Oracle® Key Vault

Release Notes

Release 18.2

F25624-01

December 2019

Release Notes

These release notes list the new features for this release of Oracle Key Vault, how to download the latest product software and documentation, and how to address known issues in Oracle Key Vault.

Changes in This Release for Oracle Key Vault

Oracle Key Vault release introduces new features that enhance the use of Oracle Key Vault in a large enterprise.

- Auto-Expiring Persistent Cache on Endpoint Database Shutdown

Oracle Key Vault Server Certificate Rotation

Server certificate in Oracle Key Vault lasts 730 days. If you do not rotate the certificate (both server and endpoint certificates), then the endpoints that use the certificate cannot connect to the Oracle Key Vault server. When this happens, you must rotate the server certificate and re-enroll the endpoint. The rotation process handles the rotation for all certificates in one operation. To avoid this scenario, you can configure an alert to remind you to rotate the certificate before the 730-day limit is up. You can set how early to get the certificate expiration alert by editing the Oracle Key Vault Server Certificate Expiration setting on the Configure Alerts page in the Oracle Key Vault management console. You can find out the expiry times of the Oracle Key Vault server certificate by checking the **Manage Server Certificate** page under **System** tab in the Oracle Key Vault management console. To find the expiry time of the endpoints' certificates, you must navigate to the **Endpoints** page and check the **Certificate Expires** column.

The certificate rotation process captures all certificates in the Oracle Key Vault server. It does not capture third-party certificates.

If you have a primary-standby or multi-master cluster configuration, then Oracle Key Vault automatically synchronizes the certificates in both systems.

Recover the Candidate Node If There Is a Failure or Error During Node Induction

Previously, you could not abort induction of a candidate node. This was a problem if you put in the wrong recovery passphrase, IP address, or certificate of the controller node. There is now an **Abort** button for the candidate node that reverts the candidate to its original pre-candidate state. The candidate node cannot be aborted after it has started to receive bundles from the controller node.

Upgrade Oracle Key Vault Server with HSM as Root of Trust Without the Need to Reverse Migrate

Upgrading an Oracle Key Vault that was HSM-enabled would not proceed for several reasons. First, if Oracle Key Vault was registered as a client of an HSM that it had to contact via hostname, after rebooting, the Oracle Key Vault DNS service,`dnsmasq`, was not running when Oracle Key Vault tried to contact the HSM. This resulted in a failure to open the TDE wallet. There was a workaround for this issue as described for Bug 24478865 that required adding DNS server entries to `/etc/resolv.conf`, but the upgrade process reset this file and so it was not a valid workaround for HSM upgrades. Bug 24478865 has since been resolved and the workaround is no longer necessary. Another issue blocking HSM-enabled Oracle Key Vault upgrades was that for nCipher HSMs, the `hardserver` service was not running when Oracle Key Vault attempted to open the TDE wallet. This resulted in a failure after the reboot during upgrade. We now start the `hardserver` service if necessary before opening the wallet. Upgrading with HSM as the root of trust is available when upgrading from versions of Oracle Key Vault version 18.1 and later.

Limit Reset of User Password to Recovery via Email Only

Oracle Key Vault prevents administrative users from manually changing passwords of other users when secure user management is enabled. Only an option to send a one time password to user's email address is provided.

Related Topics

- Changing Another User's Password

Automatically Update Endpoint Configuration with changes to Reverse-SSH Tunnels in the Cluster

New reverse-ssh tunnels that an endpoint can use but are created after an endpoint was enrolled are automatically added to the endpoint configuration, `okvclient.ora`. With the addition or deletion of a node in the cluster, like other endpoints, the DBCS endpoints' automatically update the list of node IP addresses in the endpoint configuration. Endpoints created on nodes of the cluster that have been deleted will get their endpoint configuration updates from other nodes in the cluster.

New tunnels are not included in `okvclient.ora` for existing endpoints, even if that endpoint could use the tunnel and has since been re-enrolled.

