Oracle® Key Vault

Root of Trust HSM Configuration Guide

Release 18.3
F25128-04
April 2020

Oracle Key Vault Root of Trust HSM Configuration Guide, Release 18.3

F25128-04

Primary Author: Mark Doran

Contents

Preface

1 Getting Started with HSM

2 Configuring an HSM for Oracle Key Vault

3 Commands Used in Previous Versions of Oracle Key Vault

4 Support Guidance

Preface

Welcome to *Oracle Key Vault Root of Trust HSM Configuration Guide* (formerly *Oracle Key Vault Integration with Hardware Security Module*). This guide explains how to integrate a hardware security module (HSM) with Oracle Key Vault.

Audience

Oracle Key Vault is meant for users who are responsible for deploying, maintaining, and managing security within the enterprise. These users can be database, system, or security administrators. This guide can be used by any information security personnel who is responsible for protecting enterprise data residing in database servers, application servers, operating systems, and other information systems.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see these Oracle resources:

- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Guide*
- *Oracle Database Administrator’s Guide*
- *Oracle Data Guard Concepts and Administration*
- *Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Fusion Middleware Understanding Oracle GoldenGate*

To download the product data sheet, frequently asked questions, links to the latest product documentation, product download, and other collateral, visit the Oracle Technology Network (OTN). You must register online before using OTN. Registration is free and can be done at

`https://www.oracle.com/database/technologies/security/key-vault.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Getting Started with HSM

To integrate a hardware security module (HSM) with Oracle Key Vault, you must install the HSM and enroll Key Vault as an HSM client.

- How Oracle Key Vault Works with Hardware Security Modules
  This guide explains how to configure Oracle Key Vault to use a supported hardware security module (HSM).
- Installing the HSM Client Software on an Oracle Key Vault Server
  After you install Oracle Key Vault, you can install the HSM client software on the Oracle Key Vault server.
- Enrolling Oracle Key Vault as a Client of the HSM
  You must enroll Oracle Key Vault as a client of HSM and ensure connectivity between the HSM client and the HSM.

1.1 How Oracle Key Vault Works with Hardware Security Modules

This guide explains how to configure Oracle Key Vault to use a supported hardware security module (HSM).

A hardware security module (HSM) contains tamper-resistant, specialized hardware that is designed to protect security objects stored within the HSM. HSMs are physical computing devices that safeguard and manage digital keys, and provide cryptographic processing for clients. HSMs do not usually allow security objects to leave the cryptographic boundary of the HSM.

Oracle Key Vault is a key management platform designed to securely store, manage and share security objects. Unlike an HSM, Oracle Key Vault allows trusted clients to retrieve security objects like decryption keys. Oracle Key Vault is a full-stack software appliance that contains an operating system, database, and key-management application. Oracle Key Vault is designed to help organizations store and manage their keys and credentials.

Your organization may require the use of an HSM to protect encryption keys. Because they are designed to not allow keys to leave the cryptographic boundary of the HSM, in most cases it is not practical to connect databases directly to an HSM. Instead, databases will connect to the Oracle Key Vault which will in turn be protected by the HSM. This configuration establishes a Root-of-Trust (RoT) for Oracle Key Vault in the HSM. When an HSM is deployed with Oracle Key Vault, the RoT remains in the HSM. The HSM RoT protects the wallet password, which protects the TDE master key, which in turn protects all the encryption keys, certificates, and other security artifacts managed by the Oracle Key Vault server. Note that the HSM in this RoT usage scenario does not store any customer encryption keys. The customer keys are stored and managed directly by the Oracle Key Vault server.

Using HSM as a RoT is intended to mitigate attempts to recover keys from an Oracle Key Vault server which has been started in an unauthorized environment. Physical loss of an Oracle Key Vault server from a facility is one example of such a scenario. An unauthorized user attempting to run a lost or stolen Oracle Key Vault server, without authorized access to the HSM,would be prevented from recovering the encryption keys stored on the appliance.

Oracle Key Vault employs a hierarchy of security controls including operating system hardening, database encryption, and data access enforcement using Database Vault. These controls are designed to mitigate the risk of users potentially extracting keys and credentials from systems they can physically access. Administrators do not need to access the internal components of the appliance for normal, day-to-day operations. Oracle Key Vault should be deployed in a secure location, and physical and logical access to the appliance should be controlled and monitored.

If your site uses HSMs from SafeNet and nCipher (a Thales company), then you can configure these HSM products with Oracle Key Vault in standalone, primary-standby, and multi-master environments.

This guide assumes that you have installed and configured Oracle Key Vault. It also assumes that you have sufficient knowledge of the of the HSM products that you plan to configure.

The general process that you must follow to configure the HSM with Oracle Key Vault is as follows:

1. Install the HSM client software on the Oracle Key Vault server.
2. Enroll Oracle Key Vault as a client of the HSM.
3. Perform further configuration operations, which are as follows:
   - Configure protection for the TDE master encryption key with the HSM.
   - Enable the HSM in a primary-standby Oracle Key Vault installation.
   - Enable the HSM in an Oracle Key Vault multi-master cluster environment.
   - Perform backup and restore operations in an HSM-enabled Oracle Key Vault instance.
   - When necessary, perform reverse-migration so that the Oracle Key Vault environment is no longer HSM-enabled.

1.2 Installing the HSM Client Software on an Oracle Key Vault Server

After you install Oracle Key Vault, you can install the HSM client software on the Oracle Key Vault server.

1. Ensure that the vendor's software includes a PKCS#11 library.

   Refer to the HSM documentation from the HSM vendor for more information.
2. Install the HSM vendor's client software on the Oracle Key Vault server.

   You can install SafeNet and nCipher HSM products.

Related Topics

- Installing the HSM Client Software on the Oracle Key Vault Server for SafeNet
  You must use the SafeNet client version 6.2 for Linux x64 for the installation.

- Installing the HSM Client Software on the Oracle Key Vault Server for nCipher
  The nCipher HSM requires a separate non-HSM computer on the network to use as the remote file system.

1.3 Enrolling Oracle Key Vault as a Client of the HSM

You must enroll Oracle Key Vault as a client of HSM and ensure connectivity between the HSM client and the HSM.

1. Install the HSM vendor's client software on the Oracle Key Vault server.
2. Ensure that the HSM client software can communicate from Oracle Key Vault to the HSM.

Related Topics

- Installing the HSM Client Software on an Oracle Key Vault Server
  After you install Oracle Key Vault, you can install the HSM client software on the Oracle Key Vault server.
- Enrolling Oracle Key Vault as a Client of a SafeNet HSM
  To perform the enrollment, you must use the `client` commands at the command line.
- Enrolling Oracle Key Vault as a Client of an nCipher HSM
  You use both the nCipher user interface and the command line to enroll Oracle Key Vault as a client of an nCipher HSM.

2
Configuring an HSM for Oracle Key Vault

The HSM can be configured to protect keys, or work in a classic primary-standby configuration or in a multi-master cluster.

- Protecting the Oracle Key Vault TDE Master Key with the HSM
  You can use the Oracle Key Vault management console to configure protection for the TDE master encryption key.
- Enabling HSM in a High Availability Key Vault Installation
  In a primary-standby Oracle Key Vault installation, you must enable the HSM separately on the primary and standby servers.
- HSMs in a Multi-Master Cluster
  You can configure HSMs in a multi-master cluster with a single node or multiple nodes.
- Backup and Restore Operations in an HSM-Enabled Oracle Key Vault Instance
  You can back up and restore an HSM-enabled Oracle Key Vault instance.
- Reverse Migration Operation
  Reverse migrating an HSM-enabled Oracle Key Vault server reverts the Key Vault server to using the recovery passphrase to protect the TDE wallet.

2.1 Protecting the Oracle Key Vault TDE Master Key with the HSM

You can use the Oracle Key Vault management console to configure protection for the TDE master encryption key.

If you plan to use a multi-master cluster, then Oracle recommends that you perform this procedure before you configure the cluster environment. Ensure that you complete the following steps on this server before you perform these steps on another Oracle Key Vault server.

