

Hardware and Software
Engineered to Work Together



Using Oracle Key Vault

Student Guide
D88454GC10
Edition 1.0 | December 2014

Learn more from Oracle University at oracle.com/education/

Copyright © 2014, 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

1 Introduction

- Course Objectives 1-2
- Oracle Key Vault Course: Overview 1-3
- Objectives 1-4
- What Is Oracle Key Vault? 1-5
- Challenges of Key Management 1-6
- Centralized Management of Security Objects 1-7
- Oracle Key Vault Environment 1-8
- High Availability for Oracle Key Vault 1-9
- What Are Endpoints? 1-10
- What Is a Virtual Wallet? 1-11
- Quiz 1-12
- Summary 1-13
- Practice 1: Overview 1-14

2 Installing Oracle Key Vault

- Objectives 2-2
- Oracle Key Vault Administrators 2-3
- Oracle Key Vault Users and Roles 2-4
- Oracle Key Vault System Administrator 2-5
- Key Administrator 2-6
- Oracle Key Vault Audit Manager 2-7
- Sample Users and Roles 2-8
- Installation Requirements 2-9
- Initial Installation and Configuration 2-10
- Understanding Your Training Configuration 2-12
- Quiz 2-13
- Summary 2-14
- Oracle Key Vault Getting Started 2-15
- Practice 2: Overview 2-16

3 Working with Endpoints

- Objectives 3-2
- Course Overview 3-3
- What You Already Know About Endpoints 3-4
- Endpoints 3-6

Endpoint Administrators	3-7
Managing Oracle Key Vault Endpoints	3-8
Enrolling, Provisioning, and Using an Endpoint	3-9
Types of Enrollment	3-10
Enrolling and Provisioning an Oracle Key Vault Endpoint	3-12
Quiz	3-13
Summary	3-14
Practice 3: Overview	3-15

4 Managing Oracle Wallets

Objectives	4-2
What You Already Know About Oracle Wallets	4-3
What You Already Know About Encryption	4-4
Creating and Opening the Keystore	4-5
Reviewing Transparent Data Encryption	4-6
Creating TDE Encrypted Test Data	4-7
Setting Up Encrypted Data in Oracle Databases	4-8
Training Environment and Workflow	4-9
What Is a Virtual Wallet?	4-10
Managing Security Objects	4-11
Uploading and Downloading an Oracle Wallet to and from Oracle Key Vault	4-12
Downloading an Oracle Wallet	4-13
Videos	4-14
Quiz	4-15
Summary	4-16
Practice 4: Overview	4-17

5 Using Direct TDE with Oracle Database 12c

Objectives	5-2
Reviewing Hardware Security Modules	5-3
Separation of Duties	5-4
Using the TDE Direct Connection with Oracle Key Vault	5-5
Using Security Objects	5-6
Quiz	5-7
Summary	5-8
Practice 5: Overview	5-9

6 Performing Administrative Tasks

Objectives	6-2
Administrative Tools	6-3
Performing Tasks as System Administrator	6-4

Video: Backing Up and Restoring Data for Oracle Key Vault	6-5
Performing Tasks as Key Administrator	6-6
Performing Tasks as Audit Manager	6-7
Oracle Key Vault Management Reports	6-8
Best Practice Tips for Oracle Key Vault	6-9
Quiz	6-11
Summary	6-12
Practice 6: Overview	6-13
Summary	6-14
Continuing Your Learning	6-15

1

Introduction

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Course Objectives

After completing this course, you should be able to:

- Install and configure Oracle Key Vault
- Enroll and provision endpoints
- Upload and download Oracle Wallets
- Use TDE direct connection to Oracle Database 12c
- Perform day-to-day administrative functions

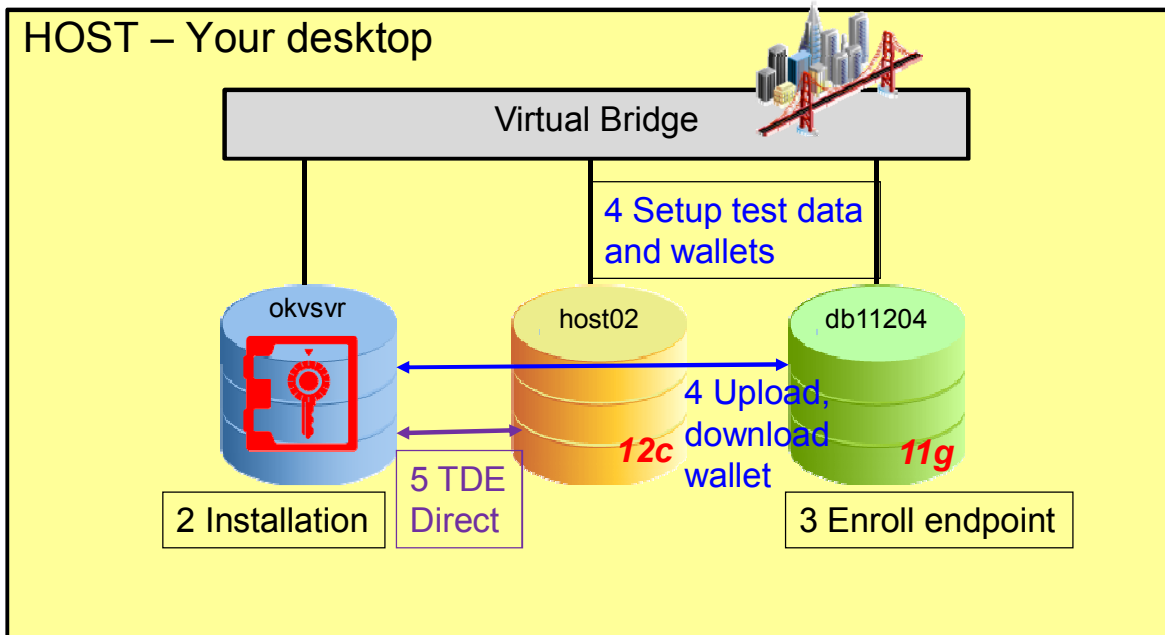
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Key Vault Course: Overview

1 Introduction

6 Admin tasks



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This slide introduces you to your training setup with three virtual machines (VMs) and the overall course topics.

The host machine is the machine that contains your desktop, from where you connect to the VMs:

- `okvsrv` is the VM for Oracle Key Vault.
- `host02` contains Oracle Database 12c.
- `db11204` contains Oracle Database 11gR2 patchset 4.

The course topics include:

1. Introduction
2. Installing and configuring Oracle Key Vault
3. Enrolling and provisioning endpoints
4. Uploading and downloading Oracle Wallets
5. Using TDE direct connection to Oracle Database 12c
6. Performing administrative functions

Objectives

After completing this lesson, you should be able to:

- Describe the functionality and benefits of Oracle Key Vault
- Identify the major concepts of Oracle Key Vault
- Analyze how Oracle Key Vault can assist in meeting the challenges of key and wallet management

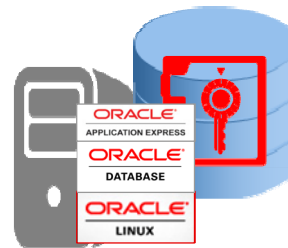
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The overall objective for this lesson is to provide an overview of Oracle Key Vault, so that you can determine whether this product would assist you with the key management challenges in your organization.

What Is Oracle Key Vault?

- Is a central, secure, key management platform for Oracle wallets, Java keystores, and credential files
- Is optimized to manage Oracle Advanced Security TDE master keys
- Is a turnkey solution based on a hardened stack
- Includes separation of duties
- Is a security-hardened software appliance:
 - Pre-configured operating system
 - Oracle database and your choice of security options
 - Oracle Key Vault application

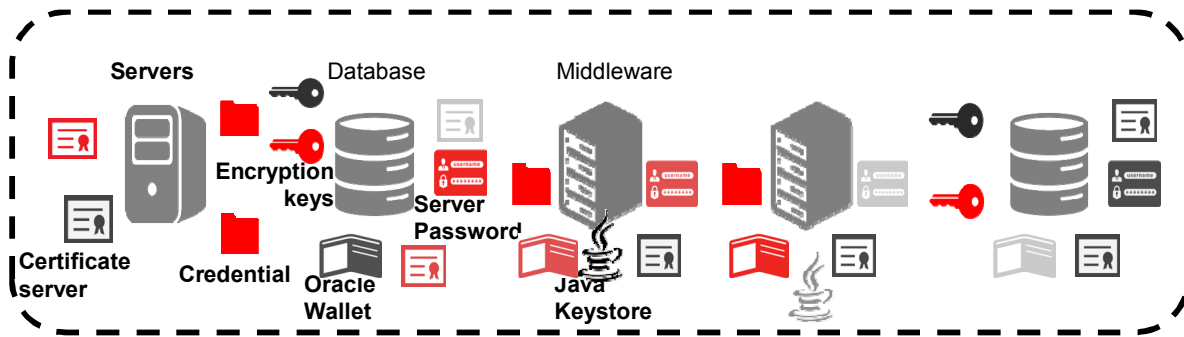


ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Oracle Key Vault is a central, secure key, management platform.
- It centrally manages encryption keys such as Oracle wallets, Java keystores, and credential files, and is optimized for Oracle Advanced Security Transparent Data Encryption (TDE) master keys.
- In other words, Oracle Key Vault is a turnkey solution that is based on a hardened stack. It is easy to install, configure, deploy, and patch.
- Oracle Key Vault includes separation of duties for administrative users, full auditing, preconfigured reports, and alerts.
- The full-stack, security-hardened software appliance uses Oracle Linux and Oracle Database technology for security, availability, and scalability. Oracle Key Vault (OKV) is a software appliance, which is delivered as a bootable disk image that contains a Linux installer that must be installed on its own dedicated server. It consists of a pre-configured operating system, an Oracle database, and the Oracle Key Vault application [built by using Oracle Application Express (APEX)].

Challenges of Key Management



Managerial challenges:

- Proliferation of encryption wallets and keys
- Authorized sharing of keys
- Key availability, retention, and recovery
- Custody of keys and key storage files

Regulatory challenges:

- Physical separation of keys from encrypted data
- Periodic key rotations
- Monitoring and auditing of keys
- Long-term retention of keys and encrypted data

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

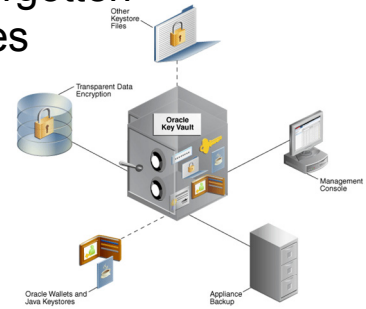
Why is Oracle Key Vault an important product?