Endpoints created on nodes of the cluster that are then deleted don't receive scan list updates.

HSM as Root of Trust Improvements

This section describes Oracle Key Vault HSM as Root of Trust improvements .

- Validate HSM Setup Periodically
- Improved Error Reporting for HSM Functionality

Validate HSM Setup Periodically

In previous versions of Oracle Key Vault with HSM as Root of Trust, the connectivity to HSM was only validated during the Oracle Key Vault setup. Now the connectivity is checked periodically to validate that the HSM is working properly. If it is not working properly, an **Invalid HSM Configuration** alert is raised.

Improved Error Reporting for HSM Functionality

The following improvements were made to the error handling:

- Reverse migrating from HSM in 18.1 in standalone mode (not cluster and not primary-standby) with the same recovery passphrase for the "old" and "new" recovery passphrase fields displays an improper error message. The "old" and "new" recovery passphrases can now be the same when reverse migrating.

- Generic error messages were received when there was an error while applying the bundle. These error messages were made more specific to better diagnose problems.
- Setting the credential for HSM using the Set Credential button with the same credential twice produced an error. This can now be completed without issues.
- The error message received when creating the HSM bundle with the wrong HSM credential did not indicate the specific problem. The error messages are now more specific as to the cause of the problem.

New and Modified Alerts

This section describes new and modified alerts in Oracle Key Vault.

- New Alerts Added In This Release
- Alerts Modified In This Release

New Alerts Added In This Release

New alerts added in this release of Oracle Key Vault are:

- **Validate HSM Setup Periodically:** If HSM-enabled, verify that the HSM configuration is valid and working properly. If it is not working properly, an Invalid HSM Configuration alert is raised.
- **Raise an Alert if Replication Lag Is Greater Than Configured Limit:** For multi-master cluster setup, there is a new alert that tracks the replication lag from other nodes to the current node. This alert is raised when replication lag is greater than the specified threshold. The default is 60 seconds.
- **Alerts Are Raised If the Alert Jobs Are Hitting Issues:** In previous versions of Oracle Key Vault, failures to check alert conditions in alert jobs were logged to `syslog` only. Now, when an alert condition check fails, an alert is raised and an email, if configured, is sent. These alerts are cleaned up if the failed alert condition runs fine on subsequent evaluation.

Alerts Modified In This Release

Alerts modified in this release of Oracle Key Vault are:

- **Retain Heartbeat Alerts for Defunct Nodes Until They Are Deleted:** Alerts about a node not contacting another node for greater than the Maximum Disable Node Duration amount of time should not get deleted, even if contact is restored, because some records may have been lost despite restoring replication between the two nodes.
- **Delete Alerts Associated with a Reverse-SSH Tunnel when the Tunnel Is Deleted:** SSH tunnel alerts were not deleted when the SSH tunnel was deleted. The alerts are now deleted when the tunnel is deleted.
- **Alerts Raised on Switchover Are Not Deleted When the Primary-Standby Are Unpaired:** Alerts from primary-standby configurations could still be seen after unpairing. The alerts are now deleted after unpairing.

Endpoint Software Installation Logs Environment Variables For Later Diagnostics

The PKCS#11 library used by Oracle Database endpoints makes use of environment variables like ORACLE_HOME, ORACLE_BASE, and OKV_HOME to look up the endpoint configuration file, `okvclient.ora`. The environment variables might change over time which may result in the creation of multiple persistent caches and/or the failure of database sessions or the background processes to find the endpoint configuration file.

To facilitate a quick diagnosis, additional information about ORACLE_HOME, ORACLE_BASE, and OKV_HOME when deploying `okvclient.jar` is included in the deployment log. This should be consistent across database processes that use PKCS#11 library. This information is available in the log file and if the `-v` option is used when deploying `okvclient.jar` it is also printed to standard output.

RESTful Services Improvements

This section describes improvements to RESTful services in Oracle Key Vault.

