Oracle® Key Vault

Release Notes

Release 18.4

F29539-02

June 2020

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.

- Management Console Idle Session Timeout
  Starting with this release, Oracle Key Vault will detect if the user session is idle, log the user out, and redirect the user to the login screen.
- Utimaco as a Supported HSM Vendor
  Utimaco is now a supported vendor for integration with Oracle Key Vault as the Root of Trust.
- Oracle Key Vault HSM Integration Supports Use of Token Labels
  Oracle Key Vault now provides the ability to choose a softcard slot based on a token label.

Management Console Idle Session Timeout

Starting with this release, Oracle Key Vault will detect if the user session is idle, log the user out, and redirect the user to the login screen.

Starting with Oracle Key Vault release 18.4, Oracle Key Vault will detect if the user's management console session is idle, log the user out, and redirect the user to the login screen. The user's session remains active as long as the user clicks a button, moves the mouse or presses a key, or is performing other management console related activities. If the user's session is idle for more than the management console timeout duration, then the user is logged out and redirected to the login screen.

The management console timeout is configurable and has a default setting of 10 minutes. Before the management console session ends, the user is notified and is given an option to extend the session. The notification is raised 2 minutes before session expiry if the timeout value is 10 minutes or longer. For smaller timeout values, the notification will be raised 10 seconds or 30 seconds prior to session expiry depending on whether the timeout value is less than or greater than 5 minutes respectively. For example, if the timeout was set to 20 minutes, then the user will be notified after 18 minutes of inactivity and can extend the session. After the session is extended, if there is another period of 18 minutes with no activity detected, the user would be requested to extend the session once again. If the user does not extend the session this time, the user is logged out and redirected to login screen.

The management console idle session timeout applies to standalone, primary-standby, and multi-master cluster environments. In a multi-master cluster environment, setting the timeout value in one node applies the value to all nodes in the cluster. The timeout value takes effect after you click **Save** in the **System Settings** page, or click **Save to Cluster** in the **Cluster System Settings** page. Any update to the timeout value affects all new management console sessions immediately but affects the currently active sessions when the user's session is extended, the user refreshes the page, or the user navigates to another page.

Utimaco as a Supported HSM Vendor

Utimaco is now a supported vendor for integration with Oracle Key Vault as the Root of Trust.

Starting with this release, you can configure Utimaco as a supported HSM vendor for integration with Oracle Key Vault, in addition to the current Safenet and nCipher vendors. For both the Hardware Security Modules and associated client-side libraries and tools, only version 4.31.1 is supported at this time.

Related Topics

- Vendor Specific Notes for Utimaco

Oracle Key Vault HSM Integration Supports Use of Token Labels

Oracle Key Vault now provides the ability to choose a softcard slot based on a token label.

HSMs may support multiple tokens each with a token label. You can now specify a token label in order to create or use keys from tokens in specific slots for HSM integration. If you do not specify a token label, Oracle Key Vault will fall back to the previous behavior where it will choose the token in the first slot of the slot list. Token Labels in Oracle Key Vault enable support for softcards in nCipher HSMs, partitions in Thales (Safenet) HSMs, and groups in Utimaco HSMs.

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 deployment, you can download the Oracle Key Vault upgrade software from the My Oracle Support website which includes a `readme` file with upgrade instructions.

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 18.4.0.0.0** or click the **+Add to Cart** button next to the **Oracle Key Vault 18.4.0.0.0**.

   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 18.4.0.0.0 - Disc 1)
   - `V`*`part_number`*`.iso` (Oracle Key Vault 18.4.0.0.0 - Disc 2)
   - `V`*`part_number`*`.iso` (Oracle Key Vault 18.4.0.0.0 - Disc 3)
8. To the right of the **Print** button, click **View Digest Details**.

   The listing for the three 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 three `V`*`part_number`*`.iso` files to a DVD-ROM disc and then label the discs:
    - `OKV 18.4 Disc 1`
    - `OKV 18.4 Disc 2`
    - `OKV 18.4 Disc 3`

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 18.4 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

This section describes general Oracle Key Vault issues.

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

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

Oracle Key Vault Boot-Time Warnings When in FIPS Mode

Issue: When an Oracle Key Vault server operating in FIPS mode is booted, warnings such as the below may be seen on console:

```
Warning : Error inserting
    serpent_avx2(/lib/modules/4.1.12-124.34.1.1.el6uek.x86_64/kernerl/arch/x86/
crypto/serpent_avx2):
    No such device
```

These are informational messages thrown on screen indicating that instruction sets for ciphers that are not available or not supported in FIPS mode are not being loaded. These warnings can be safely ignored.

