ORACLE
UNIVERSITY

Using Oracle Key Vault

Activity Guide

D88454GC10

Edition 1.0 | December 2014

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

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.

This book was published using: Oracle Tutor

Table of Contents

Practices for Lesson 1: Introduction

Chapter 1

Practices for Lesson 1: Overview

Practices Overview

In these practices, you will see background information.

Practice 1-1: Introduction

As self-assessment, determine the right definition for each term.

Choose the right definition for each term:

a. Oracle Key Vault

b. Endpoint

c. Virtual wallet

1. Can be a database server, middleware server, or generic server system that contains the keys that you want to manage with Oracle Key Vault
2. Is a container for security objects in Oracle Key Vault that you upload from endpoints to share access by group of servers
3. Is a software appliance that consists of a pre-configured operating system, an Oracle database, and an APEX application

(*The answers are at the end of the Oracle Key Vault activity guide*.)

Optionally, if you want to review additional material, see the following:

- Product documentation: *Oracle Key Vault Administrator's Guide* (E41361)
- Product home page: http://www.oracle.com/technetwork/database/options/key-management/overview/index.html

Practices for Lesson 2: Installing Oracle Key Vault

Chapter 2

Practices for Lesson 2: Overview

Practices Overview

In these practices, you will perform Oracle Key Vault installation and post-installation configuration tasks.

Practice 2-1: Installing Oracle Key Vault

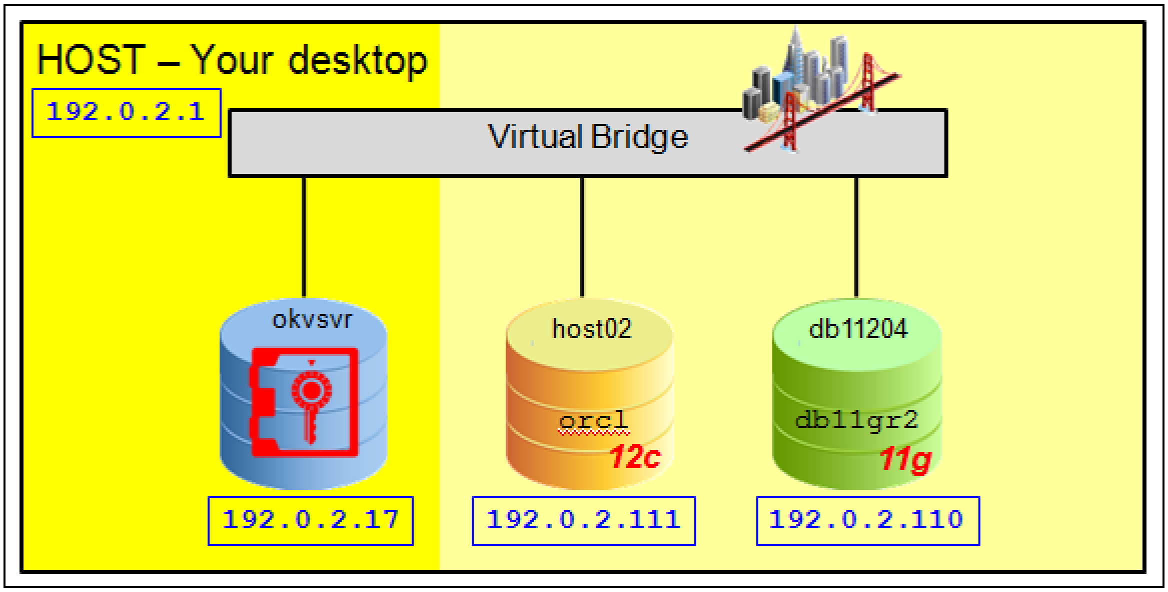
Overview

In this practice, you either install Oracle Key Vault or watch installation videos.

Assumptions

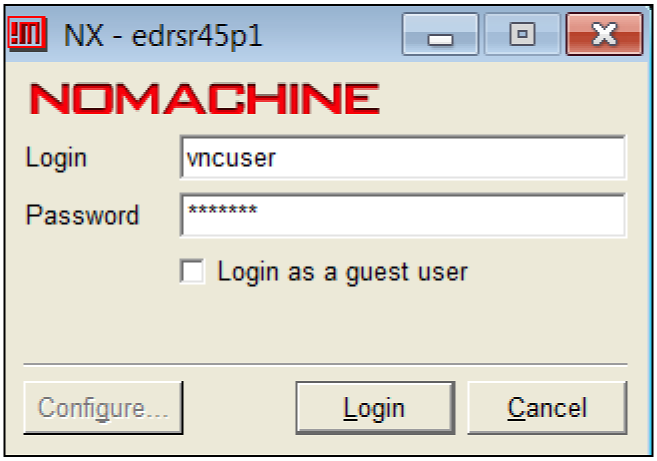
Your instructor will provide the necessary passwords.

Your training environment has three Virtual Machines (VM) with fixed IP addresses, as indicated in the following graphic:



Tasks

1. Log in to your training environment as the `vncuser` user by using an NX client.



Login: vncuser

Password: *******

☐ Login as a guest user

2. Double-click the terminal icon to open a terminal window on your host machine.

3. Become the root OS user and navigate to the /OVS/running_pool/okvsvr directory. This is your Oracle Key Vault installation directory on the training VM.

```
$ su - root
Password: <<< Enter root OS password >>>>
# cd /OVS/running_pool/okvsvr
#
```

Note: Your entries are in bold.

4. Confirm that there is no entry for okvsvr as a VM. You want to see the following error:

```
# xm list -l okvsvr | grep location
Error: Domain 'okvsvr' does not exist.
#
```

5. Start the okvsvr VM with the installation CD.

```
# xm create /OVS/running_pool/okvsvr/vm_wcd.cfg
Using config file "/OVS/running_pool/okvsvr/vm_wcd.cfg".
Started domain okvsvr (id=36)
#
```

6. Find the vnc port that the okvsvr VM is using for communication.

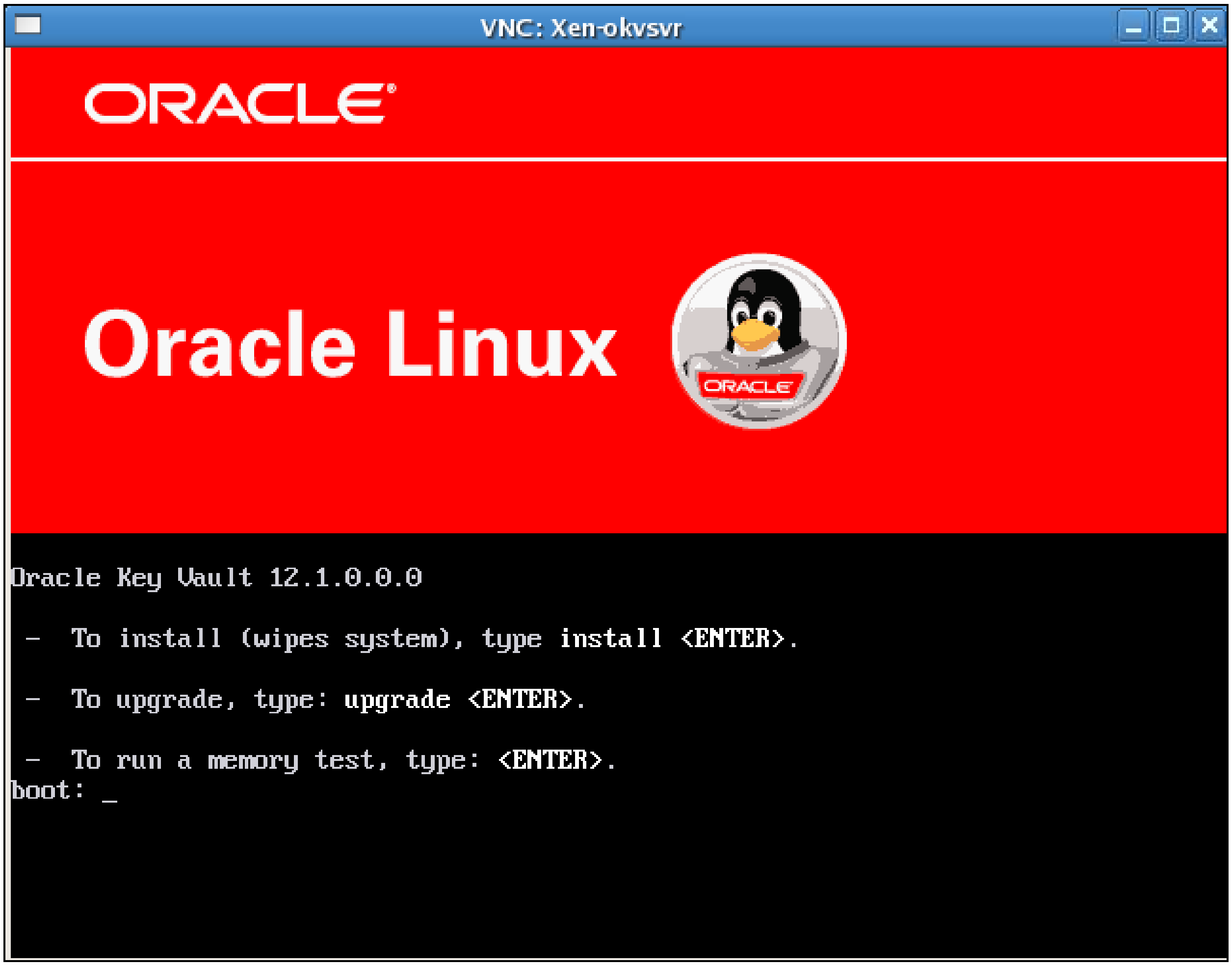
```
# xm list -l okvsvr | grep location
            (location 0.0.0.0:5900)
            (location 3)
#
```

Note: You see a location line with :590x, 5900 in this example. Use your port to connect. Your port number may be different. Each time you issue the xm create command, the vncviewer could change; so check each time before you execute an xm command.

7. Open the vncviewer from your command line with port 590x.

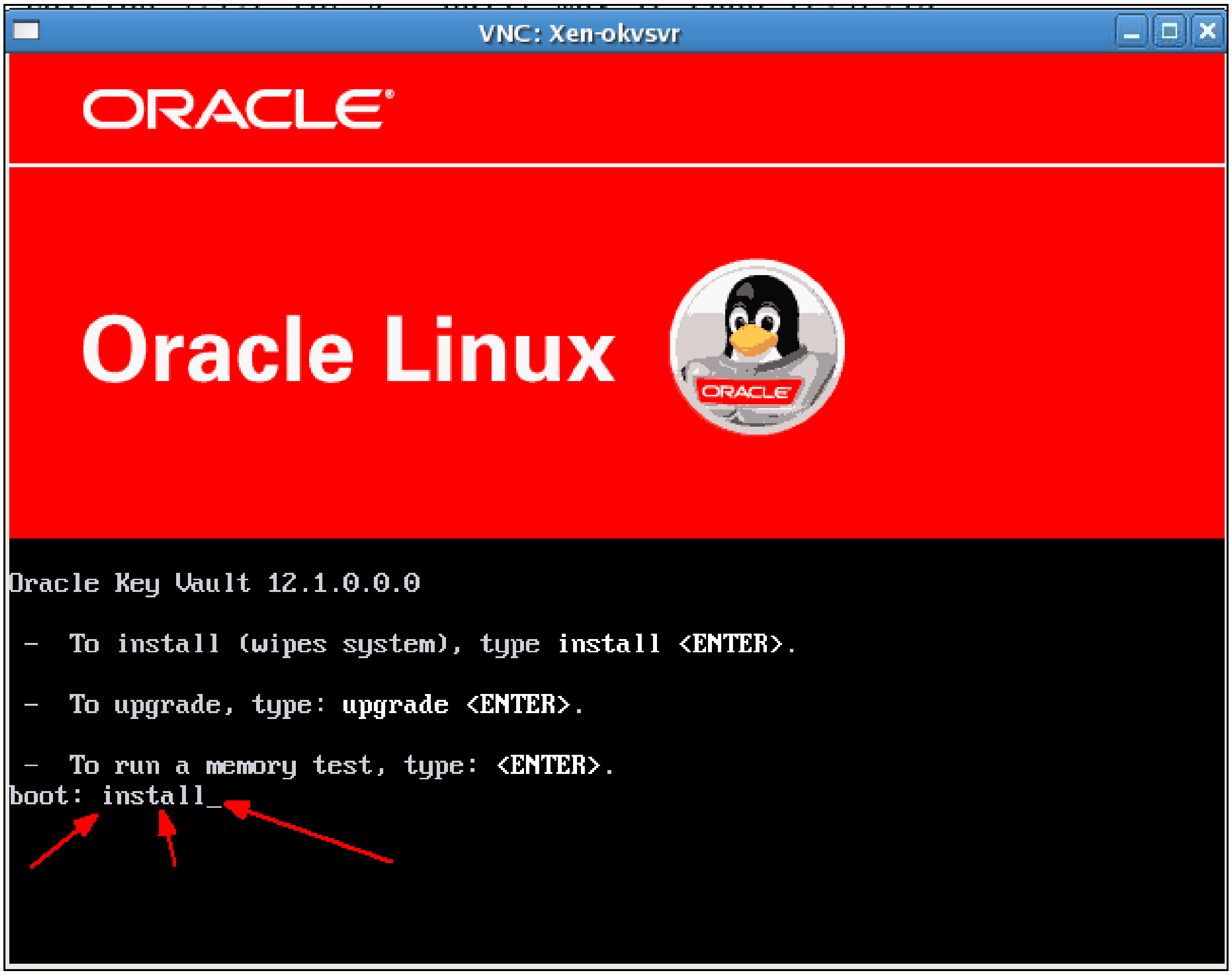
```
# vncviewer :5900

VNC Viewer Free Edition 4.1.2 for X - built May 12 2006 17:42:13
Copyright (C) 2002-2005 RealVNC Ltd.
See http://www.realvnc.com for information on VNC.

Wed Oct 29 14:08:23 2014
 CConn:       connected to host localhost port 5900
 CConnection: Server supports RFB protocol version 3.8
 CConnection: Using RFB protocol version 3.8

Wed Oct 29 14:08:24 2014
 TXImage:     Using default colormap and visual, TrueColor,
depth 24.
 CConn:       Using pixel format depth 6 (8bpp) rgb222
 CConn:       Using ZRLE encoding
 CConn:        Throughput 20000 kbit/s - changing to hextile
encoding
 CConn:        Throughput 20000 kbit/s - changing to full colour
 CConn:        Using pixel format depth 24 (32bpp) little-endian
rgb888
 CConn:        Using hextile encoding
```

8. The Oracle Key Vault installation window automatically appears.



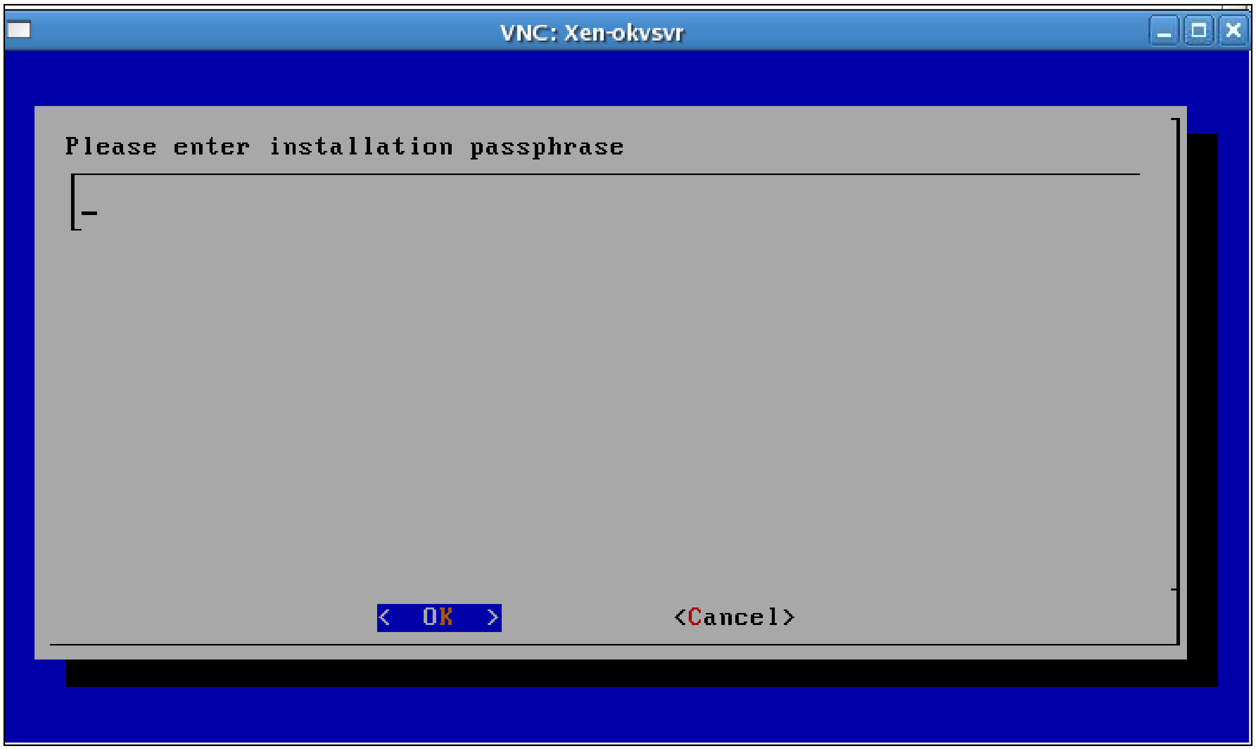
```
Oracle Key Vault 12.1.0.0.0

 -  To install (wipes system), type install <ENTER>.

 -  To upgrade, type: upgrade <ENTER>.

 -  To run a memory test, type: <ENTER>.
boot: _
```

9. Enter **`install`** after the "`boot:`" prompt and press the Enter key.



```
Oracle Key Vault 12.1.0.0.0

 -  To install (wipes system), type install <ENTER>.

 -  To upgrade, type: upgrade <ENTER>.

 -  To run a memory test, type: <ENTER>.
boot: install_
```

10. As the installer lays out the bits for the operating system and for other binaries, the installation process displays several different windows. Wait for the following window to appear. (*In our tests, it took 15–20 minutes.)*

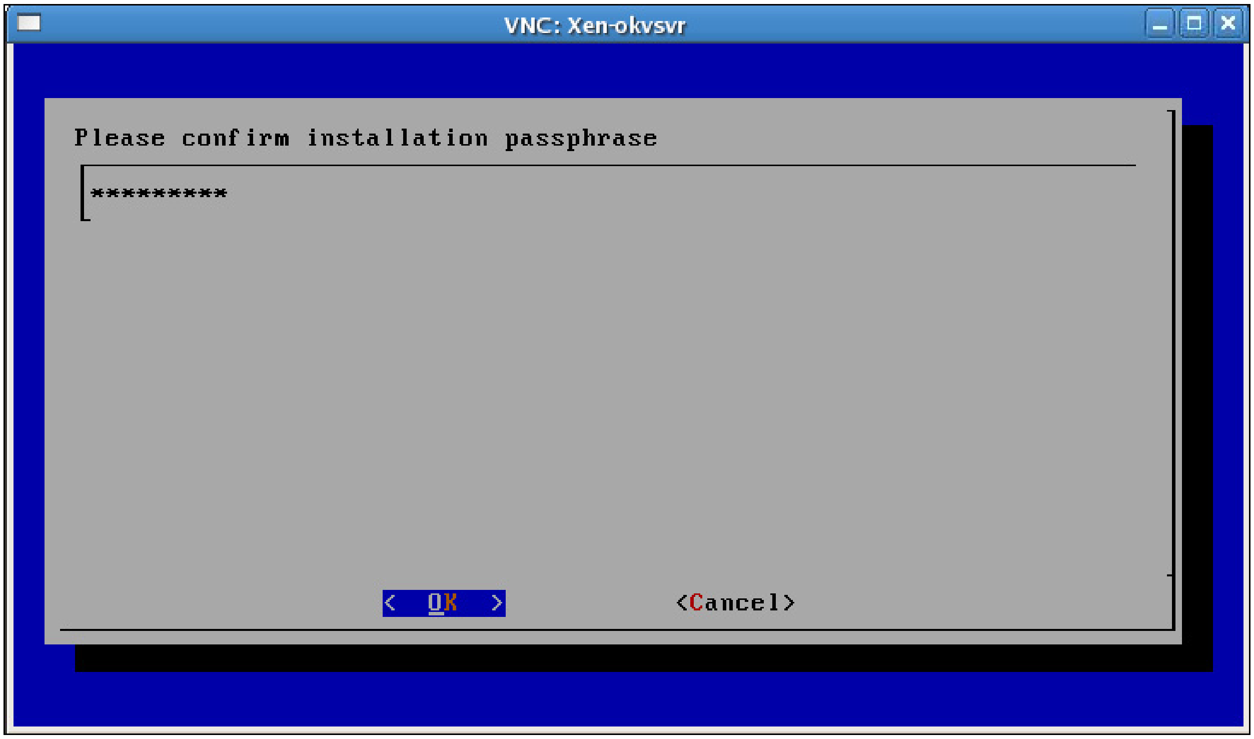


VNC: Xen-okvsvr

Please enter installation passphrase

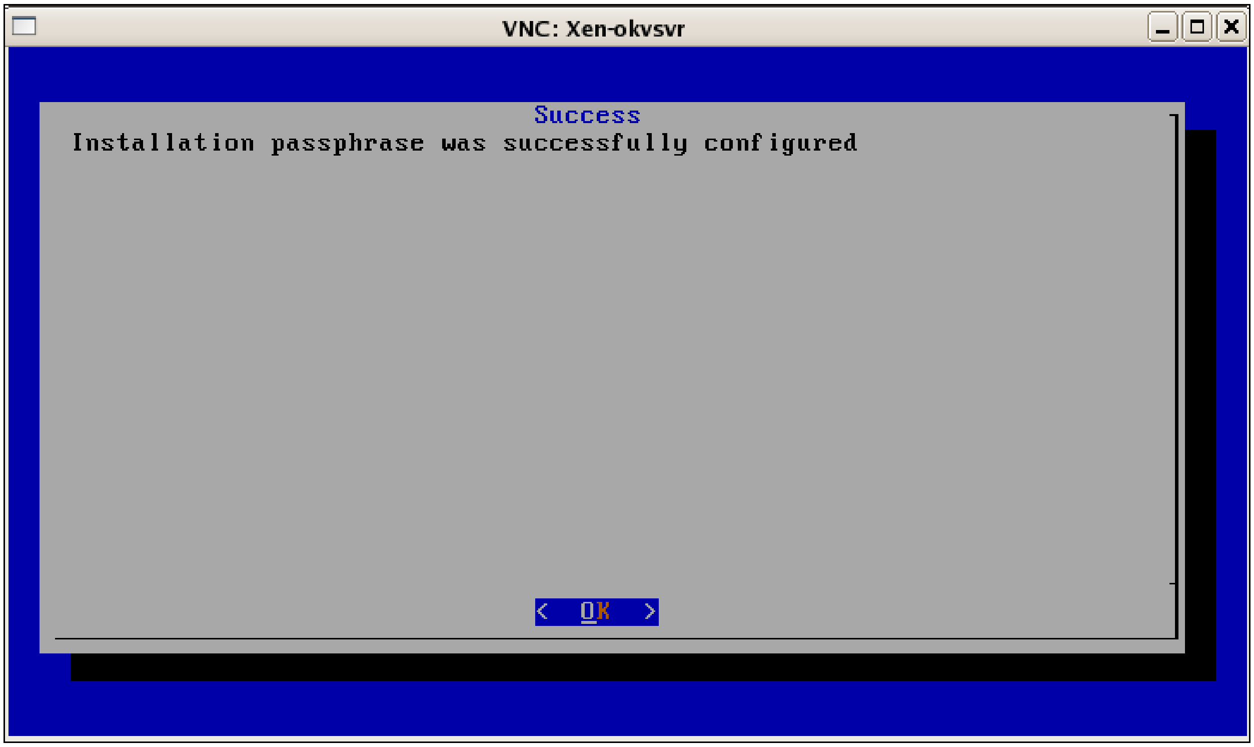
11. Enter your installation passphrase. You must provide this passphrase when you log in to the graphical user interface for the first time. It is important to remember it! Press the Tab key to navigate to <OK>, and then press Enter.