Security threats and increased regulation of personally identifiable information, payment card data, healthcare records, and other sensitive information have expanded the use of encryption in a data center. As a result, management of encryption keys, certificates, wallets, and other secrets has become a vital part of the data center, impacting both security and business continuity.

Oracle Key Vault is a central, secure, key management product that addresses the managerial and regulatory challenges listed in the slide. It facilitates deployment of encryption across the enterprise.

Centralized Management of Security Objects

- Centralizes security objects such as encryption keys, Oracle Wallets, Java keystores, credential files, certificates, passwords, and opaque objects
- Secures, shares, and manages keys and secrets for enterprises
- Manages lifecycle stages, including creation, rotation, and expiration
- Prevents loss of keys and wallets due to forgotten passwords or accidentally deleted keystores
- Offers management console as the graphical user interface



ORACLE

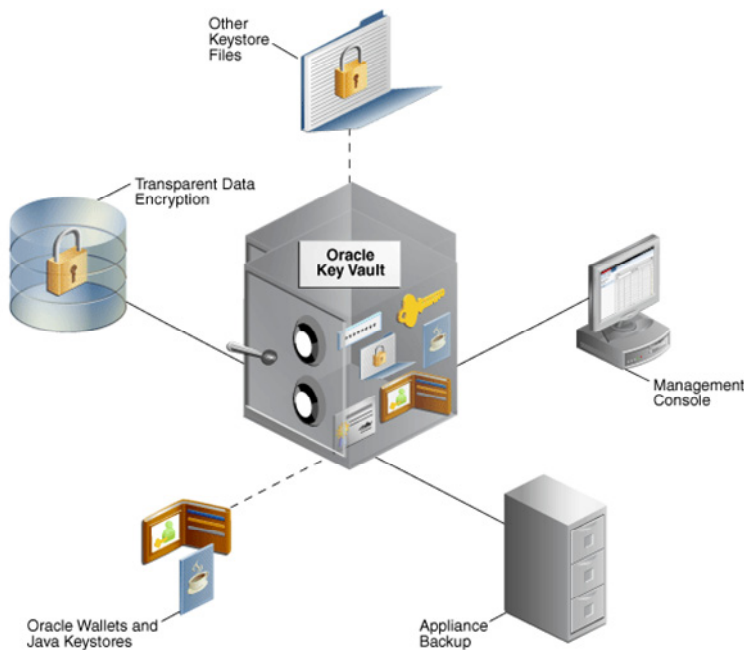
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Key Vault enables customers to quickly deploy encryption and other security solutions by centrally managing encryption keys, Oracle Wallets, Java keystores, and credential files.

The centralized Oracle Key Vault platform enables you to achieve the following:

- Manage the key life cycle, including creation, rotation, and removal, for all endpoints. This includes the ability to share access to security objects among multiple endpoints. Endpoints can be databases, middleware, and other data sources that contain the keys that you want to manage with Oracle Key Vault.
- Prevent the loss of keys and wallets due to forgotten passwords or accidentally deleted wallets and keystores.
- Log in to the graphical management console (which is an APEX application) to perform your tasks.

Oracle Key Vault Environment



- Transparent Data Encryption
- Other keystore files
- Management console
- Appliance backup
- Oracle Wallets and Java keystores

ORACLE

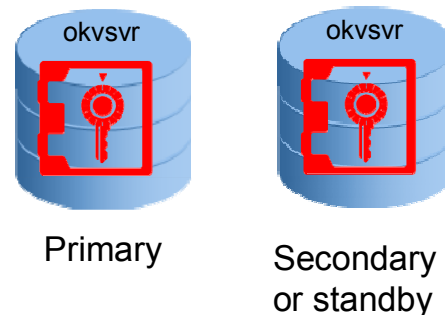
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Key Vault works with the following elements:

- Transparent Data Encryption (TDE) refers to Oracle databases that have tables and tablespaces configured to use TDE.
- Other keystore files can be Java JCEKS keystores that you upload to Oracle Key Vault from endpoints or download from Oracle Key Vault to endpoints.
- Management console refers to the Oracle Key Vault graphical user interface, which you log in to, to manage the objects that you upload to Oracle Key Vault.
- Appliance backup refers to a backup device for Oracle Key Vault data, which you configure for a high availability environment.
- Oracle Wallets and Java keystores refer to the wallets and keystores that you upload to Oracle Key Vault and download to endpoints.

High Availability for Oracle Key Vault

- Recommended to ensure continued access to your security objects
- Configuration:
 - Providing each other's IP address and certificate
 - Before enrolling endpoints
- Primary: Servicing endpoint requests
- Standby: Ready to take over if primary fails
- Switchable roles



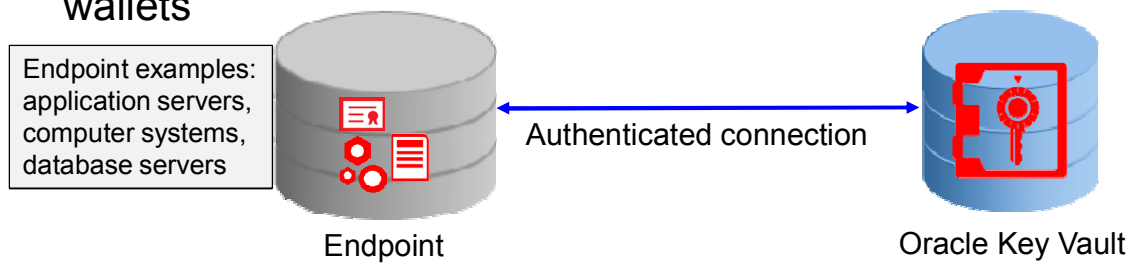
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Oracle recommends that you configure high availability to ensure continued access to your security objects if Oracle Key Vault fails.
- Configuring HA involves connecting to the primary appliance and providing it with the IP address and certificate of the standby, and then doing the same thing for the primary in the standby appliance.
- If you plan to configure high availability, you must do so before you begin to create endpoints. An endpoint knows about the standby appliance only if the standby was configured before the endpoint was enrolled.
- The primary appliance is the one that services requests from endpoints. The standby appliance takes over as the primary if the primary fails for any reason. You can switch primary and standby nodes and even unconfigure high availability.

What Are Endpoints?

- Are systems where cryptographic operations occur
- Request Key Vault to store and retrieve security objects
- Are easy to enroll and provision:
 - Single package with binaries, configuration files, and endpoint certificates
 - Mutually authenticated connections with Oracle Key Vault
- Support industry standard OASIS KMIP protocol
- Can be grouped for ease of management and sharing of wallets

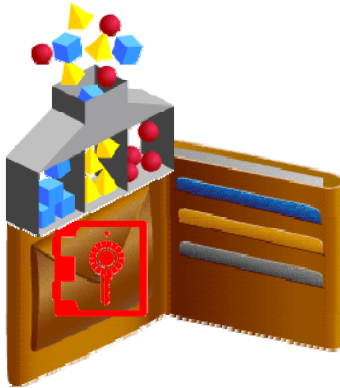


Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Endpoints are the database servers, application servers, and computer systems where actual cryptographic operations, such as encryption or decryption, are performed.
- Endpoints request Oracle Key Vault to store and retrieve security objects.
- It is easy to enroll and provision endpoints, that is, to configure the connections between Oracle Key Vault and endpoints. Endpoint provisioning uses a single package that contains all the necessary software binaries and configuration files, as well as the endpoint certificates, needed for mutually authenticated connections with Oracle Key Vault.
- OASIS Key Management Interoperability Protocol (KMIP) standardizes the key management operations between the key management servers and the endpoints that are provided by different vendors. See also: <http://docs.oasis-open.org/kmip/spec/v1.1/os/kmip-spec-v1.1-os.html> for information about the OASIS KMIP specification.
- You can group endpoints for ease of management. For example, if the nodes of an Oracle RAC cluster are set up in an endpoint group, they can share wallets and wallet contents.

What Is a Virtual Wallet?

- Is a container for the security objects that you upload from endpoints
- Is a grouping of keys and other security objects in Oracle Key Vault
- Enables shared access to security objects by group of server endpoints (not by groups of users)



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Oracle Key Vault allows grouping of keys and other security objects to form a virtual wallet. These security objects are typically public and private keys, TDE master encryption keys, passwords, credentials, certificates, and so on.
- The main purpose of a virtual wallet is to allow access to security objects by endpoints other than the endpoint that created the objects. Key administrators create virtual wallets. After creation, you can assign or remove access from an endpoint or endpoint group to a virtual wallet.
- For ease of management and sharing, you can provide access for a group of server endpoints to a virtual wallet.

Quiz

Select all statements that are TRUE for Oracle Key Vault:

- a. Oracle Key Vault is a software appliance that can be installed on an open x86-64 hardware.
- b. Oracle Key Vault centralizes the management of encryption keys, Oracle Wallets, Java keystores, and credential files.
- c. Security objects can be grouped, but they cannot be shared between endpoints and users.
- d. Oracle Key Vault supports separation of duties.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a, b, d

Summary

In this lesson, you should have learned how to:

- Describe the functionality and benefits of Oracle Key Vault
- Identify the major concepts of Oracle Key Vault
- Analyze how Oracle Key Vault can assist with meeting the challenges of key and wallet management

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Practice 1: Overview

This practice covers the following topic:

- 1-1: Introduction

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This practice involves self-assessment. It includes pointers to additional material.

2

Installing Oracle Key Vault

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Objectives





After completing this lesson, you should be able to:

- Determine how separation of duties is implemented with Oracle Key Vault
- Distinguish between the Oracle Key Vault administrators
- Install Oracle Key Vault
- Perform post-installation configuration tasks

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Key Vault Administrators

- Separation of duties for secure systems
- Oracle Key Vault predefined roles:
 - System administrator 
 - Key administrator 
 - Audit manager 
- Two or more administrators performing related parts of an operation
- Endpoint administrator: 
 - No default Oracle Key Vault role
 - Upload and download of security objects between Oracle Key Vault and the endpoint with the `okvutil` utility
 - Role delegated to the DBA or the IT security personnel

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Separation of administrative duties is required for secure systems.
- Oracle Key Vault distinguishes between key, system, and audit management functions. The corresponding roles for these functions are system administrator, key administrator, and audit manager.
- If desired, one user can be granted multiple roles. However, for separation of duties, it is recommended that different users have different administrative roles. This would enable one administrator to perform one part of an operation and the other to perform a different but related part of the operation: for example, only system administrators can enroll endpoints and only key administrators can create endpoint groups.
- Endpoint administrators, by default, do not have a default Oracle Key Vault role. Their task is to upload and download security objects between Oracle Key Vault and the endpoints with the `okvutil` utility. Some organizations delegate the endpoint administrator tasks to their DBAs and other organizations delegate it to their IT security personnel.