1. If you have implemented nCipher Hardware Security Module (HSM), then run the following command as user `oracle`:

   ```
   oracle$ /opt/nfast/bin/rfs-sync --update
   ```

2. Log into the Oracle Key Vault management console as a user with the System Administrator role.

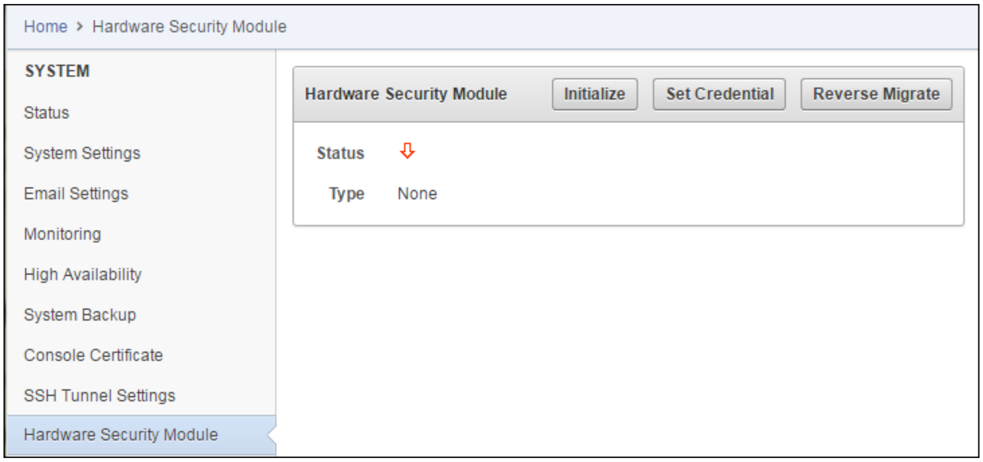
   If you are using a multi-master cluster environment, then log into the Oracle Key Vault node that you want to HSM-enable.

3. Click the **System** tab.

   The Status page appears.

4. Click **Hardware Security Module** in the left sidebar.

   The Hardware Security Module page appears. The red downward arrow shows the non-initialized **Status**. The **Type** field displays **None**.

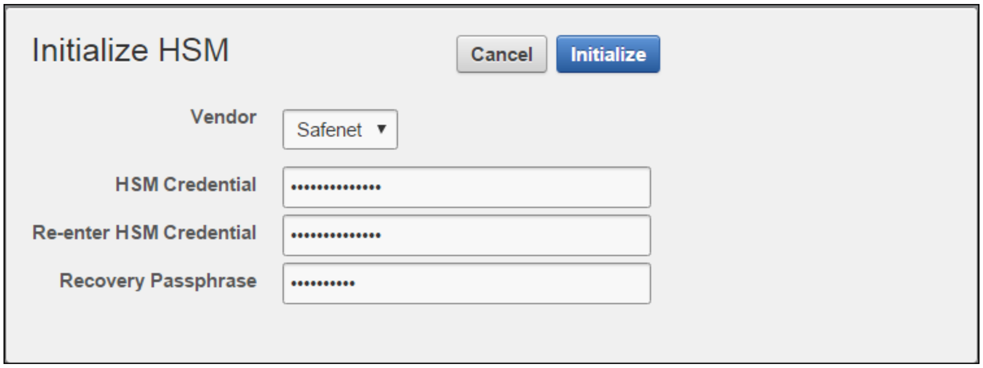


Status ⇩

Type None

5. Click **Initialize**.

   The Initialize HSM dialog box appears.



Vendor: Safenet ▾

HSM Credential: ••••••••••••••

Re-enter HSM Credential: ••••••••••••••

Recovery Passphrase: ••••••••••

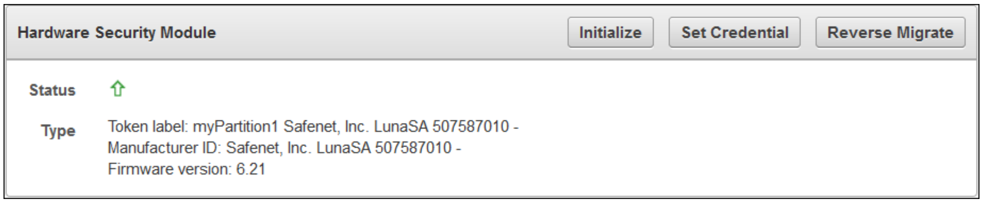
6. Enter the HSM credential two times: first in **HSM Credential** and second in **Re-enter HSM Credential**.

   Consult the HSM documentation for this credential. The HSM credential for SafeNet is the SafeNet partition password. For nCipher, the credential is the Operator Card Set password.

7. Enter the **Recovery Passphrase** for Oracle Key Vault.

8. Click **Initialize**.

   At the end of a successful initialize operation, the **Hardware Security Module** page appears. The initialized **Status** is indicated by an upward green arrow. The **Type** field displays details of the HSM in use.



Status ⇧

Type Token label: myPartition1 Safenet, Inc. LunaSA 507587010 - Manufacturer ID: Safenet, Inc. LunaSA 507587010 - Firmware version: 6.21

9. If you have implemented nCipher HSM, then run the following command as user `oracle`:

   ```
   oracle$ /opt/nfast/bin/rfs-sync --commit
   ```

   If you do not perform this step after each initialization when using nCipher, then multiple features will break, including restoring backups and using the primary-standby configuration.

10. Verify that the operation was successful by checking the most recent initialization log files in the `/var/okv/log/hsm/` directory.

If the initialize operation fails, then you will be redirected to the Hardware Security Module page with non-initialized **Status** and **Type** None.

> **Note:**
>
> If you change the HSM credential on the HSM after initialization, then you must also update the HSM credential on the Oracle Key Vault server using the **Set Credential** command.

2.2 Enabling HSM in a High Availability Key Vault Installation

In a primary-standby Oracle Key Vault installation, you must enable the HSM separately on the primary and standby servers.

You must perform this task before pairing these two servers in a primary-standby configuration. If you have already HSM-enabled either the primary or the standby server, or both, but do not follow these steps and then do a primary-standby pairing, then the configuration will fail. If the servers are already paired but neither are HSM-enabled, then you must unpair them, reinstall the standby server, and the follow these steps.

1. Install two separate Oracle Key Vault instances.
2. Choose one to be the primary node and the other to be the standby node.
3. Install the HSM client software on both the primary and the standby node.
4. Enroll the primary and standby nodes as clients of HSM.
5. Initialize HSM use on the primary.

   Log in to the designated primary server through SSH as user `support`, switch user (`su`) to `root`, then switch user (`su`) to `oracle`.

   ```
   $ ssh support@okv_primary_instance_ip_address
   support$ su root
   root# su oracle
   ```

6. Perform the following manual steps on the primary server as user `oracle`:

   ```
   oracle$ cd /usr/local/okv/hsm/wallet
   oracle$ scp cwallet.sso support@okv_standby_instance_ip_address:/tmp
   oracle$ scp enctdepwd support@okv_standby_instance_ip_address:/tmp
   oracle$ cd /usr/local/okv/hsm/restore
   oracle$ scp ewallet.p12 support@okv_standby_instance_ip_address:/tmp
   ```

7. Log in to the designated standby server through SSH as user `support`, then switch user (`su`) to `root`.

   ```
   $ ssh support@okv_standby_instance_ip_address
   support$ su root
   ```

8. Open the `okv_security.conf` file.

   A sample `okv_security.conf` file before enabling HSM in the node appears as follows:

   ```
   SNMP_ENCRYPTION_PWD="snmp_encryption_password"
   SNMP_AUTHENTICATION_PWD="snmp_auth_password"
   SNMP_USERNAME="snmpuser"
   SMTP_TRUSTSTORE_PWD="smtp_truststore_password"
   HSM_ENABLED="0"
   FIPS_ENABLED="fips_value"
   HSM_FIPS_ENABLED="1"
   ```

   Versions of Oracle Key Vault earlier than release 18 may not contain the `FIPS_ENABLED` or the `HSM_FIPS_ENABLED` parameter in the `okv_security.conf` file. Consult the documentation for earlier releases for more information.

9. Set up the HSM-related files and in the `okv_security.conf` file, set the `HSM_ENABLED` and `HSM_PROVIDER` parameters.

   ```
   root# cd /usr/local/okv/hsm/wallet
   root# mv /tmp/enctdepwd .
   root# mv /tmp/cwallet.sso .
   root# chown oracle *
   root# chgrp oinstall *
   root# cd /usr/local/okv/hsm/restore
   root# mv /tmp/ewallet.p12 .
   root# chown oracle *
   root# chgrp oinstall *
   root# vi /usr/local/okv/etc/okv_security.conf
      Set HSM_ENABLED="1"
      Set HSM_PROVIDER="provider_value"
   ```

   In this specification:

   - `HSM_ENABLED` is set in this example to `1` to enable the HSM for this node. Setting it to `0` disables the HSM.
   - `HSM_PROVIDER` refers to the HSM provider. For SafeNet, set this value to `1`. For nCipher, set it to `2`.