12. To confirm, enter the installation passphrase a second time, press Tab, and then press Enter.



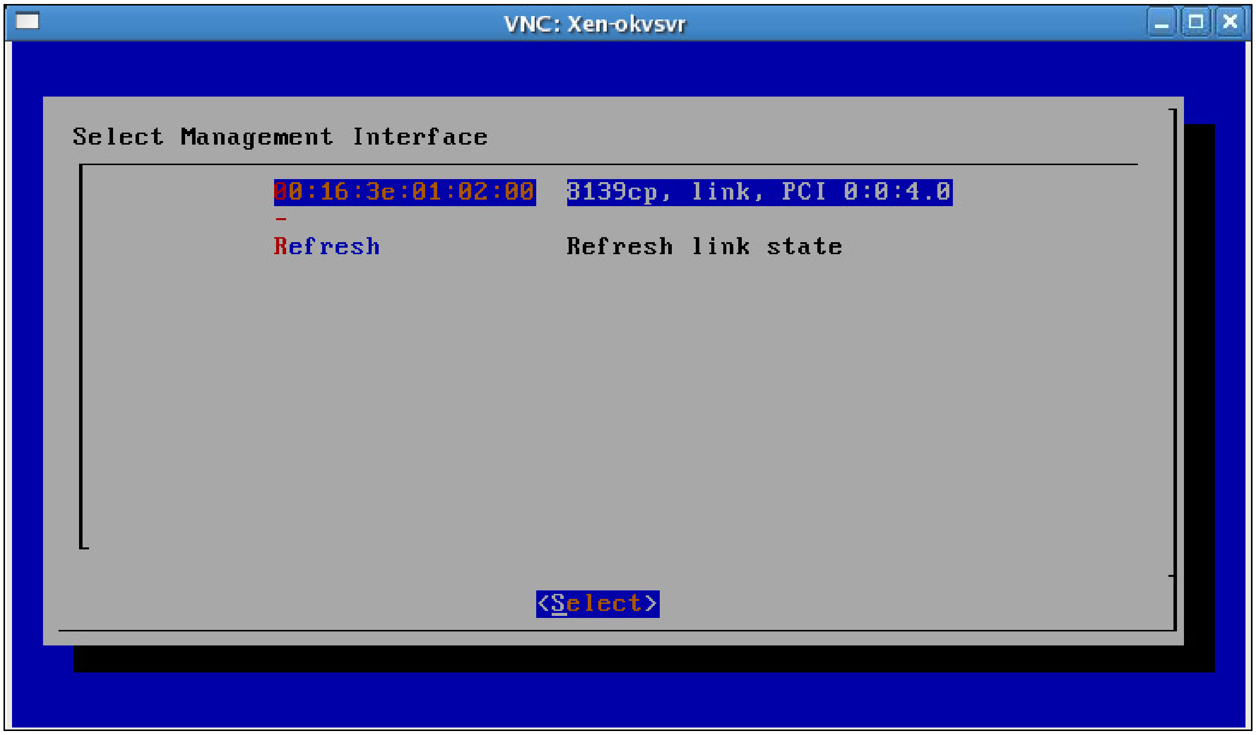
```
Please confirm installation passphrase
**********
```

13. You should see a success message. Press Enter to acknowledge the success message.



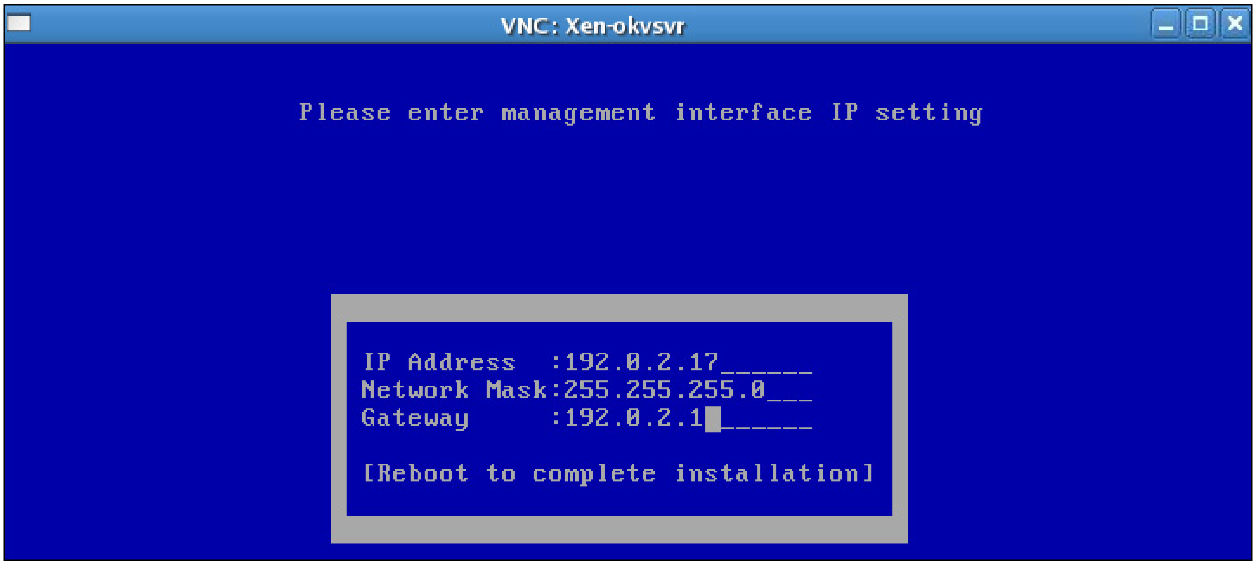
```
Success
Installation passphrase was successfully configured
```

14. Press Enter on the Select Management Interface screen to accept the default values.



```
Select Management Interface

        00:16:3e:01:02:00    8139cp, link, PCI 0:0:4.0
        Refresh              Refresh link state

                    <Select>
```

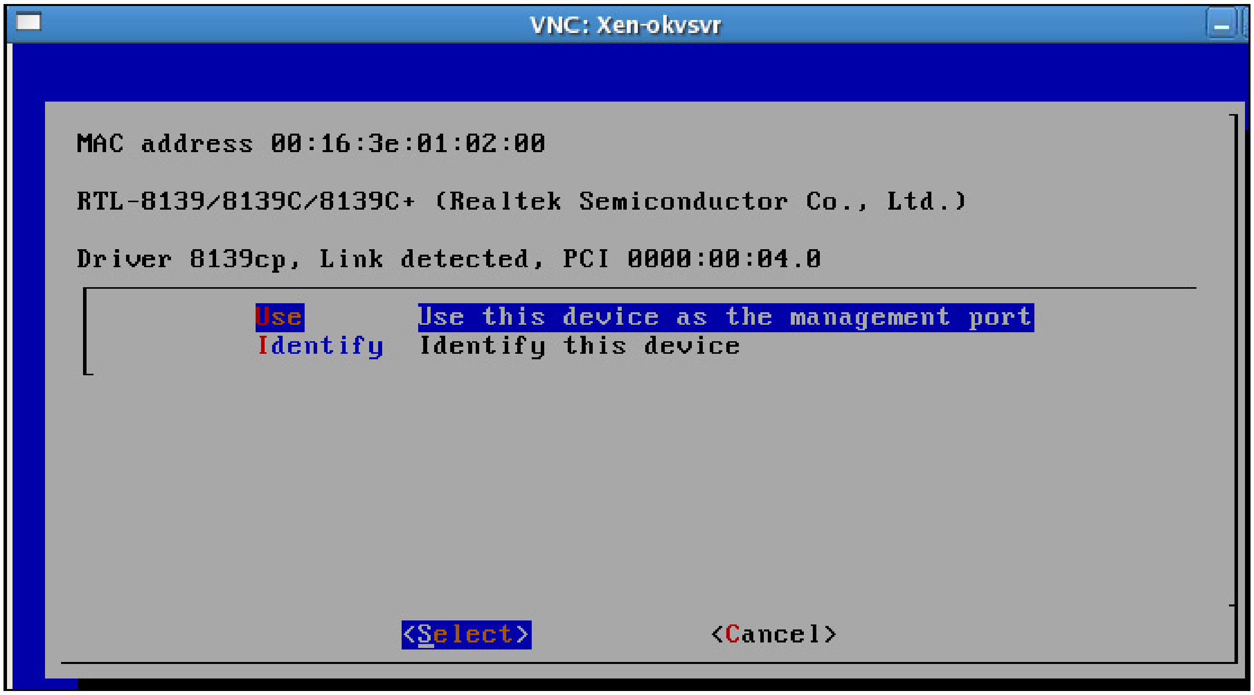
15. Press Enter on the following screen to accept the default values:



```
Please enter management interface IP setting

IP Address   :192.0.2.17______
Network Mask:255.255.255.0___
Gateway      :192.0.2.1_______

[Reboot to complete installation]
```

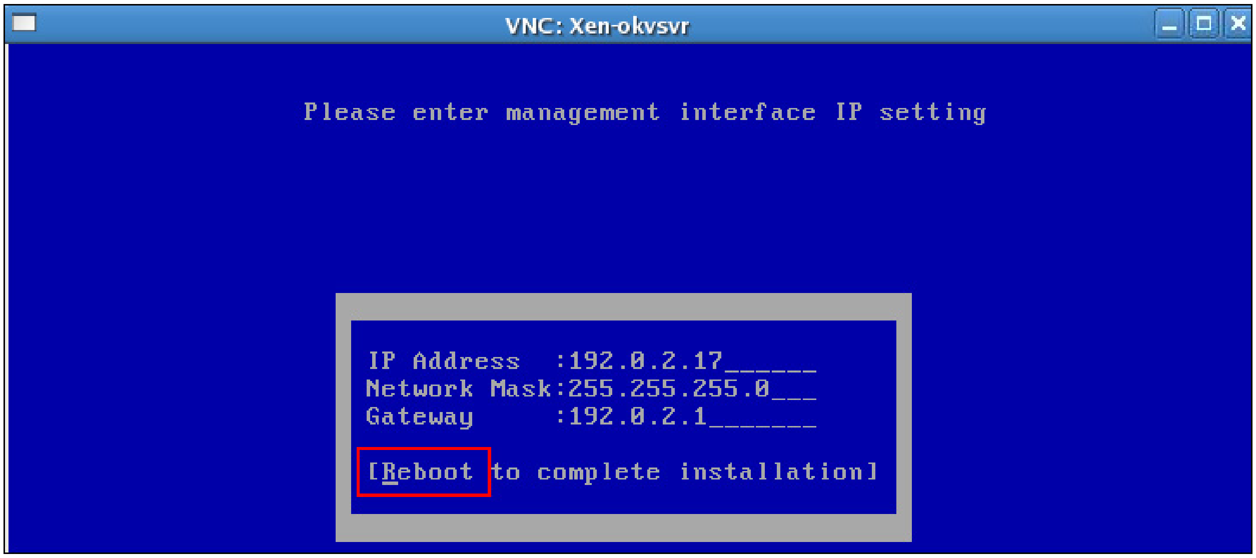
16. Enter the following values in the training setup, unless your instructor provides different ones, and press the Tab key.

```
IP Address   : 192.0.2.17
Network Mask: 255.255.255.0
Gateway      : 192.0.2.1
```



```
MAC address 00:16:3e:01:02:00

RTL-8139/8139C/8139C+ (Realtek Semiconductor Co., Ltd.)

Driver 8139cp, Link detected, PCI 0000:00:04.0

Use         Use this device as the management port
Identify    Identify this device
```

17. With the cursor on Reboot, press Enter.



```
Please enter management interface IP setting

IP Address   :192.0.2.17______
Network Mask:255.255.255.0___
Gateway      :192.0.2.1_______

[Reboot to complete installation]
```

Note: The Oracle Key Vault installer screen closes automatically.

18. Logged in a terminal window as the `root` OS user, stop the VM.

```
# xm shutdown -w okvsvr
Domain okvsvr terminated
All domains terminated
#
```

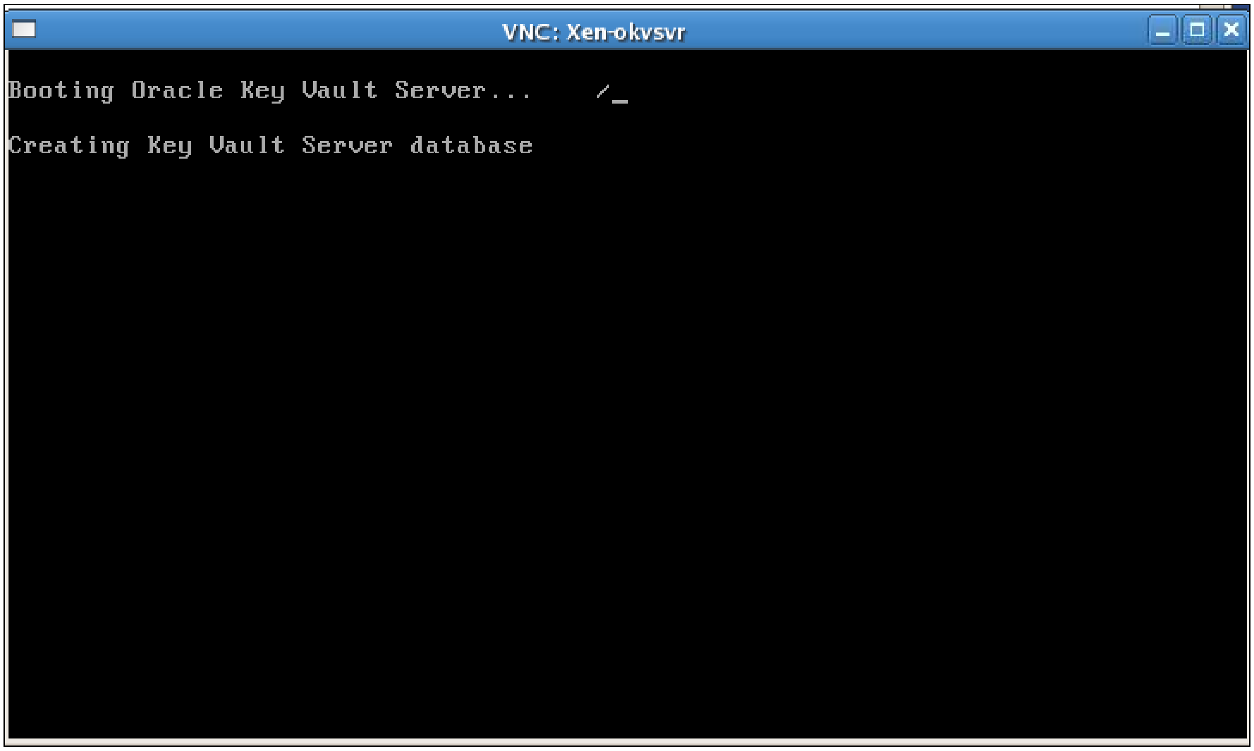
19. Restart the VM without the installation CD.

```
# xm create /OVS/running_pool/okvsvr/vm.cfg
Using config file "/OVS/running_pool/okvsvr/vm.cfg".
Started domain okvsvr (id=38)
#
```

20. Confirm the `vnc` port for the `okvsvr` VM and restart the `vncviewer` with your port number.

```
# xm list -l okvsvr | grep location
            (location 0.0.0.0:5900)
            (location 3)
# vncviewer :5900
. . . <<<output removed to avoid clutter>>>
```

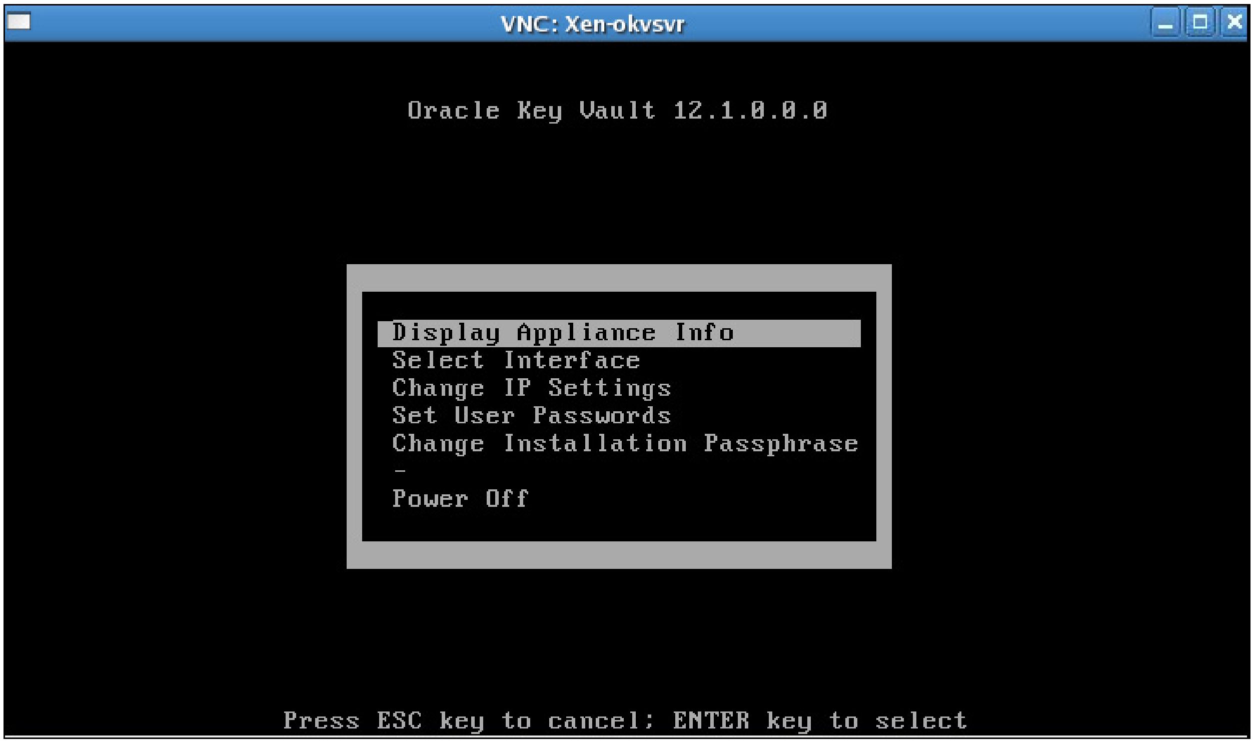
21. The Oracle Key Vault installer continues with installing a database and other Oracle software. It configures the operating system, database, and Oracle Key Vault on the server to make it a self-contained hardened appliance.



```
Booting Oracle Key Vault Server...    /_

Creating Key Vault Server database
```

Note: This process takes several minutes, during which time the screen may turn off due to the screen saver.

22. To see whether the installation has completed, press the **Shift** key (which wakes up the screen without executing additional commands).
23. If the installation has completed successfully, the following screen appears. Exit the window.



Oracle Key Vault 12.1.0.0.0

Press ESC key to cancel; ENTER key to select

24. Continue as the `root` OS user. After the installation has completed, stop the VM.

```
# xm shutdown -w okvsvr
Domain okvsvr terminated
All domains terminated
#
```

25. Sometimes you may need to perform tasks such as capturing a VM image for subsequent tests. In training, simply restart the VM.

```
# xm create /OVS/running_pool/okvsvr/vm.cfg
#
```

26. As the `root` user, confirm that all three VMs are up and running. Your values may be different.

```
# xm list
Name                                        ID   Mem VCPUs
State   Time(s)
Domain-0                                     0  1024     2
r-----  53112.9
db11204                                     41  3500     1     -
-----      4.0
host02                                      40  3500     2     -
b----     11.4
okvsvr                                      39  2048     1     -
b----    164.2
```

```
[root@EDRSR45P1 ~]#
```

Note your Oracle Key Vault appliance and two pre-installed database servers.

27. In this example, all three VMs are up and running. But if one or two were missing, you would use the appropriate `xm start` command. For example:

    ```
    xm create /OVS/running_pool/host02/vm.cfg
    xm create /OVS/running_pool/db11204/vm.cfg
    ```

    Note: If you execute the commands when the VMs are running, you receive an error.

28. Exit the `root` user account and close all terminal windows.

    ```
    # exit
    $
    ```

Practice 2-2: Performing Post-Installation Tasks for Oracle Key Vault

Overview

In this practice, you perform mandatory post-installation tasks to configure Oracle Key Vault.

Assumptions

The previous practice has been completed successfully.

Tasks

1. From the desktop, start a terminal session on the `host02` VM.

```
$ ssh -X oracle@host02
oracle@host02's password: <<<Enter oracle OS user password >>>
Last login: Wed Oct 29 08:21:51 2014 from 192.0.2.1
$
```

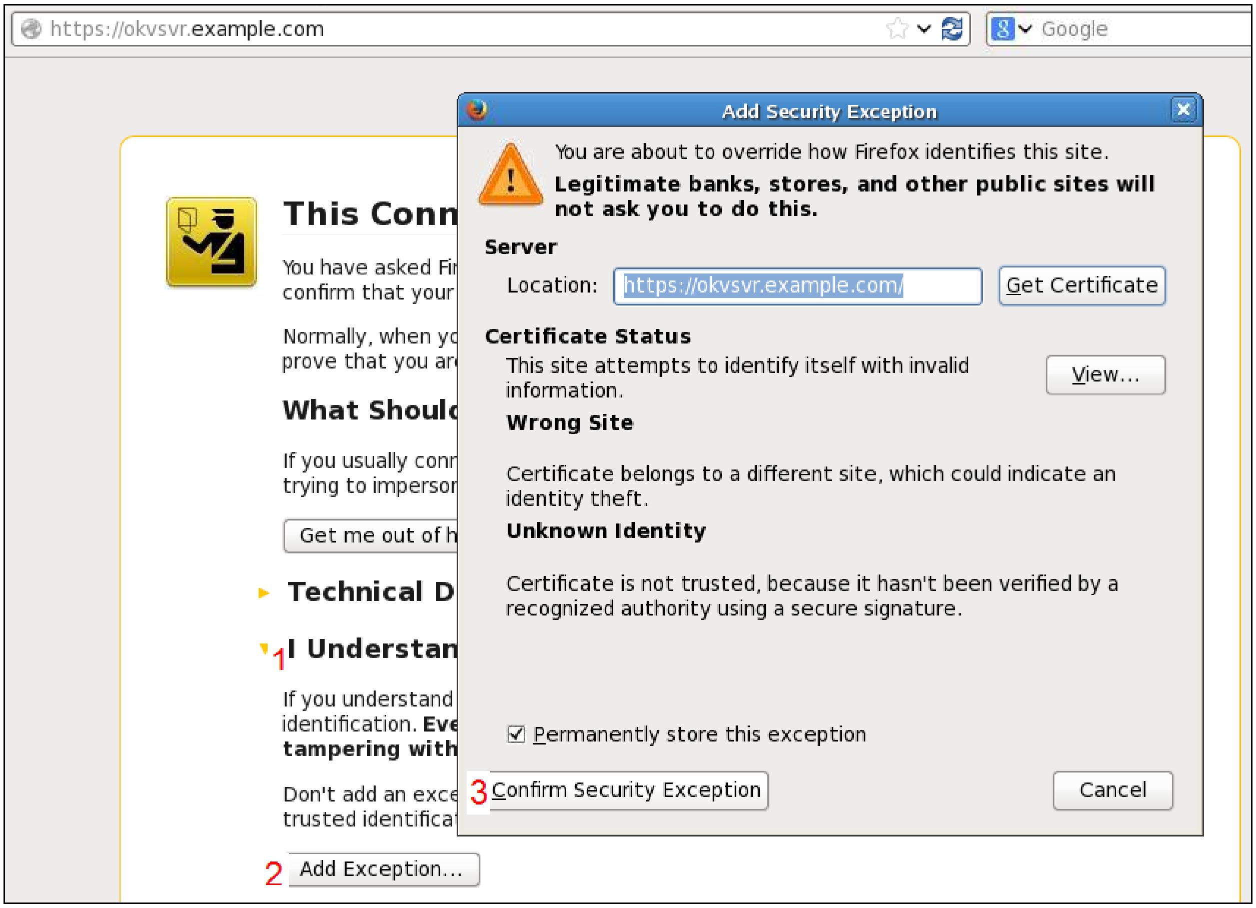
2. Start firefox from the `host02` terminal session. (Ignore the “server not found” error, if it appears.)

```
$ firefox
```

3. Enter `https://okvsvr.example.com` as the URL for the Oracle Key Vault appliance in the browser window.

https://okvsvr.example.com

4. The first time you connect, you need to accept the connection as a trusted one. Click the appropriate prompts and buttons:
   1. I Understand the Risks
   2. Add Exception
   3. Confirm Security Exception



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://okvsvr.example.com/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

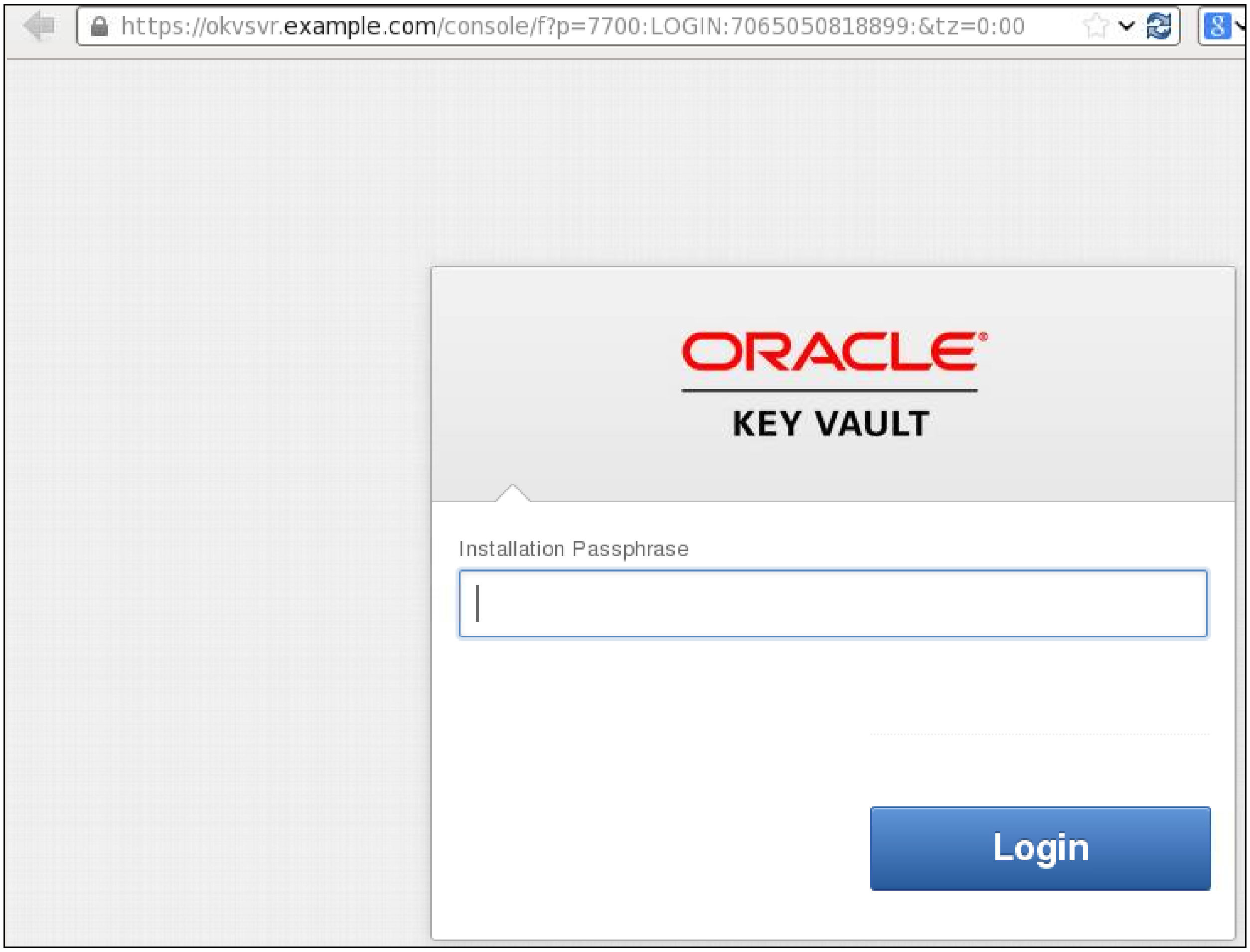
Certificate belongs to a different site, which could indicate an identity theft.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

