Oracle® Key Vault

Release Notes

Release 21.9

F96296-03

February 2025

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.

About These Release Notes

These release notes provide information that you should be aware of before using Oracle Key Vault.

The release notes cover changes in this new release, how to download the Oracle Key Vault software and documentation, known issues, considerations, supported Oracle Database versions, and critical patches that have been included in this release.

Changes in This Release for Oracle Key Vault

In each release, Oracle Key Vault introduces several new features and enhancements to improve performance, configuration, monitoring, and reporting.

- Changes for Oracle Key Vault Release 21.7
  Oracle Key Vault release 21.7 introduces several new features.
- Changes for Oracle Key Vault Release 21.6
  Oracle Key Vault release 21.6 introduces several new features.
- Changes for Oracle Key Vault Release 21.5
  Oracle Key Vault release 21.5 introduces several new features.
- Changes for Oracle Key Vault Release 21.4
  Oracle Key Vault release 21.4 introduces several new features.
- Changes for Oracle Key Vault Release 21.3
  Oracle Key Vault release 21.3 introduces several new features.
- Changes for Oracle Key Vault Release 21.2
  Oracle Key Vault release 21.2 introduces new features that are related to installation and upgrade operations.
- Changes for Oracle Key Vault Release 21.1
  Oracle Key Vault release 21.1 introduces several new features.

Changes for Oracle Key Vault Release 21.9

Oracle Key Vault release 21.9 introduces several new features.

- Configure Auditing for Select Audit Event IDs and Audit Event Categories
  When you enable auditing in Oracle Key Vault, all system operations are audited by default. Starting with Oracle Key Vault release 21.9, you can selectively enable auditing of specific operations based on the audit event categories and audit event IDs.
- Describe Endpoint Details Using okvutil
  In Oracle Key Vault release 21.8 and earlier, it was not possible for an endpoint to gather the endpoint details like endpoint name, description, or default wallet information about itself. For this information, the endpoint depends on the Oracle Key Vault administrator.
- Improve Overall Certificate Rotation Time
  Starting with Oracle Key Vault release 21.9, endpoints are redirected to the node that generated their new certificates to speed up the CA certificate rotation process.
- List the Wallet Membership of an Object Using RESTful Services Utility Command
  Starting with Oracle Key Vault release 21.9, you can now list all the wallet memberships of a given managed object.
- Allow List for Approved RESTful Connections
  Starting with Oracle Key Vault release 21.9, you can enable access to RESTful services utility from the allowed IP addresses only.

Configure Auditing for Select Audit Event IDs and Audit Event Categories

When you enable auditing in Oracle Key Vault, all system operations are audited by default. Starting with Oracle Key Vault release 21.9, you can selectively enable

auditing of specific operations based on the audit event categories and audit event IDs.

Audit event ID identifies the audit operation type. Audit event IDs for operations that are functionally related are grouped into audit event categories.

You can use custom events configuration to selectively enable auditing for operations of your interest using audit event categories, individual audit event IDs or combination of both. Selecting an audit event category enables auditing of all events from that category. You can also selectively exclude an audit event from the selected audit event category.

You can modify and save custom events audit configuration before making it effective. Once you complete custom events audit configuration, you can switch from auditing all events to auditing custom events to apply the configuration.

> **Note:**
>
> Selective auditing may impact the reports that are based on the audit report.

Describe Endpoint Details Using okvutil

In Oracle Key Vault release 21.8 and earlier, it was not possible for an endpoint to gather the endpoint details like endpoint name, description, or default wallet information about itself. For this information, the endpoint depends on the Oracle Key Vault administrator.

Starting with Oracle Key Vault release 21.9, endpoint managers can use `okvutil` on the endpoint host to list the endpoint details.

Improve Overall Certificate Rotation Time

Starting with Oracle Key Vault release 21.9, endpoints are redirected to the node that generated their new certificates to speed up the CA certificate rotation process.

Endpoint certificates have to be regenerated when CA certificates are rotated. Endpoint certificates are generated by a designated cluster node and shipped back to the endpoint when the endpoint communicates with the designated cluster node. Considering that the endpoint picks a cluster node at random from the endpoint node scan list to communicate with, it may take some time for the endpoint to connect to the designated node, especially since each successive attempt may only be made after the expiration of the time for the keys to live in persistent cache. CA certificate rotation is incomplete till all the endpoint certificates are rotated.

Starting with Oracle Key Vault release 21.9, when the endpoint certificates are ready and the endpoint communicates with a cluster node, then Oracle Key Vault node redirects the endpoint to the designated cluster node to fetch the certificate. This process eliminates the need for multiple attempts to fetch the endpoint certificate thus accelerating the completion of the CA certificate rotation.

List the Wallet Membership of an Object Using RESTful Services Utility Command

Starting with Oracle Key Vault release 21.9, you can now list all the wallet memberships of a given managed object.

Following command is added to RESTful services utility to support this enhancement:

```
okv manage-access wallet list-object-wallets --uuid <uuid>
```

The RESTful services utility command is run by a user. Only those wallets that this user has access to, will be listed. The object may be a member of the wallets that the user running the command has no access to. These wallets are not listed.

Allow List for Approved RESTful Connections

Starting with Oracle Key Vault release 21.9, you can enable access to RESTful services utility from the allowed IP addresses only.

With this new feature, only the configured list of IP addresses can use the RESTful services utility. In earlier Oracle Key Vault releases, you could either enable or disable the RESTful services utility only.

Changes for Oracle Key Vault Release 21.8

Oracle Key Vault release 21.8 introduces several new features.

- Enforce Separation of Administrator Roles
  Starting with Oracle Key Vault release 21.8, you can configure Oracle Key Vault such that an Oracle Key Vault user can have no more than one Oracle Key Vault administrative role.
- Console Certificate Supports Subject Alternative Name (SAN)
  Starting with Oracle Key Vault release 21.8, Oracle Key Vault supports a fully qualified domain name (FQDN) for the console certificates without changing the hostname.
- Alert for Platform Certificate Expiration
  Starting with Oracle Key Vault release 21.8, an alert will be generated when the Oracle Key Vault platform certificates are going to expire within a period defined by the alert configuration.
- RESTful Services Utility Commands Support for Custom Attributes
  Starting with Oracle Key Vault Release 21.8, you can specify custom-attributes and KMIP-attributes of security objects as command line options when using RESTful services utility commands, such as `add`, `modify`, `delete`, and `get`. The `fetch` and `locate` commands also support additional attributes on the command line.
- Server-side Filtering for RESTful Services Utility Commands
  Starting in Oracle Key Vault release 21.8, you can now specify options to do server-side filtering for the RESTful services utility commands that list

endpoints or wallets, list objects that endpoints have access to, list objects in wallet and for those that list completed backups.