10. Save and quit by entering the following sequence of characters in the vi file: `:wq!`

    After you enable the HSM, the `okv_security.conf` file will be similar to the following:

    ```
    SNMP_ENCRYPTION_PWD="snmp_encryption_password"
    SNMP_AUTHENTICATION_PWD="snmp_auth_password"
    SNMP_USERNAME="snmpuser"
    SMTP_TRUSTSTORE_PWD="smtp_truststore_password"
    HSM_ENABLED="1"
    FIPS_ENABLED="fips_value"
    HSM_PROVIDER="2"
    ```

    Versions of Oracle Key Vault earlier than release 18 may not contain the `FIPS_ENABLED` or the `HSM_FIPS_ENABLED` parameter in the `okv_security.conf` file. Consult the documentation for earlier releases for more information.

11. Without restarting the Oracle Key Vault instances, navigate to the primary and standby Oracle Key Vault management consoles and configure primary-standby environment.

Related Topics

- *Oracle Key Vault Administrator's Guide*

2.3 HSMs in a Multi-Master Cluster

You can configure HSMs in a multi-master cluster with a single node or multiple nodes.

- About HSMs in a Multi-Master Cluster
  An HSM in Oracle Key Vault stores a top level master encryption key that acts as a Root of Trust (RoT).
- Configuring an HSM for a Multi-Master Cluster Starting with Single Node (Recommended)
  Oracle recommends that to use an HSM with a multi-master cluster, you start with a single HSM-enabled node and add additional HSM-enabled nodes using the node induction process.
- Configuring an HSM for a Multi-Master Cluster with Multiple Nodes
  You can configure HSM for multiple nodes by copying a bundle from the first HSM-enabled node to the other nodes in the cluster before configuring HSM for the other nodes.

2.3.1 About HSMs in a Multi-Master Cluster

An HSM in Oracle Key Vault stores a top level master encryption key that acts as a Root of Trust (RoT).

This RoT protects master encryption keys that Oracle Key Vault uses. HSMs are built with specialized tamper-resistant hardware which is harder to access than normal servers. This protects the RoT and makes it difficult to extract encrypted data, lowering the risk of compromise. In addition, you can use HSMs in FIPS 140-2 level 3 mode, which enables you to meet certain compliance requirements.

> **Note:**
>
> An existing Oracle Key Vault deployment cannot be migrated to use an HSM as a RoT.

In a multi-master Oracle Key Vault installation, any Key Vault node in the cluster can use any HSM. The nodes in the multi-master cluster can use different TDE wallet passwords, RoT keys, and HSM credentials.

> **Note:**
>
> To ensure complete security, you must HSM-enable all Oracle Key Vault nodes in the cluster.

2.3.2 Configuring an HSM for a Multi-Master Cluster Starting with Single Node (Recommended)

Oracle recommends that to use an HSM with a multi-master cluster, you start with a single HSM-enabled node and add additional HSM-enabled nodes using the node induction process.

Oracle recommends the following steps to configure an HSM for a multi-master cluster with a single node:

1. Convert an Oracle Key Vault server into the first node of the cluster.
2. HSM-enable the first node before adding any new nodes.
3. HSM-enable the candidate node before adding it to the cluster.
4. Add the HSM-enabled candidate node to the cluster using a controller node that is also HSM-enabled.
   Note the following:
   - If any node in the cluster is already HSM-enabled, you cannot add a new node that is not HSM-enabled.
   - The Add Node to Cluster page will require the controller node's HSM credential.

Related Topics

- Configuring an HSM for a Multi-Master Cluster with Multiple Nodes
  You can configure HSM for multiple nodes by copying a bundle from the first HSM-enabled node to the other nodes in the cluster before configuring HSM for the other nodes.
- *Oracle Key Vault Administrator's Guide*

2.3.3 Configuring an HSM for a Multi-Master Cluster with Multiple Nodes

You can configure HSM for multiple nodes by copying a bundle from the first HSM-enabled node to the other nodes in the cluster before configuring HSM for the other nodes.

- About Configuring an HSM for a Multi-Master Cluster with Multiple Nodes
  The general procedure is to perform steps first on the original node, then on the nodes that you want to add to the cluster.
- Step 1: Configure the First HSM-Enabled Node
  After configuring the HSM on the first node in the multi-master cluster, you must create the bundle and copy it to the other nodes in the cluster.
- Step 2: Configure the Remaining Nodes
  After you configure the first node, you are ready to install the bundle on the remaining nodes.

2.3.3.1 About Configuring an HSM for a Multi-Master Cluster with Multiple Nodes

The general procedure is to perform steps first on the original node, then on the nodes that you want to add to the cluster.

The instructions for configuring an HSM for a multi-master cluster starting with a single node explain how to configure an HSM for a multi-master cluster, starting with a single node of the cluster and is the recommended way to configure a cluster to use HSM(s). However, if you have already configured a multi-master cluster, you can still configure the cluster to use HSMs. However, there are extra steps needed, involving manually copying a bundle from the first HSM-enabled node to all of the other nodes in the cluster and applying it before proceeding to HSM-enable any other node. Note that if the first node that is HSM-enabled has a read-write peer node, then the read-write peer will not be able to decrypt the replicated information from the HSM-enabled node until the bundle is copied and applied successfully to the read-write peer. This could result in data loss if the bundle is not immediately successfully created and applied to the read-write peer.

After you HSM-enable the first node in the cluster, use the following steps to create the bundle on the HSM-enabled node and copy and apply it on all other nodes in the cluster before you proceed to HSM-enable any other node.

Related Topics

- Configuring an HSM for a Multi-Master Cluster Starting with Single Node (Recommended)
  Oracle recommends that to use an HSM with a multi-master cluster, you start with a single HSM-enabled node and add additional HSM-enabled nodes using the node induction process.

2.3.3.2 Step 1: Configure the First HSM-Enabled Node

After configuring the HSM on the first node in the multi-master cluster, you must create the bundle and copy it to the other nodes in the cluster.

1. Log in to the Oracle Key Vault management console as a user who has the System Administrator role.
2. Ensure that you have followed the instructions in *Oracle Key Vault Administrator's Guide* to create the first (initial) node of a cluster.
3. Click the **System** tab.
4. On the left side of the System page, click **Hardware Secure Module**.
5. On the HSM-enabled node, click **Create Bundle** on the **HSM** page.
6. Log in to the HSM-enabled node through SSH as user `support`.

   ```
   $ ssh support@hsm_enabled_node
   ```

7. Switch to the `root` user.

   ```
   support$ su root
   ```

8. To copy the bundle to the `/usr/local/okv/hsm` location on each of the other nodes using the IP address, use `SCP`.

   Ensure that you perform this step using the IP address of all other nodes in the cluster.

   ```
   root# scp /usr/local/okv/hsm/hsmbundle support@ip_address:/tmp
   ```

Related Topics

- *Oracle Key Vault Administrator's Guide*

2.3.3.3 Step 2: Configure the Remaining Nodes

After you configure the first node, you are ready to install the bundle on the remaining nodes.

Complete this procedure as soon as possible after you have HSM-enabled the first node and copied the bundle to all other nodes.

1. Log in to each node in the cluster using the IP address (except the original HSM-enabled node):.

   ```
   $ ssh support@ip_address
   ```

2. On each node, switch to the `root` user.

   ```
   support$ su root
   ```

3. Perform the following steps on each node:

   ```
   root# cp /tmp/hsmbundle /usr/local/okv/hsm/
   root# chown oracle:oinstall /usr/local/okv/hsm/hsmbundle
   ```

4. On each node except the original HSM-enabled node, click **Apply Bundle** on the **HSM** page.

You must apply the bundle immediately on all nodes before you reverse-migrate the original HSM-enabled node.

5. Proceed to HSM-enable each of these nodes in the same way that you HSM-enabled the first node.
6. After you have HSM-enabled all nodes and verified the replication between all nodes, remove the `hsmbundle` file from all of the nodes.

2.4 Backup and Restore Operations in an HSM-Enabled Oracle Key Vault Instance

You can back up and restore an HSM-enabled Oracle Key Vault instance.

- Backup Operations in an HSM-Enabled Oracle Key Vault Instance
  Backing up Oracle Key Vault data in an HSM-enabled instance is the same as backing up an instance that has not been HSM enabled.
- Restore Operations in an HSM-Enabled Oracle Key Vault Instance
  Only backups made to an HSM-enabled Oracle Key Vault instance can be restored onto an HSM-enabled Oracle Key Vault instance.

2.4.1 Backup Operations in an HSM-Enabled Oracle Key Vault Instance

Backing up Oracle Key Vault data in an HSM-enabled instance is the same as backing up an instance that has not been HSM enabled.

You can use the Oracle Key Vault management console to perform a backup operation.

