

Implementing Oracle Audit Vault

Student Guide

D55406GC10

Edition 1.0

August 2010

D68648

ORACLE

Author

Donna Keesling

**Technical Contributors
and Reviewers**

Tammy Bednar
Heinz-Wilhelm Fabry
Joel Goodman
Patricia Huey
Vipul M. Shah
Rodney Ward

Editors

Malavika Jinka
Raj Kumar

Graphic Designer

Priya Saxena

Publishers

Nita Brozowski
Jobi Varghese

Copyright © 2010, Oracle and/or its affiliates. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Preface

1 Introduction to Oracle Audit Vault

- Objectives 1-2
- Responding to Compliance Regulations 1-3
- Problems with In-House Auditing Implementations 1-5
- Oracle Audit Vault: Trust but verify 1-6
- Oracle Audit Vault Reports: Overview 1-7
- Oracle Audit Vault Security: Protecting Audit Data 1-9
- Oracle Audit Vault Alerts: Early Detection with Alerting 1-10
- Oracle Audit Vault Data Warehouse: Scalable and Flexible Warehouse 1-11
- Oracle Audit Vault Policies: Centralized Management of Audit Policies 1-12
- Quiz 1-13
- Oracle Audit Vault Components 1-14
- Audit Vault Architecture: Overview 1-15
- Deploying Audit Vault 1-16
- Audit Vault Services: Overview 1-17
- Audit Vault Framework 1-18
- Audit Vault Users: Overview 1-20
- Audit Vault Roles: Overview 1-21
- Oracle Database Vault: Enforcing Separation of Duties 1-22
- Audit Vault Data Warehouse: Overview 1-23
- Audit Vault Interfaces 1-24
- Summary 1-26

2 Installing the Oracle Audit Vault Server

- Objectives 2-2
- Oracle Audit Vault Components 2-3
- Types of Audit Vault Server Installations 2-4
- Hardware Requirements for Audit Vault Server on Linux 2-5
- Understanding Oracle Audit Vault Storage Requirements 2-7
- Included Oracle Options 2-8
- Installation Methods 2-9
- Quiz 2-10
- Installing the Audit Vault Server 2-11

Installing Audit Vault in an Oracle RAC Configuration: Overview	2-12
Selecting the Installation Type	2-13
Providing Input During Audit Vault Server Installation	2-14
Specifying Advanced Installation Details	2-15
Specifying Database Vault User Credentials	2-16
Performing Product-Specific Prerequisite Checks	2-17
Specifying Database Storage Options	2-18
Specifying Backup and Recovery Options	2-19
Specifying Database Schema Passwords	2-20
Reviewing Audit Vault Server Installation Summary Information	2-21
Monitoring the Installation	2-22
Monitoring the Configuration Assistants	2-23
Monitoring the Database Configuration Assistant	2-24
Responding to the Database Configuration Assistant	2-25
Executing the root.sh Script	2-26
Performing an Advanced Installation of the Audit Vault Server	2-27
Understanding Audit Vault Users and Configuration Information	2-28
Performing the Audit Vault Server 10.2.3.2 Patch Set Upgrade	2-29
Audit Vault Server Patch Set Upgrade Preinstallation Steps	2-30
Installing the Oracle Audit Vault Server Patch Set	2-31
Managing the Audit Vault Console	2-32
Summary	2-33
Practice 2: Overview	2-34
3 Installing the Oracle Audit Vault	
Collection Agent Objectives	3-2
Installing the Audit Vault Collection Agent	3-3
Performing Audit Vault Collection Agent Preinstallation Tasks	3-4
Understanding Audit Vault Users and Configuration Information	3-5
Providing Input During Audit Vault Collection Agent Installation	3-6
Quiz	3-7
Installing an Audit Vault Collection Agent	3-8
Performing Product-Specific Prerequisite Checks	3-9
Viewing Audit Vault Collection Agent Installation Summary Information	3-10
Viewing the Installation Page	3-11
Monitoring the Configuration Assistants	3-12
Completion of the Audit Vault Collection Agent Installation	3-13
Understanding Audit Vault Users and Configuration Information	3-14
Performing the Audit Vault Collection Agent Patch Upgrade	3-15
Audit Vault Collection Agent Patch Upgrade Preinstallation Steps	3-16