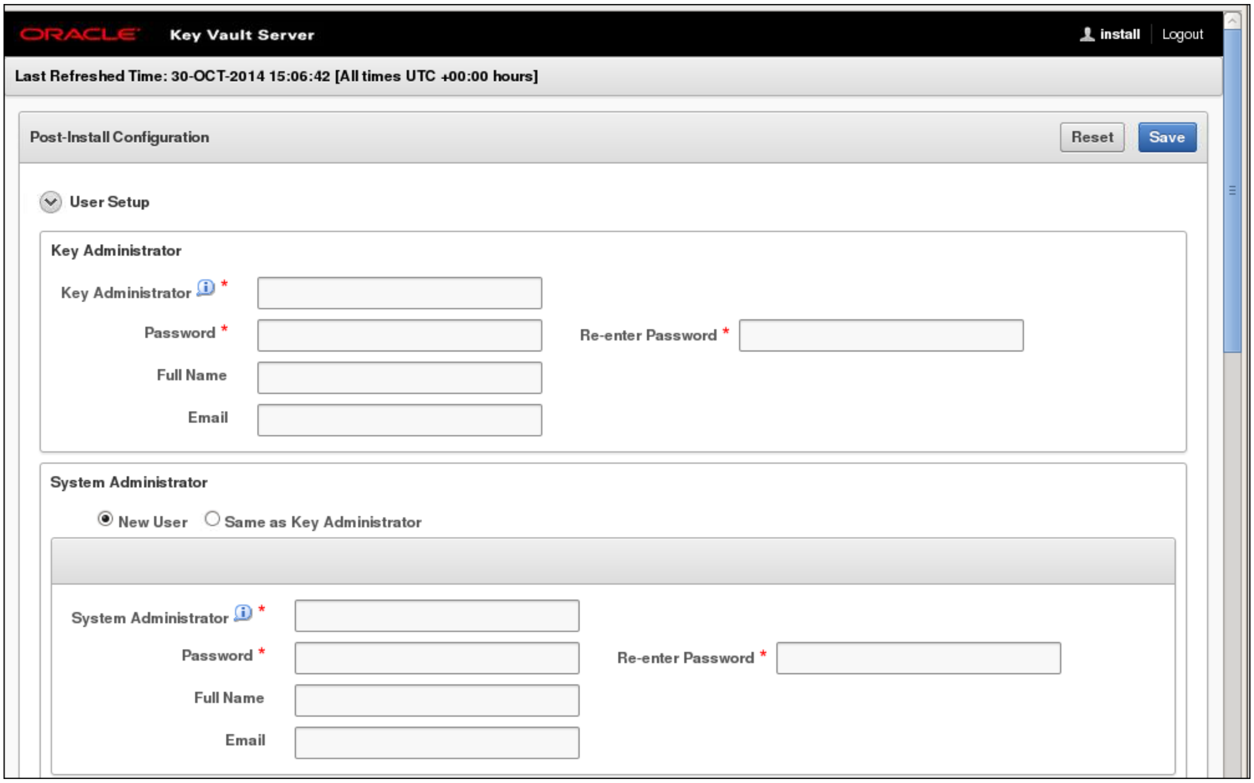
☑ Permanently store this exception

The Oracle Key Vault management console appears.



https://okvsvr.example.com/console/f?p=7700:LOGIN:7065050818899:&tz=0:00

5. Enter your **installation passphrase** and click **Login**.



Last Refreshed Time: 30-OCT-2014 15:06:42 [All times UTC +00:00 hours]

Post-Install Configuration

User Setup

Key Administrator

Key Administrator *

Password * Re-enter Password *

Full Name

Email

System Administrator

● New User ○ Same as Key Administrator

System Administrator *

Password * Re-enter Password *

Full Name

Email

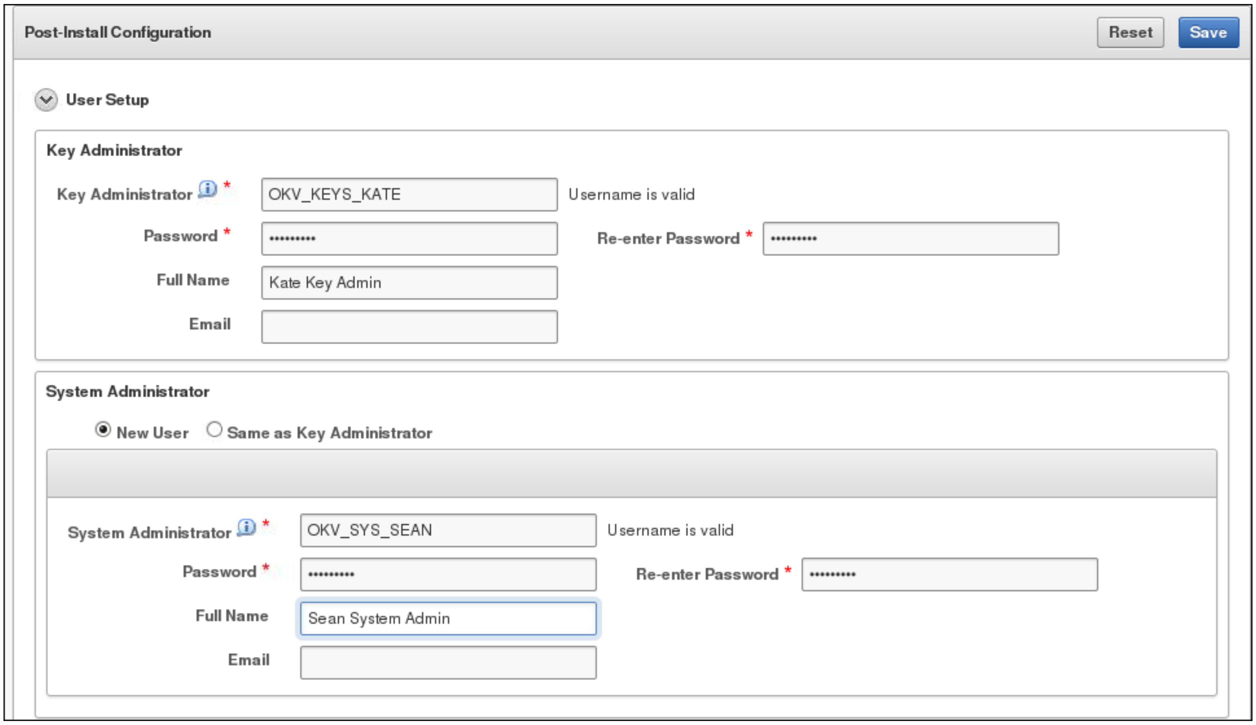
To implement separation of duties for system administration, key administration, and audit manager, enter three different sample users. In your production environment, you should enter all values correctly, including **Full Name** and **Email**.

6. On the Post-Configuration page, enter the following values, and then click **Save**.

Key Administrator	`OKV_KEYS_KATE`
Password	`oracle_4U`
Re-enter Password	`oracle_4U`
Full Name	`Kate Key Admin`
Email	
System Administrator	`OKV_SYS_SEAN`
Password	`oracle_4U`
Re-enter Password	`oracle_4U`
Full Name	`Sean System Admin`
Email	
Audit Manager	`OKV_AUD_AUDREY`
Password	`oracle_4U`
Re-enter Password	`oracle_4U`
Full Name	`Audrey Audit Mgr`

Email	
Recovery Passphrase	*Note your recovery passphrase; training example:* `oracle_4U`
Re-enter Password	*Enter the same passphrase.*
Root Password	*Enter your root OS user password.*
Re-enter Password	*Enter the same password.*
Support User Password	*Enter your oracle OS user password.*
Re-enter Password	*Enter the same password.*

Best practice tip: In your production environment, use a strong passphrase and store it in a safe location because this passphrase is used for the duration of the product life cycle.



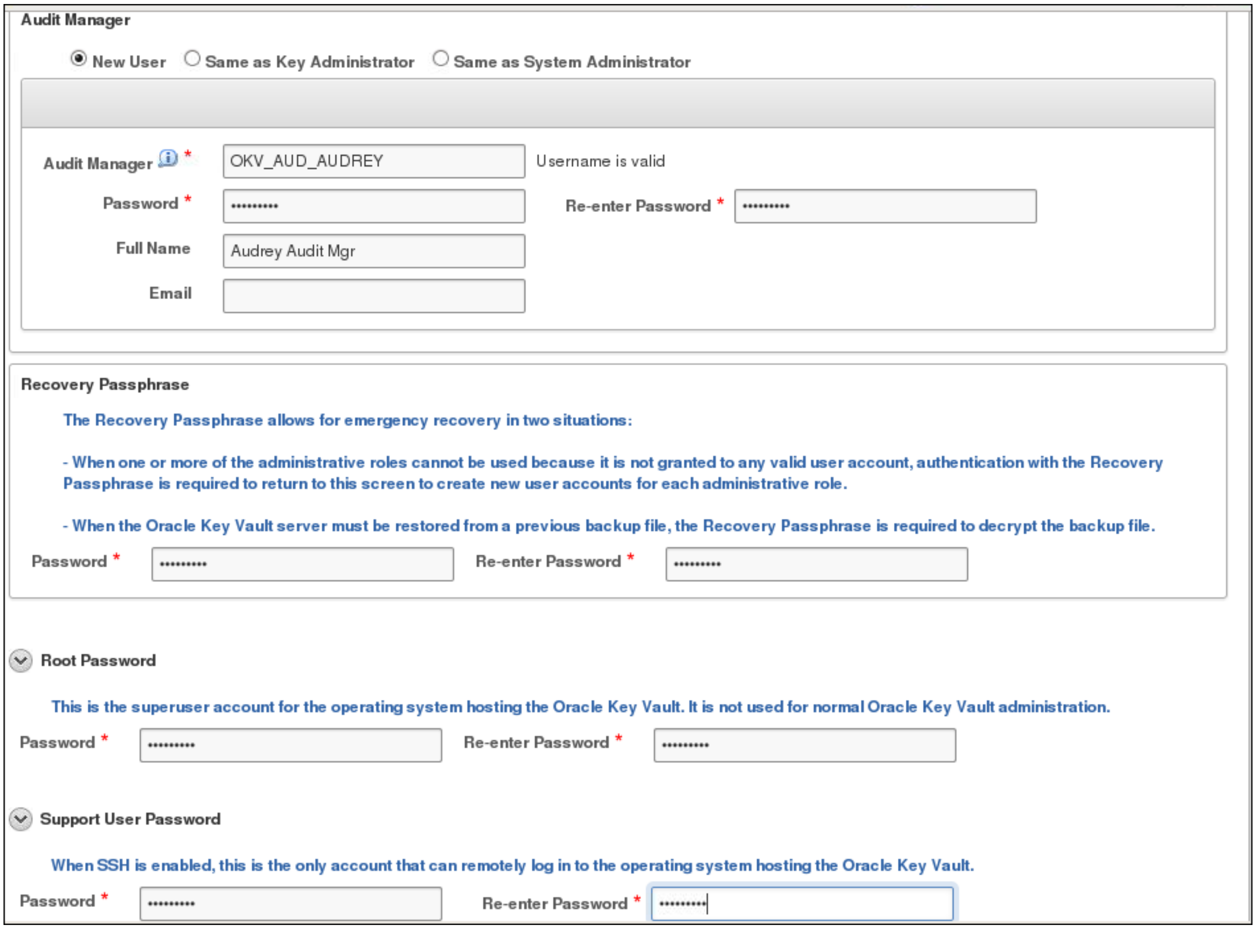
Key Administrator

Key Administrator *	OKV_KEYS_KATE	Username is valid	
Password *	•••••••••	Re-enter Password *	•••••••••
Full Name	Kate Key Admin		
Email			

System Administrator

● New User ○ Same as Key Administrator

System Administrator *	OKV_SYS_SEAN	Username is valid	
Password *	•••••••••	Re-enter Password *	•••••••••
Full Name	Sean System Admin		
Email			



Audit Manager

● New User ○ Same as Key Administrator ○ Same as System Administrator

Audit Manager *	OKV_AUD_AUDREY	Username is valid	
Password *	•••••••••	Re-enter Password *	•••••••••
Full Name	Audrey Audit Mgr		
Email			

Recovery Passphrase

The Recovery Passphrase allows for emergency recovery in two situations:

- When one or more of the administrative roles cannot be used because it is not granted to any valid user account, authentication with the Recovery Passphrase is required to return to this screen to create new user accounts for each administrative role.

- When the Oracle Key Vault server must be restored from a previous backup file, the Recovery Passphrase is required to decrypt the backup file.

Password * ••••••••• Re-enter Password * •••••••••

Root Password

This is the superuser account for the operating system hosting the Oracle Key Vault. It is not used for normal Oracle Key Vault administration.

Password * ••••••••• Re-enter Password * •••••••••

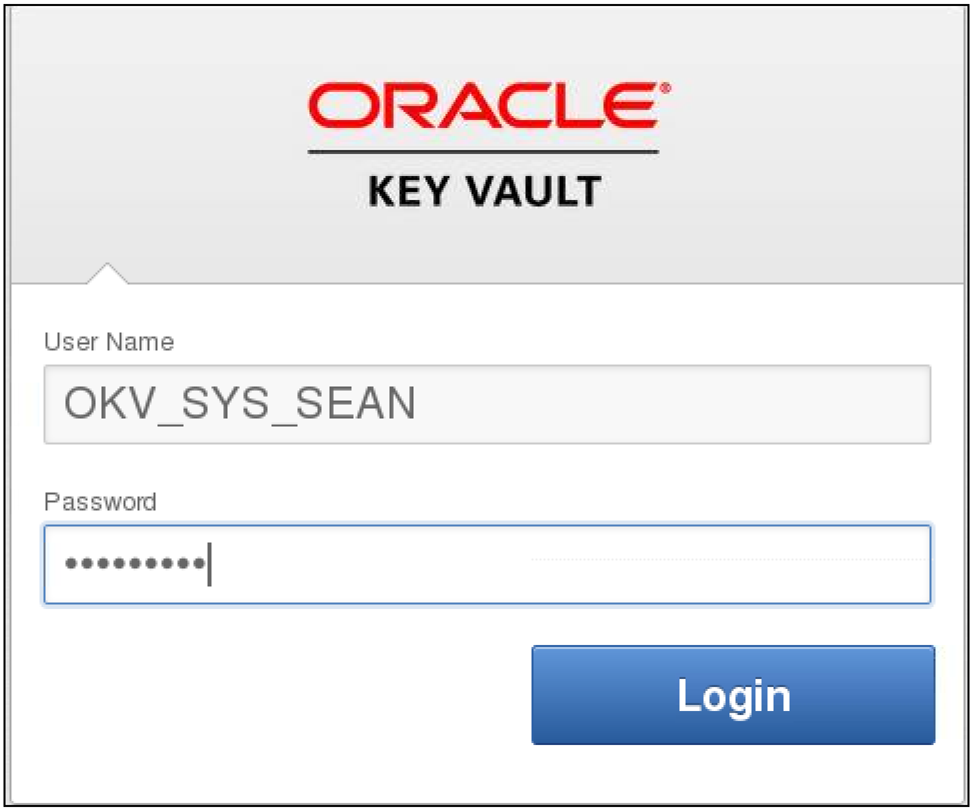
Support User Password

When SSH is enabled, this is the only account that can remotely log in to the operating system hosting the Oracle Key Vault.

Password * ••••••••• Re-enter Password * •••••••••

The Oracle Key Vault Login screen appears.

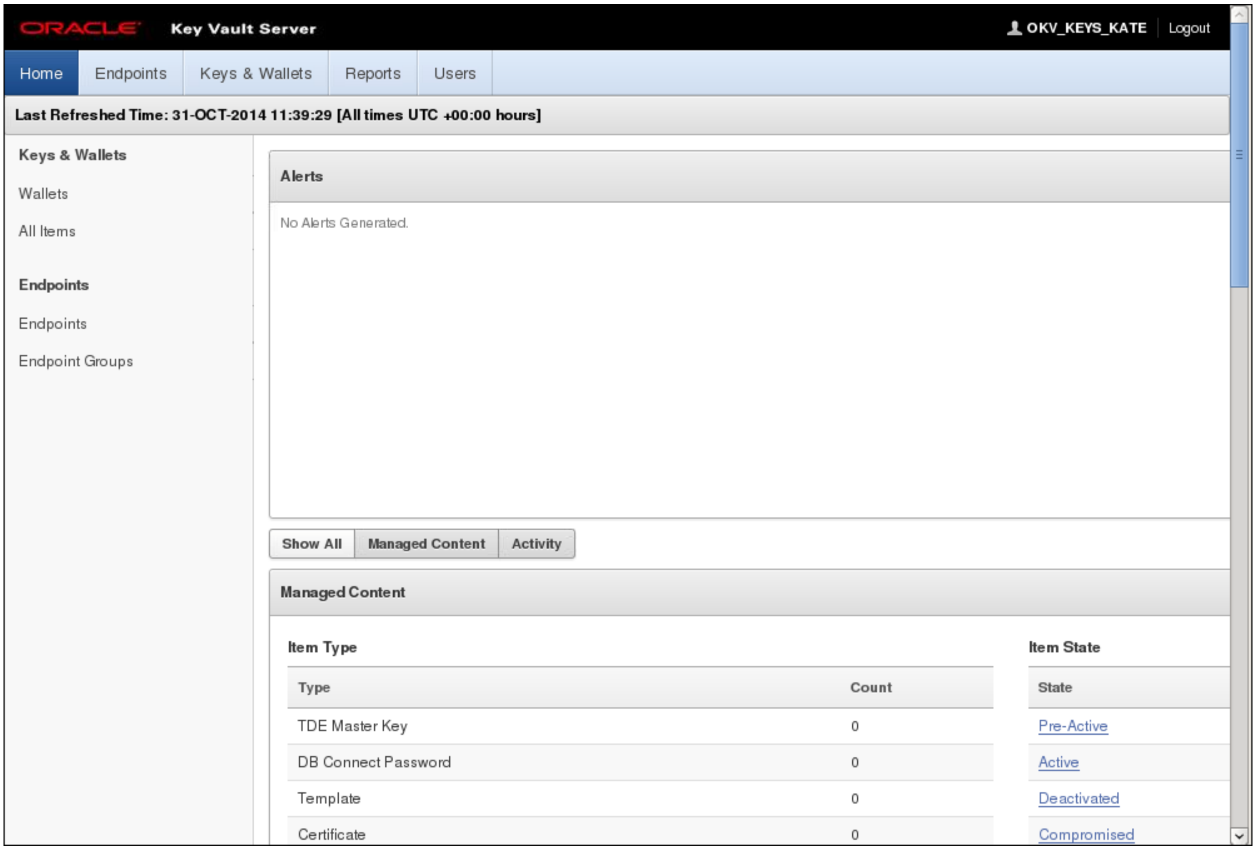
7. Test the login for your Oracle Key Vault administrators. Enter `OKV_SYS_SEAN` as **User Name** and `oracle_4U` as **Password**, and then click **Login**.



User Name: OKV_SYS_SEAN

Password: ••••••••••

8. Optionally, review the **Home** page and the **Users** page.



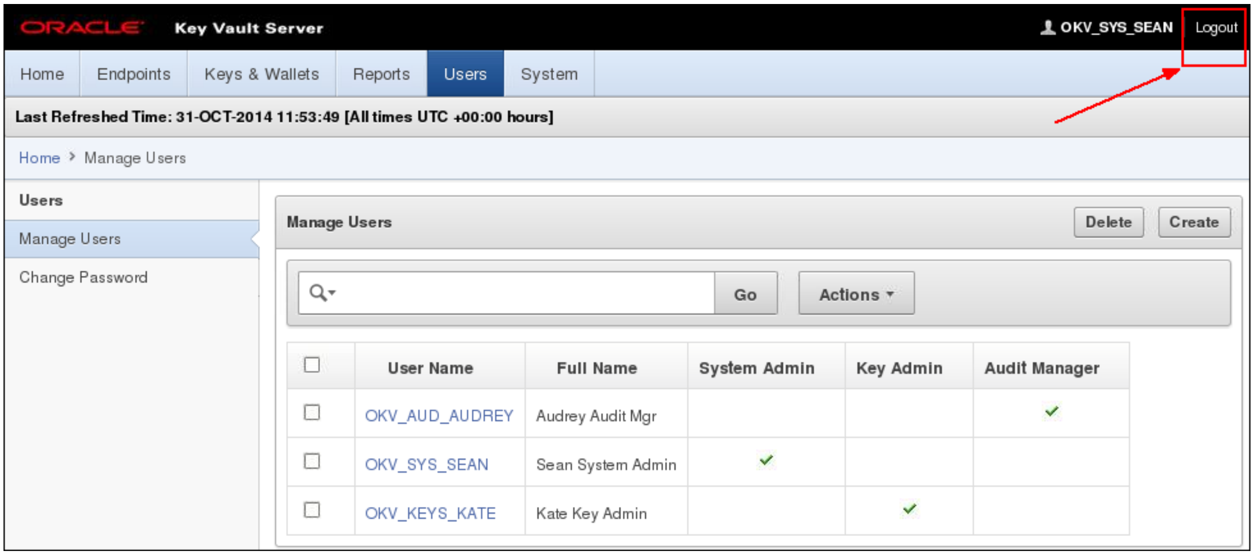
Last Refreshed Time: 31-OCT-2014 11:39:29 [All times UTC +00:00 hours]

No Alerts Generated.

Type	Count
TDE Master Key	0
DB Connect Password	0
Template	0
Certificate	0

State
Pre-Active
Active
Deactivated
Compromised

9. Click **Logout** (top-right) to test the next administrator.



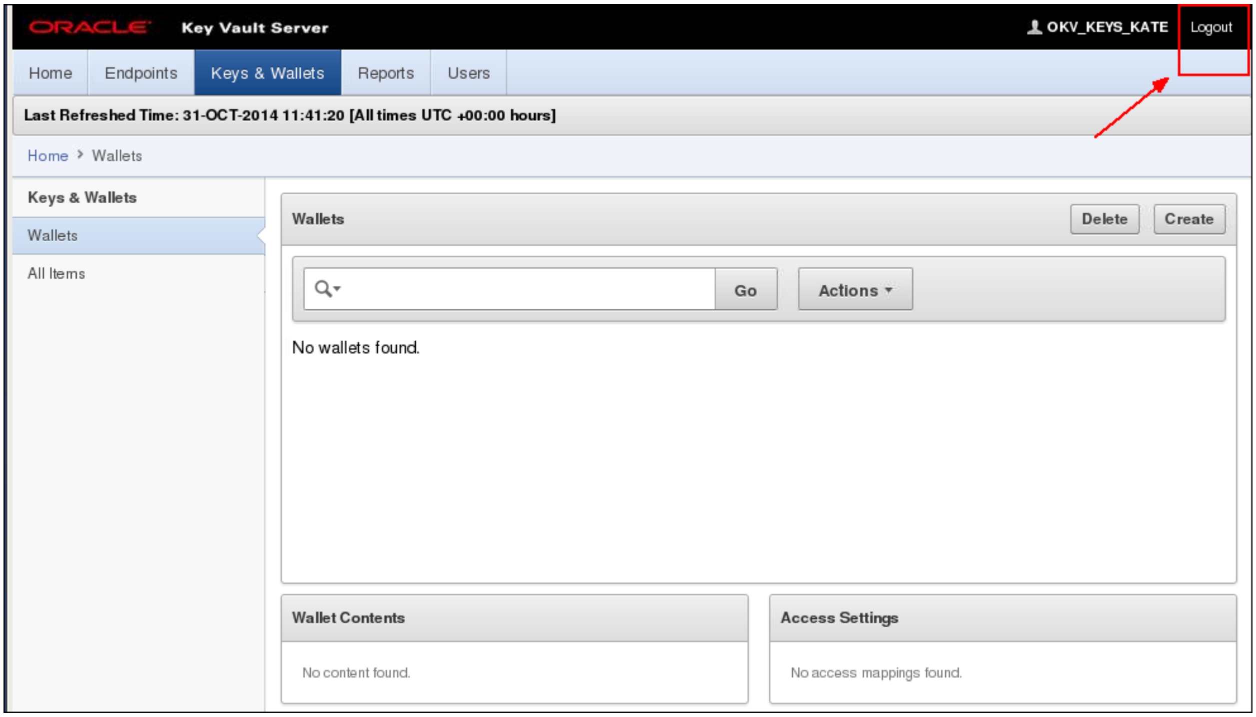
Last Refreshed Time: 31-OCT-2014 11:53:49 [All times UTC +00:00 hours]

□	User Name	Full Name	System Admin	Key Admin	Audit Manager
□	OKV_AUD_AUDREY	Audrey Audit Mgr			✓
□	OKV_SYS_SEAN	Sean System Admin	✓		
□	OKV_KEYS_KATE	Kate Key Admin		✓	

10. On the Oracle Key Vault Login page, enter `OKV_KEYS_KATE` as **User Name** and `oracle_4U` as **Password**, and then click **Login**.

    Note: The Oracle Key Vault Login page is displayed on the preceding page and will not be repeated to avoid cluttering this Activity Guide.

11. Optionally, review the **Keys & Wallets** page, and then click **Logout**.



Last Refreshed Time: 31-OCT-2014 11:41:20 [All times UTC +00:00 hours]

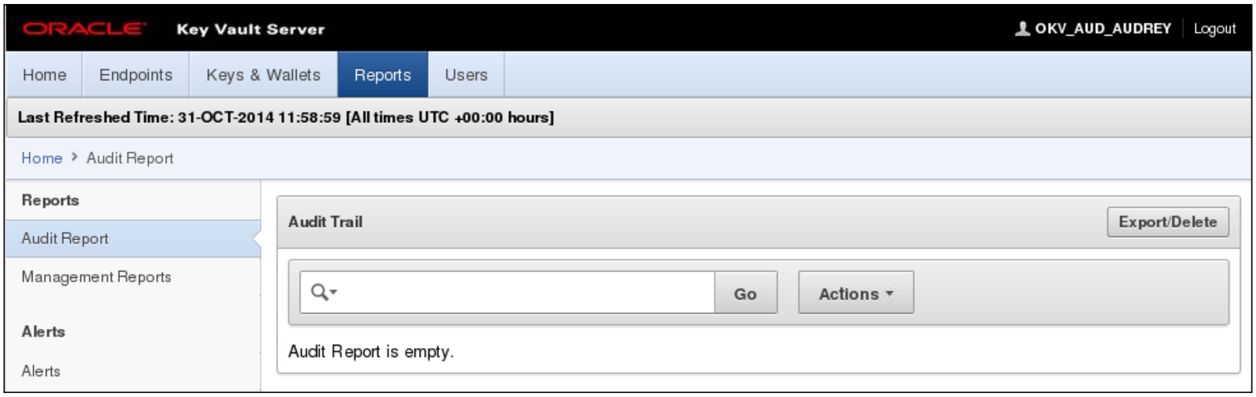
No wallets found.