- KMIP REST Locate Supports Filtering by Key Name
- Re-Enroll All Endpoints With a Single RESTful Command
- New wallet_root Option for the REST Provision Command

KMIP REST Locate Supports Filtering by Key Name

Given a human readable name of the KMIP object, users can find the KMIP identifier associated with the object. Oracle Key Vault RESTful service now provides the `-name` option in the `locate` command to retrieve KMIP UUID more easily because the UUID is difficult to remember. Once you get the UUID by using the `-name` option using the `locate` command, you can use this UUID in other KMIP REST calls.

Re-Enroll All Endpoints With a Single RESTful Command

In Oracle Key Vault deployments with large number of endpoints, re-enrolling all endpoints one by one, even with the RESTful API, may be time consuming. Oracle Key Vault provides a single RESTful command to re-enroll all endpoints. The new RESTful command is `re_enroll_all`.

New wallet_root Option for the REST Provision Command

A new `wallet_root` option has been added to the RESTful service `provision` command. Unlike the `dir` option, it doesn't create the endpoint name directory. As a result, user can provide the TDE `WALLET_ROOT` root directory with this option. The user can choose between the `wallet_root` option or the `dir` option, based on requirement.

Related Topics

- About Configuring Transparent Data Encryption

Refresh Cached OKV Configuration Periodically In Long Running Processes

In releases prior to OKV 18.2, the endpoint database's `gen0` process didn't pick up new `okvclient.ora` values periodically. As a result, changes to `okvclient.ora` parameters (such as the SERVER list, PKCS11_CACHE_TIMEOUT, PKCS11_PERSISTENT_CACHE_TIMEOUT, PKCS11_PERSISTENT_CACHE_REFRESH_WINDOW, etc.) were not picked up even when the key was refreshed from Oracle Key Vault. Now, per process, if the time since `okvclient.ora` was last read is greater than the new PKCS11_CONFIG_PARAM_REFRESH_INTERVAL value, in minutes, the next time that an in-memory cache key expires and has to be refreshed either from the persistent cache or from the Oracle Key Vault server, `okvclient.ora` is re-read and the changed values are uptaken by the process.

Auto-Expiring Persistent Cache on Endpoint Database Shutdown

Installing the OKVclient without a password configures the persistent cache as an auto-open wallet. Installing the OKVclient with a password applies this password also to the persistent cache. The new option to create an auto-expiring persistent cache protects the persistent cache with an automatically generated password that is not known to anyone, therefore it cannot be opened after database restart or OS restart.

Downloading the Oracle Key Vault Software and the Documentation

At any time, you can download the latest version of the Oracle Key Vault software and documentation.

- Downloading the Oracle Key Vault Installation Software
- Downloading the Oracle Key Vault Documentation

Downloading the Oracle Key Vault Installation Software

For a fresh installation, you can download the Oracle Key Vault software from the Software Delivery Cloud. You cannot use this package to upgrade Oracle Key Vault. For an upgrade from an existing Oracle Key Vault 12.2 deployment, you can download the Oracle Key Vault upgrade software from the My Oracle Support website.

1. Use a web browser to access the Oracle Software Delivery Cloud portal:

   https://edelivery.oracle.com

2. Click **Sign In**, and if prompted, enter your **User ID** and **Password**.
3. In the **All Categories** menu, select **Release**. In the next field, enter **Oracle Key Vault** and then click **Search**.

4. From the list that is displayed, select **Oracle Key Vault 18.2.0.0.0** or click the **+Add to Cart** button next to the **Oracle Key Vault 18.2.0.0.0**.

   The download is added to your cart. (To check the cart contents, click **View Cart** in the upper right of the screen.)

5. Click **Checkout**.

6. On the next page, verify the details of the installation package, and then click **Continue**.

7. In the **Oracle Standard Terms and Restrictions** page, after you have read the terms and restrictions and agree with them, select **I have reviewed and accept the terms of the Commercial License, Special Programs License, and/or Trial License**, and click **Continue**.

