluster and target applications and data sources to the cluster
- Create a second Oracle Access Manager server instance
- Instantiate the second OAM Server in the cluster
- Set request cache type
- Create a new OHS Instance as load-balancer for Oracle Access Manager server instances
- Modify and reconfigure the definition for Oracle Access Manager 11g WebGate
- Test HA deployment

### **Module 4: Enable Windows Native Authentication (WNA) with OAM using multi-domain Active Directory (AD) deployment architecture**

- Study the multi-domain AD configuration with transitive trust relationship
- Create OAM system accounts in AD

- Create keytab file and modify krb5.conf files
- Configure parameter values for the custom authentication module for the Kerberos Plug-in
- Modify the authentication scheme and protected application domain to use the Kerberos plug-in
- Set custom logging to troubleshoot any WNA Kerberos Issues
- Test WNA for users on both AD domains

### **Module 5: Integrate Oracle Adaptive Access Manager (OAAM) with OAM for strong authentication capabilities**

- Extend OAM domain to configure OAAM
- Register the OAAM Server as a Partner Application with OAM
- Validate the TAPScheme Definition in Oracle Access Manager
- Run setupOAMTapIntegration.sh to configure OAM for TAP integration.
- Protect a Resource with the TAP Scheme
- Set Up One Time Pin (OTP)
- Configure OTP challenge for step-up authentication usecase
- Validate Strong authentication capabilities of OAAM

### **Module 6: Setup Oracle Mobile service with OAM**

- Configure OAM domain for Mobile Support
- Enable Adaptive Authentication Service
- Perform OTP using the Oracle Mobile Authenticator
- Create mobile application profile entry
- Create pre and post authentication rules

**Module 7: Configure OAM for Federated Login  
using SAML**

- Extend OAM for federation support
- Configure the identity provider
- Configure the service provider
- Configure policy for federated login
- Test login to service provider using SAML assertion

**Module 8: Monitor and Tune Performance for  
OAM**

- Use performance monitoring tools: DMS Spy, Enterprise Manager, and JConsole
- Monitor and tune performance for JVM, OAM, Coherence, OUD and WLS data sources
- Configure testing tool to simulate a workload for the environment

**END OF PAGE**