No content found.

No access mappings found.

12. Enter `OKV_AUD_AUDREY` as **User Name** and `oracle_4U` as **Password**, and then click **Login**.

13. Optionally, review the **Reports** page, and then click **Logout**.



Last Refreshed Time: 31-OCT-2014 11:58:59 [All times UTC +00:00 hours]

Audit Report is empty.

Practices for Lesson 3: Working with Endpoints

Chapter 3

Practices for Lesson 3: Overview

Practices Overview

In these practices, you will enroll an Oracle Database 11.2.0.4 server as an Oracle Key Vault endpoint and learn to use the Oracle Key Vault management console.

Practice 3-1: Enrolling an Endpoint

Overview

In this practice, you enroll an Oracle Database 11.2.0.4 server as an Oracle Key Vault endpoint. The task steps are performed from the Oracle Key Vault management console, as well as the command-line interface.

Assumptions

Tasks

1. Connect to the `db11204` VM, and with your web browser, open the Oracle Key Vault management console.
   a. From the desktop, start a new terminal session on the `db11204` VM.

```
$ ssh -X oracle@db11204
oracle@ db11204's password: <<<Enter oracle OS user password >>>
Last login: Tue Oct 28 13:21:52 2014 from 192.0.2.1
$$
```

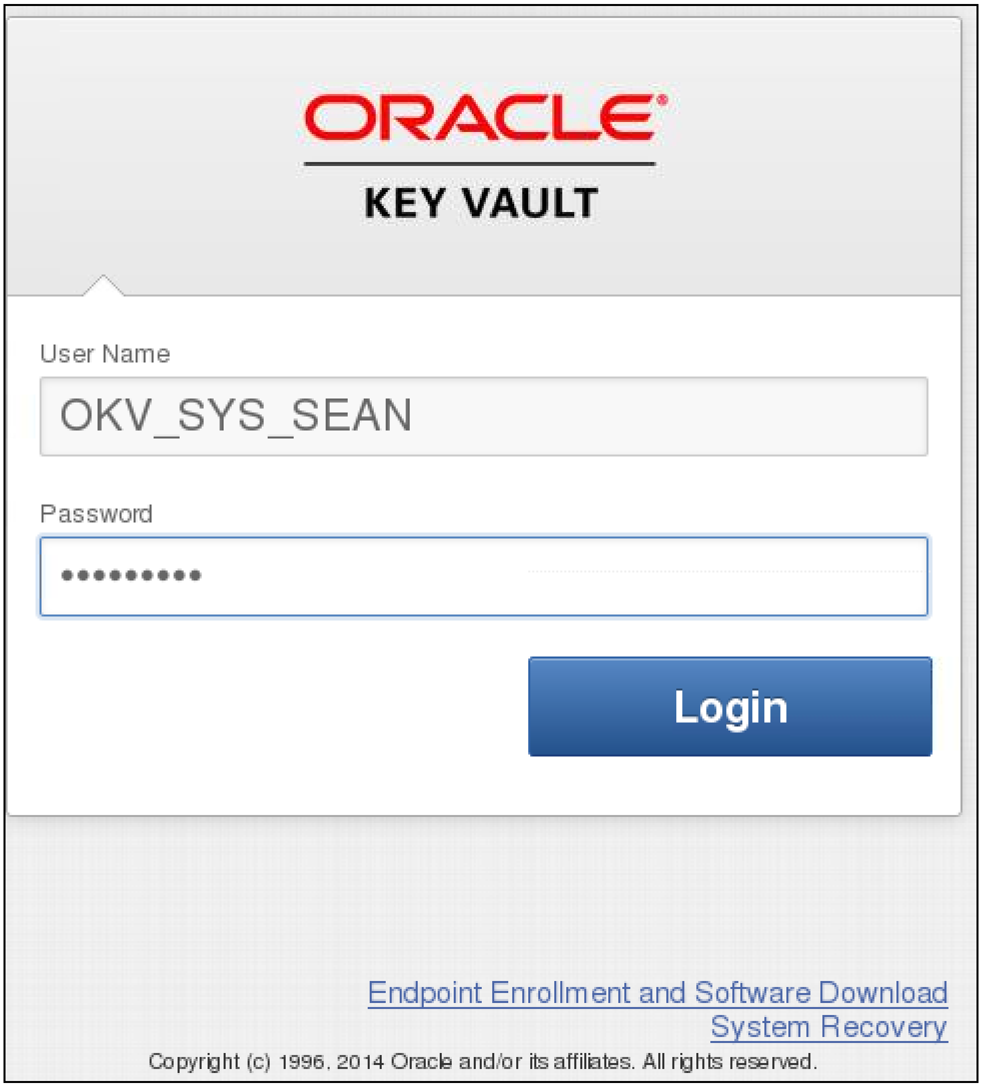
   b. Start firefox as your web browser.

```
$ firefox
```

   c. Enter `https://okvsvr.example.com` as the URL for the Oracle Key Vault appliance in the browser window.

https://okvsvr.example.com

2. To log in as the Oracle Key Vault system administrator, enter `OKV_SYS_SEAN` as **User Name**, `oracle_4U` as **Password**, and click **Login**.

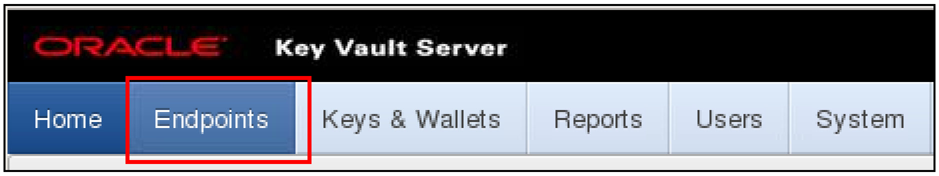


User Name: OKV_SYS_SEAN

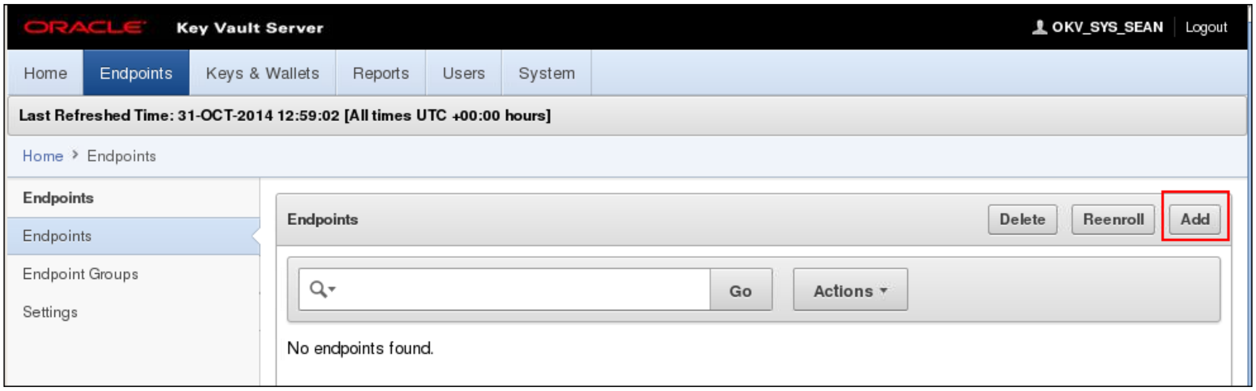
Password: ••••••••••

Copyright (c) 1996, 2014 Oracle and/or its affiliates. All rights reserved.

3. Click **Endpoints**.



4. Click **Add**.



Last Refreshed Time: 31-OCT-2014 12:59:02 [All times UTC +00:00 hours]

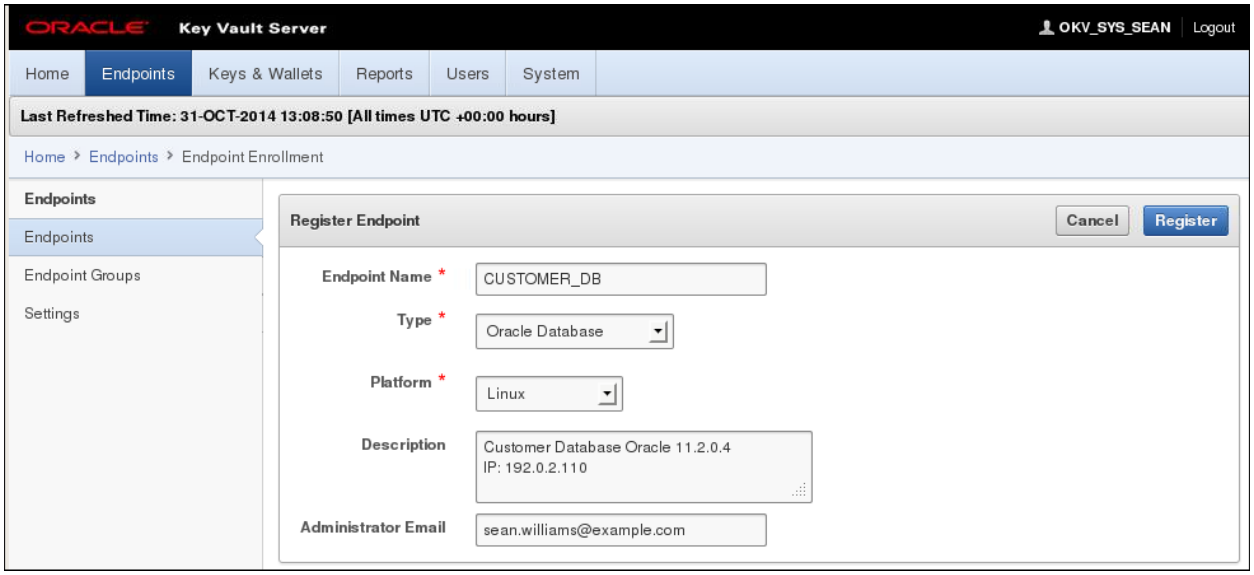
No endpoints found.

5. Enter and confirm the following values, and then click **Register**:

Endpoint Name	`CUSTOMER_DB`
Type	Oracle Database
Platform	Linux

Description	`Customer Database Oracle 11.2.0.4`
	`IP: 192.0.2.110`

Administrator Email	`sean.williams@example.com`



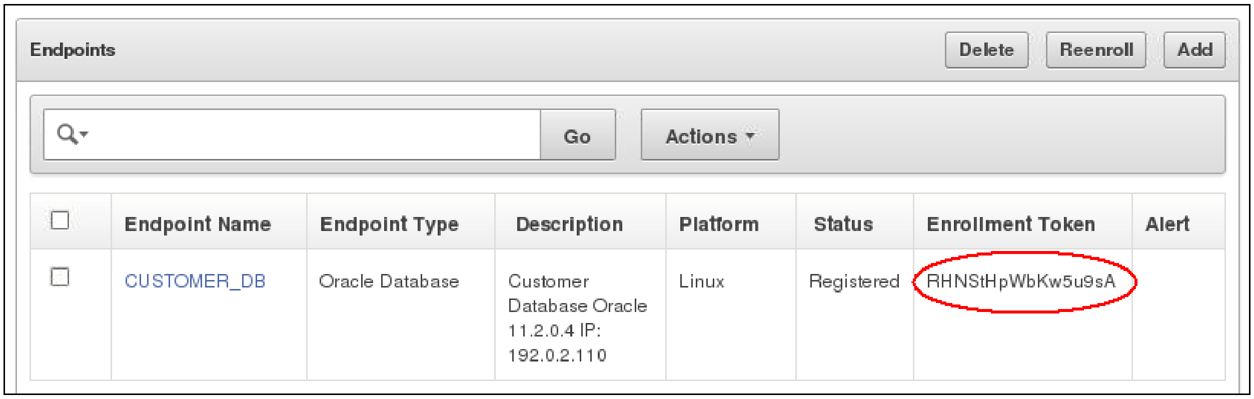
Last Refreshed Time: 31-OCT-2014 13:08:50 [All times UTC +00:00 hours]

Endpoint Name *	CUSTOMER_DB
Type *	Oracle Database
Platform *	Linux
Description	Customer Database Oracle 11.2.0.4 IP: 192.0.2.110
Administrator Email	sean.williams@example.com

After successful registration, the endpoint appears with an enrollment token. In real world deployments, the enrollment token is communicated by the system administrator in a secure way to the endpoint administrator. This enrollment token is used for authentication to download the endpoint software by the endpoint administrator.

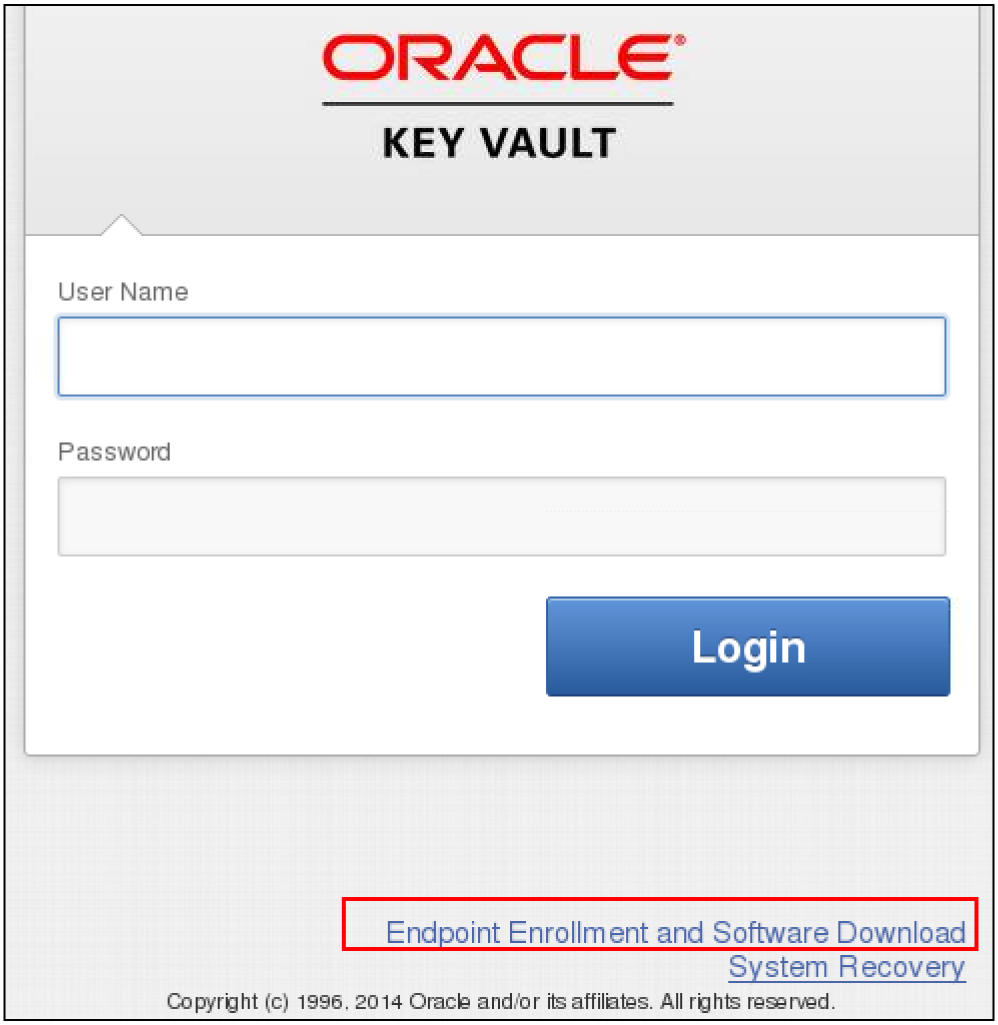
Simulate this interaction by copying the enrollment token as the system administrator and pasting it as the endpoint administrator.

6. Select and copy your enrollment token value, and then click Logout as the system administrator.

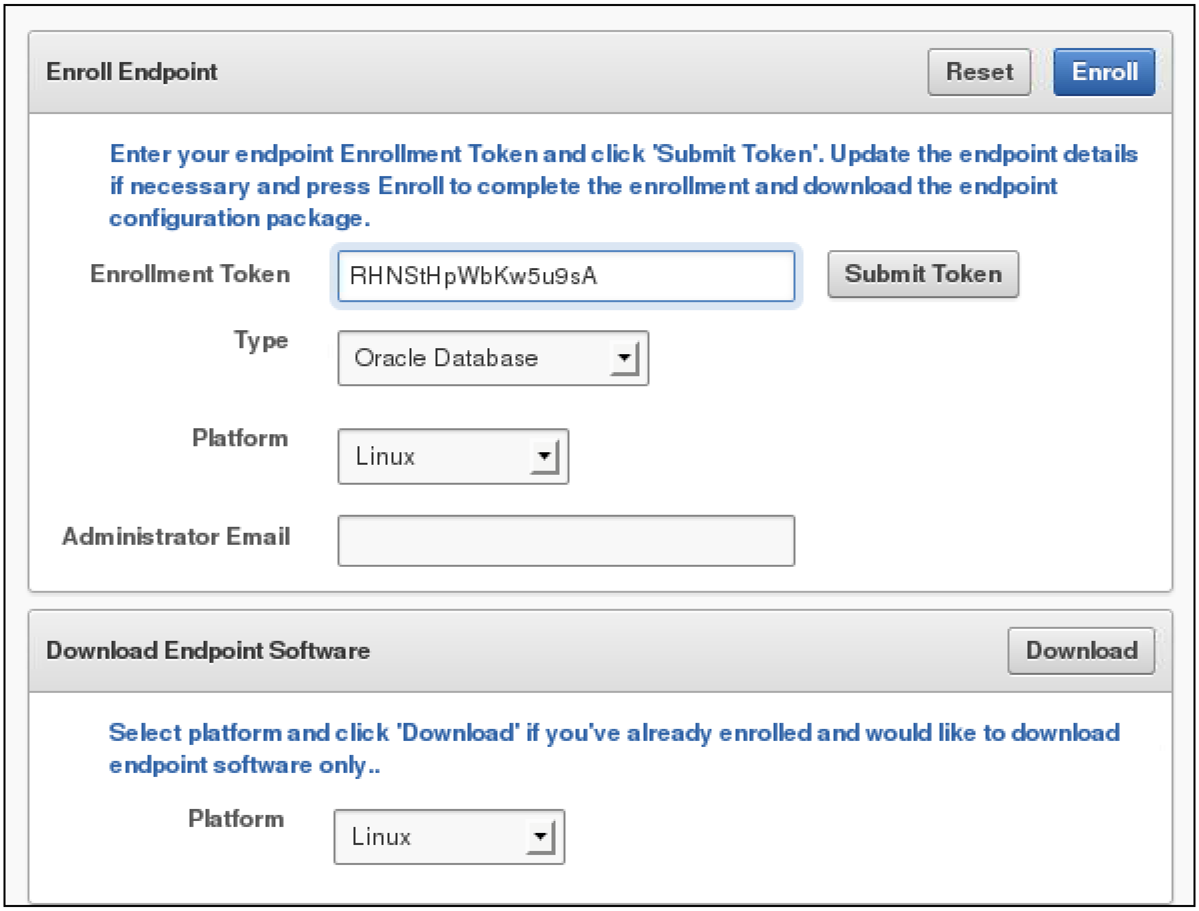


☐	Endpoint Name	Endpoint Type	Description	Platform	Status	Enrollment Token	Alert
☐	CUSTOMER_DB	Oracle Database	Customer Database Oracle 11.2.0.4 IP: 192.0.2.110	Linux	Registered	RHNStHpWbKw5u9sA	

7. As the endpoint administrator (without logging in to the Oracle Key Vault management console), click the **Endpoint Enrollment and Software Download** link.


ORACLE
KEY VAULT
User Name
Password
Login
Endpoint Enrollment and Software Download
System Recovery
Copyright (c) 1996, 2014 Oracle and/or its affiliates. All rights reserved.

8. Paste or enter the enrollment token and click **Submit Token**.



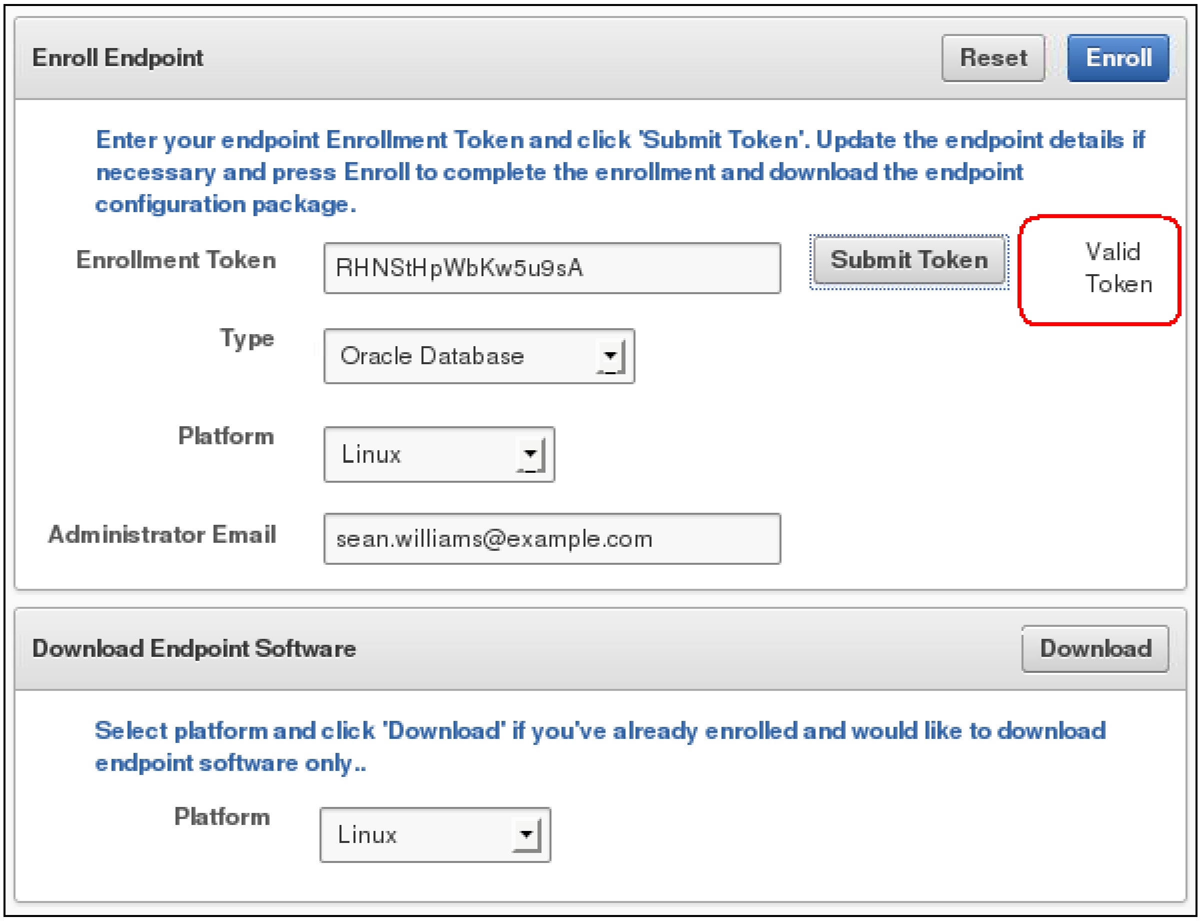
Enter your endpoint Enrollment Token and click 'Submit Token'. Update the endpoint details if necessary and press Enroll to complete the enrollment and download the endpoint configuration package.

Enrollment Token	RHNStHpWbKw5u9sA
Type	Oracle Database
Platform	Linux
Administrator Email	

Select platform and click 'Download' if you've already enrolled and would like to download endpoint software only..

Platform	Linux

9. You should get the message “Valid Token.” Click the **Enroll** button.



Enter your endpoint Enrollment Token and click 'Submit Token'. Update the endpoint details if necessary and press Enroll to complete the enrollment and download the endpoint configuration package.

Enrollment Token: RHNStHpWbKw5u9sA

Valid Token

Type: Oracle Database

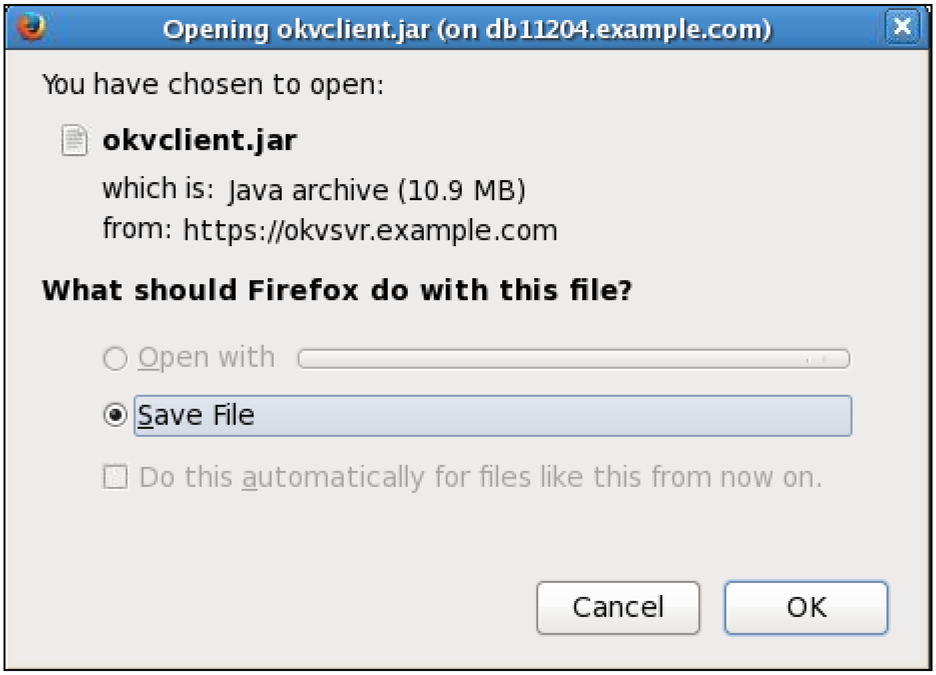
Platform: Linux

Administrator Email: sean.williams@example.com

Select platform and click 'Download' if you've already enrolled and would like to download endpoint software only..