   The download page appears, which lists the following Oracle Key Vault ISO files:

   - V*part_number*.iso (Oracle Key Vault 18.2.0.0.0 - Disc 1)
   - V*part_number*.iso (Oracle Key Vault 18.2.0.0.0 - Disc 2)

8. To the right of the **Print** button, click **View Digest Details**.

   The listing for the two ISO files expands to display the SHA-1 and SHA-256 checksum reference numbers for each ISO file.

9. Copy the SHA-256 checksum reference numbers and store them for later reference.

10. Click **Download** and select a location to save the ISO files.

    You can save each file individually by clicking its name and then specifying a location for the download.

11. Click **Save**.

    The combined size of both ISO files exceeds 4 GB, and will take time to download, depending on the network speed. The estimated download time and speed are displayed in the **File Download** dialog box.

12. After the ISO files are downloaded to the specified location, verify the SHA-256 checksums of the downloaded files:

    a. From a Linux or Unix machine, generate a SHA256 checksum for the first V*part_number*.iso:

       ```
       $ sha256sum Vpart_number.iso
       ```

       Ensure that the checksum matches the value that you copied from the **File Download** dialog box in step 9.

    b. Generate a SHA-256 checksum for the second V*part_number*.iso:

       ```
       $ sha256sum Vpart_number.iso
       ```

       Ensure that the checksum matches the value that you copied from the **File Download** dialog box in step 9.

13. Optionally, burn each of the two V*part_number*.iso files to a DVD-ROM disc and then label the discs:
    - OKV 18.2 Disc 1
    - OKV 18.2 Disc 2

You can now install Oracle Key Vault on a server machine.

Downloading the Oracle Key Vault Documentation

1. Access the Oracle documentation site.

   https://docs.oracle.com/en/database/
2. Select **Oracle Database Related Products**.
3. In the Database Security section, search for and download the most current version of the Oracle Key Vault 18.2 documentation, including these release notes.

Known Issues

At the time of this release, there are issues with Oracle Key Vault that could occur in rare circumstances. For each issue, a workaround is provided.

- General Issues
- Upgrade Issues
- Primary-Standby Issues
- Multi-Master Cluster Issues

General Issues

This section describes general Oracle Key Vault issues.

- On HP-UX System, SELECT FROM V$ENCRYPTION_KEYS May Return ORA-28407 Occasionally
- OKV 12.2 BP1: User Gets Locked and Expired with Multiple Failed Logins
- OKV Alerts Still Show in the List After Fixing the Problem
- Private Keys Are Not Overwritten When a Java Keystore Is Uploaded Using the -o Option of the okvutil Utility
- HSM Credentials Are Asked While Creating Bundle Even When HSM Is Not Initialized

On HP-UX System, SELECT FROM V$ENCRYPTION_KEYS May Return ORA-28407 Occasionally

Issue: On HP-UX operating system, a Transparent Data Encryption (TDE) query such as the following that is executed in a long-running database process or session may occasionally result in an `ORA-28407 Hardware Security Module error detected` error:

```
SELECT * FROM V$ENCRYPTION_KEYS;
```

This is because the system could not create another thread-specific data key because the process had reached or exceeded the system-imposed limit on the total number of keys per process, which is controlled by the `PTHREAD_KEYS_MAX` setting. `PTHREAD_KEYS_MAX` is typically set to `128`.

Workaround: Switch the database sessions and execute the TDE query again. If it is not convenient to switch the sessions, then set `PTHREAD_USER_KEYS_MAX` to `16384` before starting the database and the listener.

Bug Number: 28270280

OKV 12.2 BP1: User Gets Locked and Expired with Multiple Failed Logins

Issue: The current password policy locks the user account for a day if the user has incorrectly entered the password more than three consecutive times. Therefore, the user will be able to log in only after the 24-hour lockout period expires.

Workaround: Make a note of the password and keep it accessible and secure.

Bug Number: 23300720

OKV Alerts Still Show in the List After Fixing the Problem

Issue: User password expiration alerts are still showing even after the user changes their password.