Oracle Key Vault Users and Roles

- Oracle Key Vault post-installation includes creating the initial roles and user accounts.
- *After installation:* Only users who have a role can grant or revoke it.
- *Emergency:* Use the recovery passphrase to repeat the post-installation configuration.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Oracle Key Vault post-installation includes creating the initial roles and users.
- After installation, only administrators who have a role can grant it to other administrators or revoke it from them.
- If a situation arises where there are no users with a particular role, you can use the recovery passphrase to repeat the post-installation configuration and grant each role to a new or an existing user account.

Oracle Key Vault System Administrator

- Creates, modifies, and deletes users
- Enrolls endpoints and deletes them
- Sets up high availability
- Configures alerts and key rotation reminders
- Schedules backups
- Starts and stops Oracle Key Vault
- Grants the System Administrator role to and revokes it from other users



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle Key Vault system administrator performs the tasks listed in the slide.

Key Administrator

- Controls user and endpoint access to virtual wallets
- Creates and manages user groups
- Creates and alters endpoint groups
- Has Read, Modify, and Manage access on all virtual wallets and security objects
- Grants the Key Administrator role to other users



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The key administrator manages access to security objects and virtual wallets, and performs the tasks listed in the slide.

Oracle Key Vault Audit Manager

- Manages the audit trail as the only user who has privileges to export or delete Oracle Key Vault audit records
- Has Read access on all security objects
- Grants the Audit Manager role to other users







ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The Oracle Key Vault audit manager manages audit data, which are records of users' and endpoints' actions. For this purpose, this role has Read access on all security objects.

Sample Users and Roles

Separation of duties with:

	 System Administrator	 Key Administrator	 Audit Manager
OKV_SYS_SEAN	YES		
OKV_KEYS_KATE		YES	
OKV_AUD_AUDREY			YES
SYS as SYSDBA	Endpoint administrator		
INFOSEC_ISABEL as SYSKM	Endpoint administrator 		

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide shows the sample users of this training unit:

- OKV_SYS_SEAN as the system administrator
- OKV_KEYS_KATE as the key administrator
- OKV_AUD_AUDREY as the audit manager

The endpoint administrators are:

- SYS as SYSDBA in the 11g instance
- The INFOSEC_ISABEL user as SYSKM in the 12c instance (This user account has been created as part of the course setup.)

Installation Requirements

- System requirements:
 - Dedicated server with a fixed IP address
 - Virtual machines for proof of concept, but **not** for production
- Supported endpoint platforms:
 - Oracle Linux (5.x and 6.x)
 - Solaris (10.x and 11.x)
- Endpoint database requirements:
 - Oracle Database 10g and later: Upload of wallets with the `okvutil` utility
 - Oracle Database 11.2 and later: Direct connections between TDE and Oracle Key Vault

The Oracle logo, consisting of the word "ORACLE" in a white, sans-serif font, centered within a red rectangular background.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide provides an overview of the installation requirements. A “dedicated server” implies that installing Oracle Key Vault removes any existing software on the server. You can use virtual machines for testing and proof of concept. However, deployment on virtual machines is *not* recommended for production systems, because VM administrators may be able to gain access to the underlying keys and secrets stored in Oracle Key Vault.

For detailed requirements, see the *Oracle Key Vault Administrator's Guide*.

Initial Installation and Configuration

- Request a fixed IP address, the network mask, and the gateway address.
- Install the Oracle Key Vault appliance.
- Perform the following one-time [post-installation](#) tasks:
 1. Log in to the Oracle Key Vault server.
 2. Provide a username and password for the key administrator, system administrator, and audit manager.
 3. Establish a longer and more complex recovery passphrase and a process for using it in emergency situations.
- Supply the `root` password and the support user password.
- Keep these lifetime passwords safe.

The Oracle logo, consisting of the word "ORACLE" in a white, sans-serif font, centered within a red rectangular background.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Before you begin, request a fixed IP address, the network mask, and the gateway address from your network administrator.

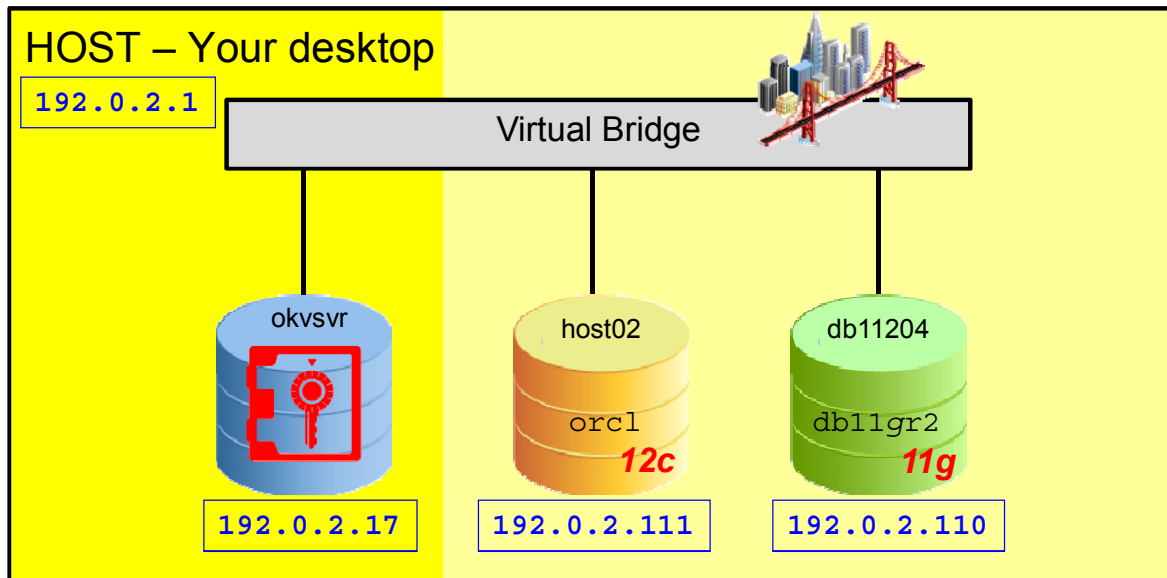
The installation process installs all the required software components onto a dedicated server. The process may take from 30 minutes to an hour to complete, depending on the server resources. The installation process will prompt for network information.

1. Start a web browser with the IP address of the Oracle Key Vault server.
2. Provide the username, password, full name (optional), and email (optional) for the key administrator, system administrator, and audit manager. These different roles exist to support the separation of duty requirements.
3. Establish a longer and more complex recovery passphrase, because it provides access to backups that contain all of the data on Key Vault. Because the recovery passphrase is extremely powerful and infrequently used, it is important to establish a process to store it securely and make it available only in emergency situations.

Supply the `root` password and the support user password that are used for patching, diagnostics, backup, and recovery. Keep these passwords in a safe place because they are critical passwords for the lifetime of the product.

If you restore an existing backup to this appliance, the `root` and support password that you set here will remain the same, but all other data and user passwords will revert to the values they had when the backup was taken. This is also true if the system is added as the standby node of a high availability cluster.

Understanding Your Training Configuration



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The host machine is the machine that contains your desktop. It is from there that you connect to the Virtual Machines (VMs) in your environment.

- `okvsr` is the VM for Oracle Key Vault. This is the first VM to be used.
- `host02` contains the `orcl` Oracle Database 12c.
- `db11204` contains the `db11gr2` Oracle Database 11gR2 patchset 4.

Deployment on virtual machines is *not* recommended for production systems, because VM administrators may be able to gain access to the underlying keys and secrets stored in Oracle Key Vault.

Quiz

Select all statements that are TRUE for Oracle Key Vault:

- a. Endpoint administrators must have a valid Oracle Key Vault role.
- b. Critical Oracle Key Vault roles are configured during post-installation. In an emergency, this step can be repeated.
- c. To install Oracle Key Vault, you need a dedicated server with a fixed IP address.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b, c

Summary

In this lesson, you should have learned how to:

- Determine how separation of duties is implemented with Oracle Key Vault
- Distinguish between the Oracle Key Vault administrators
- Install Oracle Key Vault
- Perform post-installation configuration tasks

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Key Vault Getting Started

VIDEO 1: Installing Oracle Key Vault

- Know a fixed IP address, the network mask, and the gateway address.
- Install the Oracle Key Vault appliance.

VIDEO 2: Performing Post-Installation Tasks

- Perform the following one-time post-installation tasks:
 1. Log in to the Oracle Key Vault server.
 2. Provide a username and password for the key administrator, system administrator, and audit manager.
 3. Establish a longer and more complex recovery passphrase and a process for using it in emergency situations.
 4. Supply the `root` and support user passwords.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The video titled “Installing Oracle Key Vault” shows you how to install an Oracle Key Vault appliance. The video titled “Performing Post-Installation Tasks” covers the basic Oracle Key Vault installation and configuration topic.

In the second video, you learn how to use the one-time Post-Install Configuration page to establish administrative roles and a recovery passphrase for Oracle Key Vault and optionally, familiarize yourself with the OKV management console.

Practice 2: Overview

This practice covers the following topics:

- 2-1: Installing Oracle Key Vault
- 2-2: Performing Post-Installation Tasks

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In seminars, you will view videos of the practices. In classroom environments, you will have hands-on practices, in addition to viewing the videos.

