

Oracle Adaptive Access Manager: Administration

Student Guide

D70569GC10

Edition 1.0

October 2008

D56328

ORACLE®

Authors

Steve Friedberg
Shankar Raman

**Technical Contributors
and Reviewers**

Philip Garm
Steve Jackle
Robert Lavallie
Derick Leo
Karl Miller

Editor

Amitha Narayan

Graphic Designer

Priya Saxena

Publisher

Jobi Varghese

Copyright © 2008, Oracle. All rights reserved.

Disclaimer

This document contains proprietary information and is protected by copyright and other intellectual property laws. You may copy and print this document solely for your own use in an Oracle training course. The document may not be modified or altered in any way. Except where your use constitutes "fair use" under copyright law, you may not use, share, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit, or distribute this document in whole or in part without the express authorization of Oracle.

The information contained in this document is subject to change without notice. If you find any problems in the document, please report them in writing to: Oracle University, 500 Oracle Parkway, Redwood Shores, California 94065 USA. This document is not warranted to be error-free.

Restricted Rights Notice

If this documentation is delivered to the United States Government or anyone using the documentation on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose these training materials are restricted by the terms of the applicable Oracle license agreement and/or the applicable U.S. Government contract.

Trademark Notice

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Preface

1 Introduction

Objectives 1-2

Course Objectives 1-3

Schedule: Day One 1-5

Schedule: Day Two 1-6

Schedule: Day Three 1-7

Product Summary 1-8

Conceptual Lab Environment 1-10

Lab Environment Implementation 1-11

Sign In to the Lab Environment 1-12

Summary 1-13

Quiz 1-14

Practice 1 Overview: Signing In to the Lab Environment 1-16

2 Identity and Access Management Arena

Objectives 2-2

Internet Attacks 2-3

Specific Internet Attack Modes 2-4

Hacking: The Solution 2-5

Phishing: The Solution 2-7

Trojans: The Solution 2-9

“Inside Job”: The Solution 2-11

Psychology of Strong Authentication 2-13

Passwords Versus Challenges 2-15

Knowledge Base of Questions 2-16

Publicly Available Information 2-17

Oracle Identity and Access Management Products 2-18

Identity and Access Management Functions 2-20

Product Functionality Matrix 2-21

Oracle Virtual Directory 2-22

Oracle Internet Directory 2-23

Oracle Role Manager 2-24

Oracle Identity Manager 2-25

Oracle Identity Federation 2-26
Oracle Adaptive Access Manager 2-27
Oracle Enterprise Single Sign-On 2-29
Oracle Access Manager 2-30
Summary 2-31
Quiz 2-32
Practice 2 2-34

3 Installation Preparation

Objectives 3-2
Minimum Hardware Prerequisites 3-3
Operating System Prerequisites 3-4
Software Prerequisites 3-5
Optional Software 3-6
Software Distribution 3-7
Scalability 3-8
Small Deployment 3-9
Medium Deployment 3-10
Large Deployment Using SOAP Calls Between Functions 3-11
Tuning Database Initialization Parameters 3-12
Extending and Populating the Database 3-14
Extending the Database Schema 3-15
Populating Seed Data 3-16
Offline Database Schemas 3-17
Sizing Recommendations 3-18
Summary 3-19
Quiz 3-20
Practice 3 Overview: Installation Preparation 3-22

4 Installing Adaptive Risk Manager and Adaptive Strong Authenticator

Objectives 4-2
Directory Structures 4-3
Directory Considerations on Multiple Host Platforms 4-4
Configuration Considerations on Multiple Tenant Hosts 4-5
Selecting Application Server OC4J Instance 4-6
Deploying `oarm.war` 4-7
Deploying `oarm.war`: Select Archive 4-8
Deploying `oarm.war`: Application Attributes 4-9
Deploying `oarm.war`: Deployment Settings 4-10
Deploying `oarm.war`: Confirmation 4-13

Directory Structure After `oarm.war` Deployment 4-14
Editing Configuration Files 4-15
Cloning Device Background Images 4-17
`bharosa_server.properties`: Location of Device Bitmap Images
for Server 4-18
`bharosa_client.properties`: Location of Device Bitmap Images
for Client 4-19
`sessions.xml`: Database Connections 4-20
`sessions.xml`: Username and Password 4-21
`log4j.xml`: Logging Options 4-22
`web.xml`: Security Options 4-23
Verifying That ARM Works 4-24
Deploying `oasa.war` 4-25
`bharosauiio.properties`: Password 4-26
Successful Adaptive Strong Authenticator Challenge 4-27
Summary 4-28
Quiz 4-29
Practice 4 Overview: Installing ARM and ASA 4-31

5 Groups

Objectives 5-2
Group Hierarchies 5-3
Kinds of Groups 5-4
Populating Geolocation Data 5-5
`bharosa_location.properties`: Geolocation Vendor and Files 5-6
Data Preparation 5-7
Creating and Editing Location Groups 5-8
Creating and Editing User ID Groups 5-9
Creating and Editing IP Groups 5-10
Creating and Editing IP Ranges 5-11
Listing IP Ranges 5-12
Creating and Editing IP Range Groups 5-13
Creating and Editing Device Groups 5-14
Query Device Report 5-15
Creating and Editing Action Groups 5-16
Creating and Editing Alert Groups 5-18
Creating and Editing Network Groups 5-19
Creating and Editing Generic Groups 5-20
Query and Report Groups 5-21
Deleting a Group 5-22