Related Topics

- *Oracle Key Vault Administrator's Guide*

2.4.2 Restore Operations in an HSM-Enabled Oracle Key Vault Instance

Only backups made to an HSM-enabled Oracle Key Vault instance can be restored onto an HSM-enabled Oracle Key Vault instance.

Before you restore a backup onto a system, you must ensure that the system can access both the HSM and the Root of Trust (RoT) that was used to make the backup. You must therefore have installed the HSM on the Oracle Key Vault server and enrolled Oracle Key Vault as a client of HSM before this step. If the backup was taken on an HSM-enabled cluster node, then when you restore the backup to a standalone server, you must ensure that the server has access to the same HSM as the node on which the backup was taken.

1. Log into the Oracle Key Vault management console as a user with the System Administrator role.

   The Oracle Key Vault Home page appears.
2. Click the **System** tab.

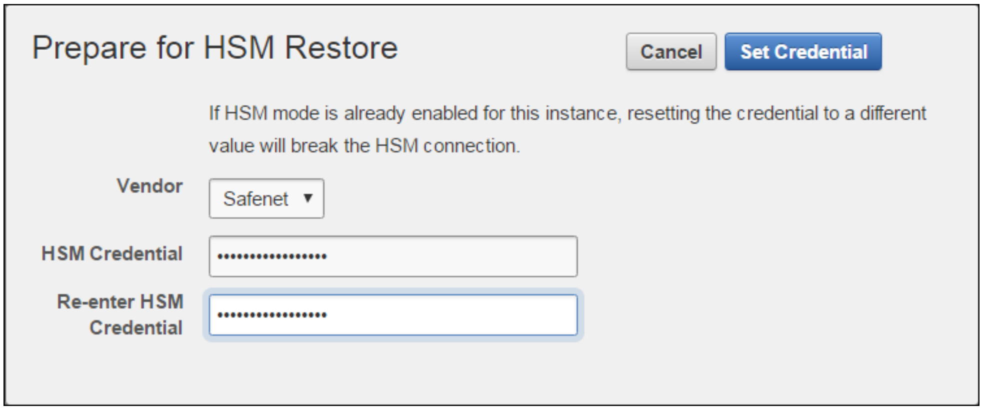
The Status page appears.

3. Click **Hardware Security Module** in the left sidebar.

   The **Hardware Security Module** page appears. On restore, the **Status** is disabled first, then enabled after the restore completes.

4. Click **Set Credential**.

   The **Prepare for HSM Restore** screen appears.



Prepare for HSM Restore

If HSM mode is already enabled for this instance, resetting the credential to a different value will break the HSM connection.

Vendor: Safenet ▾

HSM Credential: ••••••••••••••••

Re-enter HSM Credential: ••••••••••••••••

5. Enter the HSM credential two times: first in **HSM Credential** and second in **Re-enter HSM Credential**.

   Consult the HSM documentation for this credential. The HSM credential for SafeNet is the SafeNet partition password. For nCipher, the credential is the Operator Card Set password.

6. Click **Set Credential**.

   > **Caution:**
   >
   > If you enter an incorrect credential for the HSM, the previous credential will continue to be stored and used. If the node is not HSM enabled, and you enter an incorrect credential for the HSM, the incorrect credential is not stored.

   The HSM credential will be stored in the system. You must manually enter this HSM credential to perform an HSM restore because it is not stored in the backup itself.

7. In the Oracle Key Vault management console, go to the **Restore** page and then restore the backup.

Related Topics

- *Oracle Key Vault Administrator's Guide*

2.5 Reverse Migration Operation

Reverse migrating an HSM-enabled Oracle Key Vault server reverts the Key Vault server to using the recovery passphrase to protect the TDE wallet.

This operation is necessary if the HSM that protects Oracle Key Vault must be decommissioned.

- Reverse Migrating a Standalone Deployment
  You can reverse migrate a standalone deployment by using the Oracle Key Vault management console.
- Reverse Migrating a Primary-Standby Deployment
  To reverse migrate a primary-standby deployment, use both the Oracle Key Vault management console and the command line.
- Reverse Migrating a Multi-Master Cluster
  You can reverse migrate a multi-master cluster by using the Oracle Key Vault management console.

2.5.1 Reverse Migrating a Standalone Deployment

You can reverse migrate a standalone deployment by using the Oracle Key Vault management console.

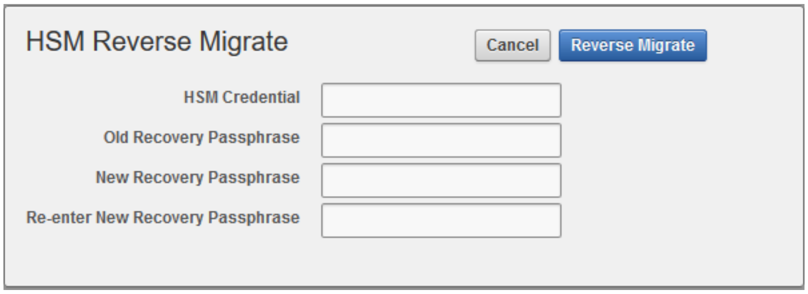
1. Log into the Oracle Key Vault management console as a user with the System Administrator role.

   The Oracle Key Vault **Home** page appears.
2. Click the **System** tab.

   The **Status** page appears.
3. Click **Hardware Security Module** in the left sidebar.

   The **Hardware Security Module** page appears.
4. Click **Reverse Migrate**.

   The **HSM Reverse Migrate** screen is displayed.



On the **HSM Reverse Migrate** screen, enter the following details:

- Enter the HSM credential in the **HSM Credential** field. Consult the HSM documentation for this credential. The HSM credential for SafeNet is the SafeNet partition password. For nCipher, the credential is the Operator Card Set password.

- Enter the old recovery passphrase in the **Old Recovery Passphrase** field.
- Enter the new recovery passphrase in the **New Recovery Passphrase** and **Re-enter New Recovery Passphrase** fields.

5. Click **Reverse Migrate**

   The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

2.5.2 Reverse Migrating a Primary-Standby Deployment

To reverse migrate a primary-standby deployment, use both the Oracle Key Vault management console and the command line.

1. On the primary server, log into the Oracle Key Vault management console as a user with system administrative privileges.

   The Oracle Key Vault **Home** page appears.

2. Click the **System** tab.

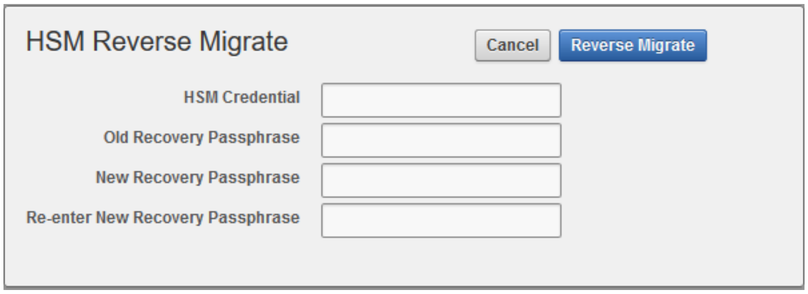
   The **Status** page appears.

3. Click **Hardware Security Module** in the left sidebar.

   The **Hardware Security Module** page appears.

4. Click **Reverse Migrate**.

   The **HSM Reverse Migrate** screen is displayed.

   On the **HSM Reverse Migrate** screen, enter the following details:

   - Enter the HSM credential in the **HSM Credential** field. Consult the HSM documentation for this credential. The HSM credential for SafeNet is the SafeNet partition password. For nCipher, the credential is the Operator Card Set password.
   - Enter the old recovery passphrase in the **Old Recovery Passphrase** field.
   - Enter the new recovery passphrase in the **New Recovery Passphrase** and **Re-enter New Recovery Passphrase** fields.

5. Click **Reverse Migrate**

   The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

6. On the standby server, log in to the Oracle Key Vault Server through SSH as user `support`, then switch user (`su`) to `root`.

   ```
   $ ssh support@okv_standby_instance
   support$ su root
   ```

7. Modify the `okv_security.conf` file.

   ```
   root# vi /usr/local/okv/etc/okv_security.conf
   ```

   - Delete the line `HSM_PROVIDER="`*`provider_value`*`"`.
   - Change the value of the parameter `HSM_ENABLED` to `"0"`.