3

Working with Endpoints

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Objectives

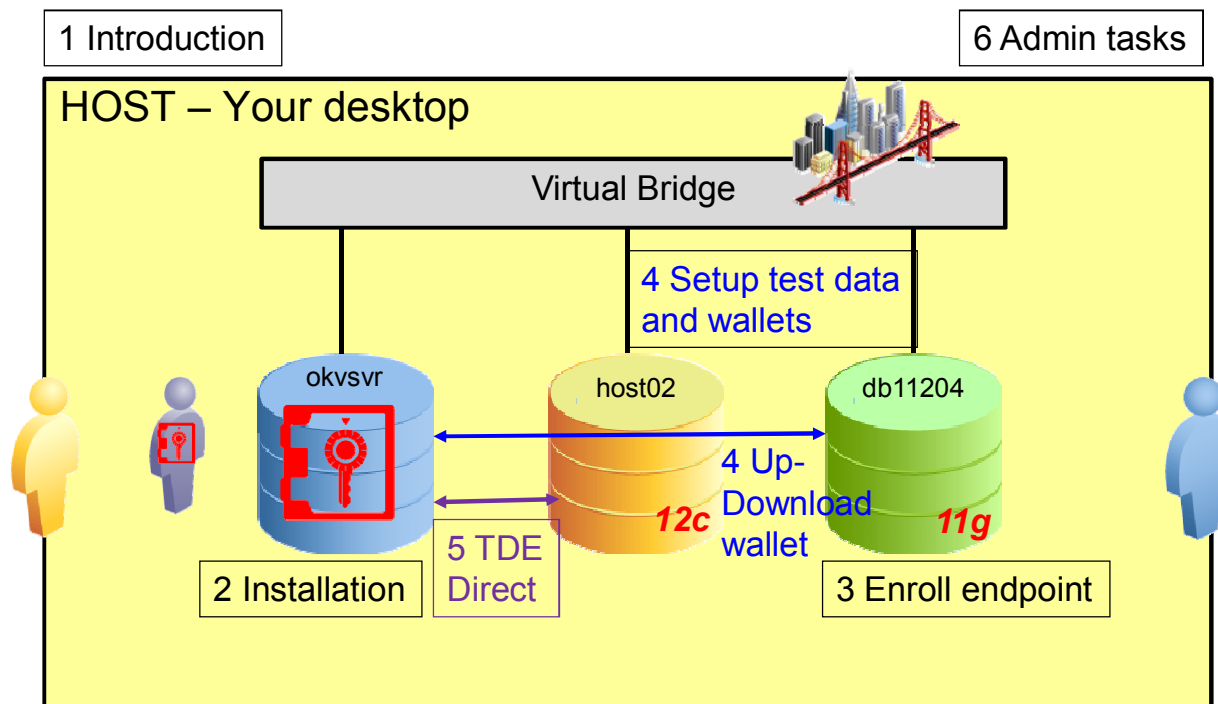
After completing this lesson, you should be able to:

- Practice separation of duties while performing Oracle Key Vault tasks
- Enroll and provision an Oracle Database 11g Release 2 database as an Oracle Key Vault endpoint

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Course Overview



ORACLE

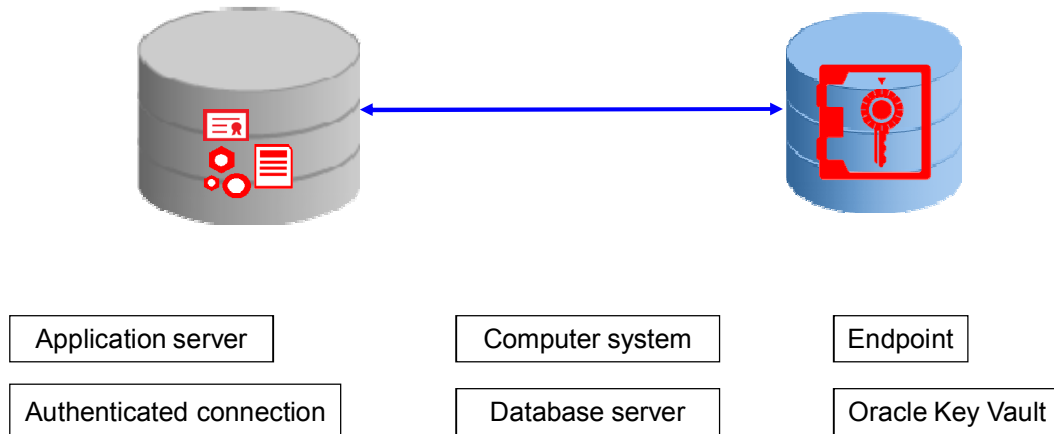
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

After installing and configuring Oracle Key Vault, this lesson focuses on the Oracle Key Vault endpoints. You can register the databases or other endpoints that contain the keys, credentials, and other secure data with Oracle Key Vault.

To implement separation of duties, the enrollment tasks are divided between the system administrator and the endpoint administrator. The endpoint management tasks are divided between the system administrator, key administrator, and endpoint administrator.

What You Already Know About Endpoints

Use the text labels to identify the items in this graphic:

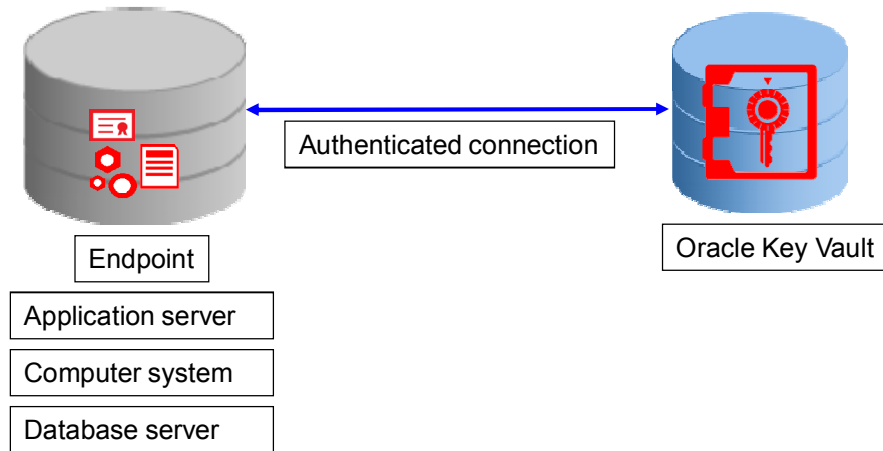


ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

What You Already Know About Endpoints

Use the text labels to identify the items in this graphic:

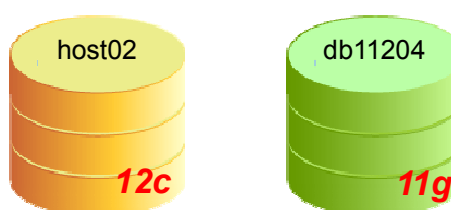


ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Endpoints

- Are Oracle Key Vault clients that use Oracle Key Vault to:
 - Store secrets for long-term retention
 - Share them with trusted peers
 - Retrieve security objects whenever needed
- Can use the TDE connection



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Endpoints are Oracle Key Vault clients. They use Oracle Key Vault to store secrets for long-term retention, share them with trusted peers, and retrieve them whenever needed. The first training example uses Oracle Database 11.2.

Endpoints can use the TDE direct connection because Oracle Key Vault provides a library that enables Transparent Data Encryption to communicate with Key Vault.

Endpoint Administrators

- Are administrators of the endpoint, such as an Oracle DBA
- Perform operations such as archiving and downloading credential files, wallet files, and Java keystores
- Do not, by default, have access to the Oracle Key Vault management console
- Use the `okvutil` utility to:
 - List available security objects
`okvutil list <arguments>`
 - Upload common key storage files
`okvutil upload <arguments>`
 - Take security items from Oracle Key Vault
`okvutil download <arguments>`



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- Endpoint administrators are administrators of the respective endpoints such as Oracle databases or application servers. For Oracle database endpoints, the endpoint administrator can be the corresponding DBA.
- Endpoint administrators perform operations such as archiving and downloading credential files, wallet files, and Java keystores.
- Although the endpoint administrator does not have Oracle Key Vault access by default, the same user could have an Oracle Key Vault user account.
- Any endpoint administrator can use the `okvutil` utility, which enables tasks such as finding, uploading, and downloading security objects. For more details, see the *Oracle Key Vault Administrator's Guide*.
 - The `okvutil list` command lists the available security objects that are uploaded:
`okvutil list [-l location -t type | -g group] [-v verbosity_level]`
 - The `okvutil upload` command uploads the contents of the common key storage files to Oracle Key Vault:
`okvutil upload [-o] -l location -t type [-g group] [-d description] [-v verbosity_level]`
 - The `okvutil download` command takes security items from Oracle Key Vault:
`okvutil download -l location -t type [-g group | -i object_id] [-o] [-v verbosity_level]`

Managing Oracle Key Vault Endpoints

With separation of duties:

- **System administrator:**



- Adds and deletes endpoints
- Changes endpoint names, endpoint types, and useful descriptive information

- **Key administrator:**



- Adds default virtual wallets
- Creates endpoint group memberships
- Example: RAC cluster with automatic access to the wallets or keys
- Grants access to existing virtual wallets

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

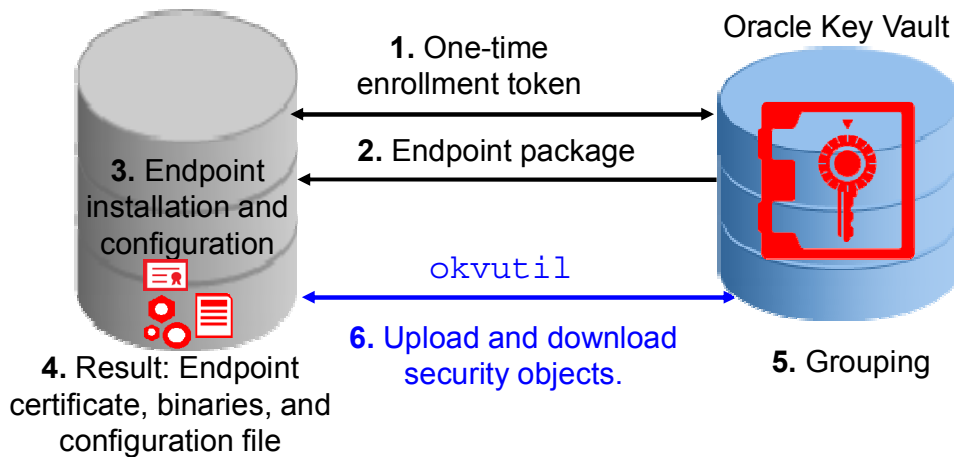
The Oracle Key Vault administrators for endpoints are:

- The System Administrator role changes endpoint names, endpoint types, descriptions (any information that would be useful), platforms, or email addresses
- The Key Administrator role changes or adds default virtual wallets, endpoint group memberships, or access to existing virtual wallets

Endpoints are systems that use Oracle Key Vault to store security objects for various cryptographic operations. You can view and search for endpoints by specific criteria, and then drill down to endpoint details. You can enroll endpoints, rename endpoints, delete endpoints, and create endpoint groups and modify their memberships.

