

Contents

I Introduction

Objectives 1-2

1 Managing Endpoints and Oracle Wallets

Objectives 1-2

What You Already Know About Endpoints 1-3

Endpoints 1-5

Endpoint Administrators 1-6

Managing Oracle Key Vault Endpoints 1-7

Enrolling, Provisioning, and Using an Endpoint 1-8

Types of Enrollment 1-9

Enrolling and Provisioning an Oracle Key Vault Endpoint 1-10

What You Already Know About Oracle Wallets 1-11

What You Already Know About Encryption 1-12

Creating and Opening the Keystore 1-13

Reviewing Transparent Data Encryption 1-14

Creating TDE Encrypted Test Data 1-15

Training Environment and Workflow 1-16

What Is a Virtual Wallet? 1-17

Managing Security Objects 1-18

Uploading and Downloading an Oracle Wallet to and from Oracle Key Vault 1-19

Downloading an Oracle Wallet 1-20

Summary 1-21

Practice 1: Overview 1-22

2 Encryption

Learning Objectives 2-2

Need for Encryption 2-3

Encryption: Overview 2-4

Encryption Is Not Access Control 2-5

Access by Privileged Users 2-6

What problems does encryption solve? 2-8

Cost of Encryption 2-9

What to Encrypt 2-10

Data Encryption: Challenges 2-11

Encrypting Data in Motion 2-12

Native Network Encryption 2-13

Configuring Network Encryption and Data Integrity 2-15

- TLS Encryption 2-17
- Using SSL 2-18
- How SSL Works in an Oracle Environment: The SSL Handshake 2-19
- SSL Authentication Process 2-20
- Encryption Wallets 2-21
- Transparent Data Encryption 2-22
- Components of TDE 2-23
- Column and Tablespace Level Encryption 2-24
- Creating Your Own TDE Master Encryption Key 2-26
- Encryption Key Management: Key Generation 2-27
- Encryption Key Management: Key Modification and Transmission 2-28
- Encryption Key Management: Storage 2-29
- Storing the Key in the Database 2-30
- Storing the Key in the File System 2-32
- Letting the User Manage the Key 2-33
- SYSKM Administrative Privilege 2-34
- Encrypting the Data Dictionary 2-35
- Conversion of Tablespaces: ONLINE Encryption 2-36
- Encryption Algorithms 2-37
- Automatic Tablespace Encryption 2-38
- Oracle Key Vault 2-39
- Summary 2-40
- Practice 2: Overview 2-41

3 Key Vault and Transparent Data Encryption

- Objectives 3-2
- Benefits of Using Oracle Key Vault 3-3
- Benefits of Using Oracle Transparent Data Encryption 3-4
- Reviewing Hardware Security Modules 3-5
- Separation of Duties 3-6
- Using the Online Master Key with Oracle Key Vault 3-7
- Using Security Objects 3-8
- Summary 3-9
- Practice 3: Overview 3-10

4 Performing Oracle Key Vault Administrative Tasks

- Objectives 4-2
- Administrative Tools 4-3
- Performing Tasks as System Administrator 4-4
- Backing Up and Restoring Data for Oracle Key Vault 4-5
- Performing Tasks as Key Administrator 4-6

Performing Tasks as Audit Manager 4-7
Oracle Key Vault Management Reports 4-8
Best Practices for Oracle Key Vault 4-9
Summary 4-11
Practice 4: Overview 4-12