- Upload of Public and Private Keys through okvutil
  With Oracle Key Vault release 21.8, `okvutil` has been enhanced to support Public and Private Keys.
- Configurable Key Lengths for Service Certificates
  Starting with Oracle Key Vault release 21.8, you can configure the key lengths for the service certificates.

Enforce Separation of Administrator Roles

Starting with Oracle Key Vault release 21.8, you can configure Oracle Key Vault such that an Oracle Key Vault user can have no more than one Oracle Key Vault administrative role.

In previous Oracle Key Vault releases, the Oracle Key Vault administrative roles (System Administrator, Key Administrator, and Audit Manager) could be granted to another Oracle Key Vault user by any user who currently has the role with **Allow Forward Grant** option.

Starting with this release, you enable **Enforce Separation of Administrator Roles** check from the **Account Management** tab of the **System Recovery** page to prevent the grant of more than one Oracle Key Vault administrative role to any Oracle Key Vault user. Each user can have at most one administrative role. Enabling the **Enforce Separation of Administrator Roles** option enforces administrative role isolation in Oracle Key Vault.

An Oracle Key Vault user may already have more than one administrative role when the **Enforce Separation of Administrator Roles** option is enabled. In this case, the user cannot exercise any of the administrative roles even though they have been granted to him. The additional roles have to be removed before the remaining one (intended) administrative role can become operational.

Console Certificate Supports Subject Alternative Name (SAN)

Starting with Oracle Key Vault release 21.8, Oracle Key Vault supports a fully qualified domain name (FQDN) for the console certificates without changing the hostname.

Prior to Oracle Key Vault release 21.8, you would have to change the hostname of the Oracle Key Vault to a fully qualified domain name (FQDN) of the Oracle Key Vault server when generating console certificates to avoid HTTPS certificate browser warnings.

Starting with Oracle Key Vault release 21.8, this change is no longer necessary. You can retain the hostname when you add an FQDN as the subject alternative name for the console certificate. Subject alternative name (SAN) is an extension to the X.509 certificate specification that allows the inclusion of additional hostname in the certificate. You can also use this feature to resolve two FQDNs to the same Oracle Key Vault server, if needed. But in this case, you must change the hostname to one of the two FQDNs.

Alert for Platform Certificate Expiration

Starting with Oracle Key Vault release 21.8, an alert will be generated when the Oracle Key Vault platform certificates are going to expire within a period defined by the alert configuration.

Platform certificates are used when a new node is added to the cluster. They are also used when shipping redo between read/write nodes of a cluster. These certificates are different from the Oracle Key Vault service certificates and have different expiration dates. They are also rotated using a different method than the Oracle Key Vault service certificates. You must rotate the platform certificates before they expire. You cannot upgrade an Oracle Key Vault system with the expired platform certificates. The default configuration for the alert is 90 days. You can change the configured value. The alert will be raised for standalone, multi-master cluster, and primary-standby deployments.

Related Topic

About Configuring Alerts

RESTful Services Utility Commands Support for Custom Attributes

Starting with Oracle Key Vault Release 21.8, you can specify custom-attributes and KMIP-attributes of security objects as command line options when using RESTful services utility commands, such as `add`, `modify`, `delete`, and `get`. The `fetch` and `locate` commands also support additional attributes on the command line.

KMIP attributes like `activation date` and `deactivation date` are now available as command line options `--activation-date` and `--deactivation-date` respectively. You can pass the custom-attributes using the new command line option `--custom-attribute`.

The following commands support this enhancement:

- `okv managed-object attribute add`
- `okv managed-object attribute modify`
- `okv managed-object attribute delete`
- `okv managed-object attribute get`
- `okv managed-object custom-attribute add`
- `okv managed-object custom-attribute modify`
- `okv managed-object custom-attribute delete`
- `okv managed-object custom-attribute get`
- `okv managed-object object locate`
- `okv managed-object object fetch`

Server-side Filtering for RESTful Services Utility Commands

Starting in Oracle Key Vault release 21.8, you can now specify options to do server-side filtering for the RESTful services utility commands that list endpoints or wallets,

list objects that endpoints have access to, list objects in wallet and for those that list completed backups.

You can filter the list of endpoints by platform, type, or registration status. You can filter the list of wallets by their type, either general or SSH server wallets. You can filter the list of objects that endpoints have access to or list objects in the wallet by type such as, secret or certificate, or state like active or compromised. You can filter the list of completed backups for a specific backup destination or filter them by type, that is, one-time or periodic, or simply filter by the backup name. You can specify more than one option for filtering and can also specify more than one value for the filtering option. For example, you can list all endpoints on Linux and Microsoft Windows platforms by using the following command with the filter options:

```
--platform "LINUX64, WINDOWS"
```

The following commands support this enhancement:

- `okv admin endpoint list`
- `okv admin endpoint list-objects`
- `okv manage-access wallet list`
- `okv manage-access wallet list-objects`
- `okv backup history list`

Upload of Public and Private Keys through okvutil

With Oracle Key Vault release 21.8, `okvutil` has been enhanced to support Public and Private Keys.

In earlier releases, RESTful services needed to be installed and configured to upload public and private keys to Oracle Key Vault. With Oracle Key Vault release 21.8, `okvutil` has been enhanced to support uploading of public and private key directly, greatly simplifying the enforcement of remote server access controls for public key authentication.

Configurable Key Lengths for Service Certificates

Starting with Oracle Key Vault release 21.8, you can configure the key lengths for the service certificates.

You can choose to set the key length of the certificate authority (CA) certificate to either 2048 bits or 4096 bits. When the next CA certificate rotation is performed, the CA, server/node, and endpoint certificates will be generated with the selected key length. Service certificates with configurable key lengths enable compliance with corporate information security policies.

Changes for Oracle Key Vault Release 21.7

Oracle Key Vault release 21.7 introduces several new features.