Endpoint groups are groups of endpoints that have shared access to virtual wallets. Administrators who have the Key Administrator role can provide access to specific or multiple virtual wallets at the endpoint group level. Then all the member endpoints of that endpoint group automatically have access to the wallets or keys. For example, if the nodes of an Oracle RAC cluster are set up in an endpoint group, they can share wallets and wallet contents.

Enrolling, Provisioning, and Using an Endpoint



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

9

1. When endpoints are enrolled, a one-time token is exchanged as proof of authentication.
2. The endpoint package is transferred. The user, for example, the `oracle` OS user must have read, write, and execute permissions in the target directory.
3. The package is automatically installed and the endpoint configured.
4. The result is that the endpoint has a certificate, binaries, and a configuration file and is ready to begin its interaction with Oracle Key Vault.

Information needed by Oracle Key Vault is stored in the `okvclient.ora` configuration file. The Oracle Key Vault endpoint libraries and endpoint utilities use this file.

5. After the endpoints are enrolled, the key administrator can manage them in endpoint groups.
6. The endpoint administrator uses the `okvutil` utility to find, upload, and download security objects, such as Oracle wallets or Java keystores.

Types of Enrollment

- Administrator-initiated enrollment:
 - The SA adds the endpoint and generates a one-time enrollment token.
 - The SA communicates the token to the endpoint administrator.
 - The endpoint administrator submits the token as proof of authentication.
- Endpoint self-enrollment:
 - Enrollment with less human intervention
 - When endpoints do not share security objects
 - Access limited to its own security objects
 - Disabled by default
 - Recommended usage for limited time

The Oracle logo, consisting of the word "ORACLE" in a white, sans-serif font, centered within a red rectangular background.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

There are two methods for enrolling an endpoint, depending on who initiates the enrollment.

- An Oracle Key Vault user who has the System Administrator (SA) role initiates the enrollment from the Key Vault side by adding the endpoint. After the endpoint is added to Key Vault, Oracle Key Vault generates a one-time token, called an enrollment token.
- This token must be communicated to the endpoint administrator by using an out-of-band method such as email or telephone.
- The endpoint administrator then submits the enrollment token, from the endpoint side, to Key Vault as proof of authentication. After the endpoint is enrolled, the enrollment token is consumed and can never be used again.

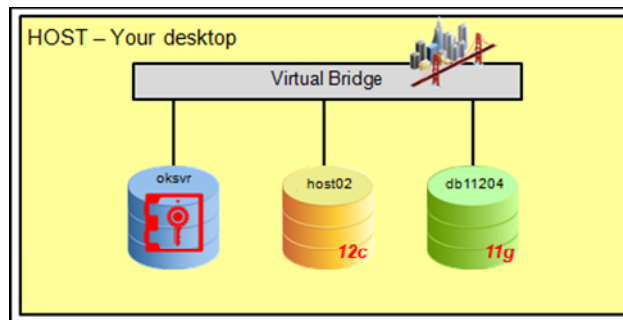
Endpoint self-enrollment is performed in an environment where it is acceptable to enroll new endpoints without action by a user who has the Key Vault System Administrator role.

- This facilitates enrollment with less human administrative intervention.
- Endpoint self-enrollment is particularly useful when the endpoints do not share security objects and use Oracle Key Vault mainly to archive and restore security objects. In addition, endpoint self-enrollment is useful for testing purposes.

- A self-enrolled endpoint is created with a generic endpoint name, such as ENDPT_001, and it initially has access only to the security objects that it uploads or creates. It does not have access to any virtual wallets. You can subsequently grant the endpoint access to virtual wallets, but you must be careful to ensure that you are granting access to the intended endpoint.
- Endpoint self-enrollment is disabled by default and must be enabled by a Key Vault administrator with the System Administrator role.
- Oracle recommends that you enable endpoint self-enrollment only during the period when you expect endpoints to self enroll.

Enrolling and Provisioning an Oracle Key Vault Endpoint

- As the system administrator, add an endpoint.
- As the endpoint administrator, enroll the endpoint and download the endpoint software. You need to know the `root` OS password to complete the endpoint software installation.
- As the `oracle` OS user, test the endpoint software installation.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Following are the detailed steps that you can see in a video:

1. Start the Oracle Key Vault appliance in the `db11204` session.
2. Log in as the system administrator and add the `CUSTOMER_DB` endpoint.
3. Copy the enrollment token and log out.

As the endpoint administrator:

4. Click the Endpoint Enrollment and Software Download link in the management console
5. Paste and submit the enrollment token
6. After you see "Valid Token," enroll the endpoint
7. Download and save the `okvclient.jar` file in the default `/home/oracle/` directory. As the `oracle` OS user, you must have Read, Write, and Execute privileges on the directory.
8. In a terminal window, use `java -jar okvclient.jar -d /home/oracle/okvutil` to install the Oracle Key Vault endpoint software
9. When prompted, use an auto-login wallet for the endpoint installation
10. As the `root` OS user, navigate to the `/home/oracle/okvutil/bin` directory and execute the `root.sh` script
11. As the `oracle` OS user in the same directory, execute the `./okvutil list` command

Quiz

Select all statements that are TRUE for Oracle Key Vault endpoints:

- a. Oracle Key Vault and endpoints share a mutually authenticated connection.
- b. If the nodes of an Oracle RAC cluster are set up in an endpoint group, they can share wallets and wallet contents.
- c. An application server cannot be an endpoint.
- d. Endpoints must be managed by one person. A separation of duties is not yet possible.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a, b

Summary

In this lesson, you should have learned how to:

- Practice separation of duties while performing Oracle Key Vault tasks
- Enroll and provision an Oracle Database 11gR2 as an Oracle Key Vault endpoint

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Practice 3: Overview

This practice covers the following topic:

- 3-1: Enrolling an endpoint

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In seminars, you will view videos of the practices. In classroom environments, you will have hands-on practices, in addition to viewing the videos.

4

Managing Oracle Wallets

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Set up a column and tablespace encrypted test case with Oracle Advanced Security TDE
- Upload an existing wallet to Oracle Key Vault for long-term retention
- Download a wallet and confirm that the encrypted data is readable

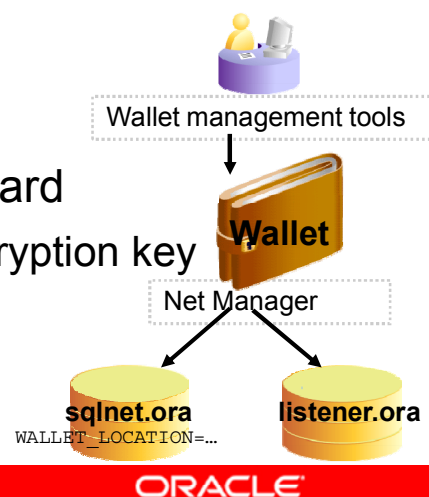
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This lesson begins by reviewing or refreshing prerequisite knowledge about Oracle Wallets and TDE encryption. You set up a column and tablespace encrypted test case, upload an existing wallet for long-term retention, download a wallet, and confirm that the encrypted data is readable. The same workflow applies to uploading and downloading Java keystores and other security objects.

What You Already Know About Oracle Wallets

- Can be managed automatically by TDE or by the `orapki` command-line tool
- Store TDE master keys, certificates, server passwords, and connection strings
- Are stored in the system's default location, in a specified directory, or in the Windows registry
- Have a wallet path and method in `sqlnet.ora` file
- Use the PKCS#12 cryptographic standard
- Are secured by a password-derived encryption key
- Can be created as auto-login wallets
- Show their status in the `V$ENCRYPTION_WALLET` view



Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle offers several tools to create the wallet, generate a request, and import the keys into the wallet. With Oracle Advanced Security TDE, wallets are automatically created during TDE setup; other products use the `orapki` command-line tool.

- Oracle database servers and clients use Oracle Wallets to store TDE master keys, certificates, server passwords, and connection strings.
- The wallet can be stored in the system's default location, in a specified directory, or in the Windows registry.
- Use Oracle Net Manager to configure the `sqlnet.ora` and `listener.ora` files, if needed. The `sqlnet.ora` file contains the wallet directory path and method.
- Oracle Wallet is a standard PKCS#12 file, which is secured by a password-derived encryption key.
- You can create auto-login wallets. Why would you want to use auto login? You must enable auto login if you want single sign-on access to multiple Oracle databases, which is disabled by default.
- To confirm the status of a wallet, you can query the `V$ENCRYPTION_WALLET` view, for example:

```
SELECT WRL_PARAMETER, STATUS, WRL_TYPE FROM V$ENCRYPTION_WALLET;
```


Creating and Opening the Keystore

```
SQL> CONNECT / AS SYSKM
SQL> ADMINISTER KEY MANAGEMENT CREATE KEYSTORE
      '/u01/app/oracle/admin/orcl/wallet'
      IDENTIFIED BY keystore_password;
```



3 types of software keystores

Password-based

Is to be opened before the keys can be retrieved or used

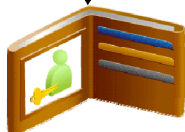
Auto-login

Does not need to be explicitly opened

Local auto-login

Cannot be opened on any computer other than the one on which they are created

```
SQL> ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN
      IDENTIFIED BY keystore_password;
```



/u01/app/oracle/admin/orcl/wallet/ewallet.p12

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

To create and open the keystore, log in to the database instance as a user who is granted the ADMINISTER KEY MANAGEMENT or SYSKM privilege.

Before the column values can be encrypted or the encrypted columns can be viewed by a user, the keystore must be created and opened as explained in the slide. *keystore_password* is the password of the keystore that the security administrator creates. The keystore created is the *ewallet.p12* file that is stored in the location defined in the statement.

Refer to the *Database Advanced Security Guide* to get detailed information about the types of keystores that you can create. TDE uses an auto-login keystore only if it is available at the correct location (*ENCRYPTION_WALLET_LOCATION*, *WALLET_LOCATION*, or the default keystore location), and the SQL statement to open an encrypted keystore has not already been executed.