   Save and quit by entering the following sequence of characters in the vi file: `:wq!`

8. On the standby server, remove the following files:

   ```
   root# cd /usr/local/okv/hsm/wallet
   root# rm -f cwallet.sso enctdepwd
   root# cd /usr/local/okv/hsm/restore
   root# rm -f cwallet.sso ewallet.p12
   root# cd /mnt/okvram
   root# rm -f cwallet.sso ewallet.p12
   root# cd /mnt/okvram/restore
   root# rm -f cwallet.sso ewallet.p12
   root# cd /usr/local/okv/tde
   root# rm -f cwallet.sso
   ```

9. Switch user (`su`) to `oracle`:

   ```
   root# su oracle
   ```

10. Run the following command:

    ```
    oracle$ /var/lib/oracle/dbfw/bin/orapki wallet create -wallet /usr/
    local/okv/tde -auto_login
    ```

11. Enter the new recovery passphrase that you specified in Step 4.

The primary-standby deployment is successfully reverse migrated.

2.5.3 Reverse Migrating a Multi-Master Cluster

You can reverse migrate a multi-master cluster by using the Oracle Key Vault management console.

1. Log into the Oracle Key Vault management console as a user with the System Administrator role.

   The Oracle Key Vault **Home** page appears.

2. Click the **System** tab.

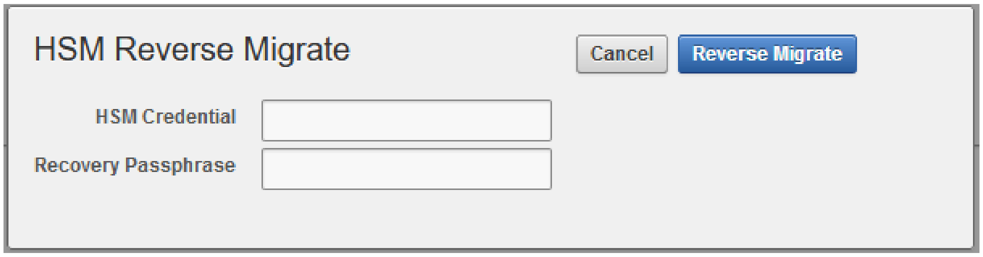
   The **Status** page appears.

3. Click **Hardware Security Module** in the left sidebar.

The **Hardware Security Module** page appears.

4. Click **Reverse Migrate**.

   The **HSM Reverse Migrate** dialog box is displayed.



   In the **HSM Reverse Migrate** dialog box, enter the following details:

   - Enter the HSM credential. Consult the HSM documentation for this credential. The HSM credential for SafeNet is the SafeNet partition password. For nCipher, the credential is the Operator Card Set password.
   - Enter the recovery passphrase.

5. Click **Reverse Migrate**

   The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

3

Commands Used in Previous Versions of Oracle Key Vault

The commands reference details commands used in Oracle Key Vault 12.2.0.5.0 and earlier.

- Enabling an HSM in a Primary-Standby Pre-Release 12.2 Oracle Key Vault Installation
  You can use SSH to enable an HSM in a primary-standby Oracle Key Vault installation on release 12.2.0.5.0 and earlier.
- Enabling the HSM_ENABLED Parameter in the Pre-Release 12.2 okv_security.conf File
  You can enable an HSM in a high availability Oracle Key Vault 12.2.0.5.0 and earlier installation.

3.1 Enabling an HSM in a Primary-Standby Pre-Release 12.2 Oracle Key Vault Installation

You can use SSH to enable an HSM in a primary-standby Oracle Key Vault installation on release 12.2.0.5.0 and earlier.

While performing the procedure *HSM in a Primary-Standby Oracle Key Vault Installation* under Vendor Specific Notes for nCipher on Oracle Key Vault 12.2.0.5.0 and earlier, use the following commands:

1. Perform the following manual steps on the intended primary as user `oracle`:

```
$ ssh support@okv_primary_instance_ip_address
support$ su root
root# su oracle
oracle$ cd /usr/local/okv/hsm/wallet
oracle$ scp cwallet.sso support@okv_standby_instance_ip_address:/tmp
oracle$ scp enctdepwd support@okv_standby_instance_ip_address:/tmp
```

2. Perform the following manual steps on the intended standby as user `root`:

```
$ ssh support@okv_standby_instance_ip_address
support$ su root
root# cd /usr/local/okv/hsm/wallet
root# mv /tmp/enctdepwd .
root# mv /tmp/cwallet.sso .
root# chown oracle *
root# chgrp oinstall *
```

Related Topics

- Enabling HSM in a High Availability Key Vault Installation
  In a primary-standby Oracle Key Vault installation, you must enable the HSM separately on the primary and standby servers.

3.2 Enabling the HSM_ENABLED Parameter in the Pre-Release 12.2 okv_security.conf File

You can enable an HSM in a high availability Oracle Key Vault 12.2.0.5.0 and earlier installation.

While performing the procedure Enabling HSM in a High Availability Key Vault Installation on Oracle Key Vault 12.2.0.5.0 and earlier, use the following commands.

1. Perform the following manual steps on the primary node as user oracle:

   ```
   root# cd /usr/local/okv/hsm/wallet
   root# scp cwallet.sso support@okv_standby_instance_ip_address:/tmp
   root# scp enctdepwd support@okv_standby_instance_ip_address:/tmp
   ```

2. Enable the HSM_ENABLED parameter in the okv_security.conf file:

   ```
   root# cd /usr/local/okv/hsm/wallet
   root# mv /tmp/enctdepwd .
   root# mv /tmp/cwallet.sso .
   root# chown oracle *
   root# chgrp oinstall *
   root# vi /usr/local/okv/etc/okv_security.conf
      Set HSM_ENABLED="1"
      Set HSM_PROVIDER="provider_value"
   ```

   In this specification:

   - HSM_ENABLED is set in this example to 1 to enable the HSM for this node. Setting it to 0 disables the HSM.
   - HSM_PROVIDER refers to the HSM provider. For SafeNet, set this value to 1. For nCipher, set it to 2.

3. Save and quit by entering the following sequence of characters in the vi file: :wq!

4

Support Guidance

The support guidance provides information about troubleshooting and vendor specific notes.

- General Troubleshooting
  Oracle Key Vault provides general troubleshooting help. Vendor-specific notes cover vendor-specific troubleshooting.
- Vendor Specific Notes for SafeNet
  Oracle Key Vault supports Oracle Key Vault integration with SafeNet Luna SA Hardware Security Modules from Thales version 7000, but does not support Host Trust Link (HTL) for SafeNet Luna HSM.
- Vendor Specific Notes for nCipher
  You can integrate Oracle Key Vault release 12.2 BP 3 and later with the HSM from nCipher nShield Connect 6000+.

4.1 General Troubleshooting

Oracle Key Vault provides general troubleshooting help. Vendor-specific notes cover vendor-specific troubleshooting.

- Trace Files for Diagnosing Issues
  Oracle Key Vault provides trace files so that you can better diagnose issues that may arise.
- HSM Alert
  Oracle Key Vault provides an alert mechanism that periodically monitors the HSM configuration to check for Root of Trust key availability and file health.
- hsm_initialize: Could Not Get Slot for HSM
  The `hsm_initialize: Could Not Get Slot for HSM` error indicates that Oracle Key Vault is not properly enrolled as a client of the HSM.
- hsm_initialize: Could Not Load PKCS#11 Library
  The `hsm_initialize: Could Not Load PKCS#11 Library` error indicates that Oracle Key Vault is not properly enrolled as a client of the HSM.
- Oracle Key Vault Management Console Does Not Start After Restarting HSM-Enabled Oracle Key Vault Server
  You can remedy this problem by using the `support` account.
- Primary-Standby Errors
  The `okv_security.conf` file contains settings that can help you diagnose primary-standby errors.
- Errors from HSM-Enabled Oracle Key Vault Backups
  You can use the `cwallet.sso` file to diagnose HSM-enabled Oracle Key Vault backup errors.

- Restoring an HSM-Enabled Backup
  Before you restore an HSM-enabled backup, ensure that you have the correct HSM credential.

4.1.1 Trace Files for Diagnosing Issues

Oracle Key Vault provides trace files so that you can better diagnose issues that may arise.

Use these trace files to more finely diagnose issues when you attempt hardware security module operations. These trace files are located in the */var/okv/log/hsm/* directory on the Oracle Key Vault server. To see the most recently failed operation, you can sort the trace files by their last modified time. For example, `ls -ltr /var/okv/log/hsm` lists the most recently modified trace files at the bottom of the list.

4.1.2 HSM Alert

Oracle Key Vault provides an alert mechanism that periodically monitors the HSM configuration to check for Root of Trust key availability and file health.