Workaround: None.

Bug Number: 30844891

Upgrade Issues

This section describes issues related to upgrading Oracle Key Vault.

- Unpair of Upgraded Primary-Standby Oracle Key Vault 18.x Servers May Fail Due to Permission Issues
- OKV SYSTEMS That Were Unpaired Before Being Upgraded Need a DB_UNIQUE_NAME Reset

Unpair of Upgraded Primary-Standby Oracle Key Vault 18.x Servers May Fail Due to Permission Issues

Issue: After having completed an upgrade to the current release of Oracle Key Vault, 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.

   ```
   $ ssh support@okv_instance_ip_address
   ```

2. Switch to user `root`.

   ```
   support$ su - root
   ```

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

   ```
   root# 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:

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

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

   ```
   root# 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 the current release of Oracle Key Vault, 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.

   ```
   $ ssh support@okv_instance_ip_address
   ```

2. Switch to user `root`.

   ```
   support$ su - root
   ```

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

   ```
   root# 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:

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

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

   ```
   root# 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`.

   ```
   root# su oracle
   ```

6. Start SQL*Plus.

   ```
   oracle$ 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:

   ```
   oracle$ service dbfwdb stop
   oracle$ service dbfwdb start
   ```

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

```
oracle$ 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.

- Audit Trail is not Sent To Remote Syslog on Switchover in Primary-Standby Pair
- SSH Tunnel Status Shows as Disabled on Failover Case in Primary-Standby
- 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
- After Primary-Standby Unpair, Re-Pairing With A New Standby With A Different IP Address Can Cause Pairing Failure

Audit Trail is not Sent To Remote Syslog on Switchover in Primary-Standby 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

SSH Tunnel Status Shows as Disabled on Failover Case in Primary-Standby

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 node in a primary-standby pair has a controlled shutdown. For example, a user performs the shutdown by pressing a power off button in the management console or executes the shutdown command from the terminal. When this happens, there will be no failover operation and the standby Oracle Key Vault node 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 node. 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 node to take over as the new primary node, instead perform a switchover.

Bug Number: 29666606

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

Issue: For a primary-standby configuration, before pairing 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

After Primary-Standby Unpair, Re-Pairing With A New Standby With A Different IP Address Can Cause Pairing Failure

Issue: This bug applies to when using the primary-standby configuration, after unpairing the primary from the standby. As documented, the previous standby is no longer usable after unpairing. When you try to pair the primary with a new, freshly installed standby, if the new standby does not have the same IP address as the old standby, the pairing operation may fail.

Workaround: When pairing a primary and a new standby after unpairing from a previous primary-standby configuration, make sure the new standby has the same IP address as the old standby before attempting to pair the primary and the new standby.

Bug Number: 30890330

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
- System Settings Changed on an OKV Node After Conversion to a Candidate Node Do Not Reflect On The Controller Node
- Read-Write Nodes in Read-Only Restricted Mode After a Reboot
- RMAN Automatically Cleans Up Archivelogs Still Necessary for OGG
- Oracle Key Vault Should Prevent Enabling From Finishing If It Takes Longer Than MDND
- Certificate Must Be Rotated Before Converting To Cluster If Upgrading From 12.2 BP4 or Older
- After Force-Deleting A Read-Write Node In 18.1 Cluster And Then Upgrading, May Not Be Able To Replace Force-Deleted Node In Higher Version

- Backup From Oracle Key Vault 18.1, 18.2 or 18.3 Cluster Node That Is Then Upgraded and Used To Make Another Cluster May Not Be Able To Add A Read-Write Peer
- Cluster Service Status Is Down After Rotating Server Certificate

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 Node After Conversion to a Candidate Node Do Not Reflect On The Controller Node

Issue: If system settings are changed on an Oracle Key Vault node 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 on both the controller and candidate nodes.

Workaround: None. Verify that the system settings of the Oracle Key Vault node 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 run 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 It 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 18.4 from Oracle Key Vault 12.2 BP4 through 18.2 and do not 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: Upgrade to Oracle Key Vault release 18.4 in two steps:

1. Upgrade from Oracle Key Vault 12.2 BP4 to 12.2 BP11, and perform a certificate rotation operation.
2. Upgrade from Oracle Key Vault 12.2 BP11 to Oracle Key Vault release 18.4.

For more information on how to perform a certificate rotation in Oracle Key Vault 12.2 BP11, refer to the *Oracle Key Vault Administrator's Guide* for release 12.2.