Workaround: In the Oracle Key Vault management console, select **Reports** and then **Configure Reports**. Then uncheck the **User Password Expiration** option. Alternatively, ignore the alert.

Bug Number: 27620622

Private Keys Are Not Overwritten When a Java Keystore Is Uploaded Using the -o Option of the okvutil Utility

Issue: When you upload a Java keystore (JKS) or Java Cryptography Extension keystore (JCEKS) to the Oracle Key Vault server using the `-o` option of the `okvutil upload` command, user-defined keys are not overwritten.

Workaround: Remove the private key from the wallet and then upload the keystore again.

Bug Number: 26887060

HSM Credentials Are Asked While Creating Bundle Even When HSM Is Not Initialized

Issue: HSM credentials are not used nor necessary when creating the HSM bundle when Oracle Key Vault is not integrated with an HSM, however they are required from the UI regardless.

Workaround: Provide the most recent HSM credential when creating the HSM bundle even when the Oracle Key Vault is not integrated with an HSM.

Bug Number: 30539386

Upgrade Issues

This section describes issues related to upgrading Oracle Key Vault.

Unpair of Upgraded Primary-Standy OKV 18.2 Servers May Fail Due to Permission Issues

Issue: After having completed an upgrade to Oracle Key Vault 18.2, attempting to unpair from a primary-standby configuration sometimes fails, with the following messages written out to the /var/log/debug files:

```
ORA-48141: error creating directory during ADR initialization: [/var/lib/oracle/diag/
rdbms/dbfwdb/dbfwdb/metadata_pv]
ORA-48189: OS command to create directory failed
```

Workaround: Before attempting an unpair in a Primary-Standby configuration that has been upgraded to Oracle Key Vault 18.1, please ensure that the `/var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb/metadata_pv` directory has the right permissions using the steps below:

1. Log into the primary Oracle Key Vault system as user `support` through ssh.
2. Switch to user `root`.

   ```
   su - root
   ```
3. Check the permissions on directory `/var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb/metadata_pv`.

   ```
   ls -l /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb
   ```

   The output should be similar to this output.

   ```
   drwxr-xr-x 2 root   oinstall  4096 Apr 24 22:01 metadata_pv
   ```
4. If the directory is owned by user `root`, as shown above, execute the following command:

```
chown oracle:oinstall /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb/metadata_pv
```

List the file and verify that the owner is now `oracle`.

```
ls -l /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb
```

The output should be similar to this output.

```
drwxr-xr-x 2 oracle oinstall 4096 Apr 24 22:01 metadata_pv
```

Bug Number: 29693700

OKV SYSTEMS That Were Unpaired Before Being Upgraded Need a DB_UNIQUE_NAME Reset

Issue: Oracle Key Vault systems that were part of an Oracle Key Vault 12.2 high availability (now primary-standby) configuration before being unpaired, and then upgraded, have their DB_UNIQUE_NAME parameters set to 'DBFWDB_HA1' or 'DBFWDB_HA2'. This parameter needs to be reset to 'DBFWDB' before the system is converted to cluster mode, as attempting to add the node to a cluster would otherwise fail.

Workaround: For a system that was the primary server in an Oracle Key Vault 12.2 high availability configuration, and then unpaired before being upgraded to Oracle Key Vault 18.2, the following commands need to be run on the system after successful upgrade and before it is converted to a cluster node:

1. Log into the primary Oracle Key Vault system as user `support` through ssh.
2. Switch to user `root`.

   ```
   su - root
   ```

3. Check the owner and group on directory `/var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb/metadata_pv`.

   ```
   ls -l /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb
   ```

   The output should be similar to this output.

   ```
   drwxr-xr-x 2 root   oinstall  4096 Apr 24 22:01 metadata_pv
   ```

4. If the directory is owned by user `root`, as shown above, execute the following command:

   ```
   chown oracle:oinstall /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb/metadata_pv
   ```

   List the file and verify that the owner is now `oracle`.

   ```
   ls -l /var/lib/oracle/diag/rdbms/dbfwdb/dbfwdb
   ```

   The output should be similar to this output.