When an Oracle Key Vault server is HSM-enabled, Oracle Key Vault contacts the HSM every five minutes (or whatever you have set the monitoring interval to) to ensure that the Root of Trust key is available and the TDE wallet password can be decrypted. When a problem in the HSM configuration arises (for example, the HSM cannot be reached or if there are conflicting keys in the HSM with the same ID), then the up arrow on the **Hardware Security Module** tab switches to a down arrow and an alert is raised. The down arrow signifies that the HSM is not configured or the HSM configuration has a problem. When the HSM configuration encounters a problem (for example, the HSM cannot be reached or if there are conflicting keys in the HSM with the same ID), the up arrow on the **Hardware Security Module** tab switches to a down arrow and an alert is raised. The down arrow signifies that the HSM is not configured or the HSM configuration has a problem. When an alert has been raised, the following error message appears: `HSM configuration error. Please refer to the HSM Alert section in the Oracle Key Vault Root of Trust HSM Configuration Guide`.

If this alert appears, then follow these steps:

1. Log in as root as follows:

   ```
   $ ssh support@okv_instance_ip_address
   support$ su - root
   ```

2. Back up the SSO wallet. For example:

   ```
   root# cp /mnt/okvram/cwallet.sso /var/lib/oracle/cwallet_hsm_backup.sso
   ```

3. Diagnose the source of the alert.
   The following `verify` command should show why the alert was raised. The `ls -ltrh` command shows the most recent log file at the bottom of the output.

   ```
   root# su - oracle
   oracle$ /usr/local/okv/hsm/bin/hsmclient verify
   oracle$ cd /var/okv/log/hsm
   oracle$ ls -ltrh
   ```

4. If you cannot resolve this problem, then contact Oracle Support.

4.1.3 hsm_initialize: Could Not Get Slot for HSM

The `hsm_initialize: Could Not Get Slot for HSM` error indicates that Oracle Key Vault is not properly enrolled as a client of the HSM.

Check the vendor-specific instructions for more information.

4.1.4 hsm_initialize: Could Not Load PKCS#11 Library

The `hsm_initialize: Could Not Load PKCS#11 Library` error indicates that Oracle Key Vault is not properly enrolled as a client of the HSM.

Check the vendor-specific instructions for more information.

4.1.5 Oracle Key Vault Management Console Does Not Start After Restarting HSM-Enabled Oracle Key Vault Server

You can remedy this problem by using the `support` account.

If the Oracle Key Vault management console does not appear after you restart the HSM-enabled Oracle Key Vault server, then log into the Oracle Key Vault server using SSH as user `support` and try manually opening the wallet as follows:

```
$ ssh support@okv_instance_ip_address
support$ su root
root# su oracle
oracle$ cd /usr/local/okv/hsm/bin
oracle$ ./hsmclient open_wallet
```

If the `open_wallet` command succeeds, the database will open and the management console will appear, unless there is another non-HSM problem. If the command does not succeed, then check the recent log files under `/var/okv/log/hsm` and check for vendor-specific instructions.

4.1.6 Primary-Standby Errors

The `okv_security.conf` file contains settings that can help you diagnose primary-standby errors.

1. Check that the files have been transported to the standby server.

   Execute the command `ls -l` as root on the standby server:

   ```
   root# ls -l /usr/local/okv/hsm/wallet
   -rw------- 1 oracle oinstall 324 May 16 22:57 cwallet.sso
   -rw------- 1 oracle oinstall 176 May 16 22:57 enctdepwd
   root# ls -l /usr/local/okv/hsm/restore
   -rw------- 1 oracle oinstall 320 May 16 22:57 ewallet.p12
   ```

   You should see `cwallet.sso` and `enctdepwd` in the `/usr/local/okv/hsm/wallet` directory and `ewallet.p12` in the `/usr/local/okv/hsm/restore` directory.

2. Check that the mode is set to HSM on the standby server:

   Open the file okv_security.conf as root on the standby server:

   ```
   root# cat /usr/local/okv/etc/okv_security.conf
    Look for the line:
    HSM_ENABLED="1"
   ```

   You should see the number within double quotes.

3. Check the vendor-specific instructions.

4.1.7 Errors from HSM-Enabled Oracle Key Vault Backups

You can use the cwallet.sso file to diagnose HSM-enabled Oracle Key Vault backup errors.

You should check that the pre_restore command has been run on the target as follows:

Execute the command ls -l as root on the Oracle Key Vault server to which you are restoring the backup:

```
root# ls -l /usr/local/okv/hsm/wallet
-rw------- 1 oracle oinstall 324 May 16 22:57 cwallet.sso
```

You should see the wallet file cwallet.sso .

You should also check that you have followed the instructions from the HSM vendor.

4.1.8 Restoring an HSM-Enabled Backup

Before you restore an HSM-enabled backup, ensure that you have the correct HSM credential.

Consult the HSM documentation for this credential. For SafeNet, the credential is the SafeNet partition password. For nCipher, the credential is the Operator Card Set password.

This procedure must only be used in a restore operation *and* you must enter the HSM credential correctly. If you enter an incorrect credential or if Oracle Key Vault is unable to connect to the HSM, then the credential will not be stored. Ensure that Oracle Key Vault is enrolled as a client of the HSM and then ensure that the correct credential has been entered.

For more information about enrolling Oracle Key Vault as a client of the HSM, see Enrolling Oracle Key Vault as a Client of the HSM.

4.2 Vendor Specific Notes for SafeNet

Oracle Key Vault supports Oracle Key Vault integration with SafeNet Luna SA Hardware Security Modules from Thales version 7000, but does not support Host Trust Link (HTL) for SafeNet Luna HSM.

- Installing the HSM Client Software on the Oracle Key Vault Server for SafeNet
  You must use the SafeNet client version 6.2 for Linux x64 for the installation.
- HSM Credential for SafeNet
  The HSM credential is the SafeNet partition password.
- Enrolling Oracle Key Vault as a Client of a SafeNet HSM
  To perform the enrollment, you must use the `client` commands at the command line.
- HSM Provider Value for SafeNet
  For SafeNet, the provider value is 1.
- HSM Vendor Specific Checks for SafeNet
  You should check the SafeNet vendor-specific settings.

4.2.1 Installing the HSM Client Software on the Oracle Key Vault Server for SafeNet

You must use the SafeNet client version 6.2 for Linux x64 for the installation.

1. Obtain the SafeNet client software package, version 6.2 for Linux x64.
2. Transport the SafeNet client software package to the Oracle Key Vault machine. Oracle recommends using SCP. For example, assuming the SafeNet client software packages is called `safenet.tar`:

   ```
   $ scp safenet.tar support@okv_instance_ip_address:/tmp
   ```

3. Install the SafeNet client software on Oracle Key Vault.
4. Log in to the Oracle Key Vault Server through SSH as user `support`, and switch user (`su`) to `root`:

   ```
   $ ssh support@okv_instance_ip_address
   support$ su root
   root# cd /usr/local/okv/hsm
   root# cp /tmp/safenet.tar /usr/local/okv/hsm
   root# tar -xvf safenet.tar
   root# cd 64
   root# ./install.sh
   ```

5. Accept the SafeNet license by typing `y` at the prompt.
6. Install the Luna SA by entering `1`, `n`, `i` at the successive prompts.

   This installs the SafeNet software in the directory `/usr/safenet/lunaclient` .
7. Delete the `safenet.tar` file from /tmp directory.

   ```
    root# rm -f /tmp/safenet.tar
   ```

4.2.2 HSM Credential for SafeNet

The HSM credential is the SafeNet partition password.

If you are using SafeNet as your HSM, then you can use the SafeNet `assignPassword` command to assign an HSM SafeNet partition password as the credential for a partition. Oracle Key Vault then uses this password when it needs to connect to the partition.

4.2.3 Enrolling Oracle Key Vault as a Client of a SafeNet HSM

To perform the enrollment, you must use the `client` commands at the command line.

1. Set the DNS servers for Oracle Key Vault via the management console. Log in to the Oracle Key Vault management console as a user who has the System Administrator role, and then to access the DNS settings area, from the **System** tab, select **System Settings**.

   This step is required for the SafeNet Luna SA HSM to communicate with Oracle Key Vault.

   You must configure the DNS servers on each Oracle Key Vault server that you plan to register as a client of the HSM. In a primary-standby environment, configure the DNS servers on both primary and standby server before pairing. For a multi-master cluster, configure DNS on each node in the cluster that will be registered as a client of the HSM.