- Controlling Access to SSH Servers Centrally with Oracle Key Vault
  Starting with this release, you can use Oracle Key Vault to centrally manage the access to the SSH servers within your enterprise.
- Improved SSH User Keys Management
  Oracle Key Vault release 21.7 further improves the centralized SSH user keys management.
- Support Key Creation from Oracle Key Vault Management Console
  Starting with release 21.7, you can now create new keys and key pairs from Oracle Key Vault Management console. This allows Oracle Key Vault users to create the keys and key pairs. Previously, only endpoints could create security objects.
- RESTful Services Utility Changes to Support SSH Keys Management
  Starting with release 21.7, you can use the Oracle Key Vault RESTful services utility to create and register SSH keys and manage SSH Server wallets and SSH Server endpoints.
- Support for Node or Cluster Scope for Alerts in Multi-Master Cluster
  Starting with Oracle Key Vault release 21.7, in a multi-master cluster, you can set the configuration for certain alerts at the Node or Cluster scope.
- Setting the Initial Password for the support and root User
  Starting with release 21.7, the initial password for the support and root user can no longer be set from the Oracle Key Vault management console during the post-installation steps.

Controlling Access to SSH Servers Centrally with Oracle Key Vault

Starting with this release, you can use Oracle Key Vault to centrally manage the access to the SSH servers within your enterprise.

SSH public key authentication is often the preferred method for accessing remote hosts for operation and administrative purposes. In an enterprise setting, multiple administrators grant or revoke access to enterprise users on large number of hosts within their domain. At this scale, the decentralized nature of the access control architecture quickly becomes overwhelming, making the system generally more prone to errors and thus more exposed to security risks.

Using Oracle Key Vault integration with the OpenSSH, you can now control access to the SSH servers centrally. Centralized access control improves security, enables quicker responses to threats, reduces human error and simplifies the server access management at scale.

With release 21.7, Oracle Key Vault adds a new type of endpoint - the **SSH Server** endpoint. The SSH Server endpoint type must be deployed on the SSH server to facilitate the integration with OpenSSH.

Oracle Key Vault release 21.7 now introduces wallet types – **SSH Server** wallet and **General** wallet. The SSH Server wallet is associated with a host user on the SSH server and is meant to contain the authorized SSH public keys of the host user. You grant or deny access to the SSH servers by adding or removing the user's SSH public keys from the SSH server wallets.

Oracle Key Vault now offers SSH server authorization, SSH server access, and other reports to simplify the management and monitoring of server access.

Improved SSH User Keys Management

Oracle Key Vault release 21.7 further improves the centralized SSH user keys management.

The Oracle Key Vault PKCS#11 library integrates with the OpenSSH to support the SSH public key authentication using a SSH key pair from Oracle Key Vault.

This enables the centralized management of SSH user keys in Oracle Key Vault. You can now create SSH keys explicitly. In the previous releases, generic public-private key pairs were used as the SSH keys, making it difficult to distinguish them from other public-private key pairs not used as SSH keys.

You can now associate an SSH user with the SSH Keys, making it easier to identify and monitor the keys. The SSH user is intended to track the actual consumer of the SSH keys, a human, an application, or a machine.

Oracle Key Vault now offers SSH private key authorization and access reports to simplify the management and monitoring of SSH keys. You can separately configure the expiration alerts for the SSH keys.

Support Key Creation from Oracle Key Vault Management Console

Starting with release 21.7, you can now create new keys and key pairs from Oracle Key Vault Management console. This allows Oracle Key Vault users to create the keys and key pairs. Previously, only endpoints could create security objects.

As an Oracle Key Vault user, you can now create generic or application specific keys and key pairs. As generic keys, Oracle Key Vault supports creation of symmetric keys and public-private key pairs.

The application keys category supports the creation of the TDE Master Encryption Key, Oracle GoldenGate Master Key, and SSH Key Pair. Once the application key is created, the corresponding application must then be configured to make use of the key from Oracle Key Vault.

At the time of key creation, you can select key algorithm and key length, set the key expiration date, and control whether the key is extractable outside of the Oracle Key Vault cluster boundary.

User created keys can be used by endpoints as usual as long as endpoints can access them.

RESTful Services Utility Changes to Support SSH Keys Management

Starting with release 21.7, you can use the Oracle Key Vault RESTful services utility to create and register SSH keys and manage SSH Server wallets and SSH Server endpoints.

The following Oracle Key Vault RESTful services utility commands have been updated to support the SSH key pair creation and registration of SSH private and public keys:

- `okv managed-object key-pair create`
- `okv managed-object private-key register`
- `okv managed-object public-key register`

A new option **--ssh-user** is added to these commands. Use of this option makes the underlying public and private key objects identified as the SSH keys.

To support the creation of SSH Server endpoint and SSH Server wallet, following commands have been updated:

- `okv admin endpoint create`
- `okv manage-access wallet create`

Support for Node or Cluster Scope for Alerts in Multi-Master Cluster

Starting with Oracle Key Vault release 21.7, in a multi-master cluster, you can set the configuration for certain alerts at the Node or Cluster scope.

In earlier releases, in a multi-master cluster, the same alert configuration was always applied to each cluster node. Using the same alert setting across cluster nodes may not always be ideal. For example, if the system is configured to take backup from a particular node, it is not ideal for the other nodes to raise the **System Backup** was never done alert. For such nodes, you can set the node scope and turn off the alerts only on these nodes.

Oracle Key Vault release 21.7 makes the alert configuration even more flexible by allowing node specific configuration for following alerts:

- Fast Recovery Area Space Utilization
- High CPU Usage
- Failed System Backup
- High Memory Usage
- Disk Utilization
- System Backup

You can even enable or disable these alerts at the per node level. On a given node, the node scope configuration overrides the cluster scope configuration for the same alert.

Setting the Initial Password for the support and root User

Starting with release 21.7, the initial password for the support and root user can no longer be set from the Oracle Key Vault management console during the post-installation steps.

With release 21.7, the root user password continues to be the one that is specified during the initial phase of Oracle Key Vault installation.

The initial password for the support user can now by set by logging in to the Oracle Key Vault terminal console as the root user immediately after the install.

Changes for Oracle Key Vault Release 21.6

Oracle Key Vault release 21.6 introduces several new features.