   ```
   drwxr-xr-x 2 oracle oinstall 4096 Apr 24 22:01 metadata_pv
   ```

5. Switch to user `oracle`.

   ```
   su oracle
   ```

6. Start SQL*Plus.

```
sqlplus / as sysdba
```

7. Execute the following statement:

```
show parameter db_unique_name;
```

8. If the `DB_UNIQUE_NAME` is something other than `DBFWDB`, then execute the following statements:

```
alter system set db_unique_name='DBFWDB' scope=spfile;
exit
```

9. As user `root`, execute the following commands:

```
service dbfwdb stop
service dbfwdb start
```

10. Verify that the `DB_UNIQUE_NAME` parameter has changed.
Start SQL*Plus.

```
sqlplus / as sysdba
```

11. Execute the following statement:

```
show parameter db_unique_name
```

The output returned should match the output shown here.

```
NAME                 TYPE        VALUE
-------------------- ----------- -----------
db_unique_name       string      DBFWDB
```

Bug Number: 29696058

Primary-Standby Issues

This section describes Oracle Key Vault issues specific to a primary-standby configuration.

- OKV 12.2 BP8: Audit Trail is not Sent To Remote Syslog on Switchover in HA Pair
- OKV 12.2 BP2: SSH Tunnel Status Shows as Disabled on Failover Case in HA
- Re-pair After Un-pair from HA 12.2 BP5 to new OKV Server Still Shows Standalone
- Failover Issues When Primary OKV Experiences a Controlled Shutdown
- HA Setup Succeeds with Different Primary & Standby RO Restricted Mode Config

OKV 12.2 BP8: Audit Trail is not Sent To Remote Syslog on Switchover in HA Pair

Description: With syslog configured on the primary, the audit logs are also written to the syslog. On switchover, the audit logs may not be written to the syslog. This is because the syslog has not been configured on the standby. Syslog needs to be configured on primary and standby separately.

Workaround: Configure the syslog on standby after switchover to enable write of audit logs to syslog.

Bug Number: 28790364

OKV 12.2 BP2: SSH Tunnel Status Shows as Disabled on Failover Case in HA

Issue: After a failover operation, the new Oracle Key Vault primary server does not show the correct status of the SSH tunnel. It shows the SSH tunnel as disabled when the SSH tunnel is available. The dashboard also shows an alert, warning that the setup of an SSH tunnel failed. This is because after the failover operation, Oracle Key Vault tried to establish two SSH tunnels to the same database as a service endpoint, resulting in the incorrect status and dashboard alert. The second SSH tunnel to the database as a service endpoint does not affect connectivity between the Oracle Key Vault server and the database as a service endpoint. The first SSH tunnel to the database as a service endpoint is functional and available after the failover.

Workaround: After a failover, the new Oracle Key Vault primary server shows the correct SSH status as available and connected to the database as a service endpoints. You also can use the `okvutil list` on the database as a service endpoint to check the status of the SSH tunnel.

Bug Number: 24679516

Re-pair After Un-pair from HA 12.2 BP5 to new OKV Server Still Shows Standalone

Issue: When an unpaired Oracle Key Vault primary server running Oracle Key Vault 12.2.0.5.0 or later is paired with a newly installed Oracle Key Vault server, the **Current status** on the **Primary-Standby** page shows that the server is in standalone mode. The Standalone status indicates that the primary-standby configuration has failed. The primary-standby setup fails because the SSH configuration on the primary server is not re-enabled.

Workaround: Before pairing an unpaired Oracle Key Vault primary server running Oracle Key Vault, disable and re-enable the SSH configuration. You should disable and then re-enable the SSH configuration after you perform the primary-standby configuration on the primary server after unpairing it with the standby server.

> **Note:**
>
> Before pairing an unpaired Oracle Key Vault primary server running Oracle Key Vault, ensure that you have closed all other browser instances.