Installing the Audit Vault Collection Agent Patch Set Upgrade 3-17
Viewing Agent Information 3-18
Postinstallation Tasks: Configuring the Audit Vault Components 3-19
Managing the Audit Vault Agent 3-20
Starting the Components in an Audit Vault Configuration 3-21
Summary 3-22
Practice 3: Overview 3-23

4 Configuring Oracle Audit Vault

Objectives 4-2
Registering Sources and Deploying Collectors 4-3
Overview of Oracle Database Collectors 4-4
Using the DBAUD Collector 4-5
Oracle Database Collectors: DBAUD 4-6
Using the OSAUD Collector 4-7
Oracle Database Collectors: OSAUD 4-8
Oracle Database Collectors: REDO 4-9
Setting Source Database Initialization Parameters for REDO Collectors 4-11
Quiz 4-12
Basic Steps to Register an Oracle Source Database and Deploy Collectors 4-13
Creating the Source User in the Source Database 4-14
Understanding Audit Vault Users and Configuration Information 4-15
Verifying the Source Database 4-16
Registering the Oracle Source Database 4-17
Configuring Collectors 4-18
Adding Collection Agent Credentials to the Oracle Source Database 4-19
Starting Collectors 4-20
Viewing Collector Information 4-21
Viewing DBAUD Collector Details 4-22
Viewing OSAUD Collector Details 4-23
Viewing REDO Collector Details 4-24
Checking the Collector Status 4-25
Viewing Collector Log Files 4-26
Altering Collector Attributes by Using Audit Vault Console 4-27
Altering Collector Attributes 4-28
Quiz 4-29
Using a Microsoft SQL Server Source Database 4-30
Overview: Registering Microsoft SQL Server Database Sources and Collector 4-31
Using a Sybase ASE Source Database 4-32
Overview: Registering Sybase ASE Database Sources and Collector 4-33
Using an IBM DB2 Source Database 4-34

Overview: Registering IBM DB2 Database Sources and Collector 4-35
Summary 4-36
Practice 4: Overview 4-37

5 Managing Audit Settings

Objectives 5-2
Using Audit Vault to Collect Audit Data 5-3
Oracle Database Auditing 5-4
Comparing Types of Auditing 5-5
Auditing Guidelines 5-6
Database Auditing 5-7
Enabling Auditing 5-8
Enabling Auditing on the Source Database 5-9
Performing Database Auditing 5-10
Focusing Database Auditing: Statement Execution 5-11
Specifying `WHENEVER SUCCESSFUL` 5-12
Specifying `WHENEVER NOT SUCCESSFUL` 5-13
Focusing Database Auditing: Number of Audit Records Generated 5-14
Specifying `BY SESSION` 5-15
Specifying `BY ACCESS` 5-16
Quiz 5-17
Fine-Grained Auditing 5-18
Creating a Fine-Grained Auditing Policy 5-19
Audited DML Statement: Considerations 5-21
Fine-Grained Auditing Guidelines 5-22
Auditing `SYSDBA` and `SYSOPER` Operations 5-23
Managing the Audit Trail 5-24
Moving the Database Audit Trail from the `SYSTEM` Tablespace 5-25
Purging Audit Trail Records 5-26
Collecting Data from the Redo Log Files 5-27
Understanding the Streams Capture Process 5-28
Using Audit Vault Console to Manage Audit Settings 5-29
Retrieving Audit Settings 5-30
Defining Audit Settings 5-31
Applying Audit Settings to the Source Database 5-32
Exporting Audit Settings to a File 5-33
Reconciling Retrieved Settings and Settings Specified in Audit Vault 5-34
Copying Audit Settings from a Source Database 5-35
Quiz 5-36
Setting a Retention Period for Audit Data 5-37
Viewing Audit Event Category Information 5-38

Summary 5-39
Practice 5: Overview 5-40

6 Configuring for Alerts and Reports

Objectives 6-2
Setting the Time Zone for Reports and Alerts 6-3
Configuring Email Notifications 6-4
Configuring Trouble Ticket Notifications 6-5
Setting Up Notifications 6-6
Creating an Email Notification Profile 6-7
Creating an Email Notification Template 6-8
Creating a Trouble Ticket Template 6-9
Quiz 6-10
Summary 6-11
Practice 6: Overview 6-12