   If you are using DNS with the HSM configuration, then due to the known issue, Bug 24478865 (fixed in Oracle Key Vault release 18.2 and later), ensure that DNS entries are both in the following locations:

   - Oracle Key Vault management console: from the **System** tab, select **System Settings**, and then check the DNS setting on that page.
   - The `/etc/resolv.conf` file

2. Exchange certificates between Oracle Key Vault and the SafeNet Luna SA HSM.

   Log in to the Oracle Key Vault Server through SSH as user `support`, and switch user (`su`) to `root`:

   ```
   $ ssh support@okv_instance_ip_address
   support$ su root
   root# cd /usr/safenet/lunaclient/bin
   root# scp admin@hsm_hostname:server.pem .
   root# ./vtl addServer -n hsm_hostname -c server.pem
   root# ./vtl createCert -n okv_hostname
   root# scp /usr/safenet/lunaclient/cert/client/okv_hostname.pem
   admin@hsm_hostname:
   ```

   You must enter the HSM administrative password when using SCP with the HSM.

3. Register Oracle Key Vault as a client of the Luna SA.

   This assumes that you have a partition set up on the SafeNet Luna SA HSM. You can use any client name that is not yet taken. Oracle recommends using a descriptive name that will identify the Oracle Key Vault instance.

Access the HSM administrative console by using SSH to `admin@hsm_hostname` and providing the administrative password:

```
$ client register -client client_name -hostname okv_hostname
$ client hostip map -c client_name -i okv_ip_address
$ client assignPartition -client client_name -partition partition_name
```

4. Verify the enrollment as follows:

   Log in to Oracle Key Vault as the support user using SSH:

   ```
   $ ssh support@okv_instance_ip_address
   support$ su root
   root# cd /usr/safenet/lunaclient/bin
   root# ./vtl verify
   ```

   The following output appears:

   ```
   The following Luna SA Slots/Partitions were found:

   Slot    Serial #        Label
   ====    ==========      =====
    1      serial_number   partition_name
   ```

4.2.4 HSM Provider Value for SafeNet

For SafeNet, the provider value is 1.

If you are setting this value manually for primary-standby, set `HSM_PROVIDER="1"` in the `okv_security.conf` file. For more information about enabling HSM in a primary-standby deployment, see Enabling HSM in a High Availability Deployment.

4.2.5 HSM Vendor Specific Checks for SafeNet

You should check the SafeNet vendor-specific settings.

You can verify the connection to the HSM for every Oracle Key Vault server as follows:

Log in to the Oracle Key Vault server as user `support` using SSH:

```
$ ssh support@okv_instance_ip_address
support$ su root
root# cd /usr/safenet/lunaclient/bin
root# ./vtl verify
```

The following output appears when the HSM is set up properly:

```
The following Luna SA Slots/Partitions were found:

Slot    Serial #        Label
====    ========        =====
 1      [serial #]      [partition name]
```

If you do not see this output, then it means that the HSM is not set up properly. You can diagnose further as follows:

1. Log into the Luna SA administrative console.
2. Type the command: `client show -client` *`client_name`*
3. Verify that the expected client exists and is assigned a partition.
4. If it does not exist, register the client with the command:

   `client register -client` *`client_name`*`-hostname` *`host_name`*
5. If no partition is assigned, assign a partition with the command:

   `client assignPartition -client` *`client_name`* `-partition` *`partition_name`*
6. Verify that all client IP addresses are mapped correctly. If entries are missing, run the command:

   `client hostip map -c` *`client_name`* `-i` *`ip_address`*
7. Verify that Oracle Key Vault can reach the HSM using the `vtl verify` command:

   ```
   $ su root
   root# cd /usr/safenet/lunaclient/bin
   root# ./vtl verify
   ```

   The output should look similar to the following output:

   ```
   The following Luna SA Slots/Partitions were found:

   Slot    Serial #        Label
   ====    ========        =====
    1      [serial #]      [partition name]
   ```

   If the command fails, then it means that the Oracle Key Vault server is unable to contact the HSM. Check the vendor’s other troubleshooting sections for instructions to restore `vtl verify` functionality. Contact your HSM administrator and confirm that Oracle Key Vault's access to the HSM has not been revoked. If you are unable to resolve the problem, then contact Oracle Support.

4.3 Vendor Specific Notes for nCipher

You can integrate Oracle Key Vault release 12.2 BP 3 and later with the HSM from nCipher nShield Connect 6000+.

- Installing the HSM Client Software on the Oracle Key Vault Server for nCipher
  The nCipher HSM requires a separate non-HSM computer on the network to use as the remote file system.
- HSM Credential for nCipher
  The HSM credential is the Operator Card Set password.
- Enrolling Oracle Key Vault as a Client of an nCipher HSM
  You use both the nCipher user interface and the command line to enroll Oracle Key Vault as a client of an nCipher HSM.

- HSM Provider Value for nCipher
  For nCipher, the provider value is 2.
- Enabling HSM Instances for nCipher
  After installing HSM software and enrolling Oracle Key Vault as an HSM client, you can enable an nCipher HSM for an Oracle Key Vault instance.
- Backup Operations for nCipher
  You can back up the Oracle Key Vault server in HSM mode.
- Restore Operations for nCipher
  You can restore an Oracle Key Vault server from a backup for nCipher.
- HSM in a Primary-Standby Oracle Key Vault Installation for nCipher
  You can pair two Oracle Key Vault servers in that have HSM-enabled nodes in a primary-standby configuration for nCipher.
- HSM Upgrades Using nCipher
  You can only upgrade while HSM-enabled when you upgrade from Oracle Key Vault release 18.1 and later to a higher version.

4.3.1 Installing the HSM Client Software on the Oracle Key Vault Server for nCipher

The nCipher HSM requires a separate non-HSM computer on the network to use as the remote file system.

You must set up this computer and copy the nCipher software files to it before you start.

1. Log in to the Oracle Key Vault server as support user using SSH:

   ```
   $ ssh support@okv_instance_ip_address
   ```

2. Switch to `root`:

   ```
   support$ su root
   ```

3. Go to the `root` directory and create the directories `ctls`, `hwsp`, and `pkcs11`:

   ```
   root# cd /root
   root# mkdir ctls
   root# mkdir hwsp
   root# mkdir pkcs11
   ```

4. Transfer the nCipher software installation files using the Secure Copy (SCP) protocol as follows:

   For example:

   ```
   root# scp user@remote_file_system_computer:/source_directory/ncipher/nfast/ctls/
   agg.tar ctls
   root# scp user@remote_file_system_computer:/source_directory/ncipher/nfast/hwsp/
   agg.tar hwsp
   root# scp user@remote_file_system_computer:/source_directory/ncipher/nfast/
   pkcs11/user.tar pkcs11
   ```

5. Install these files as follows:

   ```
   root# cd /
   root# tar xvf /root/ctls/agg.tar
   root# tar xvf /root/hwsp/agg.tar
   ```

```
root# tar xvf /root/pkcs11/user.tar
root# /opt/nfast/sbin/install
```

6. As `root`, perform additional edits on the Oracle Key Vault server:

   ```
   root# usermod -a -G nfast oracle
   root# cd /etc/rc.d/rc5.d
   root# mv S50nc_hardserver S40nc_hardserver
   root# cd /etc/rc.d/rc3.d
   root# mv S50nc_hardserver S41nc_hardserver
   ```

7. Switch to user `oracle` and verify the installation:

   ```
   root# su oracle
   oracle$ PATH=/opt/nfast/bin:$PATH
   oracle$ export PATH
   oracle$ enquiry
   ```

   The state should say `operational` in the output.

8. Restart Oracle Key Vault for the group change to take effect.

   In the Oracle Key Vault management console, log in as a user with the System Administrator role. Select the **System** tab, and then select **System Settings**. Then click the **Reboot** button.

4.3.2 HSM Credential for nCipher

The HSM credential is the Operator Card Set password.

4.3.3 Enrolling Oracle Key Vault as a Client of an nCipher HSM

You use both the nCipher user interface and the command line to enroll Oracle Key Vault as a client of an nCipher HSM.

1. Log in to the nCipher user interface as an HSM administrator.
2. Add the Oracle Key Vault server IP address to the client list on the HSM using the front panel. Select privileged on any port.
   - In a primary-standby environment, register both the primary server and the standby server to use the nCipher HSM.
   - In a multi-master cluster environment, register each Oracle Key Vault node that will use the nCipher HSM.
3. Switch to user `oracle`:

   ```
   root# su oracle
   oracle$ PATH=/opt/nfast/bin:$PATH
   oracle$ export PATH
   ```

4. On the Oracle Key Vault server, enroll with the HSM :

   ```
   oracle$ nethsmenroll hsm_ip_address hsm_esn hsm_keyhash
   ```

5. Configure the TCP sockets:

   ```
   oracle$ config-serverstartup --enable-tcp --enable-privileged-tcp
   ```

6. Switch to `root` and restart the hardserver (nCipher client process that communicates with the HSM):

```
oracle$ su root
root# /opt/nfast/sbin/init.d-ncipher restart
```

7. On the remote file system computer, run the following command:

   ```
   $ rfs-setup --gang-client --write-noauth okv_server_ip_address
   ```

8. On the Oracle Key Vault server as user `oracle`, run the following commands:

   ```
   oracle$ rfs-sync --setup --no-authenticate remote_file_system_ip_address
   oracle$ rfs-sync --update
   ```

9. Test PKCS#11 access as follows:

   ```
   root# /opt/nfast/bin/ckcheckinst
   ```

   A prompt appears listing the module. You can confirm or exit.

