

Oracle Database 11g: Implement Database Vault

Student Guide

D52474GC10

Edition 1.0

August 2008

D55707

ORACLE®

Authors

Tom Best
James Spiller
Deirdre Matishak

Technical Contributors and Reviewers

Tom Bolick
John Boyle
Harald van Breederode
Jack Brinson
M.J. Bryksa
Madhavi Buchi
Ben Chang
Chi Ching Chui
Scott Gaetjen
Greg Gagnon
Philip Garm
Joel Goodman
Thomas Hoogerwerf
Pat Huey
Sushma Jagannath
Donna Keesling
Russ Lowenthal
Yi Lu
Kurt Lysy
Sabiha Miri
Paul Needham
Roman Niehoff
Ashwini Surpur
Kamal Tbeileh
Peter Wahl
Anthony Woodell
John Zimmerman

Editors

Vijayalakshmi Narasimhan
Aju Kumar

Publishers

Sujatha Nagendra
Veena Narasimhan
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
- Suggested Schedule 1-3
- What Is Database Vault? 1-4
- Database Vault Option 1-5
- Benefits of Database Vault 1-6
- Database Vault: Effects 1-8
- Database Vault Versus VPD and OLS 1-9
- Access Control Components 1-10
- Realms: Introduction 1-11
- Factors: Introduction 1-12
- Identities: Introduction 1-13
- Rule Sets: Introduction 1-14
- Command Rules: Introduction 1-15
- Secure Application Roles: Introduction 1-16
- Component Relationships: Static 1-17
- Component Relationships: Dynamic 1-18
- Scenarios 1-19
- Database Vault Example: Separation of Duties 1-20
- Database Vault Administrator (DVA) 1-21
- Reporting 1-22
- Monitoring 1-23
- Database Vault API 1-24
- Summary 1-25

2 Installing Database Vault

- Objectives 2-2
- Installation and Configuration: Overview 2-3
- Installation Requirements 2-4
- Database Vault Software: Preinstallation Steps 2-5
- Running OUI to Install Oracle Database Vault Option 2-6
- Database Vault Software: Postinstallation Steps 2-10
- Using `dbca` to Register Oracle Database Vault 2-11

Database Parameters Altered During Configuration 2-13
Performing a Clustered Installation 2-15
Logging In to Database Vault Administrator 2-16
Database Vault Roles 2-17
Database Vault Accounts 2-19
DV_OWNER Versus DV_ACCTMGR 2-20
Database Vault Schemas 2-21
Summary 2-22
Practice 2 Overview: Installing Database Vault 2-23

3 Configuring Realms

Objectives 3-2
Realms: Concepts 3-3
Realms: Static Component Context 3-4
Realms: Dynamic Component Relationships 3-5
Realms: Concepts 3-6
Effect of Realms on Nonmembers 3-7
Benefits of Using Realms 3-8
Realm Attributes 3-9
Creating Realms 3-10
Editing Realms 3-11
Adding Objects to Realms 3-12
Adding Authorizations to Realms 3-13
Realm Authorizations and Rule Sets 3-14
Realm Algorithm 3-15
Protecting Objects from DBAs by Using Realms: Example 3-16
Schema Owner Access: Example 3-17
Greatest Level of Access 3-18
Protecting Roles by Using Realms 3-19
Protecting Roles: Example 3-21
Delivered Realms 3-23
Realm Views 3-24
Realm Views Relative to DVA 3-26
Realm Reporting: Configuration Issues 3-27
Realm Audit Report 3-28
Realm API 3-29
Summary 3-30
Practice 3 Overview: Configuring Realms 3-31

4 Defining Factors

- Objectives 4-2
- Factors: Static Component Context 4-3
- Factors: Dynamic Component Relationships 4-4
- Factors: Concepts 4-5
- Using Factors 4-6
- Predefined Factors 4-7
- Factors and Contexts 4-9
- Factor Scenarios 4-10
- Creating and Editing Factors 4-11
- The Create Factor Page 4-12
- Factor Types 4-13
- Factor Identification 4-14
- Factor Evaluation 4-15
- Retrieval Method 4-16
- DVSYST.SET_FACTOR 4-17
- Validation Method 4-18
- Factor Audit Options 4-19
- Error Options 4-20
- Deleting Factors 4-21
- Factor Views 4-22
- Factor Configuration Issues Report 4-23
- Factor Audit Report 4-24
- Factors API 4-25
- Summary 4-27
- Practice 4 Overview: Working with Factors 4-28

5 Defining Identities

- Objectives 5-2
- Identities: Static Component Context 5-3
- Identities: Dynamic Component Relationships 5-4
- Identities: Concepts 5-5
- Purpose of Identities 5-6
- Identity Example: All Possible Identities 5-7
- Identity Example: Adding Trust Levels 5-8
- Identity Example: Mapping Child Factors 5-9
- Editing Factors: Creating an Identity 5-10
- Creating an Identity 5-11
- Trust Levels 5-12
- Mapping Identities 5-14
- Identities Mapped to Factors: Examples 5-16

- Map Conditions 5-17
- Deleting Identities 5-18
- Integrating Factors and Oracle Label Security 5-19
- Oracle Label Security 5-20
- Oracle Label Security Policies 5-21
- Editing OLS Policies 5-22
- OLS Merge Algorithms 5-23
- Factor Labeling 5-24
- Identities and OLS 5-25
- Identity View 5-26
- Identity Map View 5-27
- Factors Without Identities Report 5-28
- Identity Configuration Issues Report 5-29
- Label Security Integration Audit 5-30
- Identities API 5-31
- Summary 5-32
- Practice 5 Overview: Managing Identities 5-33