Platform: Linux

10. When prompted, select **Save File** and click **OK**.



Opening okvclient.jar (on db11204.example.com)

You have chosen to open:

okvclient.jar

which is: Java archive (10.9 MB)

from: https://okvsvr.example.com

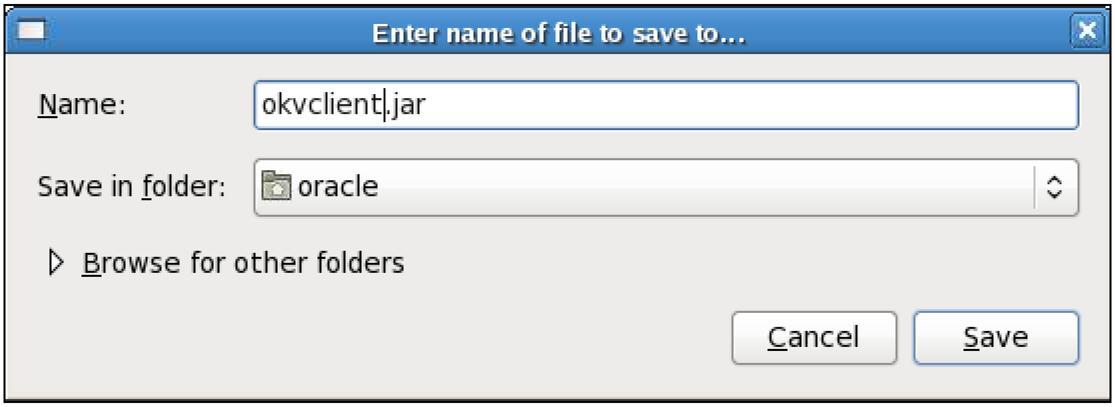
What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

11. In training, accept the defaults and click **Save**.



12. Close the Oracle Key Vault window.

Back in the db11204 terminal window, as the oracle OS user, install the Oracle Key Vault endpoint software. Ensure that installation is performed as the user who owns the environment; in this example, as the oracle OS user.

13. Confirm that your directory has the okclient.jar file. If not, navigate to the directory that contains this file.

```
$ ls okv*
okvclient.jar
$
```

Java is a prerequisite to install the endpoint software. In this training environment, Java is already setup. In a new environment, you must set the PATH or the JAVA_HOME environment variable to run Java.

14. Use the java -jar okvclient.jar -d /home/oracle/okvutil command to install the Oracle Key Vault endpoint software. The -d option specifies the location where the Oracle Key Vault endpoint software will be installed. The endpoint administrator who is performing the endpoint software installation must have read and write access to this location. In training, use the auto-login wallet by pressing Enter when prompted.

```
$ java -jar okvclient.jar -d /home/oracle/okvutil
Detected JAVA_HOME: /usr/lib/jvm/java-1.7.0-openjdk-
1.7.0.51.x86_64/jre
Enter new Key Vault endpoint password (<enter> for auto-login):
Oracle Key Vault endpoint software installed successfully.
$
```

Note: The endpoint software keeps the credentials that are used to connect to the Oracle Key Vault server in an Oracle wallet file. This wallet file requires a password to open or can be set up as an auto-login wallet.

In training, use the auto-login wallet. If you chose to use a password, note the password carefully because you must use this password whenever the endpoint software connects with the Oracle Key Vault server.

15. When you see the success message, switch to the `root` OS user with the appropriate password.

```
$ su - root
Password:
#
```

16. Execute the `root.sh` script in the `/home/oracle/okvutil/bin` directory to copy the `pkcs#11` library file, so that the Oracle database endpoint with Oracle Advanced Security TDE can directly connect with Oracle Key Vault.

```
# cd /home/oracle/okvutil/bin
# ./root.sh
Creating directory: /opt/oracle/extapi/64/hsm/oracle/1.0.0/
Copying PKCS library to /opt/oracle/extapi/64/hsm/oracle/1.0.0/
Setting PKCS library file permissions
Installation successful.
#
```

17. Switch back to the `oracle` OS user. If you want to confirm your login, use the `whoami` command.

```
# exit
logout
$ whoami
oracle
$
```

18. Execute the `okvutil list` command in the `/home/oracle/okvutil/bin` directory to check whether the Oracle Key Vault endpoint software has been enrolled and provisioned properly.
    - If the endpoint software is able to successfully connect to the Oracle Key Vault server, the “No objects found” message appears for a new installation.
    - If you see the “Server connect failed” message or any other message, your endpoint software installation has some potential issues that must be resolved before continuing with this training.

```
$ cd /home/oracle/okvutil/bin
$ ./okvutil list
No objects found
$
```

Practices for Lesson 4: Managing Oracle Wallets

Chapter 4

Practices for Lesson 4: Overview

Practices Overview

In these practices, you will set up test users and encrypted data in two database instances, upload an existing Oracle wallet from the Oracle Database 11.2 endpoint to Oracle Key Vault, download the wallet, and demonstrate that you can query encrypted data by using the downloaded wallet.

Practice 4-1: Setting Up Encrypted Data in Oracle Databases

Overview

In this practice, you set up test users and data in two database instances and encrypt them with Transparent Data Encryption (TDE) for subsequent practices.

Assumptions

Two database instances are up and running:

- `db11gr2` is version 11.2.0.4 (or later).
- `orcl` is version 12.1.0.1 (or later).

Tasks

1. Log in to the `db11204` VM.

```
$ ssh -X oracle@db11204
oracle@db11204's password:
Last login: Sat Nov  1 12:02:41 2014 from 192.0.2.1
[oracle@db11204 ~]$
```

2. Confirm that a database instance is up and running. If not, start it.

```
$ pgrep -lf pmon
$
```

3. No output means that no instance is running. To start it, first set the environment variables, and then start the `db11gr2` instance as `SYSDBA` in SQL*Plus.

```
$ . oraenv
ORACLE_SID = [oracle] ? db11gr2
The Oracle base has been set to /u01/app/oracle
[oracle@db11204 ~]$ sqlplus / as sysdba
SQL*Plus: Release 11.2.0.4.0 Production on Sat Nov 1 12:06:03
2014
Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Connected to an idle instance.

SQL> startup
ORACLE instance started.

Total System Global Area  784998400 bytes
Fixed Size                  2257352 bytes
Variable Size             268439096 bytes
Database Buffers          507510784 bytes
Redo Buffers                6791168 bytes
Database mounted.
Database opened.
```

```
SQL>
```

4. View the encryption parameters and confirm that Transparent Data Encryption is enabled.

```
SQL> select * from v$option where parameter like '%Encryption%';

PARAMETER
----------------------------------------------------------------
VALUE
----------------------------------------------------------------
Transparent Data Encryption
TRUE

Backup Encryption
TRUE

SecureFiles Encryption
TRUE
SQL>
```

5. Before executing a script, optionally, use the `cat` command to display its content.

```
SQL> !cat /home/oracle/labs/okv_setup11.sql
REM -- DISCLAIMER:
REM -- This script is provided for educational purposes only. It
is
REM -- NOT supported by Oracle World Wide Technical Support.
REM -- The script has been tested and appears to work as
intended.
REM -- You should always run new scripts on a test instance
initially.

REM -- Assumption: . oraenv has set the envrionment variables
connect / as sysdba

REM -- Create administrative users
drop user infosec_isabel cascade;
create user infosec_isabel identified by "oracle_4U";
grant create session to infosec_isabel;
REM [only in 12c] grant syskm to infosec_isabel;

REM -- Create DBA user
drop user dba_debra cascade;
create user dba_debra identified by "oracle_4U";
grant create session to dba_debra;
grant dba to dba_debra;
```

```
REM -- As endpoint DBA, create a sample tablespace
conn dba_debra/oracle_4U;
drop tablespace bankingCLEAR including contents and datafiles;
create tablespace bankingCLEAR datafile
'/u01/app/oracle/oradata/db11gr2/bankingCLEAR.dbf' size 1m;

REM -- Create a test user
DROP USER   banking cascade;
CREATE USER  banking identified by "oracle_4U" default
tablespace bankingCLEAR;
grant unlimited tablespace to banking;

REM -- Create a table with sample data
drop table banking.customers;
create table banking.customers (first_name varchar(20),
last_name varchar(20), ccn varchar(20)) tablespace bankingCLEAR;

insert into banking.customers values('Mike','Anderson','5421-
5424-1451-5340');
insert into banking.customers values('Jon','Hewell','5325-8942-
5653-0031');
insert into banking.customers values('Andrew','Forsyth','4553-
0984-2344-4101');
insert into banking.customers values('Ellen','Kane','4489-4023-
0489-0492');
insert into banking.customers values('Randall','Summers','5193-
0013-0002-2345');
insert into banking.customers values('Julia','Cortez','4545-
5702-4211-8889');
insert into banking.customers values('Melissa','Hiam','5900-
4451-8812-7171');
insert into banking.customers values('Elise','Fenters','4331-
4921-5031-9871');
insert into banking.customers values('Paul','Watts','4442-1902-
7477-3239');
insert into banking.customers values('Jim','Johnson','4921-1212-
6612-0080');
insert into banking.customers values('Scott','Manning','5890-
1454-3554-9886');
commit;
alter system flush buffer_cache;
SQL>
```

6. To create test users and test data, execute the `okv_setup11.sql` script. (Rows with only space are removed to avoid cluttering the output.)

```
SQL> @/home/oracle/labs/okv_setup11.sql
User dropped.
User created.
Grant succeeded.
User dropped.
User created.
Grant succeeded.
Grant succeeded.
Connected.
Tablespace dropped.
Tablespace created.
User dropped.
User created.
Grant succeeded.
drop table banking.customers
                  *
ERROR at line 1:
ORA-00942: table or view does not exist
Table created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
Commit complete.
System altered.
SQL>
```

7. Your output may look a little different depending on your environment. Confirm that you can query the data that is to be encrypted, and then exit.

```
SQL> select ccn from banking.customers;

CCN
--------------------
5421-5424-1451-5340
```

```
5325-8942-5653-0031
4553-0984-2344-4101
4489-4023-0489-0492
5193-0013-0002-2345
4545-5702-4211-8889
5900-4451-8812-7171
4331-4921-5031-9871
4442-1902-7477-3239
4921-1212-6612-0080
5890-1454-3554-9886

11 rows selected.

SQL> exit
$
```

8. If it does not exist, create a directory for the Oracle wallet.

```
$ ls $ORACLE_BASE/admin/db11204/wallet
ls: cannot access /u01/app/oracle/admin/db11204/wallet: No such
file or directory
$ mkdir -p $ORACLE_BASE/admin/db11204/wallet
$
```

9. Confirm that the `sqlnet.ora` file contains a path that points to the wallet directory.

```
$ cat $ORACLE_HOME/network/admin/sqlnet.ora
# -- DISCLAIMER:
# -- This script is provided for educational purposes only. It
is
# -- NOT supported by Oracle World Wide Technical Support.
# -- The script has been tested and appears to work as intended.
# -- You should always run new scripts on a test instance
initially

# For local wallet keystore
ENCRYPTION_WALLET_LOCATION=
 (SOURCE =
  (METHOD = FILE)
   (METHOD_DATA =
    (DIRECTORY = /u01/app/oracle/admin/db11204/wallet)))

$
```

Note: The path points to the directory for the local wallet.

10. If it does not exist, create an Oracle wallet.

```
$ ls $ORACLE_BASE/admin/db11204/wallet
$
```

11. There is no `ewallet.p12` file. Create it as `SYSDBA` by setting an encryption key.

```
$ sqlplus / as sysdba
SQL>
SQL> ALTER SYSTEM set encryption key identified by "secretKEY";

System altered.
SQL>
```

12. Confirm that `ewallet.p12` exists and is open.

```
SQL> ! ls -l /u01/app/oracle/admin/db11204/wallet
total 4
-rw-r--r-- 1 oracle oinstall 2845 Nov  1 12:24 ewallet.p12

SQL>
SQL> SELECT WRL_PARAMETER, STATUS, WRL_TYPE FROM
V$ENCRYPTION_WALLET;

WRL_PARAMETER
----------------------------------------------------------------
----------------
STATUS             WRL_TYPE
------------------ --------------------
/u01/app/oracle/admin/db11204/wallet
OPEN               file

SQL>
```

13. Connect as the `DBA_DEBRA` user and encrypt the `CCN` column.

```
SQL> conn dba_debra
Enter password:
Connected.
SQL> ALTER TABLE banking.customers MODIFY (ccn ENCRYPT);

Table altered.

SQL>
```

14. Confirm that the test data displays correctly.

```
SQL> SELECT * from banking.customers;

FIRST_NAME           LAST_NAME            CCN
-------------------- -------------------- --------------------
Mike                 Anderson             5421-5424-1451-5340
Jon                  Hewell               5325-8942-5653-0031
Andrew               Forsyth              4553-0984-2344-4101
Ellen                Kane                 4489-4023-0489-0492
Randall              Summers              5193-0013-0002-2345
Julia                Cortez               4545-5702-4211-8889
Melissa              Hiam                 5900-4451-8812-7171
Elise                Fenters              4331-4921-5031-9871
Paul                 Watts                4442-1902-7477-3239
Jim                  Johnson              4921-1212-6612-0080
Scott                Manning              5890-1454-3554-9886

11 rows selected.
SQL>
```

15. As the `DBA_DEBRA` user, encrypt a tablespace with TDE.

```
SQL> DROP TABLESPACE   bankingENC including contents and
datafiles;
CREATE TABLESPACE bankingENC
   datafile '/u01/app/oracle/oradata/db11gr2/bankingENC.dbf'
size 1M
   encryption using 'AES256' default storage(encrypt);
DROP TABLESPACE   bankingENC including contents and datafiles
*
ERROR at line 1:
ORA-00959: tablespace 'BANKINGENC' does not exist

SQL>   2    3
Tablespace created.
SQL>
```

16. Create a test table in the encrypted tablespace.

```
SQL> DROP TABLE   banking.customersENC cascade constraints;
CREATE TABLE banking.customersENC tablespace bankingENC as
select * from banking.customers;
DROP TABLE   banking.customersENC cascade constraints
                     *
ERROR at line 1:
ORA-00942: table or view does not exist
```

```

SQL>
Table created.
SQL>
```

17. Confirm that the data can be queried, and then exit.

```
SQL> select * from banking.customersENC;

FIRST_NAME           LAST_NAME            CCN
-------------------- -------------------- --------------------
Mike                 Anderson             5421-5424-1451-5340
Jon                  Hewell               5325-8942-5653-0031
Andrew               Forsyth              4553-0984-2344-4101
Ellen                Kane                 4489-4023-0489-0492
Randall              Summers              5193-0013-0002-2345
Julia                Cortez               4545-5702-4211-8889
Melissa              Hiam                 5900-4451-8812-7171
Elise                Fenters              4331-4921-5031-9871
Paul                 Watts                4442-1902-7477-3239
Jim                  Johnson              4921-1212-6612-0080
Scott                Manning              5890-1454-3554-9886

11 rows selected.

SQL> exit
$
```

18. Go through the same workflow on the host02 VM. Log in to the host02 VM.

```
$ ssh -X oracle@host02
oracle@host024's password:
Last login: Sat Nov  1 12:02:41 2014 from 192.0.2.1
$
```

19. Confirm that a database instance is up and running. If not, start it.

```
$ pgrep -lf pmon
1696 ora_pmon_orcl
$
```

20. The ORCL instance is up and running. Set the environment variables.

```
$ . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base has been set to /u01/app/oracle
[oracle@host02 ~]$
```

21. Log in to SQL*Plus as `SYSDBA` and confirm that Transparent Data Encryption is enabled.

```
$ sqlplus / as sysdba

SQL> select * from v$option where parameter like '%Encryption%';

PARAMETER
----------------------------------------------------------------
VALUE
----------------------------------------------------------------
Transparent Data Encryption
TRUE

Backup Encryption
TRUE

SecureFiles Encryption
TRUE
SQL>
```

22. To create test users and test data, execute the `okv_setup12.sql` script. (The `okv_setup11` and `okv_setup12` scripts are almost identical, with the exception that `okv_setup12` contains an additional grant (new with the Oracle Database 12*c*): `grant syskm to infosec_isabel;`)

```
SQL> @/home/oracle/labs/okv_setup12.sql
User dropped.
User created.
Grant succeeded.
User dropped.
User created.
Grant succeeded.
Grant succeeded.
Connected.
Tablespace dropped.
Tablespace created.
User dropped.
User created.
Grant succeeded.
Table dropped.
Table created.
1 row created.
1 row created.
1 row created.
1 row created.
```

```
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
1 row created.
Commit complete.
System altered.
SQL>
```

23. Your output may look a little different depending on your environment. Confirm that you can query the data that is to be encrypted, and then exit.

```
SQL> select ccn from banking.customers;
CCN
--------------------
5421-5424-1451-5340
5325-8942-5653-0031
4553-0984-2344-4101
4489-4023-0489-0492
5193-0013-0002-2345
4545-5702-4211-8889
5900-4451-8812-7171
4331-4921-5031-9871
4442-1902-7477-3239
4921-1212-6612-0080
5890-1454-3554-9886

11 rows selected.

SQL> exit
$
```

24. If it does not exist, create a directory for the Oracle wallet.

```
$ ls $ORACLE_BASE/admin/orcl/wallet
ls: cannot access /u01/app/oracle/admin/orcl/wallet: No such
file or directory
$ mkdir -p $ORACLE_BASE/admin/orcl/wallet
$
```

25. Confirm that the `sqlnet.ora` file contains a path that points to the wallet directory.

```
$ cat $ORACLE_HOME/network/admin/sqlnet.ora
# sqlnet.ora Network Configuration File:
/u01/app/oracle/product/12.1.0/dbhome_1/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.
```

```
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)

# -- DISCLAIMER:
# -- This script is provided for educational purposes only. It
is
# -- NOT supported by Oracle World Wide Technical Support.
# -- The script has been tested and appears to work as intended.
# -- You should always run new scripts on a test instance
initially

# For local training wallet keystore
ENCRYPTION_WALLET_LOCATION=
 (SOURCE =
  (METHOD = FILE)
   (METHOD_DATA =
    (DIRECTORY = /u01/app/oracle/admin/orcl/wallet)))

#    Initial migration of existing wallet into OKV
# ENCRYPTION_WALLET_LOCATION=
#  (SOURCE =
#   (METHOD = HSM)
#    (METHOD_DATA =
#     (DIRECTORY = /u01/app/oracle/admin/orcl/wallet)))

#   For fresh start with OKV or ongoing usage of OKV
# ENCRYPTION_WALLET_LOCATION = (SOURCE = (METHOD = HSM))


$
```

26. Confirm that a directory exists for a local wallet.

```
$ ls $ORACLE_BASE/admin/orcl/wallet
$
```

27. The directory exists and contains no wallet. Create one in SQL*Plus.

```
$ sqlplus / as sysdba

SQL> ALTER SYSTEM set encryption key identified by "secretKEY";

System altered.

SQL>
```

28. Confirm that the wallet exists in the directory and is open.

```
SQL> ! ls -l /u01/app/oracle/admin/orcl/wallet
total 4
-rw-r--r-- 1 oracle oinstall 3112 Nov  1 17:26 ewallet.p12

SQL> SELECT WRL_PARAMETER, STATUS, WRL_TYPE FROM
V$ENCRYPTION_WALLET;

WRL_PARAMETER
----------------------------------------------------------------
----------------
STATUS                         WRL_TYPE
------------------------------ --------------------
/u01/app/oracle/admin/orcl/wallet
OPEN                           FILE

SQL>
```

29. As the DBA_DEBRA user, encrypt the CCN column and confirm that the data can be displayed.

```
SQL> conn dba_debra
Enter password:
Connected.
SQL>
SQL> ALTER TABLE banking.customers MODIFY (ccn ENCRYPT);

Table altered.

SQL> SELECT * from banking.customers;

FIRST_NAME           LAST_NAME            CCN
-------------------- -------------------- --------------------
Mike                 Anderson             5421-5424-1451-5340
Jon                  Hewell               5325-8942-5653-0031
Andrew               Forsyth              4553-0984-2344-4101
Ellen                Kane                 4489-4023-0489-0492
Randall              Summers              5193-0013-0002-2345
Julia                Cortez               4545-5702-4211-8889
Melissa              Hiam                 5900-4451-8812-7171
Elise                Fenters              4331-4921-5031-9871
Paul                 Watts                4442-1902-7477-3239
Jim                  Johnson              4921-1212-6612-0080
Scott                Manning              5890-1454-3554-9886
```

```

11 rows selected.
SQL>
```

30. Create an encrypted tablespace.

```
SQL> DROP TABLESPACE   bankingENC including contents and
datafiles;
CREATE TABLESPACE bankingENC
   datafile '/u01/app/oracle/oradata/orcl/bankingENC.dbf' size
1M
   encryption using 'AES256' default storage(encrypt);
DROP TABLESPACE   bankingENC including contents and datafiles
*
ERROR at line 1:
ORA-00959: tablespace 'BANKINGENC' does not exist



SQL>   2    3
Tablespace created.

SQL>
```

31. Create a test table in the encrypted tablespace and confirm that you can read the data. Then exit.

```
SQL> DROP TABLE   banking.customersENC cascade constraints;
CREATE TABLE banking.customersENC tablespace bankingENC as
select * from banking.customers;
DROP TABLE   banking.customersENC cascade constraints
                     *
ERROR at line 1:
ORA-00942: table or view does not exist
SQL>
Table created.

SQL> select * from banking.customersENC;

FIRST_NAME           LAST_NAME            CCN
-------------------- -------------------- --------------------
Mike                 Anderson             5421-5424-1451-5340
Jon                  Hewell               5325-8942-5653-0031
Andrew               Forsyth              4553-0984-2344-4101
Ellen                Kane                 4489-4023-0489-0492
Randall              Summers              5193-0013-0002-2345
Julia                Cortez               4545-5702-4211-8889
Melissa              Hiam                 5900-4451-8812-7171
```

```
Elise                Fenters              4331-4921-5031-9871
Paul                 Watts                4442-1902-7477-3239
Jim                  Johnson              4921-1212-6612-0080
Scott                Manning              5890-1454-3554-9886

11 rows selected.
SQL> exit
$
```

Practice 4-2: Up- and Downloading Wallets with Oracle Key Vault

Overview

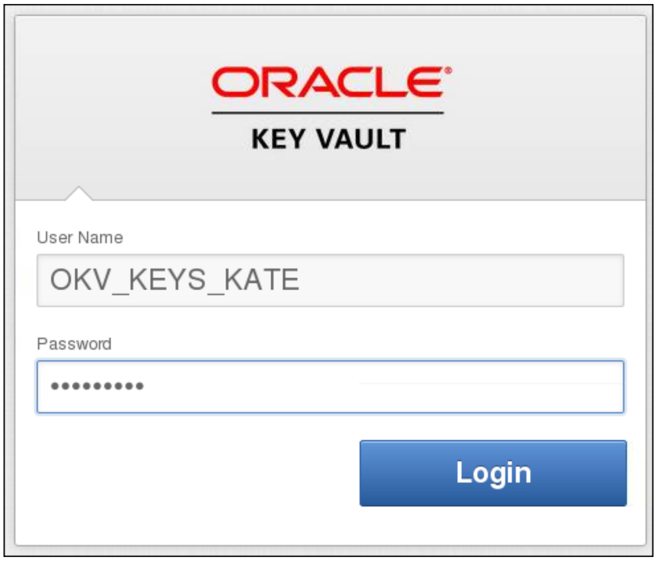
In this practice, you upload an existing Oracle wallet from the Oracle Database 11.2 endpoint to Oracle Key Vault for long-term retention. Then you download the wallet and demonstrate that you can query encrypted data by using the downloaded wallet.

Assumptions

You successfully completed the previous practice.

Tasks

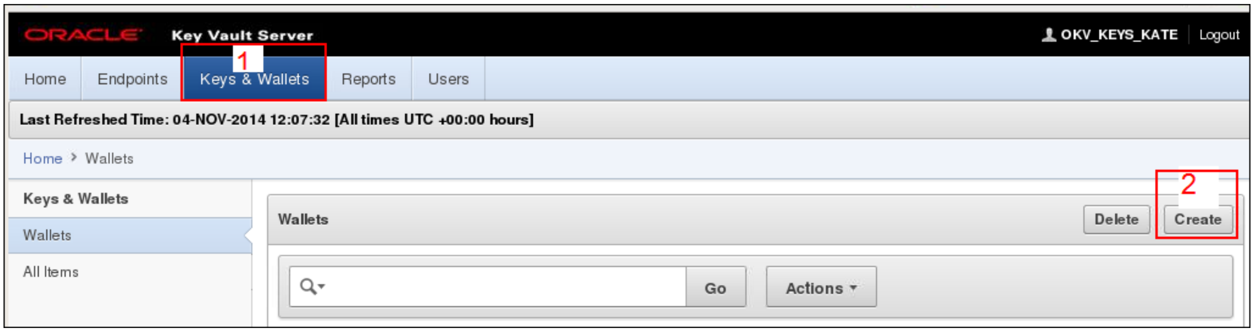
1. Connected to the `db11204` VM, open the Oracle Key Vault management console in your web browser. Log in as the `OKV_KEYS_KATE` key administrator.