Summary 5-23
Quiz 5-24
Practice 5 Overview: Administering Groups 5-27

6 Policies, Models, and Rules

Objectives 6-2
Hierarchy of Policies, Models, and Rules 6-3
Relationships Between Rules and Groups 6-4
List of Rule Types 6-6
Import Models 6-7
Import Rule Templates 6-9
Run Times 6-10
Making Your Own Model 6-12
Making Your Own Model: Creating a Model 6-13
Creating a Model 6-14
Making Your Own Model: Adding a Rule 6-15
Adding Rules 6-16
Making Your Own Model: Need More Rules? 6-18
Making Your Own Model: Manual Overrides 6-19
Manual Overrides 6-20
Making Your Own Model: Linking Groups 6-22
Linking Groups 6-23
Exporting a Rule or Model 6-24
Importing a Rule 6-25
Risk Scoring 6-26
Summary 6-27
Quiz 6-28
Practice 6 Overview: Creating Rules and Models 6-31

7 Oracle Access Manager Integration

Objectives 7-2
Oracle Access Manager 7-3
Access System Architecture 7-4
Access Server 7-5
WebGate 7-6
Access System Flow Without Oracle Adaptive Access Manager 7-7
Physical Access System Flow with Oracle Adaptive Access Manager 7-8
Logical Access System Flow with Oracle Adaptive Access Manager 7-9
Sign In to Access Manager, Access System Console 7-10
Adding New AccessGate for ASA 7-11
Associating Access Server with ASA 7-13

- Adding New AccessGate for Web Server 7-14
- Adding Second AccessGate for Web Server 7-15
- Associating Access Server with Web Server 7-16
- Adding Authentication Scheme to Oracle Access Manager 7-17
- Adding Plugins 7-18
- Enabling Authentication Scheme 7-19
- Adding Host Identifiers 7-20
- Installing Access Server SDK for ASA 7-21
- Installing Access Server SDK 7-22
- Configuring Access Server SDK for ASA 7-24
- WebGate Installation Utility 7-25
- Deploying OAAM Plugin 7-28
- Adding Server Properties Environment Variables 7-29
- Configuring OAM Policy Domain Mechanisms: General and Resources 7-30
- Configuring OAM Policy Domain Mechanisms: Authorization Rules 7-31
- Configuring OAM Policy Domain Mechanisms: Default Rules 7-32
- Configuring OAM Policy Domain Mechanisms: Policies 7-34
- Summary 7-35
- Quiz 7-36
- Practice 7 Overview: Integrating OAM with Adaptive Access Manager 7-38

8 Integration with Applications

- Objectives 8-2
- SOAP: XML Messaging for Web Services 8-3
- Communication with SOAP 8-4
- SOAP Messages 8-5
- SOAP Messages: Example 8-7
- Application Integration 8-8
- SOAP Services 8-9
- Online Documentation 8-10
- Sample Code 8-11
- Sample JavaServer Pages 8-12
- Native API 8-13
- Adaptive Risk Manager Online Native Client API Web Services/SOAP 8-14
- Adaptive Risk Manager Online Native Client API Static Linking 8-15
- Adaptive Risk Manager Only 8-16
- ARM, ASA, and KBA: Part One 8-18
- ARM, ASA, and KBA: Part Two 8-20
- Files to Install, Copy, and Edit for API Integration 8-22
- Editing `client.properties` for API Integration 8-23
- Edit `log4j.xml` for API Integration 8-24

Edit `server.properties` for API Integration 8-25
Considerations for Adaptive Risk Manager 8-26
Alternatives to Native Integration 8-27
Universal Installation Option (UIO) Proxy Architecture 8-28
Configuring UIO Proxy Interceptors 8-29
Configuring ISA Server 8-31
Summary 8-32
Quiz 8-33
Practice 8 Overview: Integrating BigBank Using SOAP APIs 8-35

9 Reports

Objectives 9-2
Assigning Roles to Users 9-3
Configuration Files for Roles 9-4
`web.xml` 9-5
`BharosaACLPageView.xml` 9-6
`BharosaACL.xml`: Deny/Grant Functions to Roles 9-8
`BharosaSystemACL.xml` 9-9
`bharosa_server.properties` 9-10
Assigning Reports to Roles 9-11
Four Types of Reports 9-12
Dashboard Reports 9-13
Query Reports 9-14
Query Report: Users 9-15
Query Report: Locations 9-16
Query Report: Devices 9-17
Query Report: Summary 9-18
Query Report: Security 9-19
Query Report: Security Alert ID 9-20
Query Report: Security Session Details 9-21
Query Report: Security Session Rules 9-22
Query Report: Knowledge Base 9-23
Query Report: Saved Reports 9-24
Query Report: Saved Queries 9-25
Query Report: Schedulers 9-26
Audit Reports 9-27
Customer Care Reports 9-28
Creating a Customer Care Case 9-29
Searching Customer Care Cases 9-30
Customer Care Case Details 9-31

Customer Care Case Actions	9-32
Administer the Knowledge Base of Questions: Adding a Question	9-33
Administer the Knowledge Base of Questions: Registration Logic	9-34
Administer the Knowledge Base of Questions: Answer Logic	9-35
Adaptive Risk Manager Offline	9-36
Offline Session Sets	9-37
Accessing Offline Data	9-38
Loading and Running Offline Data	9-39
Summary	9-40
Quiz	9-41
Practice 9 Overview: Enabling Roles and Viewing Reports	9-43

Appendix A: Practices and Solutions

Glossary

Index