6 Defining Rule Sets

- Objectives 6-2
- Rule Sets: Concepts 6-3
- Rule Sets: Static Component Context 6-5
- Rule Sets: Dynamic Component Relationships 6-6
- Using Rule Sets 6-7
- Rule Sets 6-8
- Creating a Rule Set 6-9
- Adding Existing Rules to a Rule Set 6-11
- Creating a Rule 6-12
- Reusing Rules 6-13
- Auditing Rule Sets 6-14
- Setting a Custom Event Handler 6-15
- Using Rule Sets with Realms 6-16
- Assignment Rule Sets for Factors 6-17
- Creating a Rule Set: Example 6-18
- Editing the New Rule Set: Example 6-20
- Adding Rules to the New Rule Set: Example 6-21
- Verifying the Rule Set Logic: Example 6-23
- Adding the Rule Set to a Factor: Example 6-24
- Delivered Rule Sets 6-25
- “Can Maintain Own Account” Rule Set 6-26
- Enabled and Disabled Rule Sets 6-27

Rule Set Views 6-28
Rule Set Reporting: Configuration Issues 6-29
Rule Set API 6-30
Summary 6-31
Practice 6 Overview: Managing Rule Sets 6-32

7 Configuring Command Rules

Objectives 7-2
Command Rules: Concepts 7-3
Command Rules: Static Component Context 7-4
Command Rules: Dynamic Component Relationships 7-5
Command Rules Page 7-6
Command Rule Attributes 7-7
Identifying a Command Rule 7-8
Command Rule: Example 7-9
Preventing Users from Using ALTER TABLE in a Schema: Example 7-12
Delivered Command Rules 7-13
DBA_DV_COMMAND_RULE View 7-15
Command Rule Report 7-16
Command Rule API 7-17
Summary 7-18
Practice 7 Overview: Managing Command Rules 7-19

8 Configuring Secure Application Roles

Objectives 8-2
Secure Application Roles: Static Component Context 8-3
Secure Application Roles: Dynamic Component Relationships 8-4
Secure Application Roles: Concepts 8-5
Secure Application Role 8-6
Using a Secure Application Role 8-7
Secure Application Role Changes in Database Vault 8-8
Creating a Rule Set 8-9
Creating Rules 8-10
Creating Secure Application Roles 8-11
Deleting Secure Application Roles 8-12
Examples 8-13
Secure Application Role Views 8-15
Secure Application Configuration Issues 8-16
Secure Application Role Audit 8-17

Secure Application Roles API 8-18
Summary 8-19
Practice 8 Overview: Managing Secure Application Roles 8-20

9 Viewing Reports

Objectives 9-2
Required Privileges 9-3
Reporting Needs 9-4
Database Vault Monitor 9-5
Security Policy Changes Detail 9-6
Security Violation Attempts 9-7
Database Configuration and Structural Changes 9-8
Database Vault Reports 9-9
Database Vault Configuration Issues Reports 9-11
Reviewing Database Vault Configuration 9-13
Database Vault Auditing Reports 9-14
Reviewing Database Vault Audit Reports 9-16
General Security Reports 9-17
Object Privilege Reports 9-18
Object Privileges by PUBLIC 9-19
Object Dependencies 9-20
Database Account System Privileges Reports 9-21
System Privileges by Database Account Reports 9-22
Sensitive Objects Reports 9-23
Privilege Management: Summary Reports 9-25
Review Privilege Reports 9-26
Powerful Database Accounts and Roles Reports 9-27
Using Powerful Database Accounts and Roles Reports 9-29
Initialization Parameters and Profiles Reports 9-30
Database Account Password Reports 9-31
Security Audit Report: Core Database Audit Report 9-32
Other Security Vulnerabilities Reports 9-33
Summary 9-35
Practice 9 Overview: Viewing Reports 9-36

10 Implementing Best Practices

Objectives 10-2
Identifying Your Security Requirements 10-3
Separation of Duty Best Practice 10-4

Separation of Duty Matrix	10-5
Application Protection Matrix	10-6
Building and Documenting Your Implementation	10-7
Trusted People for Trusted Positions	10-8
Recommended Naming Conventions	10-9
Transition to Production	10-10
Implementing Separation of Duties	10-11
Application DBA: Attributes	10-12
Application DBA: Implementation	10-13
Application DBA: Example	10-14
Application DBA: Result	10-17
Dual Key Security	10-18
Dual Key Security: Realm Access Example	10-19
Dual Key Security: Procedure Execution Example	10-20
Database Account Considerations	10-21
Dynamic Auditing	10-23
Protecting from Accidental Object Loss	10-24
Connection Pooling Considerations	10-25
Enforcing Connections from an Application Server	10-26
Fast Response to Policy Changes	10-27
Performance Considerations: Auditing	10-28
Performance Considerations: Unused Factors	10-29
Diagnosing Database Vault Using Trace Files	10-30
Enabling and Disabling Database Vault	10-31
Steps for Disabling Database Vault	10-32
Steps for Enabling Database Vault	10-33
Password Policy Considerations	10-34
Guidelines for Procedures and Packages	10-35
Other Guidelines	10-37
Miscellaneous Recommendations	10-39
Summary	10-40
Practice 10 Overview: Implementing Best Practices	10-41

Appendix A: Practices and Solutions

Index