User Name: OKV_KEYS_KATE

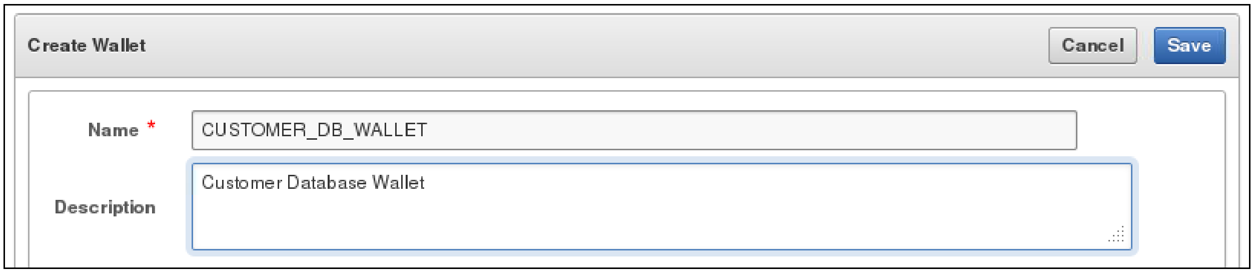
Password: ●●●●●●●●●●

2. Navigate to **Keys & Wallets** and click the **Create** button.



Last Refreshed Time: 04-NOV-2014 12:07:32 [All times UTC +00:00 hours]

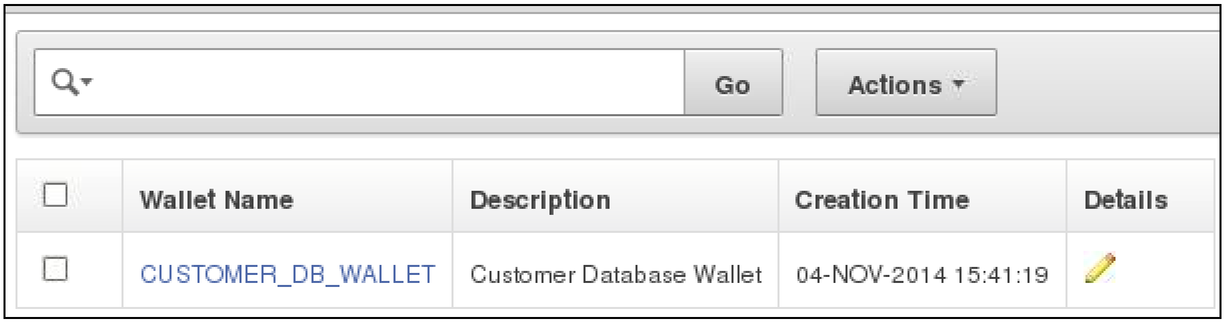
3. Enter `CUSTOMER_DB_WALLET` as **Name,** `Customer Database Wallet` as **Description,** and then click **Save**.



Name * CUSTOMER_DB_WALLET

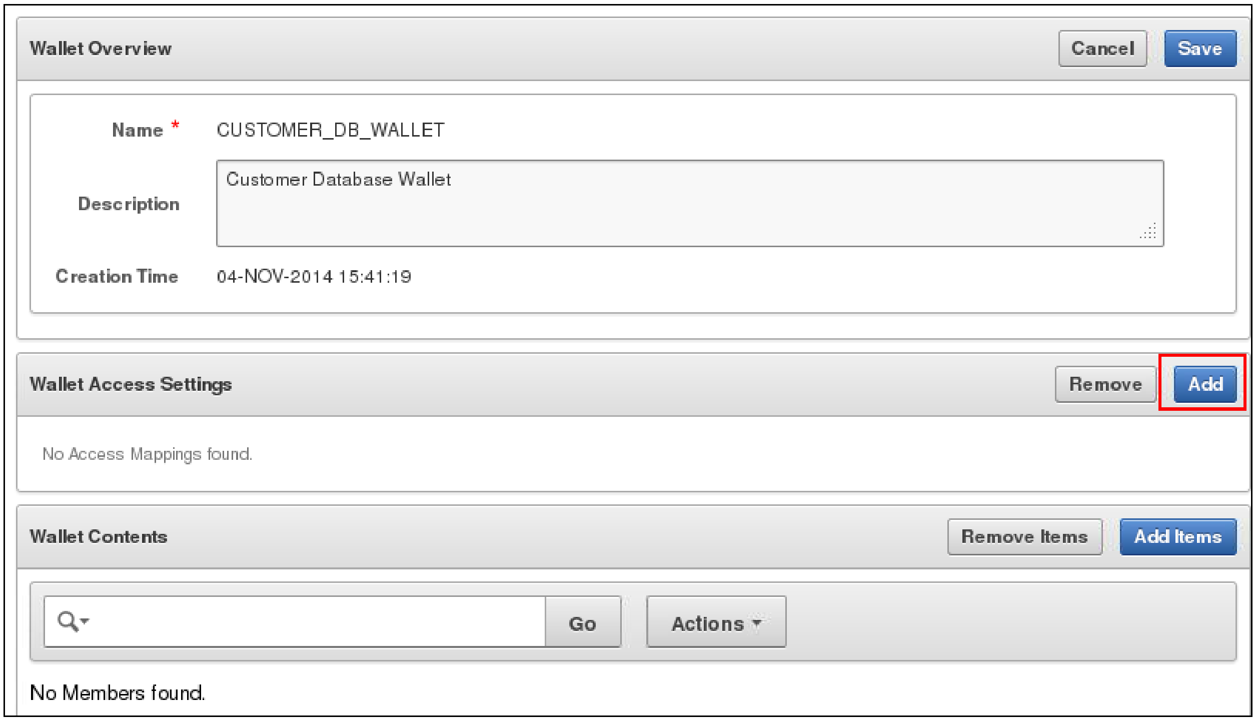
Description Customer Database Wallet

4. When the `CUSTOMER_DB_WALLET` wallet appears on the page (which means that it has been created), click the **Details** pencil icon.



□	Wallet Name	Description	Creation Time	Details
□	CUSTOMER_DB_WALLET	Customer Database Wallet	04-NOV-2014 15:41:19	✎

5. Click **Add** in the Wallet Access Settings section.



Name * CUSTOMER_DB_WALLET

Description Customer Database Wallet

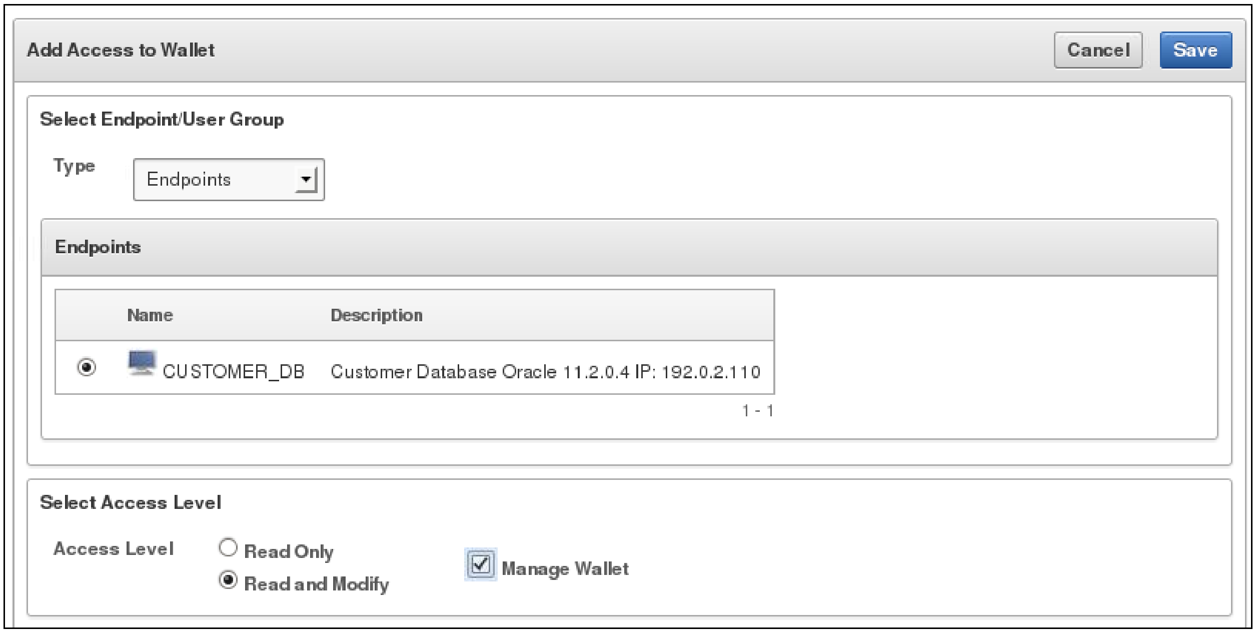
Creation Time 04-NOV-2014 15:41:19

No Access Mappings found.

No Members found.

6. Enter and confirm the following values, and then click **Save**.

Type	Endpoints
CUSTOMER_DB	*<selected>*
Read and Modify	*<selected>*
Manage Wallet	*<selected>*



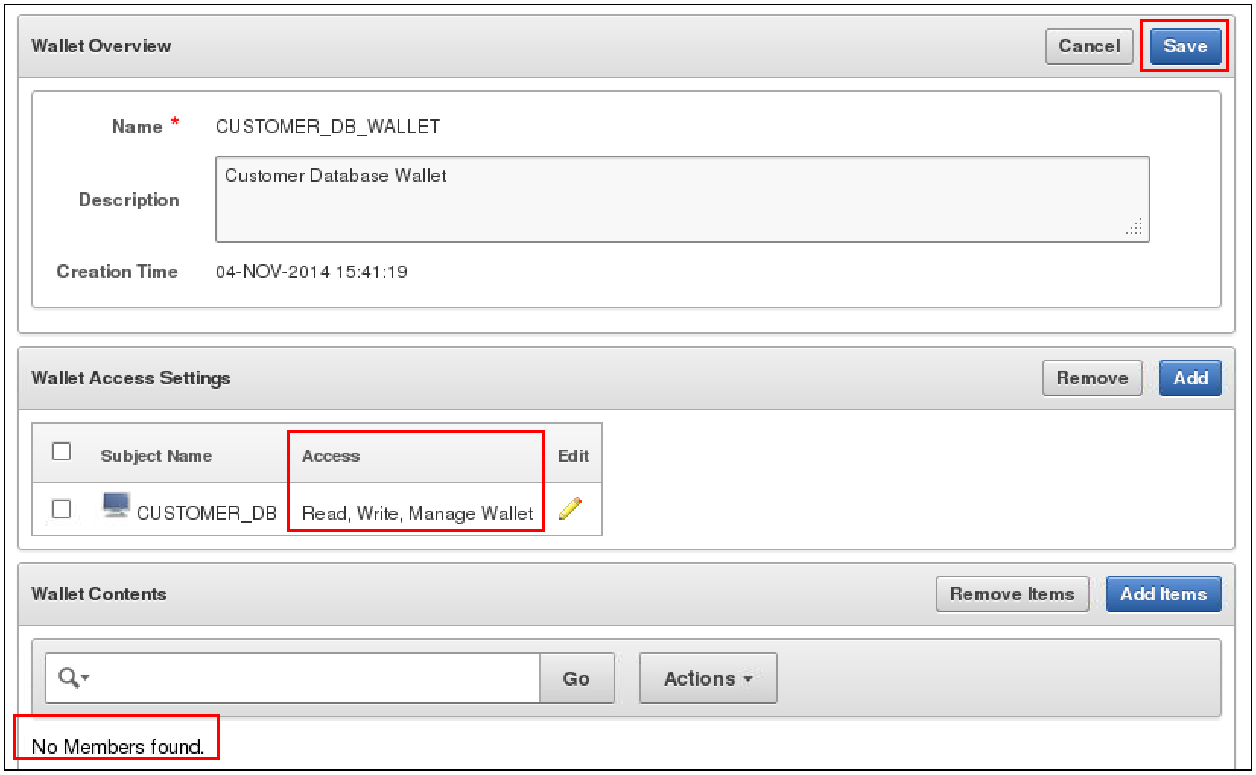
Type: Endpoints

	Name	Description
●	CUSTOMER_DB	Customer Database Oracle 11.2.0.4 IP: 192.0.2.110

1 - 1

Access Level: ○ Read Only ● Read and Modify ☑ Manage Wallet

7. Note the changed **Access**. Because you are viewing a newly created wallet in Oracle Key Vault, it displays **No Members found** in the Wallet Contents section. Click **Save** again.



Name *: CUSTOMER_DB_WALLET

Description: Customer Database Wallet

Creation Time: 04-NOV-2014 15:41:19

□	Subject Name	Access	Edit
□	CUSTOMER_DB	Read, Write, Manage Wallet	

No Members found.

8. Minimize the Oracle Key Vault management console and open a new terminal window on the `db11204` VM. (As always, set the environment variables to the `db11gr2` instance.)

```
[oracle@db11204 ~]$ . oraenv
ORACLE_SID = [oracle] ? db11gr2
The Oracle base has been set to /u01/app/oracle
[oracle@db11204 ~]$
```

9. Upload the contents of the `ewallet.p12` wallet file in the directory to Oracle Key Vault with the `okvutil upload` command.

   a. Ensure that the listener is up. If not, start it with: `lsnrctl start`.

```
[oracle@db11204 ~]$ lsnrctl status

LSNRCTL for Linux: Version 11.2.0.4.0 - Production on 04-NOV-
2014 14:06:54
Copyright (c) 1991, 2013, Oracle.  All rights reserved.

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=db11204.example.com)(P
ORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 11.2.0.4.0
- Production
Start Date                04-NOV-2014 14:03:19
Uptime                    0 days 0 hr. 3 min. 34 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
/u01/app/oracle/product/11.2.0.4/dbhome_1/network/admin/listener
.ora
Listener Log File
/u01/app/oracle/diag/tnslsnr/db11204/listener/alert/log.xml
Listening Endpoints Summary...

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=db11204.example.com)(P
ORT=1521)))
Services Summary...
Service "db11gr2.example.com" has 1 instance(s).
  Instance "db11gr2", status READY, has 1 handler(s) for this
service...
Service "db11gr2XDB.example.com" has 1 instance(s).
  Instance "db11gr2", status READY, has 1 handler(s) for this
service...
```

```
The command completed successfully
[oracle@db11204 ~]$
```

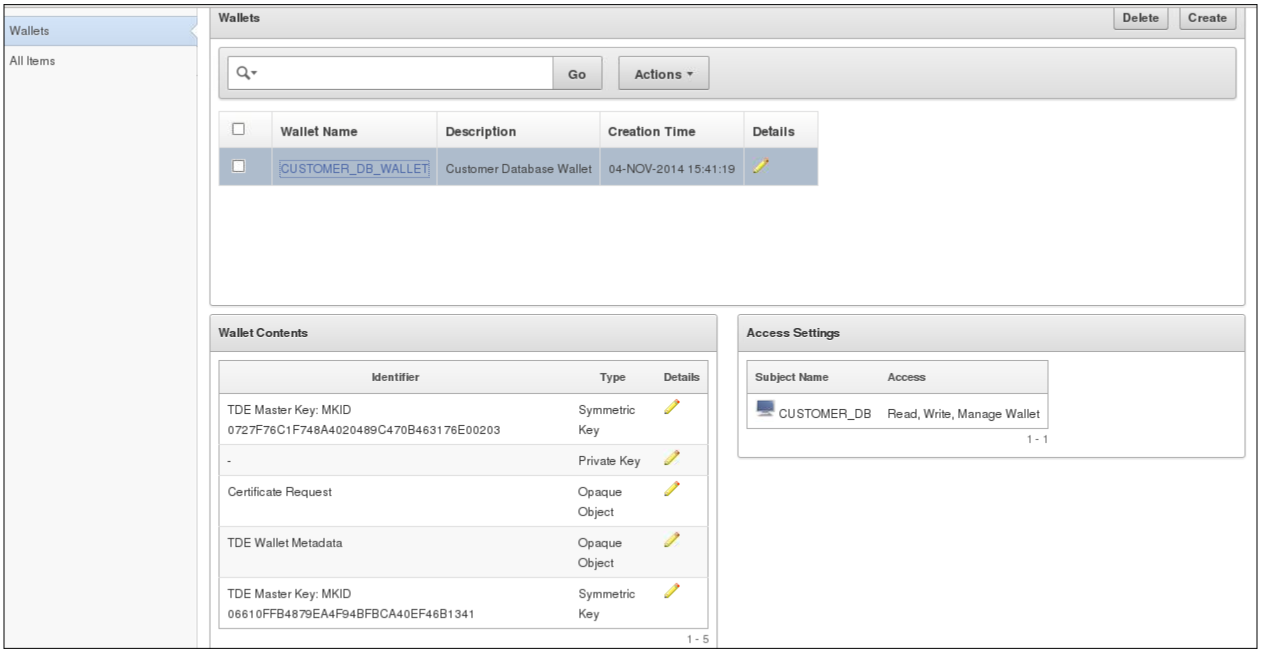
b. Navigate to your `okvutil/bin` directory.

```
[oracle@db11204 ~]$ cd /home/oracle/okvutil/bin
[oracle@db11204 bin]$
```

c. Start the upload and provide the password of the wallet; `secretKEY`, in this example.

```
[oracle@db11204 bin]$ ./okvutil upload -t WALLET -l
/u01/app/oracle/admin/db11204/wallet -g CUSTOMER_DB_WALLET
Enter source wallet password:
Upload succeeded
[oracle@db11204 bin]$
```

10. Return to the Oracle Key Vault management console in your browser. On the Wallets page, click the `CUSTOMER_DB_WALLET` link and notice that entries appear in the **Wallet Contents** section.



☐	Wallet Name	Description	Creation Time	Details
☐	CUSTOMER_DB_WALLET	Customer Database Wallet	04-NOV-2014 15:41:19	✎

Wallet Contents

Identifier	Type	Details
TDE Master Key: MKID 0727F76C1F748A4020489C470B463176E00203	Symmetric Key	✎
-	Private Key	✎
Certificate Request	Opaque Object	✎
TDE Wallet Metadata	Opaque Object	✎
TDE Master Key: MKID 06610FFB4879EA4F94BFBCA40EF46B1341	Symmetric Key	✎

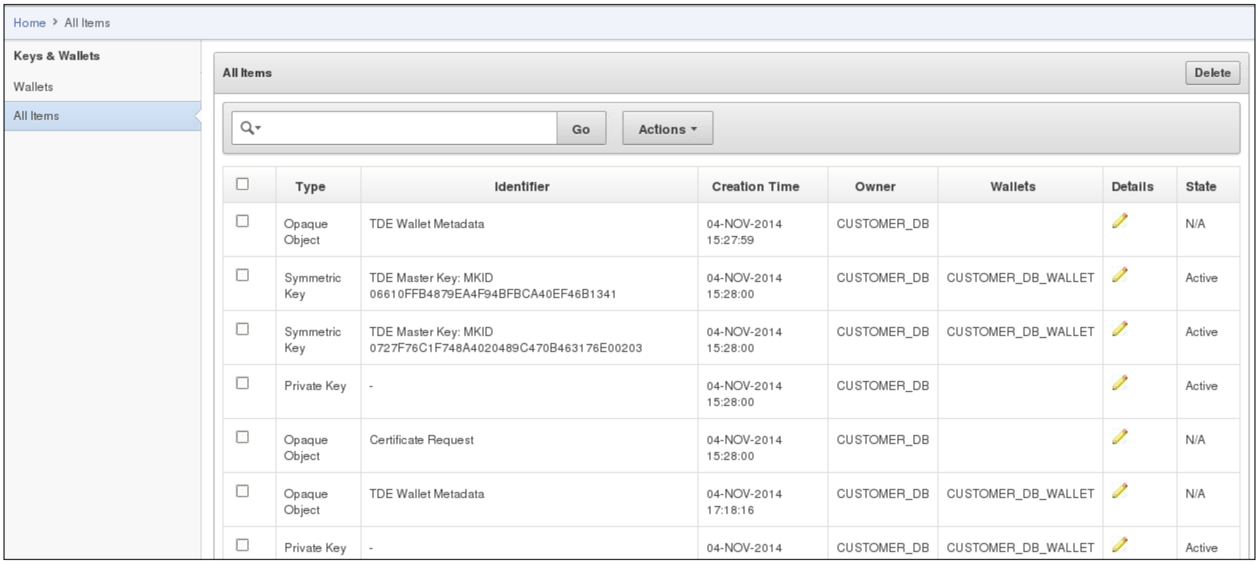
1 - 5

Access Settings

Subject Name	Access
CUSTOMER_DB	Read, Write, Manage Wallet

1 - 1

11. Alternatively, view the wallet content by clicking **All Items**.



□	Type	Identifier	Creation Time	Owner	Wallets	Details	State
□	Opaque Object	TDE Wallet Metadata	04-NOV-2014 15:27:59	CUSTOMER_DB		✎	N/A
□	Symmetric Key	TDE Master Key: MKID 06610FFB4879EA4F94BFBCA40EF46B1341	04-NOV-2014 15:28:00	CUSTOMER_DB	CUSTOMER_DB_WALLET	✎	Active
□	Symmetric Key	TDE Master Key: MKID 0727F76C1F748A4020489C470B463176E00203	04-NOV-2014 15:28:00	CUSTOMER_DB	CUSTOMER_DB_WALLET	✎	Active
□	Private Key	-	04-NOV-2014 15:28:00	CUSTOMER_DB		✎	Active
□	Opaque Object	Certificate Request	04-NOV-2014 15:28:00	CUSTOMER_DB		✎	N/A
□	Opaque Object	TDE Wallet Metadata	04-NOV-2014 17:18:16	CUSTOMER_DB	CUSTOMER_DB_WALLET	✎	N/A
□	Private Key	-	04-NOV-2014	CUSTOMER_DB	CUSTOMER_DB_WALLET	✎	Active

12. Download the wallet from Oracle Key Vault. If a wallet file exists in the same directory location as specified with the `-l` option, the existing wallet file is automatically backed up. When prompted, provide a new wallet password. This example uses `welcome1`.

```
[oracle@db11204 bin]$ ./okvutil download -t WALLET -l
/u01/app/oracle/admin/db11204/wallet -g CUSTOMER_DB_WALLET
Enter new wallet password (<enter> for auto-login):
Confirm new wallet password:
Download succeeded
[oracle@db11204 bin]$
```

13. Optionally, list the wallet directory to view the backup.

```
[oracle@db11204 bin]$ ls /u01/app/oracle/admin/db11204/wallet
ewallet.p12  ewallet.p12.1415120596.bak
[oracle@db11204 bin]$
```

14. Log in to SQL*Plus as `SYSDBA`. Close the old wallet and open the new one.

```
$ sqlplus / as sysdba
SQL>
SQL> alter system set encryption wallet close identified by
"secretKEY";

System altered.
SQL>
SQL> alter system set encryption wallet open identified by
"welcome1";

System altered.
SQL>
```

15. Query both test tables to confirm that the data is readable, and then exit.

```
SQL> SELECT * from banking.customers;

FIRST_NAME           LAST_NAME            CCN
-------------------- -------------------- --------------------
Mike                 Anderson             5421-5424-1451-5340
Jon                  Hewell               5325-8942-5653-0031
Andrew               Forsyth              4553-0984-2344-4101
Ellen                Kane                 4489-4023-0489-0492
Randall              Summers              5193-0013-0002-2345
Julia                Cortez               4545-5702-4211-8889
Melissa              Hiam                 5900-4451-8812-7171
Elise                Fenters              4331-4921-5031-9871
Paul                 Watts                4442-1902-7477-3239
Jim                  Johnson              4921-1212-6612-0080
Scott                Manning              5890-1454-3554-9886

11 rows selected.

SQL> SELECT * from banking.customersenc;

FIRST_NAME           LAST_NAME            CCN
-------------------- -------------------- --------------------
Mike                 Anderson             5421-5424-1451-5340
Jon                  Hewell               5325-8942-5653-0031
Andrew               Forsyth              4553-0984-2344-4101
Ellen                Kane                 4489-4023-0489-0492
Randall              Summers              5193-0013-0002-2345
Julia                Cortez               4545-5702-4211-8889
Melissa              Hiam                 5900-4451-8812-7171
Elise                Fenters              4331-4921-5031-9871
Paul                 Watts                4442-1902-7477-3239
Jim                  Johnson              4921-1212-6612-0080
Scott                Manning              5890-1454-3554-9886

11 rows selected.

SQL> exit
$
```

Practices for Lesson 5: Using Direct TDE with Oracle Database 12c

Chapter 5

Practices for Lesson 5: Overview

Practices Overview

In these practices, you will use the TDE direct connection with Oracle Key Vault and perform a number of different tasks, switching between the system, endpoint, and key administrator roles.

Practice 5-1: Using the TDE Direct Connection with Oracle Key Vault

Overview

In this practice, you perform a number of different tasks, switching between the system, endpoint, and key administrator roles.

- As system administrator, enroll and provision another endpoint for the 12*c* database server.
- As endpoint administrator, download and install the client-side Oracle Key Vault software.
- As key administrator, 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.

Assumptions

The previous practices have been completed successfully.