- Ability to Restrict the Extraction of Private Encryption Keys from Oracle Key Vault
  Oracle Key Vault release 21.6 allows private keys uploaded to Oracle Key Vault to be marked as non extractable, so that they do not leave the Oracle Key Vault deployment boundary.
- Ability to Create Asymmetric Key Pairs in Oracle Key Vault
  Starting release 21.6, you can now create an asymmetric key pair in Oracle Key Vault.
- Ability to Clone an Oracle Key Vault VM
  Starting with Oracle Key Vault release 21.6, a fresh installation of an Oracle Key Vault VM guest can be stored as a `template`, and the VM platform cloning capability can be used to clone Oracle Key Vault cluster nodes.
- Support the Ability to Provide an Alternate Host Name or an IP Address
  Starting Oracle Key Vault release 21.6, you can configure Oracle Key Vault with a fully qualified domain name or IP address, such as the public IP address of systems running in cloud infrastructure environments.
- Support SAMLv2 Based Single Sign-On (SSO) Authentication for Oracle Key Vault
  Starting with Oracle Key Vault release 21.6, Oracle Key Vault supports SAML based Single Sign-On (SSO) authentication.
- Support for Unified Application-Level Tracing and Simplified Diagnostics Collection
  Starting with Oracle Key Vault release 21.6, a unified application-level tracing is introduced with the ability to centrally control the tracing level. The diagnostics download process is also simplified.
- Aborting Oracle Audit Vault Integration with Oracle Key Vault
  Starting with Oracle Key Vault release 21.6, Oracle Key Vault integration with Oracle Audit Vault can be aborted, when integration is not successful.
- Event ID Support in Auditing Records
  Starting with Oracle Key Vault release 21.6, all the operation events are now categorized using the event IDs.
- Support for Disk and Network I/O and Application Metrics in Oracle Key Vault Metrics Framework
  Starting with Oracle Key Vault release 21.6, Oracle Key Vault expands the metrics framework to include Disk, Network I/O, and Application metrics.
- Support for Sign and Signature Verify Operations
  Starting with Oracle Key Vault release 21.6, C and Java SDKs now provide Sign and Verify capability.
- Sign and Verify Operations in Oracle Key Vault
  Starting with Oracle Key Vault release 21.6, sign and verify operations can be performed using Oracle Key Vault's RESTful services, or the Oracle Key Vault client tool `okvutil`:
- Oracle Key Vault Deployments in Microsoft Azure and Amazon AWS
  Starting with Oracle Key Vault release 21.6, you can deploy Oracle Key Vault on Microsoft Azure and Amazon AWS cloud platforms.

- Endpoint IP Address Attribute Added to endpoint get RESTful Command
  Oracle Key Vault supports endpoint IP address in the `endpoint get` RESTful command.

Ability to Restrict the Extraction of Private Encryption Keys from Oracle Key Vault

Oracle Key Vault release 21.6 allows private keys uploaded to Oracle Key Vault to be marked as non extractable, so that they do not leave the Oracle Key Vault deployment boundary.

You can now restrict private keys, as well as symmetric keys, and make them non-extractable by setting the extractable attribute value to *false*. The false attribute value ensures that the cryptographic objects remain within the Oracle Key Vault boundary.

To control whether private encryption keys can be retrieved (extracted) from Oracle Key Vault, you can use the Oracle Key Vault management console, RESTful services utility commands, the C SDK APIs, and Java SDK APIs.

Related Topics

- Managing the Extraction of Symmetric or Private Keys from Oracle Key Vault

Ability to Create Asymmetric Key Pairs in Oracle Key Vault

Starting release 21.6, you can now create an asymmetric key pair in Oracle Key Vault.

You may create the private key as non-extractable, or make it non-extractable afterward to ensure that the private key never leaves the Oracle Key Vault deployment boundary.

You can create an asymmetric key pair using RESTful services utility commands, C and JAVA SDK APIs.

With the support of the non-extractable private keys and the sign operations on-board Oracle Key Vault, you can now implement public key authentication using openssh and Oracle Key Vault's PKCS#11 library such that user's ssh private key never leaves Oracle Key Vault. During public key authentication, the PKCS#11 library now performs the sign operation within Oracle Key Vault itself. This helps you in enforcing centralized key governance and eliminating locally downloaded, vulnerable private keys.

Ability to Clone an Oracle Key Vault VM

Starting with Oracle Key Vault release 21.6, a fresh installation of an Oracle Key Vault VM guest can be stored as a `template`, and the VM platform cloning capability can be used to clone Oracle Key Vault cluster nodes.

With Oracle Key Vault cluster, using the cloned template, the system administrator can significantly shorten the provisioning time, compared to performing a full installation of each individual cluster node.

Oracle Key Vault supports the cloning feature of the underlying virtualization platform. This eliminates the need to go through the full installation process for each individual cluster node. You can clone an Oracle Key Vault system (installed as a VM) after the

installation is complete, but before performing post-installation tasks. When a clone is started up for the first time, it goes through a series of steps to regenerate system-specific configuration that makes it unique (and separate from all other clones). The (remote) cloning capability provided by virtualization platforms allows to clone from an Oracle Key Vault **Template**, which is an Oracle Key Vault installation that is stopped before this Oracle Key Vault is made unique. It regenerates all of the system-specific configuration; the clone becomes unique by completing the remaining installation steps.

Support the Ability to Provide an Alternate Host Name or an IP Address

Starting Oracle Key Vault release 21.6, you can configure Oracle Key Vault with a fully qualified domain name or IP address, such as the public IP address of systems running in cloud infrastructure environments.

Oracle Key Vault provides the ability to provide two alternate host names. You can choose whether to have endpoints use one of these alternate host names when communicating with the Oracle Key Vault server or node. The alternate host name is required to be provided for each node and you can also choose if the endpoint should use the provided host name in a multi-master cluster environment.

This feature is not supported in (deprecated) primary-standby deployments.

Support SAMLv2 Based Single Sign-On (SSO) Authentication for Oracle Key Vault

Starting with Oracle Key Vault release 21.6, Oracle Key Vault supports SAML based Single Sign-On (SSO) authentication.

Oracle Key Vault release 21.6 now supports SSO. The SSO feature is SAML based and the user is authenticated via an Identity Provider (IdP). The IdP supported Single Sign-On (SSO) Authentication provides multi-factor authentication (MFA). This provides the ability to minimize the login attempts to one set of credentials hence improving the enterprise security. Single Sign-On (SSO) Authentication is part of an identity and access management (IAM) solution, it utilizes a central directory that controls user access to resources at a more granular level. This allows organizations to comply with regulations that require provisioning users with appropriate permissions. The SSO solution also de-provisions users quickly, another common compliance requirement meant to ensure that former employees, partners, or others cannot access the sensitive data.

Related Topics

-

Support for Unified Application-Level Tracing and Simplified Diagnostics Collection

Starting with Oracle Key Vault release 21.6, a unified application-level tracing is introduced with the ability to centrally control the tracing level. The diagnostics download process is also simplified.

Previously, to collect the diagnostics, the system administrator logs on to the Oracle Key Vault management console, downloads the readme, logs on to the Oracle Key Vault server as the `root` user, and runs commands manually to install the diagnostics utility, and enable selected log options. The system administrator then logs back on the Oracle Key Vault management console to download the diagnostics bundle.