Bug Number: 26617880

Failover Issues When Primary OKV Experiences a Controlled Shutdown

Issue: Periodically, the primary Oracle Key Vault server in a primary-standby pair has a controlled shutdown. For example, a user performs the shutdown by pressing a

power off button in the user interface or executes the shutdown command from the terminal. When this happens, there will be no failover operation and the standby Oracle Key Vault server will not take over as the primary server. This can be predicted by the existence of the file `/var/lock/subsys/dbfwdb` on the primary Oracle Key Vault server. If the file exists on the primary at the time of the controlled shutdown, there will not be a failover. If it does not exist, then a failover should occur.

Note that failover still does occur in other situations such as power loss on the primary or database failure, regardless of the file's existence.

Workaround: If performing a controlled shutdown in an attempt to cause the standby to take over as the new primary, instead perform a switchover.

Bug Number: 29666606

HA Setup Succeeds with Different Primary & Standby RO Restricted Mode Config

Issue: For a primary-standby configuration, if read-only restricted mode is enabled on one Oracle Key Vault server and not on the other Oracle Key Vault server, then the configuration succeeds. This mismatch can lead to issues and confusion in a primary-standby deployment.

Workaround: Use the Oracle Key Vault management console to ensure that both servers have the same read-only restricted mode state applied. To do so, select the **System** tab, then **Primary-Standby**. Select the **Allow Read-Only Restricted Mode** option. Only then apply the primary-standby configuration on each server.

Bug Number: 26536033

Multi-Master Cluster Issues

This section describes Oracle Key Vault issues specific to a multi-master cluster configuration.

Replication May Fail to Resume After Multiple System Failures in OKV Cluster

Issue: Due to GoldenGate Bug 29624366, after multiple system failures in an Oracle Key Vault cluster, replication from some nodes may fail to resume. Specifically, GoldenGate replicats will terminate and not be able to process new change logs in the GoldenGate trail file when it happens.

Workaround: Manually reposition such replicats to skip erroneous records in the trail file or forcefully delete the troubled Oracle Key Vault nodes from the cluster and add new nodes to replace them.

Bug Number: 29700647

System Settings Changed on an OKV System After Conversion to a Candidate Node Do Not Reflect On The Controller Node

Issue: If system settings are changed on an Oracle Key Vault system after it has been converted to a candidate node, and after the controller node's initial attempt to verify the candidate node's settings has failed, the updated settings do not reflect on the controller node. The pairing process must be aborted and the candidate node re-installed.

Workaround: None. Verify that the Oracle Key Vault system's settings match with those of the cluster before attempting to convert it into a candidate node and induct it into a cluster.

Bug Number: 29430349

Read-Write Nodes in Read-Only Restricted Mode After a Reboot

Issue: After rebooting a read-write node, sometimes the node or its read-write peer will become stuck in Read-Only Restricted Mode.

Workaround: When you reboot a node, it is normal for a node's read-write peer node to temporarily become in read-only restricted mode. However, soon after the node finishes booting, the read-write peer should transition back to read-write mode within a few minutes. The node that was rebooted may come up in read-only restricted mode, but should also transition back to read-write mode within a few minutes. However, if either a node or its read-write peer does not leave read-only restricted mode, redo shipping may be stuck. It may be fixed by rebooting the node still in read-only restricted mode.

Bug Number: 30589921

RMAN Automatically Cleans Up Archivelogs Still Necessary for OGG

Issue: RMAN automatically manages the archivelogs in the fast recovery area. Under normal circumstances, RMAN will not delete archivelogs that may still be needed by Oracle GoldenGate. However, under space pressure, RMAN may clean up the needed archivelogs. These archivelogs getting cleaned up will break replication from the current node to all other nodes except the node's read-write peer node. Oracle Key Vault attempts to mitigate this issue by performing regular clean up of the fast recovery area, but under rare circumstances, the fast recovery area may be filled up and this issue may occur.

Workaround: Identify the source of space pressure in the fast recovery area and remedy the issue. You may identify space pressure in the fast recovery area by keeping tabs on the disk space. The fast recovery area is located under `/var/lib/oracle/fast_recovery_area/`.