If the keystore is not opened and the user attempts to access an encrypted column, an error message is generated as shown in the following example:

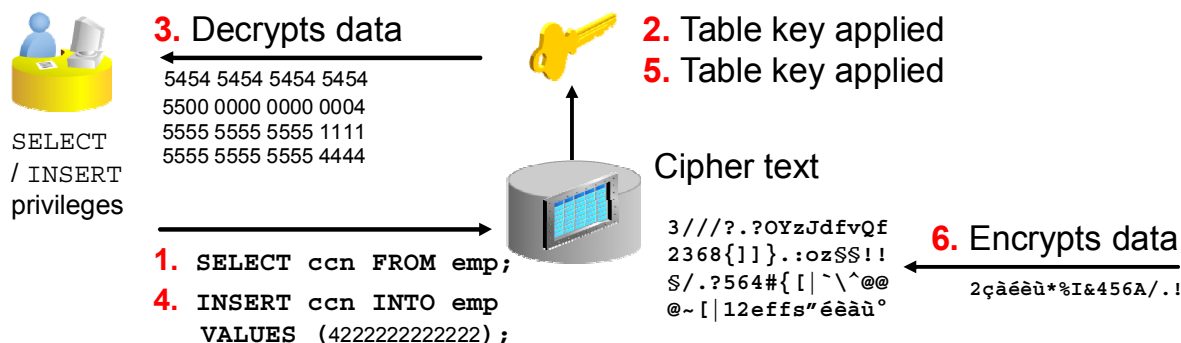
```
SQL> select * from cust_payment_info;
```

*

ERROR at line 1:

ORA-28365: wallet is not open

Reviewing Transparent Data Encryption



- Encrypts data in the following:
 - Data files (tablespaces, columns, indexes)
 - Redo log and archive log files
 - Memory (only for column encryption)
 - File backups
- Manages keys automatically
- Does not require changes to the application

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

TDE is available with Oracle Advanced Security and provides easy-to-use protection for your data without requiring changes to your applications. TDE allows you to encrypt sensitive data in individual columns or entire tablespaces without having to manage encryption keys. TDE does not affect access controls, which are configured by using database roles, secure application roles, system and object privileges, views, Virtual Private Database (VPD), Oracle Database Vault, and Oracle Label Security. Any application or user that previously had access to a table will still have access to an identical encrypted table.

TDE is designed to protect data in storage, but does not replace proper access control.

TDE is transparent to existing applications. Encryption and decryption occur at different levels depending on whether they are at the tablespace or column level, but in either case, encrypted values are not displayed and are not handled by the application. For example, with TDE, applications that are designed to display a 16-digit credit card number do not have to be recoded to handle an encrypted string that may have many more characters.

TDE eliminates the ability of anyone who has direct access to the data files to gain access to the data by circumventing the database access control mechanisms. Even users with access to the data file at the operating system level cannot see the data unencrypted. TDE stores the master key outside the database in an external security module, thereby minimizing the possibility of both personally identifiable information (PII) and encryption keys being compromised. TDE decrypts the data only after database access mechanisms have been satisfied.

Creating TDE Encrypted Test Data

- To create an encrypted column, use the `ENCRYPT` attribute when the table is created or altered.

```
SQL> ALTER TABLE banking.customers MODIFY (ccn ENCRYPT);
```

- To create an encrypted tablespace with an open encryption wallet:

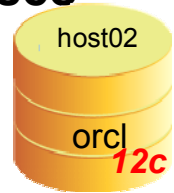
```
SQL> CREATE TABLESPACE bankingENC datafile  
'/u01/app/oracle/oradata/db11gr2/bankingENC.dbf'  
size 1M  
encryption using 'AES256'  
default storage(encrypt);
```

The Oracle logo, consisting of the word "ORACLE" in a white, sans-serif font, centered on a red rectangular background.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

- To create an encrypted column, use the `ENCRYPT` attribute when the table is created or altered.
- TDE tablespace encryption enables you to encrypt an entire tablespace. All the objects that are created in the encrypted tablespace are automatically encrypted. The `CREATE TABLESPACE` command has an `ENCRYPTION` clause that sets the encryption properties, and an `ENCRYPT` storage parameter that causes the encryption to be used. You specify `USING 'encrypt_algorithm'` to indicate the name of the algorithm to be used. Valid algorithms are `3DES168`, `AES128`, `AES192`, and `AES256`. The default is `AES128`. You can view the properties in the `V$ENCRYPTED_TABLESPACES` view.

Setting Up Encrypted Data in Oracle Databases



- Confirm that the database instance is up and running and that TDE is enabled.
- Create test users and test data.
- Create and confirm that you have an open, local `ewallet.p12` file and that the `sqlnet.ora` file contains the path to that directory.
- Encrypt the `CCN` column in the `BANKING.CUSTOMERS` table and confirm that you can read the encrypted data.
- Create an encrypted tablespace with the `BANKING.CUSTOMERSEC` table and confirm that you can read the encrypted data.



ORACLE

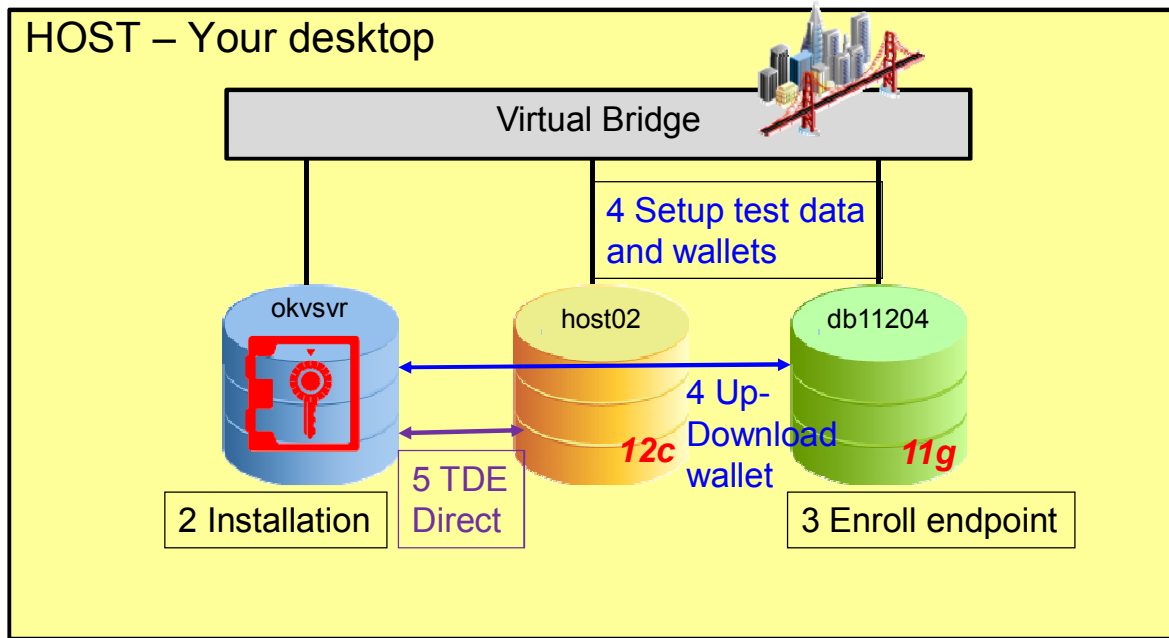
Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The task steps in this slide are shown in the video titled “Setting Up Encrypted Data in Oracle Databases,” which is a prerequisite for all the videos that follow and, if applicable, the hands-on activities.

Training Environment and Workflow

1 Introduction

6 Admin tasks



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

You have set up the encrypted test data and can continue with the tasks of an endpoint administrator: to upload and download wallets.

What Is a Virtual Wallet?

- Oracle Key Vault group of security objects (including public and private keys, TDE master encryption keys, passwords, credentials, certificates, and so on)
- Shared between users and endpoints
- Created by key administrators
- Managed by key administrators and users with direct access

The Oracle logo, consisting of the word "ORACLE" in white, uppercase letters on a red rectangular background.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Oracle Wallets and Oracle Key Vault Virtual Wallets are not the same thing. A virtual wallet is an Oracle Key Vault group of security objects that can be shared between users and endpoints. These security objects are typically public and private keys, TDE master encryption keys, passwords, credentials, certificates, and so on.

Key administrators can create the virtual wallets. The user who creates the virtual wallet is automatically granted the Read, Read and Modify, and Manage Wallet access on the virtual wallet. You can add items to the wallet if you have at minimum the Read privilege on the item.

Key administrators have access to all virtual wallets. Additionally, for granular management, you can grant users direct access to a virtual wallet. Then they can manage it without the key administrator role.

Managing Security Objects

- Are managed by Oracle Key Vault for security
- Include passwords, keys, certificates, and credentials
- Include the following states:
 - Pre-active
 - Active
 - Deactivated
 - Compromised
 - Destroyed
 - Destroyed Compromised



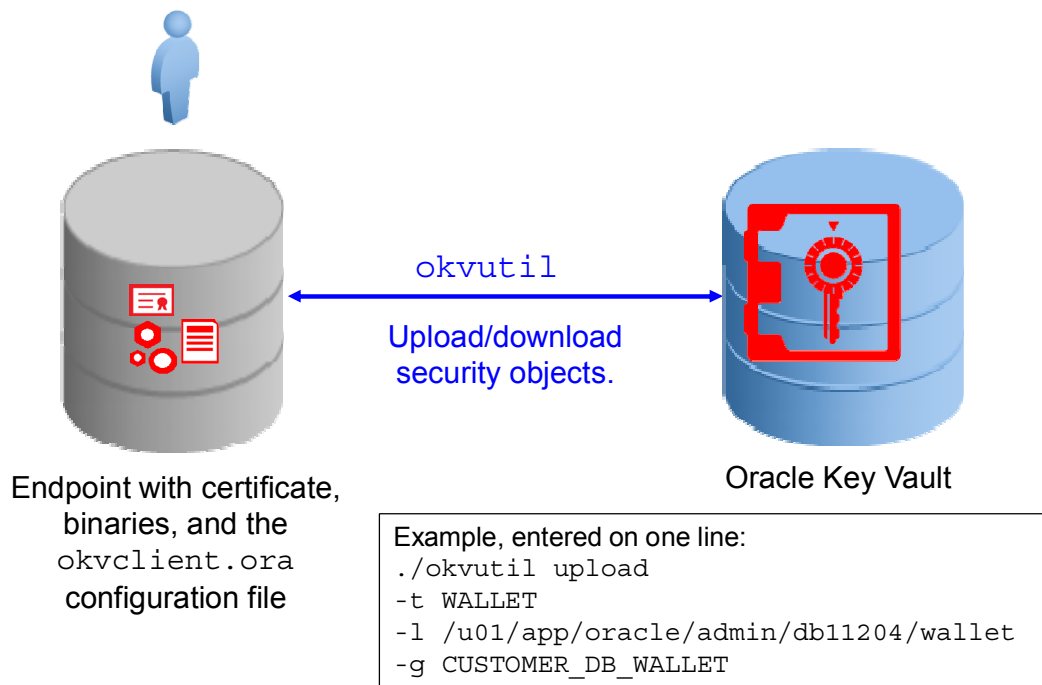
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Security objects are objects managed by Oracle Key Vault for security, including passwords, keys, certificates, and credentials. They go through the states listed in the slide.