7 Using Audit Vault Reports

Objectives 7-2
Using the Audit Vault Overview Page (Dashboard) 7-3
Finding the Most-Accessed Objects
and Failed Logins 7-4
Reporting Activities 7-5
Understanding Audit Vault Event Categories 7-6
Report Categories 7-8
Accessing Reports 7-9
Filtering Report Data 7-10
Viewing and Filtering Compliance Reports 7-11
Scheduling the Creation of a Report 7-12
Viewing Generated Reports 7-13
Quiz 7-14
Retrieving Entitlement Audit Data 7-15
Viewing Snapshot Data in an Entitlement Report 7-16
Creating Snapshot Labels 7-17
Adding Snapshots to a Label 7-18
Viewing Comparison Snapshot Data in an Entitlement Report 7-19
Quiz 7-20
Attesting Reports 7-21
Attesting and Annotating a Report 7-22
Creating Custom Reports 7-23
Summary 7-24
Practice 7: Overview 7-25

8 Configuring Alerts

- Objectives 8-2
- Alert Processing 8-3
- Creating and Responding to Alerts 8-4
- Enabling and Disabling Alert Processing 8-5
- Creating Alert Status Values 8-6
- Creating an Alert Rule 8-7
- Creating a Basic Alert 8-8
- Creating an Advanced Alert 8-9
- Quiz 8-10
- Viewing Alert information 8-11
- Viewing Alerts 8-13
- Responding to an Alert 8-14
- Summary 8-15
- Practice 8: Overview 8-16

9 Securing Oracle Audit Vault

- Objectives 9-2
- Oracle Audit Vault: Security Components 9-3
- Integration with Oracle Database Vault 9-4
- Managing Users and Roles in the Audit Vault Server 9-5
- Unlocking and Resetting User Passwords 9-6
- Enabling Remote SYSDBA Privilege Connections 9-7
- Audit Vault Database Users 9-8
- Understanding Audit Vault Usage 9-10
- Managing User Authentication Metadata: Audit Vault Server Wallet 9-11
- Managing User Authentication Metadata: Audit Vault Agent Wallet 9-12
- Quiz 9-13
- Securing Audit Vault Server and Audit Vault Agent Communication 9-14
- Securing the HTTP-Based Communication Channel 9-15
- Securing XDB Services 9-17
- Using Oracle Advanced Security Option Encryption 9-18
- Setting Encryption Parameters on the Audit Vault Server Host 9-19
- Updating the Wallets 9-21
- Updating the Audit Vault Server Wallet 9-22
- Updating the Audit Vault Agent Wallet 9-23
- Summary 9-24
- Practice 9: Overview 9-25

10 Managing Your Oracle Audit Vault Configuration

- Objectives 10-2
- Monitoring the `SYSAUX` Tablespace 10-3
- Monitoring the Archived Redo Log Destination 10-4
- Viewing Flash Recovery Area Usage Information 10-5
- Backing Up Oracle Audit Vault 10-6
- Using AVCTL to View the Status of Audit Vault Components 10-7
- Quiz 10-9
- Managing Audit Vault Server Log and Error Files 10-10
- Managing Audit Vault Collection Agent Log and Error Files 10-12
- Managing Audit Vault Agent Log and Error Files 10-13
- Troubleshooting Collection Agent Problems 10-14
- Verifying that DBAUD Collector is Collecting 10-15
- Verifying that OSAUD Collector is Collecting 10-16
- Summary 10-17
- Practice 10: Overview 10-18

11 Managing the Audit Vault Data Warehouse

- Objectives 11-2
- Audit Vault Data Warehouse: Overview 11-3
- Audit Vault Data Warehouse: Schema 11-4
- Understanding Dimensions 11-5
- Audit Vault Data Warehouse: Dimensions 11-6
- Automatic Refresh of the Data Warehouse 11-7
- Quiz 11-8
- Scheduling Data Warehouse Operations and Viewing Historical Information 11-9
- Controlling the Data Warehouse Retention Time 11-10
- Configuring the Data Warehouse Retention Time 11-11
- Loading Additional Data into the Data Warehouse 11-12
- Purging the Data Warehouse 11-13
- Summary 11-14
- Practice 11: Overview 11-15