Oracle Key Vault release 21.6 simplifies the process. Log on to the Oracle Key Vault management console as a system administrator, select the required diagnostics to download, and then click **Download**.

In addition to facilitating centralized trace generation, Oracle Key Vault release 21.6 introduces component-based tracing that allows the system administrator to adjust the trace level for specific Oracle Key Vault components from the Oracle Key Vault management console. These trace levels (in increasing levels of severity) are: MANDATORY, ERROR, WARNING, INFO, and DEBUG.

Related Topics

-

Aborting Oracle Audit Vault Integration with Oracle Key Vault

Starting with Oracle Key Vault release 21.6, Oracle Key Vault integration with Oracle Audit Vault can be aborted, when integration is not successful.

From the Oracle Key Vault management console you can now **Abort** the integration of AVDF. This is helpful when the integration of AVDF takes longer than usual time to get integrated with Oracle Key Vault.

Event ID Support in Auditing Records

Starting with Oracle Key Vault release 21.6, all the operation events are now categorized using the event IDs.

This feature adds a new field, **Event ID**, to Oracle Key Vault audit records. The **Event ID** represents a stable identity that is uniquely associated with an audited operation (type).

- Multiple audit records for the same audit operation use the same **Event ID**.
- Event IDs remains unchanged and remains mapped to the same operation forever as the **Event IDs** are statically baked into the Oracle Key Vault source code.
- The text description of the **Operation**, however, could still change across releases.
- New operations that are added as part of the new functionality will be given new unique Event ID.

Related Topics

-

Support for Disk and Network I/O and Application Metrics in Oracle Key Vault Metrics Framework

Starting with Oracle Key Vault release 21.6, Oracle Key Vault expands the metrics framework to include Disk, Network I/O, and Application metrics.

This feature adds metrics for Disk, Network I/O, Application metrics. The current available metrics at any time in Oracle Key Vault helps in determining the system capability and resource usage.

- Disk I/O: Gives insight into database cache assuming most of the Oracle Key Vault activities are going to be from the database.
- Network I/O: Gives insight into number of bytes received/sent during a particular time interval. You can compare the data with the historical date to analyze the usage and activity of endpoints. This also provides data as an average value.
- Application: Gives insight into number of KMIP connections accepted to process the connections in an interval.

Related Topics

-

Support for Sign and Signature Verify Operations

Starting with Oracle Key Vault release 21.6, C and Java SDKs now provide Sign and Verify capability.

You can use either RESTful services utility commands, okvutil, or C and Java SDK to perform sign and signature verify operations.

C SDK APIs

- KMIP cryptographic operations are as follows:
  - `okvSign`
  - `okvSignVerify`
- Cryptographic utility operations are as follows:
  - `okvCryptoContextGetCryptoAlgo`
  - `okvCryptoContextGetHashingAlgo`
  - `okvCryptoContextGetDigitalSignAlgo`
  - `okvCryptoContextSetHashingAlgo`
  - `okvCryptoContextSetCryptoAlgo`
  - `okvCryptoContextSetDigitalSignAlgo`
  - `okvCryptoResponseGetSignatureData`
  - `okvCryptoResponseGetRecoveredData`
  - `okvCryptoResponseGetValidity`
  - `okvSignResponseCreate`
  - `okvSignVerifyResponseCreate`

  - `okvSignResponseFree`
  - `okvSignVerifyResponseFree`

Java SDK APIs

- KMIP cryptographic operations are as follows:
  - `okvSign`
  - `okvSignVerify`
- Cryptographic utility operations are as follows:
  - `getCryptoAlgo`
  - `getHashingAlgo`
  - `getDigitalSignAlgo`
  - `setCryptoAlgo`
  - `setHashingAlgo`
  - `setDigitalSignAlgo`
  - `getSignatureData`
  - `getRecoveredData`
  - `getValidity`

RESTful APIs

- `okv crypto data sign`
- `okv crypto data sign-verify`

okvutil

- `okvutil sign`
- `okvutil sign-verify`

Related Topics

- Oracle Key Vault Client C SDK API Reference
- Oracle Key Vault Client Java SDK API Reference

Sign and Verify Operations in Oracle Key Vault

Starting with Oracle Key Vault release 21.6, sign and verify operations can be performed using Oracle Key Vault's RESTful services, or the Oracle Key Vault client tool `okvutil`:

Both of the Oracle Key Vault RESTful API and Oracle Key Vault client utility `okvutil` provide sign and verify functionality.

The new or updated commands are as follows:

- `okv crypto data sign`
- `okv crypto data sign-verify`
- `okv crypto data sign`
- `okv crypto data sign-verify`
- `okvutil sign`
- `okvutil sign-verify`

Oracle Key Vault Deployments in Microsoft Azure and Amazon AWS

Starting with Oracle Key Vault release 21.6, you can deploy Oracle Key Vault on Microsoft Azure and Amazon AWS cloud platforms.

In addition to on-premises data centers and Oracle Cloud Infrastructure (OCI), Oracle Key Vault release 21.6 can also be deployed in Microsoft Azure and Amazon AWS.

Endpoint IP Address Attribute Added to endpoint get RESTful Command

Oracle Key Vault supports endpoint IP address in the `endpoint get` RESTful command.

The endpoint IP address that was used at enrollment time is now recorded, and displayed with the `okv admin endpoint get --endpoint` *`endpoint_name`* command.

Changes for Oracle Key Vault Release 21.5

Oracle Key Vault release 21.5 introduces several new features.

- Support for SSH Public Key Authentication using SSH User Keys from Oracle Key Vault

  Starting in Oracle Key Vault release 21.5, you can use SSH key-based authentication with a key pair stored only in Oracle Key Vault.
- Automatic Purging of Audit Records Based on a Retention Policy

  Starting in Oracle Key Vault release 21.5, you can now purge the old audit records automatically based on a retention policy.
- Ability to Rotate Endpoint Certificates

  Starting in Oracle Key Vault release 21.5, you can rotate an endpoint in order to increase its certificate validity without incurring endpoint downtime.
- Endpoint and Endpoint Group Privileges Support for LDAP Users

  Starting in Oracle Key Vault release 21.5, you can grant the endpoint and endpoint group privileges to LDAP users through the LDAP group mappings.
- User Account Management

  Starting in Oracle Key Vault release 21.5, you can configure the user account profile parameters to meet your corporate user management security policies for the Oracle Key Vault users.