Bug Number: 30558372

Oracle Key Vault Should Prevent Enabling From Finishing If Takes Longer Than MDND

Issue: If you enable or disable an Oracle Key Vault node before the Maximum Disable Node Duration time limit, but the enabling does not finish before the Maximum Disable Node Duration time limit expires, it is possible that there could be cleanup of archivelogs and trail files that would cause inconsistency in the cluster. Don't allow the enabling process to finish in this case.

Workaround: Delete or force delete the node from the cluster if it takes longer than the Maximum Disable Node Duration amount of time to finish enabling.

Bug Number: 30533066

Certificate Must Be Rotated Before Converting To Cluster If Upgrading From 12.2 BP4 or Older

Issue: If you attempt to upgrade to Oracle Key Vault 18.2 from Oracle Key Vault 12.2 BP4 through 18.1 and do no generate a new certificate before the upgrade, you will receive the following error message:

```
Failed to convert server to cluster node, detected use of weak signature
algorithms in OKV server credentials. Please perform a certificate
rotation operation before converting this server to a cluster node.
```

Workaround: Generate a new certificate before attempting the upgrade to Oracle Key Vault 18.2.

Bug Number: 30673249

Oracle Key Vault Considerations

Below are details and changes of behavior of Oracle Key Vault 18.2.

- Oracle TDE and Oracle Key Vault Integration
- Reports are Affected by Audit Replication in a Multi-Master Cluster
- Updates in a Multi-Master Cluster are Slower Than in a Single Instance

Oracle TDE and Oracle Key Vault Integration

Depending on the Oracle Database version used and on the feature of TDE used, there might be a need to patch the Oracle database for smooth operations.

Refer to the MOS-NOTE with Doc ID 2535751.1 to ascertain if your deployment needs a database patch.

The MOS-NOTE lists known issues with Oracle Database Transparent Data Encryption (TDE) feature when it is configured to use Oracle Key Vault as the keystore. The document also lists the fixes that resolve the issues enabling smoother integration between Oracle Database TDE and Oracle Key Vault. The issues could be defects, reducing the user burden with simplified operations, or improving the integration between TDE and OKV. The document is for Database Administrators and others tasked with managing the TDE Master Keys with Oracle Key Vault.

Reports are Affected by Audit Replication in a Multi-Master Cluster

Oracle Key Vault reports and details in the home page are generated from Oracle Key Vault audit records. Each node will show reports of the operations specifically done on that node if audit replication is turned off. Each node will show reports of the operations done on all nodes in the cluster if audit replication is turned on.

The recommendation is to turn off audit replication and use a security information and event management (SIEM) solution like Oracle Audit Vault and Database Firewall (AVDF) to collect audit records from all nodes.

Updates in a Multi-Master Cluster are Slower Than in a Single Instance

An update in a multi-master cluster might check for an object's existence, which may result in a scan of all nodes in the cluster slowing down the update operation. The time will increase proportional to the number of nodes in the cluster. The update could take several minutes to complete.

Setting and rotating the TDE master encryption key are examples of update operations.

Supported Database Versions

The following versions of Oracle Database are supported with Oracle Key Vault 18.2:

- Oracle DB 11.2 with the compatible parameter set to 11.2
- Oracle DB 12.1 with the compatible parameter set to 11.2
- Oracle DB 12.2
- Oracle DB 18c
- Oracle DB 19c

Critical Patch Updates Included in Release 18.2.0.0.0

Oracle Key Vault release 18.2 updated the underlying infrastructure to incorporate the October 2019 Release Update for Oracle Database 18 (18.8 DB RU) - October Release Update. Please log in for full details.

https://www.oracle.com/security-alerts/cpuoct2019.html

Oracle Key Vault release 18.2 also includes security and stability fixes for Java and Oracle Linux (OL) operating system.

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.

Oracle® Key Vault Release Notes, Release 18.2
F25624-01