- **Pre-active:** The object exists but is not yet usable for any cryptographic purpose.
- **Active:** The object is available for use. Endpoints examine the Cryptographic Usage Mask attribute to determine which uses are appropriate for this object.
- **Deactivated:** The object is no longer active and should not be used to apply cryptographic protection (for example, encryption or signing). It may still be appropriate to use for decrypting or verifying previously protected data.
- **Compromised:** The object is believed to be compromised and should not be used.
- **Destroyed:** The object is no longer usable for any purpose.
- **Destroyed Compromised:** The object was compromised and subsequently destroyed. It is no longer usable for any purpose.

Uploading and Downloading an Oracle Wallet to and from Oracle Key Vault



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Information that is necessary to use Oracle Key Vault is stored in the `okvclient.ora` configuration file, which the Oracle Key Vault endpoint libraries and endpoint utilities use. The Oracle Key Vault `okvutil` utility enables endpoint administrators to find, upload, and download security objects, such as Oracle wallets or Java keystores.

Short syntax (for more details, see the *Oracle Key Vault Administrator's Guide*):

```
okvutil upload [-o] -l location -t type [-g group] [-d description]
[-v verbosity_level]
```

Notes about the options used in the slide:

- `-t`: Data type of the object. Valid values are: WALLET, JKS, JCEKS, SSH, KERBEROS, and OTHER.
- `-l`: Location of the security object to be uploaded
- `-g`: Case-sensitive name, which must match the name of the virtual wallet in Oracle Key Vault

Some options, such as `-o` override, are not used in this example.

Downloading an Oracle Wallet

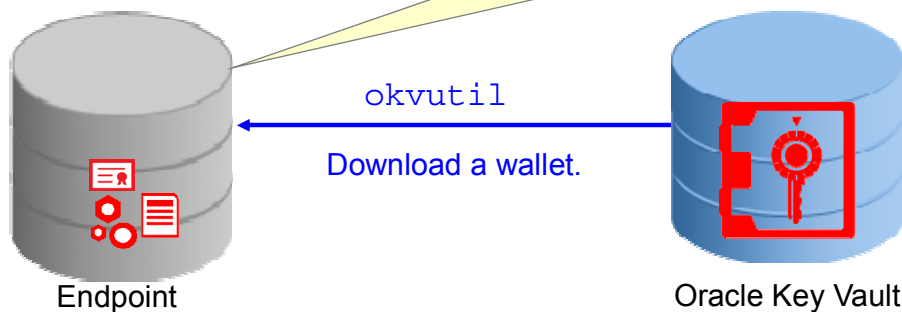


Example, entered on one line:

```
./okvutil download
-t WALLET
-l /u01/app/oracle/admin/db11204/wallet
-g CUSTOMER_DB_WALLET
```

- Automatic backup
- Creation of new wallet

Close old wallet to ensure that new one is used.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Short syntax (for more details, see the *Oracle Key Vault Administrator's Guide*):

```
okvutil download -l location -t type [-g group] [-d description]
[-v verbosity_level]
```

Notes about the options used in the slide:

- **-t**: Data type of the object. Valid values are: WALLET, JKS, JCEKS, SSH, KERBEROS, and OTHER.
- **-l**: Location of the security object to be uploaded
- **-g**: Case-sensitive name, which must match the name of the virtual wallet in Oracle Key Vault

Logged in to SQL*Plus, close the older wallet to ensure that the newly downloaded one is used.

Videos

Setting Up Encrypted Data in Oracle Databases

This video shows you how to set up a column and tablespace encrypted test case with Oracle Advanced Security TDE both in Oracle Database 11g and in Oracle Database 12c.

Uploading and Downloading an Oracle Wallet to and from Oracle Key Vault

This video shows you how to upload an Oracle wallet to and download an Oracle wallet from Oracle Key Vault. The tasks are divided between the key administrator and the endpoint administrator.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The two videos listed in the slide are created to reinforce the lesson topics and to show how to perform the various task steps.

Quiz

Select all statements that are TRUE for Oracle wallets:

- a. Oracle Key Vault cannot manage the wallets that are securing the database endpoints.
- b. Wallets are automatically created during TDE setup.
- c. You cannot download an Oracle wallet to the same directory where an earlier version exists.
- d. You can download an Oracle wallet to the same directory; the earlier version is automatically backed up and a new version is created.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: b, d

Summary

In this lesson, you should have learned how to:

- Set up a column and tablespace encrypted test case with Oracle Advanced Security TDE
- Upload an existing wallet to Oracle Key Vault for long-term retention
- Download a wallet and confirm that the encrypted data is readable

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Practice 4: Overview

This practice covers the following topics:

- 4-1: Setting Up Encrypted Data in Oracle Databases
- 4-2: Uploading and Downloading an Oracle Wallet to and from Oracle Key Vault

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In seminars, you will view videos of the practices. In classroom environments, you will have hands-on practices, in addition to viewing the videos.

5

Using Direct TDE with Oracle Database 12c

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Practice separation of duties by performing tasks as different administrators
- Enroll and provision an endpoint for the Oracle Database 12c database server
- Create a virtual wallet
- Upload an existing wallet for retention
- Migrate a wallet to Oracle Key Vault
- Rotate a TDE master key

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

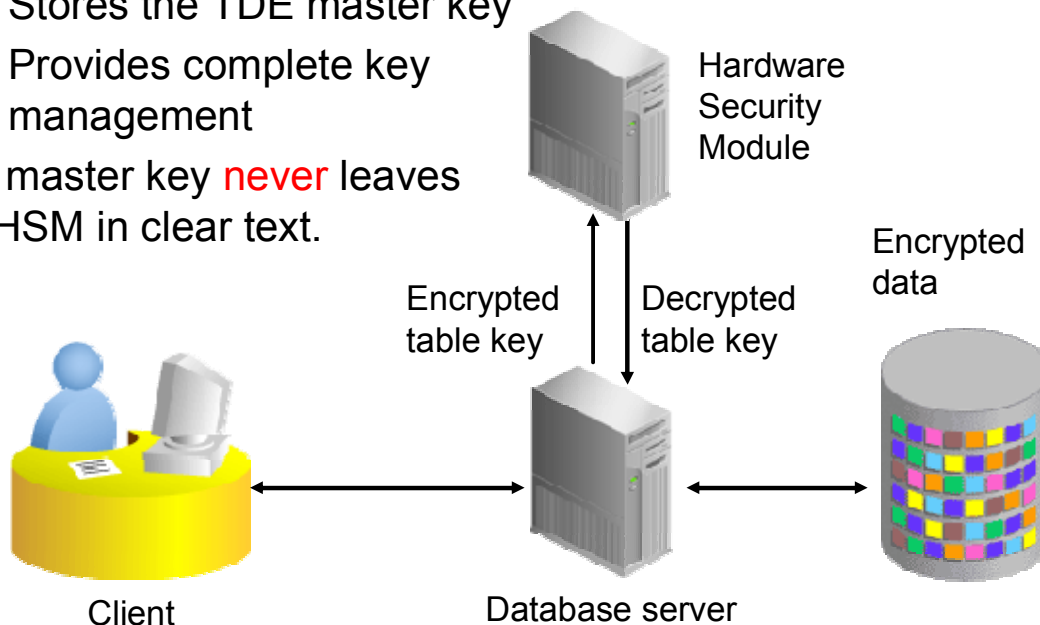
The concepts behind the objectives of this lesson have been previously covered and do not need to be duplicated. The practice is the most important element for reaching the objectives of this lesson. In that sense, this lesson is like a mini workshop to deepen your understanding and competence in performing Oracle Key Vault tasks.

Reviewing Hardware Security Modules

HSM:

- Stores the TDE master key
- Provides complete key management

The master key **never** leaves the HSM in clear text.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.





A Hardware Security Module (HSM) is a physical device that provides secure storage for encryption keys. It also provides secure computational space (memory) to perform encryption and decryption operations. HSM is a more secure alternative to the software keystore.

Transparent Data Encryption can use an HSM to provide enhanced security for sensitive data. An HSM is used to store the master encryption key that is used for TDE. The key is secure from unauthorized access attempts because the HSM is a physical device and not an operating system file. All encryption and decryption operations that use the master encryption key are performed inside the HSM. This means that the master encryption key is never exposed in non-secure memory.

There are several vendors that provide Hardware Security Modules. The vendor must also supply the appropriate libraries.

Separation of Duties

Performing tasks with TDE direct connection:

- Enroll and provision an endpoint for the Oracle Database 12c database server. 
- Download and install the client-side Oracle Key Vault software. 
- Create a virtual wallet. 
- Upload the existing Oracle Wallet to retain all historical TDE master keys. 
- Migrate the TDE master key from the wallet to Oracle Key Vault.
- Rotate the TDE master key.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide shows how separation of duties is implemented in the practice.

Using the TDE Direct Connection with Oracle Key Vault

1. As the system administrator, enroll and provision another endpoint for the Oracle Database 12c database server.
2. As the endpoint administrator, download and install the client-side Oracle Key Vault software.
3. As the key administrator, create a virtual wallet.
4. Upload the existing Oracle Wallet to retain all historical TDE master keys.
5. Migrate the TDE master key from the wallet to Oracle Key Vault:
 - Close the existing wallet.
 - As the `oracle` OS user, modify the `sqlnet.ora` file to set the `METHOD` attribute to `HSM`.
 - Perform migration and view the newly created TDE master key in the Oracle Key Vault management console.
6. Rotate the TDE master key.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide shows the task list of the video titled “Using the TDE Direct Connection with Oracle Key Vault.”