- Severity based Alert Categorization
  Starting in Oracle Key Vault release 21.5, alerts are categorized based on their severity levels to improve ease of administration.
- Displaying Endpoint Group Membership Column in Endpoint Metadata Report
  Starting with Oracle Key Vault release 21.5, additional column for Endpoint Group Membership is available in Endpoint Metadata Report.
- Ability to Determine Time of Last Endpoint Activity
  Starting in Oracle Key Vault release 21.5, you can quickly determine when an endpoint was last active by checking the Endpoints page on the Oracle Key Vault Management Console.
- UEFI Support for OCI marketplace Image
  Starting in Oracle Key Vault release 21.5, the Oracle Key Vault OCI marketplace images are available in UEFI mode only.
- Separate Alerts for CA Certificate Expiration and Server/Node Certificate Expiration
  Starting in Oracle Key Vault release 21.5, you can configure the alerts for the CA certificate expiration and server/node certificate expiration separately.
- Support for Cluster Management and Monitoring using RESTful Services Utility
  Starting in Oracle Key Vault release 21.5, you can deploy, manage, and monitor the multi-master cluster using RESTful services utility.
- Support for System Resources Monitoring using RESTful Services Utility
  Starting in Oracle Key Vault release 21.5, you can obtain the current and historical utilization metrics of the system resources such as CPU and memory using RESTful services utility. These system metrics would help you appropriately configure system resources for the Oracle Key Vault servers to meet the performance and scalability requirements of your deployment.
- RESTful Services Utility Commands Reduce Need for Intermediate JSON Files
  Starting in Oracle Key Vault release 21.5, you can specify custom-attributes and certain KMIP attributes as the command line options when using RESTful services utility to create, register, fetch and locate security objects.
- Support for Text Output Format in RESTful Services Utility
  Starting in Oracle Key Vault release 21.5, several RESTful services utility commands are enhanced to support the output in the **text** format.

Support for SSH Public Key Authentication using SSH User Keys from Oracle Key Vault

Starting in Oracle Key Vault release 21.5, you can use SSH key-based authentication with a key pair stored only in Oracle Key Vault.

The Oracle Key Vault PKCS#11 library supports SSH public key authentication using a SSH key pair that is uploaded to Oracle Key Vault. The centralized management of SSH user keys in Oracle Key Vault simplifies key life-cycle management, enables key governance and makes it easier to enforce policies. You can centrally perform actions such as, rotating the keys and revoking them when needed. This also allows you to minimize the risks that are associated with the SSH user keys footprint on local disks.

Related Topics

- Managing Online and Offline Secrets

Automatic Purging of Audit Records Based on a Retention Policy

Starting in Oracle Key Vault release 21.5, you can now purge the old audit records automatically based on a retention policy.

You can now better manage the disk space consumed by Oracle Key Vault audit records without the need to manually delete them once they are deemed no longer needed. You can configure Oracle Key Vault to automatically purge older audit records based on a retention policy. For example, you can configure and apply a policy to automatically purge audit records that are older than 180 days.

Ability to Rotate Endpoint Certificates

Starting in Oracle Key Vault release 21.5, you can rotate an endpoint in order to increase its certificate validity without incurring endpoint downtime.

With Oracle Key Vault release 21.5, you can rotate an endpoint in order to increase its certificate validity without incurring endpoint downtime. Previously, this could only be done by re-enrolling the endpoint. You can choose to rotate multiple endpoints at once if required. Rotating an endpoint certificate this way is independent of the CA or server/node certificate rotation processes.

Related Topics

- Managing Endpoints

Endpoint and Endpoint Group Privileges Support for LDAP Users

Starting in Oracle Key Vault release 21.5, you can grant the endpoint and endpoint group privileges to LDAP users through the LDAP group mappings.

The privileges to the LDAP users are granted through the LDAP groups mappings. You map the endpoint or endpoint group privileges to an LDAP group. LDAP users that are members of this group are granted the mapped endpoint or endpoint group privileges at the time of login.

Related Topics

- Managing LDAP User Authentication and Authorization in Oracle Key Vault

User Account Management

Starting in Oracle Key Vault release 21.5, you can configure the user account profile parameters to meet your corporate user management security policies for the Oracle Key Vault users.

User account profile parameters govern the rules and requirements for the user passwords, and the account lockout behavior of Oracle Key Vault users. These settings apply to Oracle Key Vault users that are created locally. For LDAP users, the user account management policies are managed in the LDAP directory server.

Oracle Key Vault now also supports unlocking of a user account through a password reset. An Oracle Key Vault administrator can unlock a user account by resetting the user's password.

Related Topics

- Managing User Accounts

Severity based Alert Categorization

Starting in Oracle Key Vault release 21.5, alerts are categorized based on their severity levels to improve ease of administration.

Oracle Key Vault supports several types of alerts. Oracle Key Vault now categories these alerts to one of the severity levels: CRITICAL, HIGH, MEDIUM, and LOW. The home page of the Oracle Key Vault management console now displays the unresolved alerts in the order of their severity. Oracle Key Vault administrators can now easily identify most critical alerts that need immediate attention to ensure operational continuity.

Related Topics

- Configuring Alerts

Displaying Endpoint Group Membership Column in Endpoint Metadata Report

Starting with Oracle Key Vault release 21.5, additional column for Endpoint Group Membership is available in Endpoint Metadata Report.

The Endpoint Metadata Report displays endpoint information and deployment configuration detail. The Metadata Report now displays the Endpoint Group Membership column.

The Endpoint Group Membership information is useful when:

- Granting privileges to Endpoint group
- Performing the Endpoint rotation

Ability to Determine Time of Last Endpoint Activity

Starting in Oracle Key Vault release 21.5, you can quickly determine when an endpoint was last active by checking the Endpoints page on the Oracle Key Vault Management Console.

Starting in Oracle Key Vault release 21.5, you can determine when an endpoint was last active from the Oracle Key Vault Management Console by navigating to the "Endpoints" page and checking the "Last Active Time" column for that endpoint. This information can be useful in quickly determining which endpoints are unused. Previously, the only way to glean this information was from the endpoint activity reports (in particular, in a multi-master cluster, by consolidating all of the endpoint activity reports from all nodes of the cluster).

Related Topics

- Adding an Endpoint as an Oracle Key Vault System Administrator or Create Endpoint User

UEFI Support for OCI marketplace Image

Starting in Oracle Key Vault release 21.5, the Oracle Key Vault OCI marketplace images are available in UEFI mode only.