Tasks

1. From the desktop, start a terminal session on the `host02` VM and point to the `orcl` database instance.

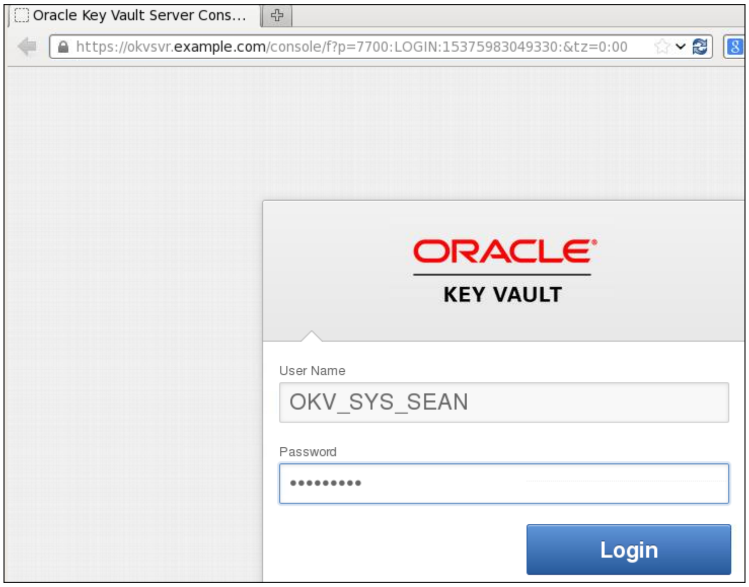
```
$ ssh -X oracle@host02
oracle@host02's password:
Last login: Sat Nov  1 16:24:39 2014 from host02.example.com
[oracle@host02 ~]$ . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base has been set to /u01/app/oracle
[oracle@host02 ~]$
```

2. Confirm that the listener is up. If not, start it with the `lsnrctl start` command.

```
[oracle@host02 ~]$ lsnrctl status

LSNRCTL for Linux: Version 12.1.0.1.0 - Production on 05-NOV-
2014 14:34:59

Copyright (c) 1991, 2013, Oracle.  All rights reserved.

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 12.1.0.1.0
- Production
Start Date                29-OCT-2014 18:09:21
Uptime                    6 days 20 hr. 25 min. 37 sec
```

```
Trace Level                 off
Security                    ON: Local OS Authentication
SNMP                        OFF
Listener Parameter File
/u01/app/oracle/product/12.1.0/dbhome_1/network/admin/listener.o
ra
Listener Log File
/u01/app/oracle/diag/tnslsnr/host02/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=host02.example.com)(PO
RT=1521)))

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=host02.example.com)(P
ORT=5500))(Security=(my_wallet_directory=/u01/app/oracle/admin/o
rcl/xdb_wallet))(Presentation=HTTP)(Session=RAW))
Services Summary...
Service "orcl.example.com" has 1 instance(s).
  Instance "orcl", status READY, has 1 handler(s) for this
service...
Service "orclXDB.example.com" has 1 instance(s).
  Instance "orcl", status READY, has 1 handler(s) for this
service...
The command completed successfully
[oracle@host02 ~]$ firefox
```

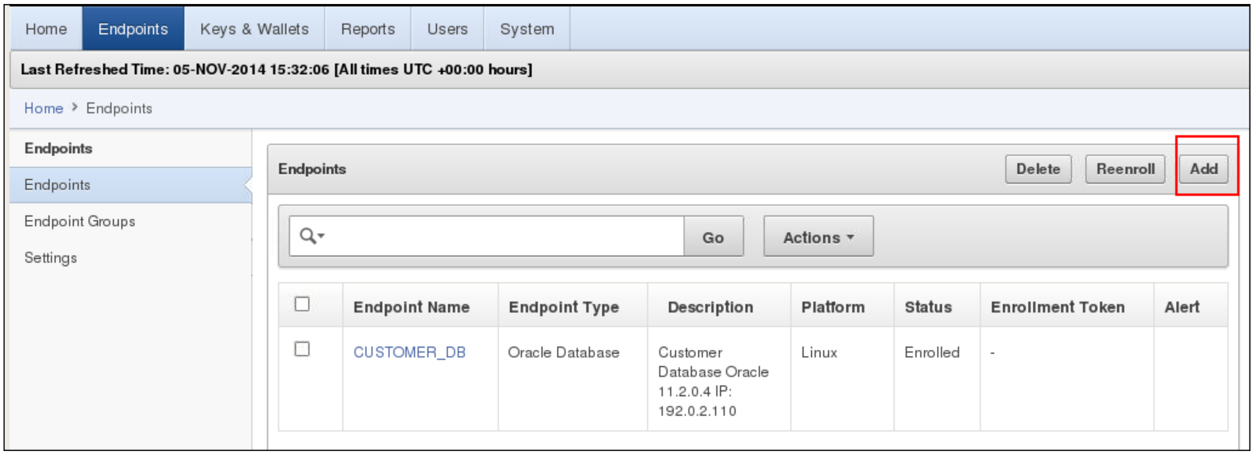
3. Invoke the Firefox browser and enter the `https://okvsvr.example.com` URL.
4. Log in as the `OKV_SYS_SEAN` system administrator.


Oracle Key Vault Server Cons...
https://okvsvr.example.com/console/f?p=7700:LOGIN:15375983049330:&tz=0:00
ORACLE
KEY VAULT
Login

User Name: OKV_SYS_SEAN

Password: •••••••••

5. To enroll and provision another endpoint, click **Endpoints**, and then click **Add**.

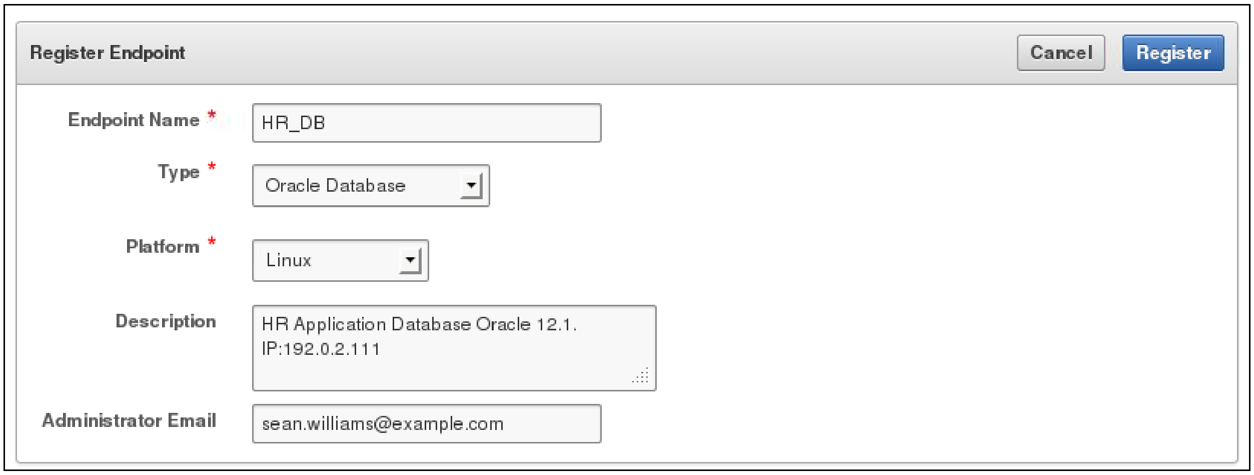


Last Refreshed Time: 05-NOV-2014 15:32:06 [All times UTC +00:00 hours]

□	Endpoint Name	Endpoint Type	Description	Platform	Status	Enrollment Token	Alert
□	CUSTOMER_DB	Oracle Database	Customer Database Oracle 11.2.0.4 IP: 192.0.2.110	Linux	Enrolled	-	

6. Enter and confirm the following values, and then click **Register**:

Endpoint Name	HR_DB
Type	Oracle Database
Platform	Linux
Description	HR Application Database Oracle 12.1. IP:192.0.2.111
Administrator Email	sean.williams@example.com



Endpoint Name *: HR_DB

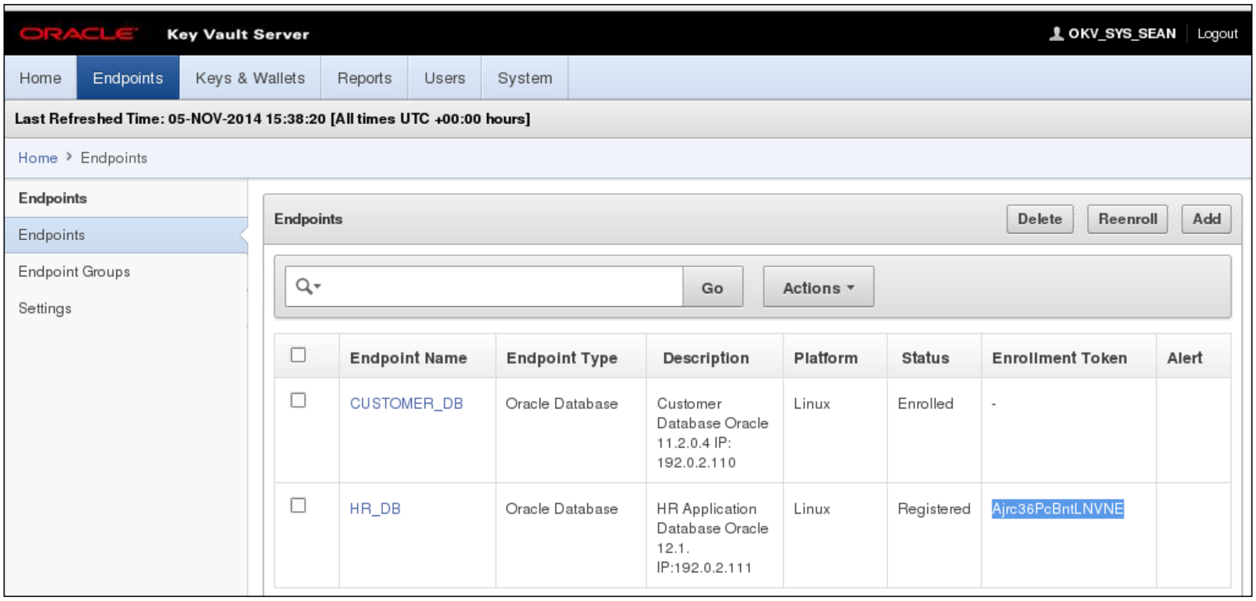
Type *: Oracle Database

Platform *: Linux

Description: HR Application Database Oracle 12.1.
IP:192.0.2.111

Administrator Email: sean.williams@example.com

7. When the endpoint is successfully registered, copy the **Enrollment Token** value and log out.

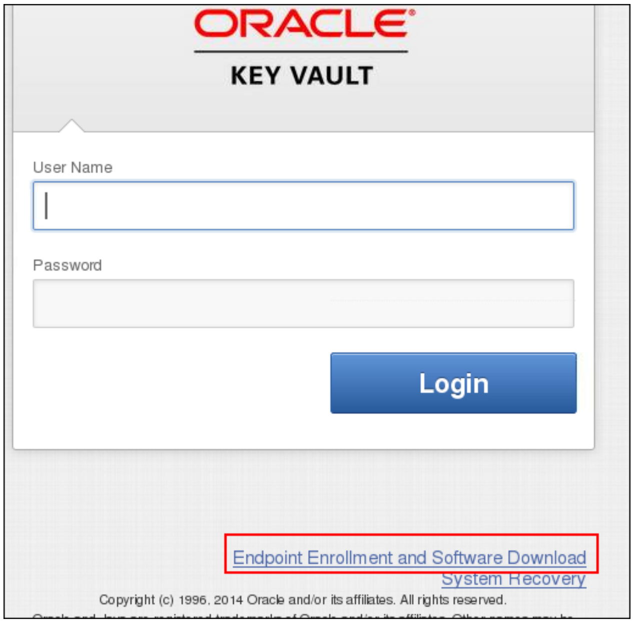


Last Refreshed Time: 05-NOV-2014 15:38:20 [All times UTC +00:00 hours]

□	Endpoint Name	Endpoint Type	Description	Platform	Status	Enrollment Token	Alert
□	CUSTOMER_DB	Oracle Database	Customer Database Oracle 11.2.0.4 IP: 192.0.2.110	Linux	Enrolled	-	
□	HR_DB	Oracle Database	HR Application Database Oracle 12.1. IP:192.0.2.111	Linux	Registered	Ajrc36PcBntLNVNE	

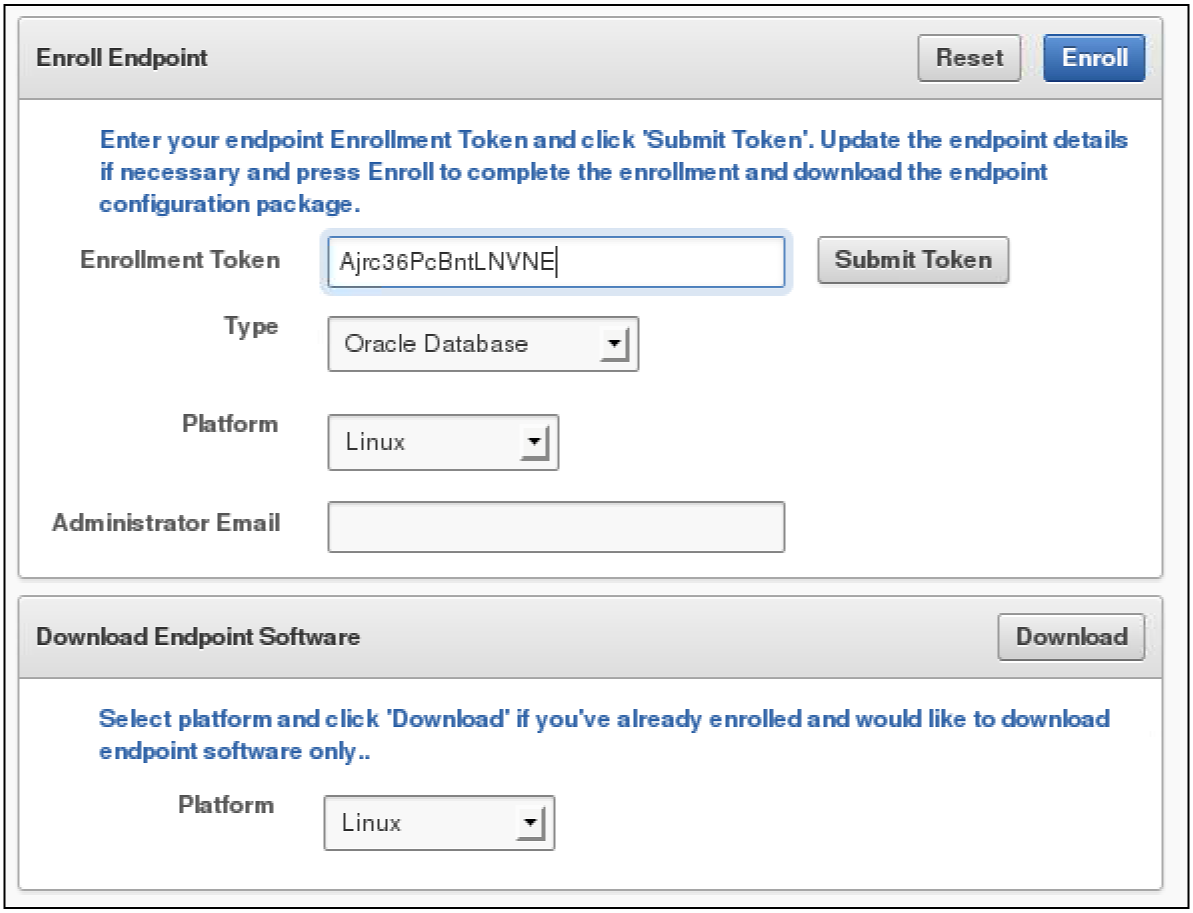
With the copy and paste, you simulate the communication between the system administrator and the endpoint administrator.

8. Switch roles to being an endpoint administrator and click the **Endpoint Enrollment and Software Download** link, without logging in to the Oracle Key Vault management console.



Copyright (c) 1996, 2014 Oracle and/or its affiliates. All rights reserved.

9. Paste or enter the enrollment token and click **Submit Token**. You should see “Valid Token.”



Enter your endpoint Enrollment Token and click 'Submit Token'. Update the endpoint details if necessary and press Enroll to complete the enrollment and download the endpoint configuration package.

Enrollment Token: Ajrc36PcBntLNVNE

Type: Oracle Database

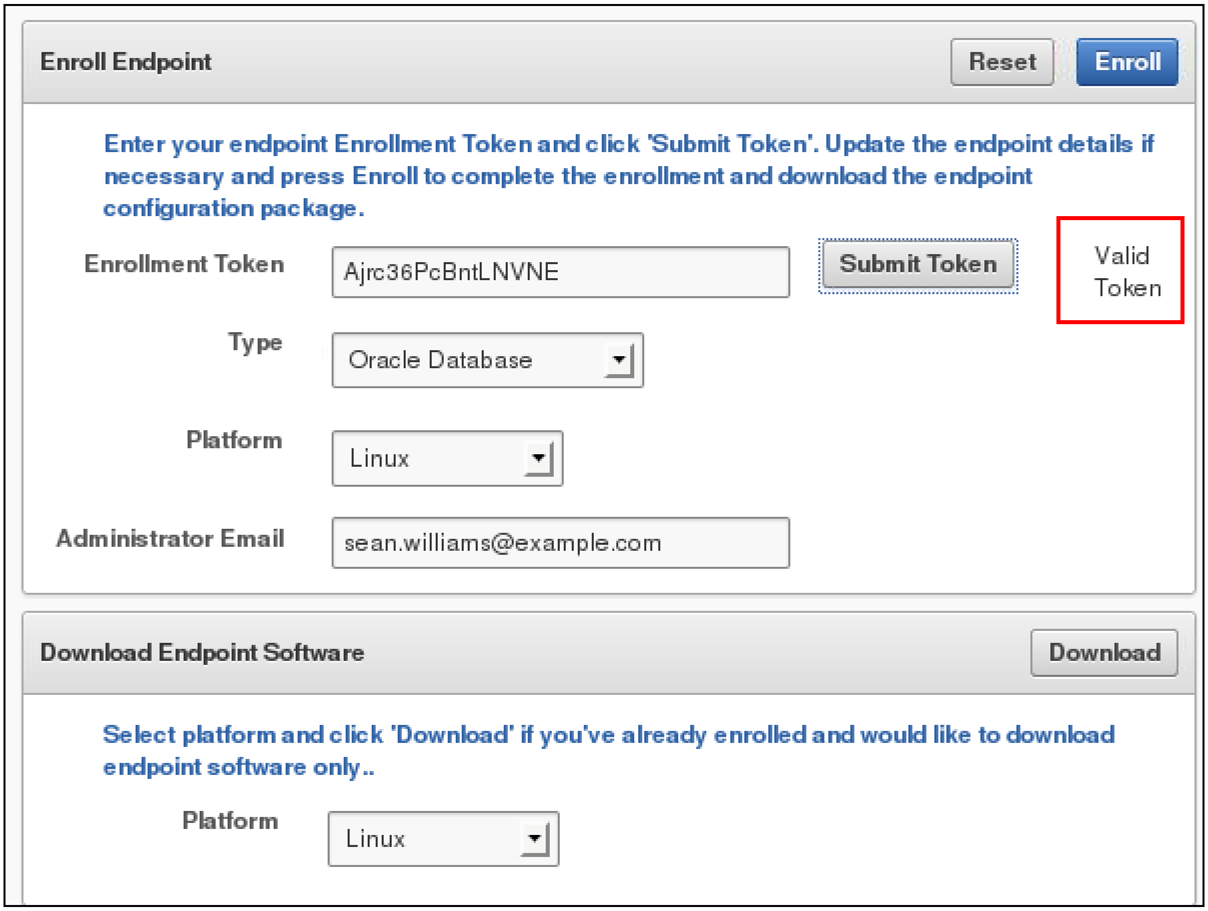
Platform: Linux

Administrator Email:

Select platform and click 'Download' if you've already enrolled and would like to download endpoint software only..

Platform: Linux

10. When you see Valid Token, click **Enroll**.



Enroll Endpoint

Enter your endpoint Enrollment Token and click 'Submit Token'. Update the endpoint details if necessary and press Enroll to complete the enrollment and download the endpoint configuration package.

Enrollment Token: Ajrc36PcBntLNVNE

Valid Token

Type: Oracle Database

Platform: Linux

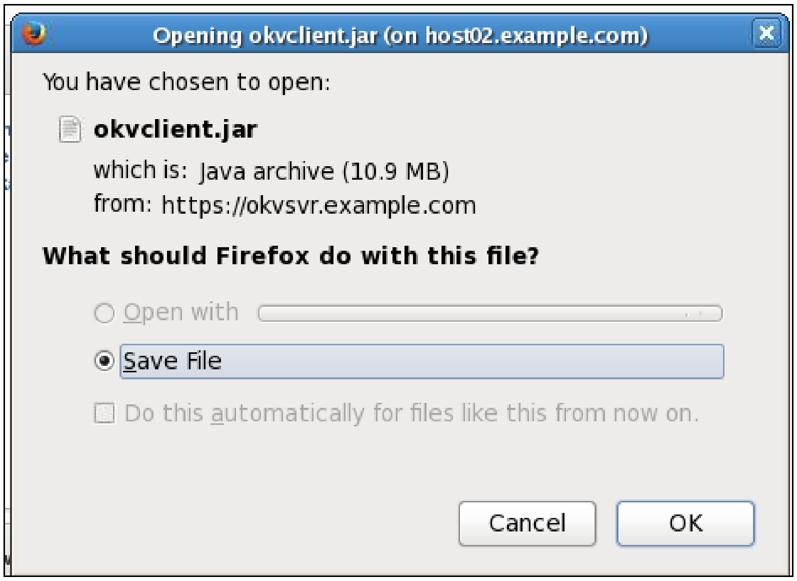
Administrator Email: sean.williams@example.com

Download Endpoint Software

Select platform and click 'Download' if you've already enrolled and would like to download endpoint software only..

Platform: Linux

11. When you see the **okvclient.jar** window, click **OK** to save the file.



Opening okvclient.jar (on host02.example.com)

You have chosen to open:

okvclient.jar

which is: Java archive (10.9 MB)

from: https://okvsvr.example.com

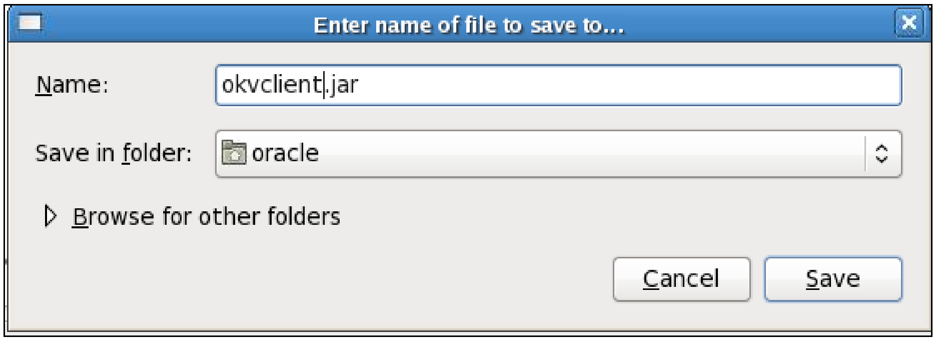
What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

12. Click **Save** to save the file to the default `/home/oracle` location. The default **Save File** location is set in your browser.



Name: okvclient.jar

Save in folder: oracle

13. Minimize the browser and navigate to a `host02` terminal window. Continue as the endpoint administrator.

In this training environment, Java is already set up. If you are using a new environment, you must set either the `PATH` or the `JAVA_HOME` environment variables appropriately to run the `java -jar` command.

14. Confirm that you are in the directory where the `okvclient.jar` is located.

```
[oracle@host02 ~]$ ls ok*
okvclient.jar
[oracle@host02 ~]$
```

15. Use the `java -jar okvclient.jar -d /home/oracle/okvutil` command to install the Oracle Key Vault endpoint software with auto-login. That is, press Enter when prompted.

```
[oracle@host02 ~]$ java -jar okvclient.jar -d /home/oracle/
Detected JAVA_HOME: /usr/lib/jvm/java-1.7.0-openjdk-
1.7.0.51.x86_64/jre
Enter new Key Vault endpoint password (<enter> for auto-login):
Oracle Key Vault endpoint software installed successfully.
[oracle@host02 ~]$
```

If you want to revisit details about this task, see Practice 3-1, step 14.

16. Switch to the `root` OS user to complete your client-side Oracle Key Vault installation.

```
[oracle@host02 ~]$ su - root
Password:
[root@host02 ~]#
```

17. Navigate to the directory where the `root.sh` file is and execute it.

```
# cd /home/oracle/bin
# ls
okveps.x64  okveps.x86  okvutil  root.sh
#
# ./root.sh
Creating directory: /opt/oracle/extapi/64/hsm/oracle/1.0.0/
Copying PKCS library to /opt/oracle/extapi/64/hsm/oracle/1.0.0/
Setting PKCS library file permissions
```

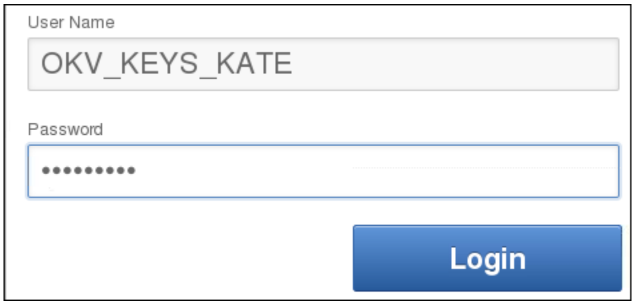
```
Installation successful.
#
```

18. After successfully completing the installation, exit the `root` user and continue as the `oracle` OS user.

```
# exit
logout
$ whoami
oracle
$
```

19. Click `ORACLE` (top-left) to exit as the endpoint administrator.

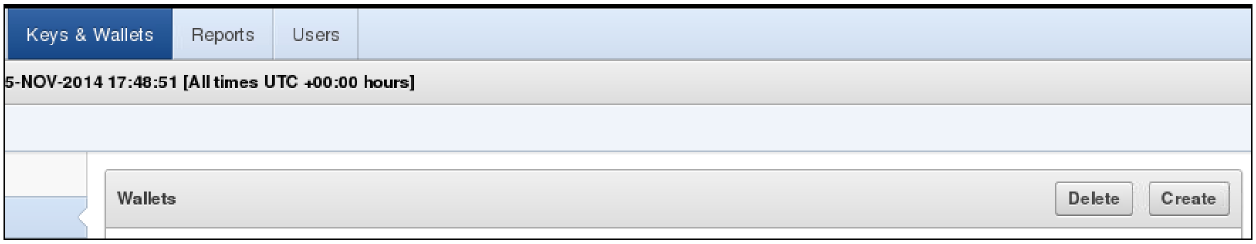
20. Log in to the Oracle Key Vault management console as the `OKV_KEYS_KATE` key administrator.