Using Security Objects

Use case scenarios:

- Uploading and Downloading Oracle Wallets
- Uploading and Downloading Java JKS and JCEKS Keystores
- Using a TDE Direct Connection with Oracle Key Vault
- Uploading and Downloading Credential Files
- Using a TDE-Configured Oracle Database in an Oracle RAC Environment
- Using a TDE-Configured Oracle Database in an Oracle GoldenGate Environment
- Using a TDE-Configured Oracle Database in an Oracle Active Data Guard Environment

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

See the *Oracle Key Vault Administrator's Guide* for more details on the use case scenarios listed in the slide.

Quiz

Transparent Data Encryption can use a Hardware Security Module to provide enhanced security for sensitive data.

- a. True
- b. False

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: a

Summary

In this lesson, you should have learned how to:

- Practice separation of duties by performing tasks as different administrators
- Enroll and provision another endpoint for the Oracle Database12c database server
- Create a virtual wallet
- Upload an existing wallet for retention
- Migrate a wallet to Oracle Key Vault
- Rotate a TDE master key

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Practice 5: Overview

This practice covers the following topic:

- 5-1: Using Direct TDE with Oracle Database 12c

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

In seminars, you will view videos of the practices. In classroom environments, you will have hands-on practices, in addition to viewing the videos.

This practice is like a mini workshop to deepen your understanding and competence in performing Oracle Key Vault tasks. You perform tasks with an Oracle Database 12c endpoint that you previously performed with an Oracle Database 11g endpoint.

6

Performing Administrative Tasks

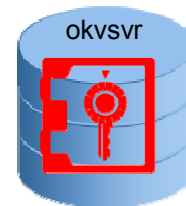
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Objectives

After completing this lesson, you should be able to:

- Perform tasks as the system administrator
- Perform tasks as the key administrator
- Perform tasks as the audit manager
- Consider Oracle Key Vault best practices for your organization



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Administrative Tools

Oracle Key Vault management console:

- Dashboards
- Alerts:
 - Configured by the system administrator
 - Open alerts, viewable by all Oracle Key Vault users
 - Possible alerts for:
 - Key rotation
 - Expiration dates for endpoint certifications and user passwords
 - Maximum amount of allowed disk space
 - Time in days for backup operations to be performed
 - Notification if system backup operations fail

The Oracle logo, consisting of the word "ORACLE" in white, uppercase letters on a red rectangular background.

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Dashboards in the management console provide a quick look at the current Oracle Key Vault status and open issues that require attention.

Oracle Key Vault provides alerts for key rotation, expiration dates for endpoint certifications and user passwords, maximum amount of allowed disk space, time in days for backup operations to be performed, and whether to be notified if system backup operations fail. Only system administrators can configure these alerts, but all Oracle Key Vault users can view the open alerts.

Performing Tasks as System Administrator

Best Practice: Identical, up to 3 NTP servers for primary and standby Oracle Key Vault server

- Set system time and the `syslog` location.
- Enable SSH access, if needed.
- Modify web access.
- View alert settings and alerts.

Covered in the video: Performing System Administration Tasks

- Perform backup and restore operations.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The video titled “Performing System Administration Tasks with Oracle Key Vault” shows how to perform the first three tasks, which are listed in this slide.

- Some system administrative tasks are performed only once. For example, setting the system time and logs is done after installation before Oracle Key Vault is available for general usage. Primary and standby Oracle Key Vault servers should have the same system time.
Best practice tip: The NTP server setting is a standard practice for production deployments. Oracle recommends that you point to the same NTP servers for the primary and standby Oracle Key Vaults. You can configure up to three NTP servers. If during time synchronization, one Oracle Key Vault server is unable to contact an NTP server, it automatically contacts the next NTP server to reliably synchronize time.
- Other tasks are performed only on demand. For example, before you apply a patch, you decide to enable SSH access and after the operation, you disable the access again.
- By default, web access is enabled. You might want to restrict it to a list of IP addresses for stricter access control.
- Oracle Key Vault has enabled some alert settings. Review the settings and view alerts, if there are any.

Video: Backing Up and Restoring Data for Oracle Key Vault

- As the system administrator:
 - Create and manage remote backup destinations
 - Schedule backups: one-time and periodic
 - Back up the Oracle Key Vault data to your remote destination
- As the key administrator: Simulate “trouble” that requires a restore operation.
- As the system administrator: Restore the Oracle Key Vault data.



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

This slide summarizes the tasks shown in the video titled “Backing Up and Restoring Data for Oracle Key Vault.” The backup and restore tasks are performed by the system administrator. For training purposes, the key administrator simulates “trouble” that requires a restore operation.

Performing Tasks as Key Administrator

- Create an endpoint group.
- Add members to this group.
- Create a virtual wallet.
- Grant access to the endpoint group (which automatically includes access to all endpoints).



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The tasks listed in this slide are shown in the video titled “Performing Key Administration Tasks with Oracle Key Vault.”

Performing Tasks as Audit Manager

- Manages the audit trail as the only user who has privileges to export or delete Oracle Key Vault audit records
- Has read access on all security objects
- Grants the Audit Manager role to and revokes the role from other users



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The audit manager manages the collection of audit data that records the actions of users and endpoints:

- Manages the audit trail as the only user who has privileges to export or delete Oracle Key Vault audit records
- Has read access on all security objects
- Grants the Audit Manager role to other users

Audit management tasks, such as exporting and deleting the audit trail, are shown in the video titled “Performing Audit Manager Tasks with Oracle Key Vault.”

Oracle Key Vault Management Reports

For audit managers and key administrators:

- Access
- Key Expiration
- Endpoint Certificate Expiration
- User Password Expiration

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide lists the currently available Oracle Key Vault management reports. Only audit managers and key administrators are permitted to view them.

Best Practice Tips for Oracle Key Vault

- Availability:
 - For High Availability, configure Oracle Key Vault as the primary and standby appliances.
 - Regularly back up Oracle Key Vault to a remote location.
- Installation:
 - Configure the primary and standby Oracle Key Vault appliances **before** enrolling endpoints.
- Deployment:
 - TDE endpoints: Start with the wallet upload and download immediately and incrementally migrate to the TDE direct connection over time.
 - TDE direct connections: Upload the existing wallet to Oracle Key Vault before migrating to the direct connection.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide lists the best practice tips for using Oracle Key Vault.

Best Practice Tips for Oracle Key Vault

- Rotation:
 - After every key rotation at a database endpoint, upload the wallet to the Oracle Key Vault appliance.
 - Similarly, every time the content of a Java keystore changes, upload the keystore to Oracle Key Vault.
- Credential file upload:
 - Use meaningful, human readable descriptions for future references and ease of identification.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

The slide continues the best practice tips for using Oracle Key Vault.

Quiz

Oracle Key Vault configures the following roles for default access of the Oracle Key Vault management console:

- a. SYSKM, Audit Manager, Key Administrator
- b. Audit Manager, Key Administrator, Endpoint Administrator
- c. Audit Manager, Key Administrator, System Administrator

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Answer: c

Summary

In this lesson, you should have learned how to:

- Perform tasks as the system administrator
- Perform tasks as the key administrator
- Perform tasks as the audit manager
- Consider Oracle Key Vault best practices for your organization

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Practice 6: Overview

This practice covers the following topic:

- 6-1: Performing Administrative Tasks

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

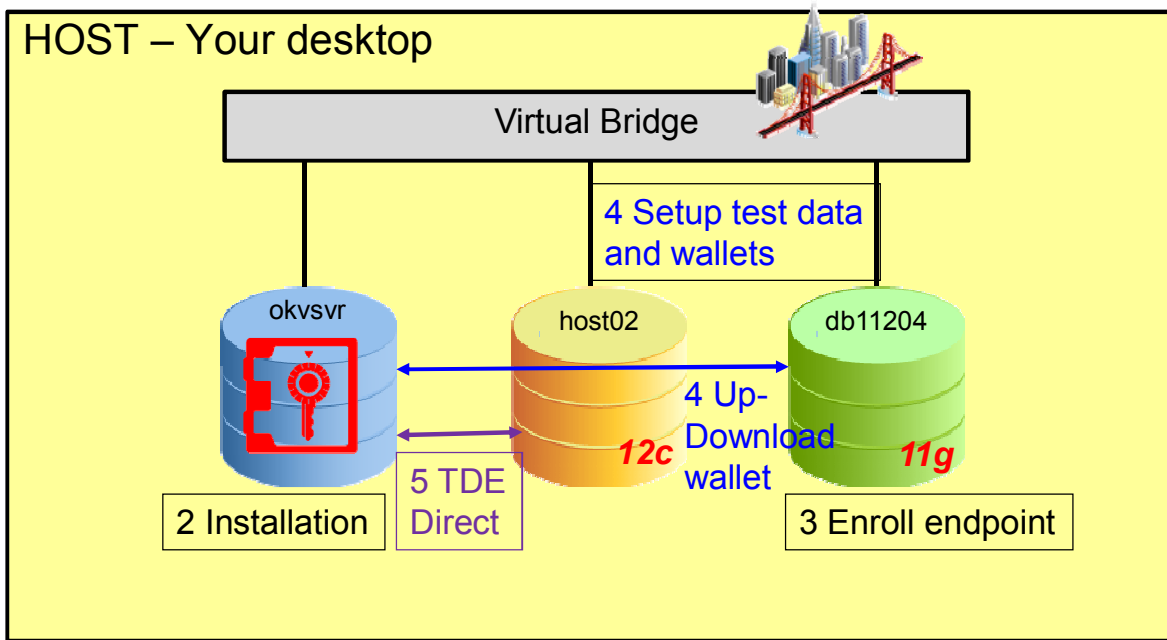
In seminars, you will view videos of the practices. In classroom environments, you will have hands-on practices, in addition to viewing the videos.

Summary

1 Introduction

6 Admin tasks

HOST – Your desktop



ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

With these administrative tasks, you reached the end of this training unit. You should now be able to:

1. Install and configure Oracle Key Vault
2. Enroll and provision endpoints
3. Upload and download Oracle Wallets
4. Use TDE direct connection to Oracle Database 12c
5. Perform administrative functions

Continuing Your Learning

- Documentation
- Oracle Technology Network (OTN)
- Oracle Key Vault product home page
- Oracle University training courses
- Oracle University self studies
- Oracle Learning Library (OLL)
- My Oracle Support (MOS)
- YouTube videos on the Oracle Learning channel

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

Documentation:

- *Oracle Key Vault Administrator's Guide*

Oracle Key Vault product home page:

- <http://www.oracle.com/technetwork/database/options/key-management/overview/index.html>

Oracle Technology Network (OTN):

- <http://www.oracle.com/technetwork/index.html>

Oracle University training courses:

- *Oracle Database 12c: Security*