Bug Number: 30673249

Related Topics

- Rotating Certificates in Oracle Key Vault release 12.2

After Force-Deleting A Read-Write Node In 18.1 Cluster And Then Upgrading, May Not Be Able To Replace Force-Deleted Node In Higher Version

Issue: When force-deleting a read-write node, it should be shutdown first. However, due to GoldenGate bug 30413969, if the force-deleted node is shut down, the downstream extract on the deleted node's read-write peer node is not fully cleaned up. The workaround for this bug is present in Oracle Key Vault versions 18.2 and higher. However, if upgrading from an Oracle Key Vault 18.1 multi-master cluster that has had a read-write node force-deleted, if attempting to replace it after upgrade, it will still not succeed because the cleanup was not executed when the force-delete happened in version 18.1.

Workaround: The following steps are to be executed with caution. Executing these steps on the wrong Oracle Key Vault server will break replication and result in having to force-delete the node on which they were executed.

Example scenario: Nodes A and B are read-write peers. Node B was force-deleted from the cluster. Node A may not have been fully cleaned up due to GoldenGate bug 30413969. Before or after upgrading, but before attempting to add another node as Node A's read-write peer, execute the following steps on node A to finish the cleanup.

```
ssh support@Oracle_Key_Vault_IP_address
su - root
su - oracle
/var/lib/oracle/dbfw/bin/sqlplus / as sysdba
exec sys.dbms_xstream_adm.drop_outbound('OGG$OKV_DEXT');
exec sys.dbms_streams_adm.remove_queue('OGG$Q_OKV_DEXT', TRUE, TRUE);
```

After the above steps are successfully executed on Node A, it can be used as the controller node to add another node to the cluster as Node A's read-write peer.

Bug Number: 31216736

Backup From Oracle Key Vault 18.1, 18.2 or 18.3 Cluster Node That Is Then Upgraded and Used To Make Another Cluster May Not Be Able To Add A Read-Write Peer

Issue: When restoring a backup taken on a cluster node to a standalone Oracle Key Vault server, the `global_name` of the database on Oracle Key Vault may be either `DBFWDB.DBFWDB` or `DBFWDB_HA2.DBFWDB`, depending on the global_name of the cluster node on which the backup was taken. If the global_name is `DBFWDB_HA2.DBFWDB`, and the standalone Oracle Key Vault server is converted to a cluster node, then it will not be able to successfully add a read-write peer node due to the `global_name` mismatch. The global name is fixed during backup restore in versions 18.4 and higher, but if the backup was taken and restored on a lower version, the issue will persist even after upgrading to 18.4 or higher.

Workaround: After restoring the backup to a standalone Oracle Key Vault server, execute these steps before converting it to a cluster node. The first select statement is to confirm that the `global_name` is `DBFWDB_HA2.DBFWDB`. Do not proceed with the `global_name` update if the `global_name` returned by the below select statement is not `DBFWDB_HA2.DBFWDB` or if the server has already been converted to a cluster node.

```
ssh support@Oracle_Key_Vault_IP_address
su - root
su - oracle
/var/lib/oracle/dbfw/bin/sqlplus / as sysdba
select global_name from global_name;
alter database rename global_name to DBFWDB.DBFWDB;
```

Bug Number: 31241245

Cluster Service Status Is Down After Rotating Server Certificate

Issue: Rotating the server certificate will stop multiple processes in order to replace the certificates. However, under normal circumstances, they are restarted soon after they are stopped. During or after certificate rotation, on the Monitoring page under the Cluster tab, the Cluster Services Status may show a downward arrow, indicating that one or more cluster services are not running. This will cause replication to be broken to and from this node. If it persists for more than a few minutes, it is likely that this bug has occurred.

Workaround: If this issue occurs, try to restart the cluster services by clicking the Restart Cluster Services button on the Monitoring page. After a few minutes, refresh the page. If the Cluster Service Status still shows a red downward arrow, contact Oracle Support.

Bug Number: 31371440

Oracle Key Vault Considerations

Below are details and changes of behavior of Oracle Key Vault 18.4.

- 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.

Related Topics

- Configuring Oracle Audit Vault Integration

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 18.4:

- 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 18.4

Oracle Key Vault release 18.4 updated the underlying infrastructure to incorporate the January 2020 Release Update for Oracle Database 18 (18.10 DB RU) - January Release Update. Please sign in for full details.

https://www.oracle.com/security-alerts/cpujan2020.html

Oracle Key Vault release 18.4 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 18.4
F29539-02