Oracle Access Manager 11g R2: Advanced Administration Workshop

CODICE	DURATA	PREZZO	LINGUA	MODALITÀ
D77285GC20	5 Giorni	2.500,00€ (iva escl.)	Italiano	Virtual Classroom Corso in aula

SCHEDULAZIONE

- A Richiesta

PREREQUISITI

Install, configure and management of Oracle Access Manager 11g R2.

A good solid working knowledge of Oracle Access Manager 11g R2.

A good understanding of webgates, datasources, host identifiers, LDAP Schemes and modules, application domains within the context of OAM 11g R2.

Diagnostics and troubleshooting of Oracle Access Manager 11g R2.

Suggested Prerequisites

General Security concepts

Knowledge of Identity and Access management products

Audience

Sales Consultants

Security Administrators

Support Engineer

System Administrator

System Integrator

Team Leader

Technical Administrator

Technical Consultant

OBIETTIVI

Perform horizontal migration of OAM domain from test to production (t2p deployment)

Configure OAM domain for high availability deployment

Enable Windows Native Authentication (WNA) with OAM using multi-domain Active Directory deployment architecture

Integrate Oracle Adaptive Access Manager (OAAM) with OAM for strong authentication capabilities

Configure the Adaptive Authentication Service to provide second factor authentication

Monitor and tune performance of the OAM components

Setup mobile services with OAM

Upgrade OAM 11g R1 (11.1.1.7) to OAM 11g R2 (11.1.2.3)

CONTENUTI

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

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

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

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

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

Setup Oracle Mobile service with OAM

Configure OAM domain for Mobile Support

Enable Adaptive Authentication Service

Perform OTP using the Oracle Mobile Authenticator

Create moble application profile entry

Create pre and post authentication rules

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

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

Description:

This Oracle Access Manager 11g R2: Administration Workshop training is designed for administrators. Once you're comfortable with installing, configuring, managing, troubleshooting, diagnosing and basic administration of Oracle Access Manager 11g R2, expert Oracle University instructors will teach you more advanced administration topics in this course.

Learn To:

Perform deployment life-cycle operations including moving from development, to testing and production environments.

Configure high availability for an OAM domain.

Create advanced pre and post authentication rules using the adaptive authentication feature.

Configure strong authentication by extending OAM with Oracle Adaptive Access Manager.

Configure Windows Native Authentication capability for Active Directory in a multi-domain architecture.

Upgrade Oracle Access Manager 11g R1 to Oracle Access Manager 11g R2.

Provide mobile authentication with with Oracle Mobile and Social services.

Benefits to You

This course is the first of its kind to provide detailed practices to reinforce new concepts. By enrolling in this training, you'll develop a deeper understanding of advanced topics. You'll get the chance to participate in an advanced level workshop, with minimal lecture.

Please Note

This workshop consists of complex use cases that strictly require practical experience of performing tasks, covered in the Oracle Access Manager 11g R2: Administration Essentials course.

Prezzi e corsi potrebbero subire variazioni; si consiglia di verificare sul sito www.novanext.it/training.