The OCI marketplace images of the earlier versions of Oracle Key Vault continue to use the BIOS mode.

Separate Alerts for CA Certificate Expiration and Server/Node Certificate Expiration

Starting in Oracle Key Vault release 21.5, you can configure the alerts for the CA certificate expiration and server/node certificate expiration separately.

You can configure different threshold values for these alerts. The default threshold value for CA certificate expiration is 90 days, while that for server/node certificate expiration is 60 days. Having separate alerts makes it easier to determine when a server/node certificate rotation is to be performed. The server/node certificate rotation is short and quick process performed on a per-node basis, as opposed to a CA certificate rotation which affects the entire Oracle Key Vault deployment and involves multiple steps. Previously, a single alert type 'Oracle Key Vault Server Certificate expiration' was raised when either the CA or the server/node certificate was expiring within the configured server certificate expiration threshold.

Support for Cluster Management and Monitoring using RESTful Services Utility

Starting in Oracle Key Vault release 21.5, you can deploy, manage, and monitor the multi-master cluster using RESTful services utility.

Using the RESTful Services Utility, you can now perform several cluster management operations including creating a cluster, adding or deleting a node, enabling or disabling a node. You can also monitor and manage the cluster services and replication links between nodes using RESTful services utility.

The new commands are as follows:

- `okv cluster node create`
- `okv cluster node status`
- `okv cluster node add`
- `okv cluster node abort-pairing`
- `okv cluster node enable`
- `okv cluster node disable`
- `okv cluster node cancel-disable`

- `okv cluster node update`
- `okv cluster service start`
- `okv cluster service stop`
- `okv cluster service monitor`
- `okv cluster link enable`
- `okv cluster link disable`
- `okv cluster link monitor`

Related Topics

- Cluster Management Commands

Support for System Resources Monitoring using RESTful Services Utility

Starting in Oracle Key Vault release 21.5, you can obtain the current and historical utilization metrics of the system resources such as CPU and memory using RESTful services utility. These system metrics would help you appropriately configure system resources for the Oracle Key Vault servers to meet the performance and scalability requirements of your deployment.

Using the RESTful services utility, you can obtain the information about the:

- Configured system resources (CPU and memory)
- CPU and memory utilization metrics over a specified period, including load averages

The new or updated commands are as follows:

- `okv metrics server get`
- `okv server status get`
- `okv server info get`

Related Topics

- Monitoring Commands

RESTful Services Utility Commands Reduce Need for Intermediate JSON Files

Starting in Oracle Key Vault release 21.5, you can specify custom-attributes and certain KMIP attributes as the command line options when using RESTful services utility to create, register, fetch and locate security objects.

In earlier releases, commands that use the attributes or custom-attributes could only be executed using the JSON input method only. The RESTful services utility is enhanced to support the passing of attributes and custom-attributes as the command line options for the commands to create or register security objects. These commands also support simplified variants of the complex input.

The KMIP attributes "activation date" and "deactivation date" are exposed as the command line options `--activation-date` and `--deactivation-date` respectively. You can pass the custom-attributes using the new command line option --custom-attribute. Several RESTful services utility commands also support simplified and complex format on name and custom attribute.

The following commands have been updated to accommodate this enhancement:

- `okv managed-object key create`
- `okv managed-object key register`
- `okv managed-object secret register`
- `okv managed-object certificate register`
- `okv managed-object certificate-request register`
- `okv managed-object opaque register`
- `okv managed-object public-key register`
- `okv managed-object private-key register`
- `okv managed-object object fetch`
- `okv managed-object object locate`

Related Topics

- Security Object Commands

Support for Text Output Format in RESTful Services Utility

Starting in Oracle Key Vault release 21.5, several RESTful services utility commands are enhanced to support the output in the **text** format.

In previous releases, the RESTful services utility commands always produced output in the JSON format. Now, you can use the new command line option **–output_format** to generate the command output in the text format. The **text** output format helps simplify the creation of automation scripts such as when the output of a command serves as input for another command.

Supported values for the --output_format option are:

- json (default value)
- text

The following commands have been updated to accommodate this enhancement:

- `okv managed-object certificate get`
- `okv managed-object certificate register`
- `okv managed-object certificate-request get`
- `okv managed-object certificate-request register`
- `okv managed-object key create`

- `okv managed-object key get`
- `okv managed-object key register`
- `okv managed-object object activate`
- `okv managed-object object destroy`
- `okv managed-object object locate`
- `okv managed-object object revoke`
- `okv managed-object opaque get`
- `okv managed-object private-key register`
- `okv managed-object public-key get`
- `okv managed-object public-key register`
- `okv managed-object secret get`
- `okv managed-object secret register`
- `okv managed-object wallet add-member`
- `okv managed-object wallet delete-member`
- `okv managed-object wallet list`

Related Topics

- Security Object Commands

Changes for Oracle Key Vault Release 21.4

Oracle Key Vault release 21.4 introduces several new features.

- Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault
  Starting in Oracle Key Vault release 21.4, to strengthen the protection of symmetric encryption keys, you now can restrict these keys from leaving the Oracle Key Vault cluster boundary.
- Support for Cryptographic Operations in RESTful Services Utility
  Oracle Key Vault release 21.4 adds the support for performing cryptographic operations within Oracle Key Vault.
- C and Java SDK APIs for Cryptographic Operations
  Oracle Key Vault Client SDK release 21.4 adds the support for cryptographic operations.
- Enhancements to Certificate Management
  Starting in Oracle Key Vault release 21.4, several enhancements to the management of certificates are available.
- Support for Policy Based Automatic Purging of Old Oracle Key Vault Backups
  Starting in Oracle Key Vault release 21.4, you can create a policy to schedule the removal of one or more remote backups.