10. Create the config file `/opt/nfast/cknfastrc` as user `root`. Write the following lines to the file:

    ```
    CKNFAST_NO_ACCELERATOR_SLOTS=1
    CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm
    ```

11. Perform the steps described in Protecting the Oracle Key Vault TDE Master Key with the HSM.

12. On the Oracle Key Vault server as user `oracle` run the command:

    ```
    oracle$ /opt/nfast/bin/rfs-sync --commit
    ```

4.3.4 HSM Provider Value for nCipher

For nCipher, the provider value is 2.

If you are setting this value manually for the primary-standby, then set `HSM_PROVIDER="2"`. For more information about enabling HSM in a primary-standby deployment, see Enabling HSM in a High Availability Deployment.

4.3.5 Enabling HSM Instances for nCipher

After installing HSM software and enrolling Oracle Key Vault as an HSM client, you can enable an nCipher HSM for an Oracle Key Vault instance.

Use the Oracle Key Vault management console to enable the nCipher HSM.

1. Log into the Oracle Key Vault management console as a user with the System Administrator role.
   For a multi-master cluster environment, log in to each Oracle Key Vault node where you want to enable the HSM.
2. Click the **System** tab.
3. Click **Hardware Security Module** in the left sidebar.
   The Hardware Security Module page appears. The red downward arrow shows the non-initialized **Status**. The **Type** field displays **None**
4. Click **Initialize**.
5. In the Initialize HSM page, do the following:
   - From the **Vendor** menu, select **nCipher**.

   - Enter and then reenter the HSM credential for the nCipher HSM, which is the Operator Card Set password.
   - Enter the Oracle Key Vault recovery passphrase.

6. Click **Initialize**.

4.3.6 Backup Operations for nCipher

You can back up the Oracle Key Vault server in HSM mode.

1. Install a new Oracle Key Vault server.
2. Install the nCipher HSM software.
3. From the Oracle Key Vault user interface add the backup destination on the **System Backup** page, just as you would in for a node that is not HSM enabled.
4. Perform a backup as usual from the user interface on the management console.

Related Topics

- Installing the HSM Client Software on the Oracle Key Vault Server for nCipher
  The nCipher HSM requires a separate non-HSM computer on the network to use as the remote file system.

4.3.7 Restore Operations for nCipher

You can restore an Oracle Key Vault server from a backup for nCipher.

1. Log in to the Oracle Key Vault management console as a user who has the System Administrator role.
2. Click the **System** tab.
3. Click **Hardware Security Module** in the left sidebar.
4. Click **Set Credential** to display the Prepare for HSM Restore page.
5. Select nCipher from the **Vendor** drop down list and enter the HSM credential twice as requested.

   The HSM credential for nCipher is the Operator Card Set password.
6. Click **Set Credential**.
7. Log in to the Oracle Key Vault Server through SSH as user `support`, switch user (`su`) to `root`, then switch user (`su`) to `oracle`.

   ```
   $ ssh support@okv_instance_ip_address
   support$ su root
   root# su oracle
   ```
8. Run the following command, which retrieves information from the remote file system:

   ```
   oracle$ /opt/nfast/bin/rfs-sync --update
   ```
9. Restore using the Oracle Key Vault management console as you would for a node that is not HSM enabled.

Related Topics

- Restore Operations in an HSM-Enabled Oracle Key Vault Instance
  Only backups made to an HSM-enabled Oracle Key Vault instance can be restored onto an HSM-enabled Oracle Key Vault instance.
- *Oracle Key Vault Administrator's Guide*

4.3.8 HSM in a Primary-Standby Oracle Key Vault Installation for nCipher

You can pair two Oracle Key Vault servers in that have HSM-enabled nodes in a primary-standby configuration for nCipher.

You must HSM-enable the nodes in both primary and standby Oracle Key Vault servers before pairing them. To configure the HSM for primary-standby, please see the vendor documentation.

1. Install Oracle Key Vault on two servers that you mean to designate as primary and standby.
2. Install the nCipher HSM software on each Oracle Key Vault server.
3. On the server to be used as the primary server, do the following:
   - Log in to the designated Oracle Key Vault primary server through SSH as user `support`, switch user (`su`) to `root`, then switch user (`su`) to `oracle`:

     ```
     $ ssh support@okv_primary_instance_ip_address
     support$ su root
     root# su oracle
     ```

   - Run the following command:

     ```
     oracle$ /opt/nfast/bin/rfs-sync --update
     ```

4. From the user interface on the Oracle Key Vault management console initialize the intended primary server for the nCipher HSM-enabled node.
5. On the server to be used as the primary server, do the following:
   - Log in to the designated Oracle Key Vault Primary Server through SSH as user `support`, switch user (`su`) to `root`, then switch user (`su`) to `oracle`:

     ```
     $ ssh support@okv_primary_instance_ip_address
     support$ su root
     root# su oracle
     ```

   - Run the following command:

     ```
     oracle$ /opt/nfast/bin/rfs-sync --commit
     ```

6. Repeat Step 3 on the intended standby server.
7. Perform the following manual steps on the intended primary as user `oracle`:

   ```
   $ ssh support@okv_primary_instance_ip_address
   support$ su root
   root# su oracle
   oracle$ cd /usr/local/okv/hsm/wallet
   oracle$ scp cwallet.sso support@standby:/tmp
   oracle$ scp enctdepwd support@standby:/tmp
   oracle$ cd /usr/local/okv/hsm/restore
   oracle$ scp ewallet.p12 support@standby:/tmp
   ```

8. Perform the following manual steps on the intended standby as user `root`:

   ```
   $ ssh support@okv_standby_instance_ip_address
   support$ su root
   root# cd /usr/local/okv/hsm/wallet
   root# mv /tmp/enctdepwd .
   root# mv /tmp/cwallet.sso .
   root# chown oracle *
   root# chgrp oinstall *
   root# cd /usr/local/okv/hsm/restore
   root# mv /tmp/ewallet.p12 .
   root# chown oracle *
   root# chgrp oinstall *
   ```

   > **Note:**
   >
   > While performing this procedure on Oracle Key Vault 12.2.0.5.0 and earlier, use the commands in Enabling an HSM in a Primary-Standby Pre-Release 12.2 Oracle Key Vault Installation.

9. Continuing as user `root`, open the file `okv_security.conf`:

   ```
   root# vi /usr/local/okv/etc/okv_security.conf
   ```

10. Make two updates to the file as follows:

    a. Set the variable `HSM_ENABLED` to 1. If the variable does not exist, add it and set its value to 1.

       ```
       HSM_ENABLED="1"
       ```

    b. Add the following line:

       ```
       HSM_PROVIDER="2"
       ```

11. Proceed to configure the primary-standby environment by using the Oracle Key Vault management console.

Related Topics

- *Oracle Key Vault Administrator's Guide*

4.3.9 HSM Upgrades Using nCipher

You can only upgrade while HSM-enabled when you upgrade from Oracle Key Vault release 18.1 and later to a higher version.

Because HSM configurations can vary, it is your responsibility to run test upgrades on non-production environments to ensure that the upgrade will work with your HSM configuration.

1. Connect as the `root` user.

   ```
   $ ssh support@okv_primary_instance_ip_address
   support$ su root
   ```

2. Execute the steps to upgrade as described in *Oracle Key Vault Administrator's Guide*, up to and including the command where you run the following command:

   ```
   root# /usr/bin/ruby/images/upgrade.rb --confirm
   ```

3. After running `/usr/bin/ruby/images/upgrade.rb --confirm` but *before* you execute the reboot operation, execute the following commands:

   ```
   root# usermod -a -G nfast oracle
   root# cd /etc/rc.d/rc5.d
   root# mv S50nc_hardserver S40nc_hardserver
   root# cd /etc/rc.d/rc3.d
   root# mv S50nc_hardserver S41nc_hardserver
   ```

4. Continue with the upgrade process as described in *Oracle Key Vault Administrator's Guide*.

Related Topics

- *Oracle Key Vault Administrator's Guide*