User Name: OKV_KEYS_KATE

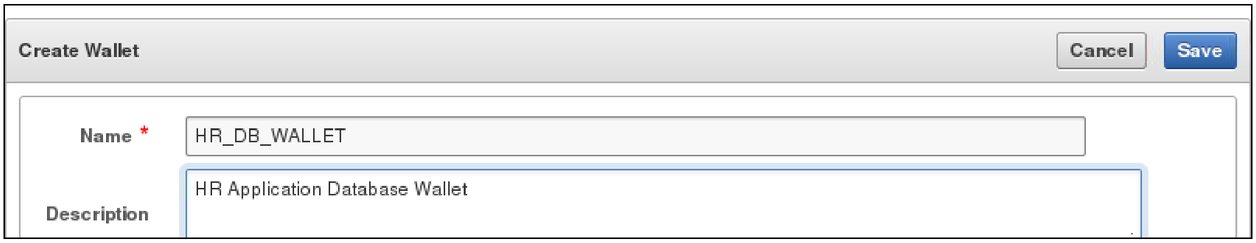
Password: •••••••••

21. To create a virtual wallet, click **Keys & Wallets** and click **Create**.



5-NOV-2014 17:48:51 [All times UTC +00:00 hours]

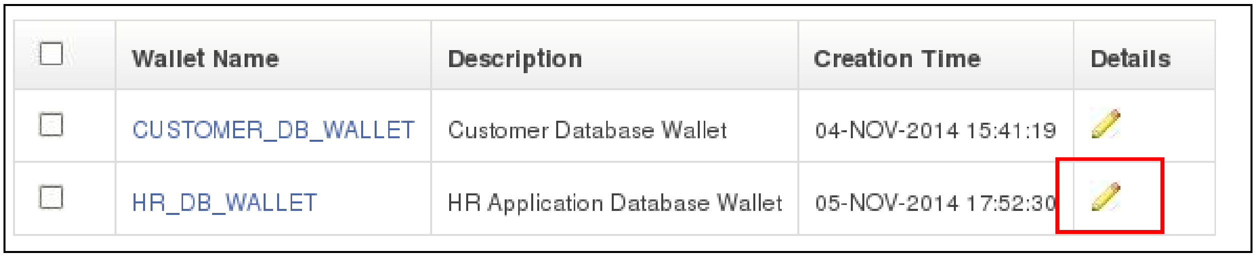
22. Enter `HR_DB_WALLET` as **Name**, `HR Application Database Wallet` as **Description**, and then click **Save**.



Name * HR_DB_WALLET

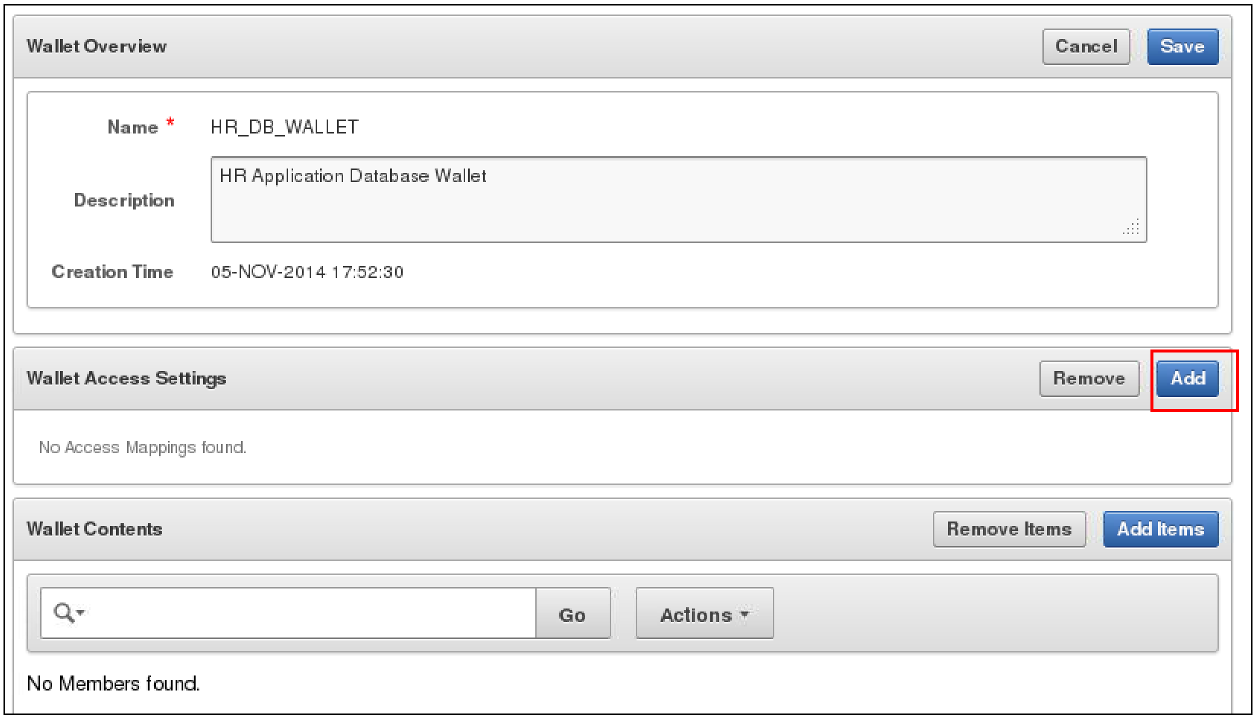
Description HR Application Database Wallet

23. The new virtual wallet appears on the Wallets page. Set up the access control relationship between the virtual wallet and the endpoint so that endpoint can read, write, and create objects in this newly created virtual wallet. Click the pencil icon in the **Details** column.



□	Wallet Name	Description	Creation Time	Details
□	CUSTOMER_DB_WALLET	Customer Database Wallet	04-NOV-2014 15:41:19	✎
□	HR_DB_WALLET	HR Application Database Wallet	05-NOV-2014 17:52:30	✎

24. Click **Add** in Wallet Access Settings section.



Name * HR_DB_WALLET

Description HR Application Database Wallet

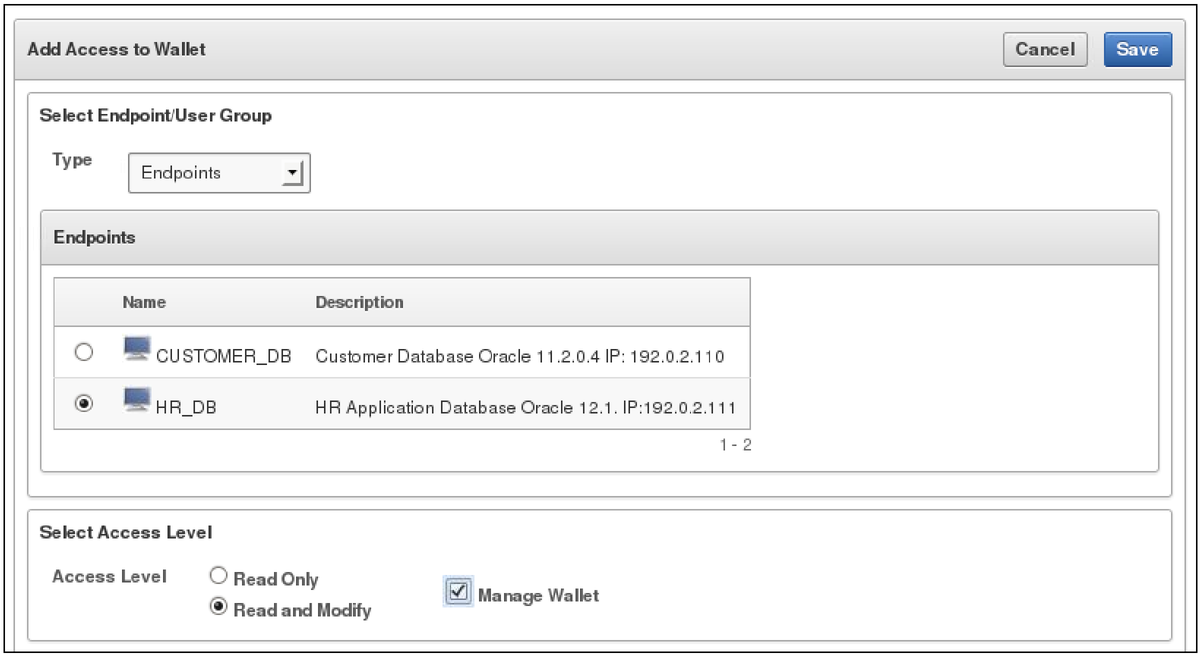
Creation Time 05-NOV-2014 17:52:30

No Access Mappings found.

No Members found.

25. To be able to upload and download security objects and manage the life cycle of the wallet, enter and confirm the following values, and then click **Save**.

Type	Endpoint
HR_DB	*<selected>*
Read and Modify	*<selected>*
Manage Wallet	*<selected>*



Add Access to Wallet — Cancel | Save

Select Endpoint/User Group

Type: Endpoints

Endpoints

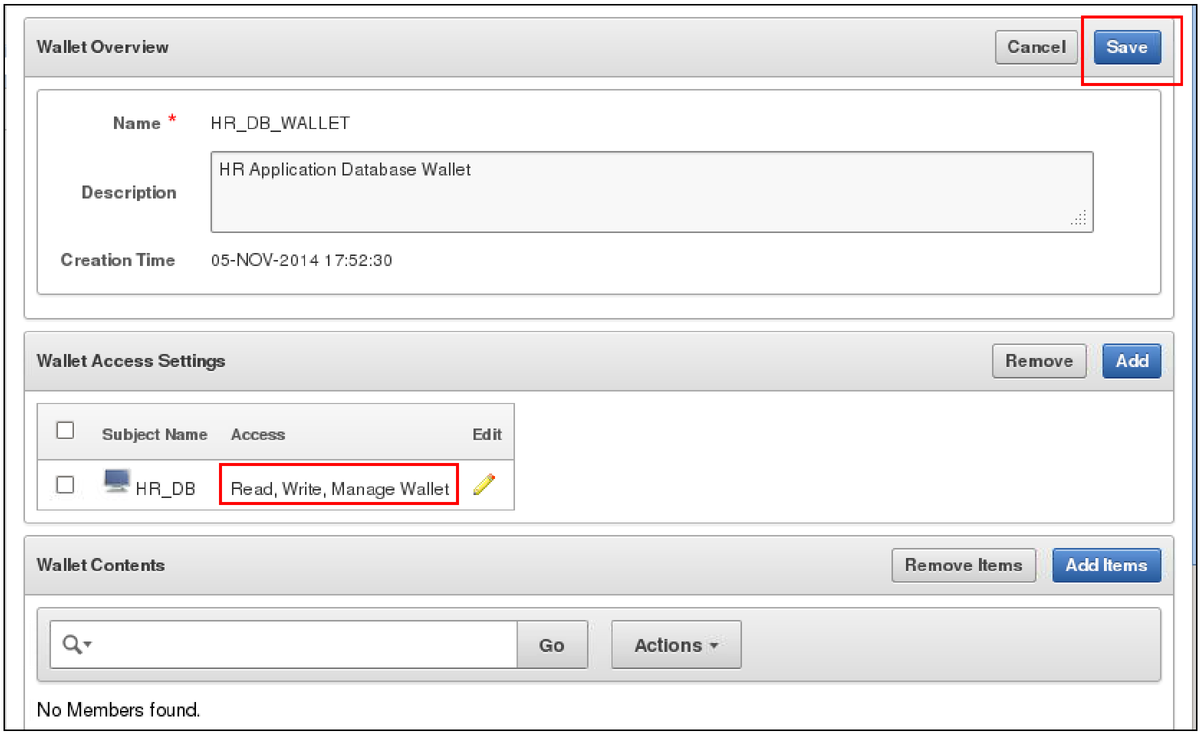
	Name	Description
○	CUSTOMER_DB	Customer Database Oracle 11.2.0.4 IP: 192.0.2.110
●	HR_DB	HR Application Database Oracle 12.1. IP:192.0.2.111

1 - 2

Select Access Level

Access Level: ○ Read Only ● Read and Modify ☑ Manage Wallet

26. Note the wallet access settings and click **Save** again.



Wallet Overview — Cancel | Save

Name *: HR_DB_WALLET

Description: HR Application Database Wallet

Creation Time: 05-NOV-2014 17:52:30

Wallet Access Settings — Remove | Add

□	Subject Name	Access	Edit
□	HR_DB	Read, Write, Manage Wallet	✎

Wallet Contents — Remove Items | Add Items

Go | Actions

No Members found.

27. Minimize the browser and return to the `host02` terminal window, logged in as the `oracle` OS user in the directory of the `okvutil` utility.

```
$ whoami
oracle
$ cd bin
$ ls
okveps.x64  okveps.x86  okvutil  root.sh
$
```

28. Confirm that you have a wallet directory and an existing `ewallet.p12` wallet. If not, see Practice 4-1, step 10 (following) for setting up your test data.

```
$ ls -al /u01/app/oracle/admin/orcl/wallet
total 12
drwxr-xr-x 2 oracle oinstall 4096 Nov  1 17:26 .
drwxr-x--- 7 oracle oinstall 4096 Oct 28 12:44 ..
-rw-r--r-- 1 oracle oinstall 3112 Nov  1 17:26 ewallet.p12
$
```

29. As the endpoint administrator, upload the existing Oracle wallet to retain all historical TDE master keys. Enter the command on one line and when prompted, enter your password. This example uses `secretKEY` as password.

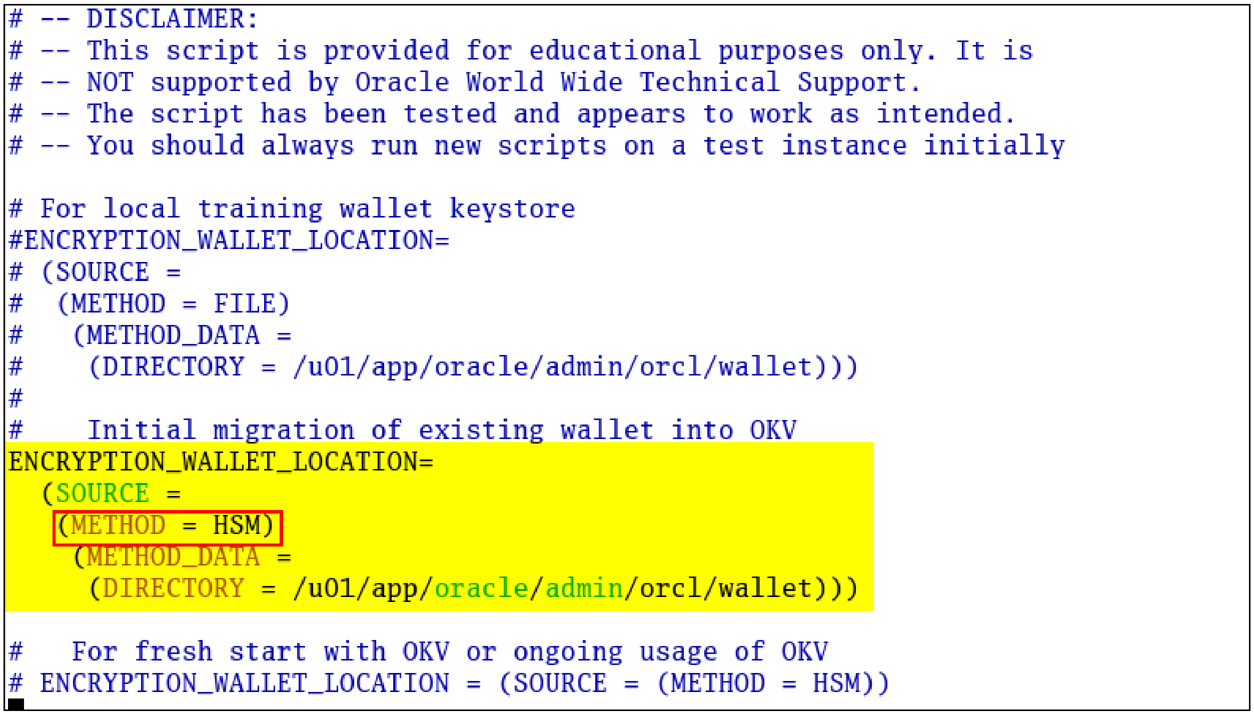
```
$ ./okvutil upload -t WALLET -l
/u01/app/oracle/admin/orcl/wallet -g HR_DB_WALLET
Enter source wallet password:
Upload succeeded
$
```

30. Before migrating to Oracle Key Vault, close the wallet in SQL*Plus by using your password.

```
$ sqlplus / as sysdba
SQL>
SQL> administer key management set keystore close identified by
"secretKEY";

keystore altered.
SQL> exit
$
```

31. Modify the `sqlnet.ora` file to change `METHOD=FILE` to `METHOD=HSM`. Choose `vi` or other available editors.

```
$ cd $ORACLE_HOME/network/admin
$ vi sqlnet.ora
```



```
# -- DISCLAIMER:
# -- This script is provided for educational purposes only. It is
# -- NOT supported by Oracle World Wide Technical Support.
# -- The script has been tested and appears to work as intended.
# -- You should always run new scripts on a test instance initially

# For local training wallet keystore
#ENCRYPTION_WALLET_LOCATION=
# (SOURCE =
#  (METHOD = FILE)
#   (METHOD_DATA =
#    (DIRECTORY = /u01/app/oracle/admin/orcl/wallet)))
#
#    Initial migration of existing wallet into OKV
ENCRYPTION_WALLET_LOCATION=
  (SOURCE =
   (METHOD = HSM)
    (METHOD_DATA =
     (DIRECTORY = /u01/app/oracle/admin/orcl/wallet)))

#   For fresh start with OKV or ongoing usage of OKV
# ENCRYPTION_WALLET_LOCATION = (SOURCE = (METHOD = HSM))
```

32. In a new SQL*Plus session, confirm that you have two wallet types: `FILE` and `HSM`, both in a `CLOSED` state.

```
$ sqlplus / as sysdba

SQL> select wrl_type, status from v$encryption_wallet;

WRL_TYPE              STATUS
--------------------  ------------------------------
FILE                  CLOSED
HSM                   CLOSED

SQL>
```

33. Use the migration command to move the TDE master key from the wallet file to Oracle Key Vault, of course, with your passwords. Because you used the auto-login wallet during the endpoint software installation, the password in this example is “null.” However, if you used an endpoint password, that password needs to be entered.

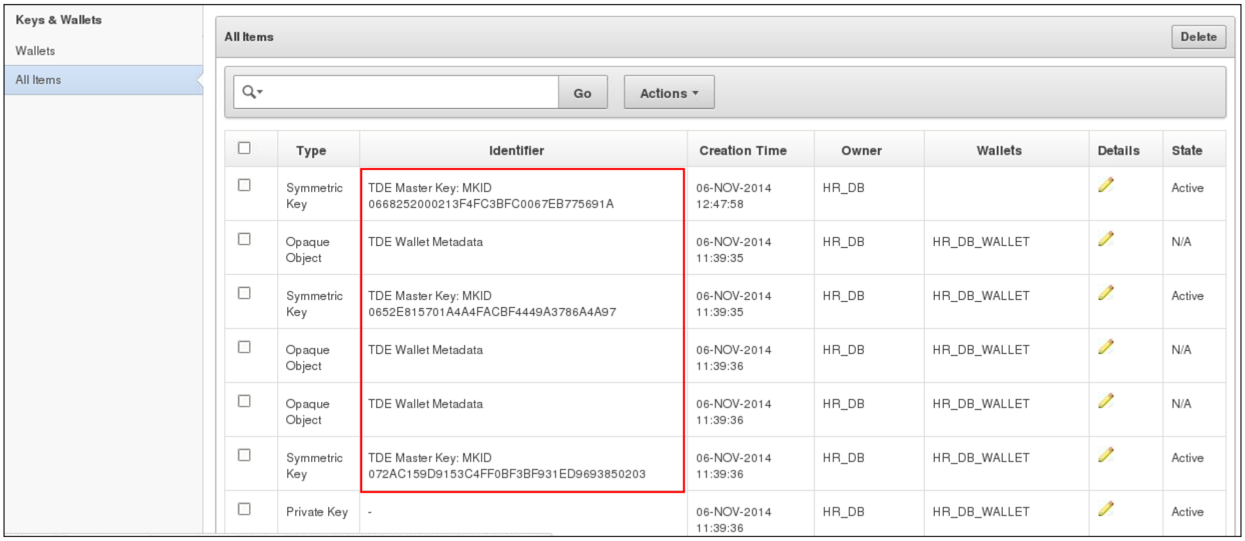
```
SQL> administer key management set encryption key identified by
"null" migrate using "secretKEY" with backup;

keystore altered.
```

```
SQL> exit
$
```

34. Optionally, list the wallet directory to view the automatically created backup file.

```
$ ls -l /u01/app/oracle/admin/orcl/wallet
total 12
-rw-r--r-- 1 oracle oinstall 3112 Nov  6 11:40
ewallet_20141106114058454.p12
-rw-r--r-- 1 oracle oinstall 5024 Nov  6 11:40 ewallet.p12
$
```

35. Logged in to the Oracle Key Vault management console as the `OKV_KEYS_KATE` key administrator, view the TDE items under **All Items.**

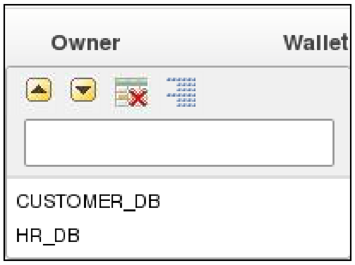


□	Type	Identifier	Creation Time	Owner	Wallets	Details	State
□	Symmetric Key	TDE Master Key: MKID 0668252000213F4FC3BFC0067EB775691A	06-NOV-2014 12:47:58	HR_DB		✎	Active
□	Opaque Object	TDE Wallet Metadata	06-NOV-2014 11:39:35	HR_DB	HR_DB_WALLET	✎	N/A
□	Symmetric Key	TDE Master Key: MKID 0652E815701A4A4FACBF4449A3786A4A97	06-NOV-2014 11:39:35	HR_DB	HR_DB_WALLET	✎	Active
□	Opaque Object	TDE Wallet Metadata	06-NOV-2014 11:39:36	HR_DB	HR_DB_WALLET	✎	N/A
□	Opaque Object	TDE Wallet Metadata	06-NOV-2014 11:39:36	HR_DB	HR_DB_WALLET	✎	N/A
□	Symmetric Key	TDE Master Key: MKID 072AC159D9153C4FF0BF3BF931ED9693850203	06-NOV-2014 11:39:36	HR_DB	HR_DB_WALLET	✎	Active
□	Private Key	-	06-NOV-2014 11:39:36	HR_DB	HR_DB_WALLET	✎	Active

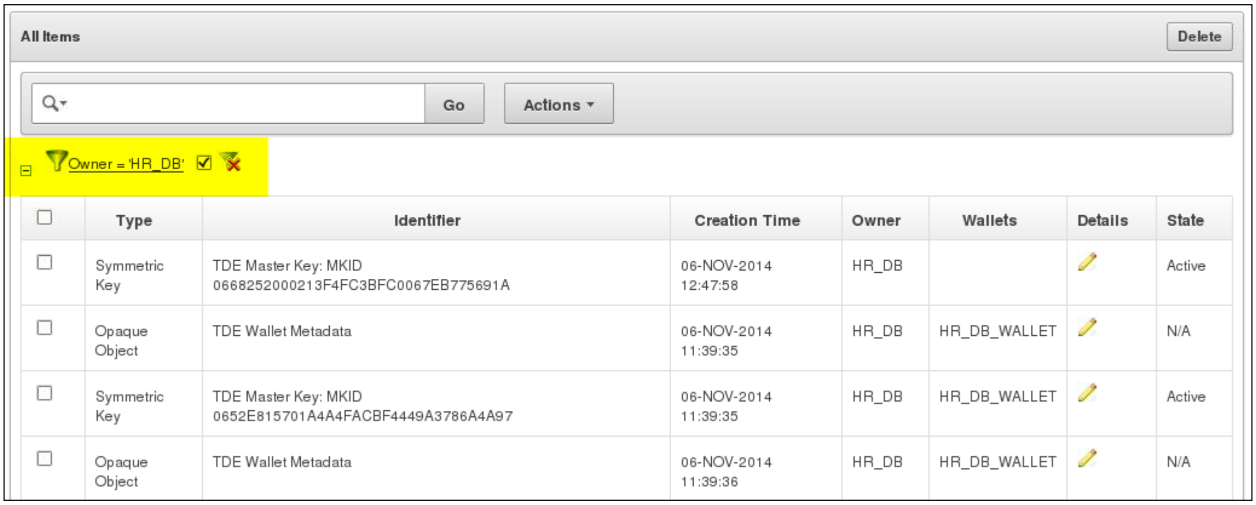
36. Optionally, filter by `HR_DB` as Owner.

    a. Click Owner.

    b. Click HR_DB.



37. Note the change on the **All Items** page.



⊟ Owner = 'HR_DB' ☑

☐	Type	Identifier	Creation Time	Owner	Wallets	Details	State
☐	Symmetric Key	TDE Master Key: MKID 0668252000213F4FC3BFC0067EB775691A	06-NOV-2014 12:47:58	HR_DB		✎	Active
☐	Opaque Object	TDE Wallet Metadata	06-NOV-2014 11:39:35	HR_DB	HR_DB_WALLET	✎	N/A
☐	Symmetric Key	TDE Master Key: MKID 0652E815701A4A4FACBF4449A3786A4A97	06-NOV-2014 11:39:35	HR_DB	HR_DB_WALLET	✎	Active
☐	Opaque Object	TDE Wallet Metadata	06-NOV-2014 11:39:36	HR_DB	HR_DB_WALLET	✎	N/A

38. Assume that six months have passed and as the endpoint administrator, you have the task of rotating the TDE master key. Because you used the auto-login wallet during the endpoint software installation, the password in this example is “null.” However, if you used an endpoint password, that password needs to be entered.

```
$ sqlplus / as sysdba

SQL> administer key management set encryption key identified by
"null";

keystore altered.

SQL> exit
$
```

39. Exit all windows.

Practices for Lesson 6: Performing Administrative Tasks

Chapter 6

Practices for Lesson 6: Overview

Practices Overview

In this practice, you view the roles of an Oracle Key Vault system administrator, key administrator, and audit manager.

Practice 6-1: Performing Administrative Tasks

Overview

In this practice, you view a number of videos that show how an Oracle Key Vault system administrator, a key administrator, and an audit manager perform their tasks.

Assumptions

Oracle Key Vault is installed and configured and some activities, such as the practices, occurred to show entries in the audit trail. But your entries may be different due to additional demos and test cases.

Tasks

1. To learn about system administration tasks, view two videos:
    - *Performing System Administration Tasks with Oracle Key Vault*
    - *Backing Up and Restoring Data for Oracle Key Vault*
2. To learn about key administration tasks, view the video: *Performing Key Administration Tasks with Oracle Key Vault*.
3. To learn about audit management tasks, view the video: *Performing Audit Manager Tasks with Oracle Key Vault*.

Answer to Self-Assessment in Practice 1-1:

- 1b
- 2c
- 3a