- Support for Policy Based Automatic Purging of Old Oracle Key Vault Backups in RESTful Services Utility
  Starting in Oracle Key Vault release 21.4, you can manually purge the local Oracle Key Vault backup or create a destination policy to purge one or more remote backups.
- Ability to Restrict Oracle Key Vault Administrative Role Grants
  Starting in Oracle Key Vault release 21.4, you can control whether a grantee of an Oracle Key Vault administrative role can grant the role to other Oracle Key Vault users.
- Enhancements to Endpoint, Endpoint Group, and Wallet-Related RESTful Services Utility Commands
  Starting in Oracle Key Vault release 21.4, additional commands are available to enable you to perform more operations with endpoints, endpoint groups, and wallets.
- Support for Updating the Configuration of Endpoints
  Starting in Oracle Key Vault release 21.4, you can update the endpoint configuration parameters and endpoint settings for keys and secrets of an endpoint using the RESTful services utility command `okv admin endpoint update`.
- RESTful Commands to Set Date and Time Accommodate ISO 8601 Standard
  Starting in Oracle Key Vault release 21.4, the *`duration`* time interval settings will follow the ISO 8601 standard, and the fixed format for date and time settings are compatible with ISO 8601 when using RESTful commands.
- Support for Command Line Help for the RESTful Services Utility
  Starting in Oracle Key Vault release 21.4, you can find the command line help information about the RESTful services utility commands.
- Preferred KMIP Version Updated to 1.1 for Oracle Key Vault KMIP Server
  Oracle Key Vault KMIP Server now uses KMIP protocol version 1.1 as its preferred version.
- Client IP Address in the Oracle Key Vault Audit Trail
  Starting in Oracle Key Vault release 21.4, the Oracle Key Vault audit trail has one new field: `Client IP`.
- Client Endpoint File Updated When A KMIP Server Operation Is Executed Using SDK
  The client endpoint file `okvclient.ora` is now updated when a KMIP server operation is executed using the SDK.
- Support for Additional Monitoring Information Through SNMP
  Starting in Oracle Key Vault release 21.4, additional monitoring information is available through the SNMP `nsExtendOutputFull` MIB base variable.

Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault

Starting in Oracle Key Vault release 21.4, to strengthen the protection of symmetric encryption keys, you now can restrict these keys from leaving the Oracle Key Vault cluster boundary.

This restriction applies to the key material of the symmetric keys, but not its metadata. For example, Transparent Database Encryption (TDE) master encryption keys are stored in Oracle Key Vault. When an endpoint needs to decrypt the key, the PKCS#11 library fetches the TDE master encryption key from Oracle Key Vault to perform the decryption. If your site requires that symmetric keys never leave Oracle Key Vault, then you can configure these keys to remain within Oracle Key Vault during operations. In this case, the PKCS#11 library will send the encrypted data encryption key to Oracle Key Vault. Decryption is then performed within Oracle Key Vault and afterward, the plaintext data encryption key is returned to the PKCS#11 library. The Oracle Key Vault PKCS#11 library performs the encryption and decryption operation within Oracle Key Vault if the TDE master encryption key is restricted to leave Oracle Key Vault, or if it cannot be extracted from Oracle Key Vault.

To control whether symmetric encryption keys can be retrieved (extracted) from Oracle Key Vault, you can use the Oracle Key Vault management console, RESTful services utility commands, the C SDK APIs, and Java SDK APIs.

The following Oracle Key Vault RESTful services utility commands have been updated to accommodate this enhancement:

- `okv managed-object attribute get`
- `okv managed-object attribute get-all`
- `okv managed-object attribute list`
- `okv managed-object attribute modify`
- `okv managed-object key create`
- `okv managed-object key register`
- `okv managed-object object locate`

New APIs for the C SDK to manage extractable attribute:

- `okvAttrAddExtractable`
- `okvAttrAddNeverExtractable`
- `okvAttrGetExtractable`
- `okvAttrGetNeverExtractable`

New APIs for the Java SDK to manage extractable attribute:

- `okvAttrAddExtractable`
- `okvAttrAddNeverExtractable`
- `okvAttrGetExtractable`
- `okvAttrGetNeverExtractable`

Related Topics

- Managing the Extraction of Symmetric Keys from Oracle Key Vault

- Configuring the Global Default Extraction for New Symmetric Keys

Support for Cryptographic Operations in RESTful Services Utility

Oracle Key Vault release 21.4 adds the support for performing cryptographic operations within Oracle Key Vault.

You can use either RESTful services utility commands or C and Java SDK to perform encryption and decryption operations.

This enhancement accommodates the use of symmetric keys that have been configured to not be extracted from Oracle Key Vault.

The new commands are as follows:

- `okv crypto data decrypt`
- `okv crypto data encrypt`

Related Topics

- Cryptographic Commands

C and Java SDK APIs for Cryptographic Operations

Oracle Key Vault Client SDK release 21.4 adds the support for cryptographic operations.

Oracle Key Vault release 21.4 adds support for performing encryption and decryption cryptographic operations within Oracle Key Vault.

You can use either RESTful services utility commands or C and Java SDK to perform encryption and decryption operations.

C SDK APIs

- KMIP cryptographic operations are as follows:
  - `okvDecrypt`
  - `okvEncrypt`
- Attribute operations are as follows:
  - `okvAttrAddExtractable`
  - `okvAttrAddNeverExtractable`
  - `okvAttrGetExtractable`
  - `okvAttrGetNeverExtractable`
- Cryptographic utility operations are as follows:
  - `okvCryptoContextCreate`
  - `okvCryptoContextFree`
  - `okvCryptoContextGetAuthEncryptionAdditionalData`

  - okvCryptoContextGetAuthEncryptionTag
  - okvCryptoContextGetBlockCipherMode
  - okvCryptoContextGetIV
  - okvCryptoContextGetPadding
  - okvCryptoContextGetRandomIV
  - okvCryptoContextSetAuthEncryptionAdditionalData
  - okvCryptoContextSetAuthEncryptionTag
  - okvCryptoContextSetBlockCipherMode
  - okvCryptoContextSetIV
  - okvCryptoContextSetPadding
  - okvCryptoContextSetRandomIV
  - okvCryptoResponseGetAuthEncryptionTag
  - okvCryptoResponseGetDecryptedData
  - okvCryptoResponseGetEncryptedData
  - okvCryptoResponseGetIV
  - okvDecryptResponseCreate
  - okvDecryptResponseFree
  - okvEncryptResponseCreate
  - okvEncryptResponseFree

Java SDK APIs

- KMIP cryptographic operations are as follows:
  - okvDecrypt
  - okvEncrypt
- Attribute operations are as follows:
  - okvAttrAddExtractable
  - okvAttrAddNeverExtractable
  - okvAttrGetExtractable
  - okvAttrGetNeverExtractable
- Cryptographic utility operations are as follows:
  - okvCryptoContextCreate

Related Topics

- Oracle Key Vault Client C SDK API Reference
- Oracle Key Vault Client Java SDK API Reference

Enhancements to Certificate Management

Starting in Oracle Key Vault release 21.4, several enhancements to the management of certificates are available.

The enhancements are as follows:

- **Support for using an Oracle Key Vault certificate authority (CA) certificate that has been signed by an external certificate signing authority:** You can choose to have the CA certificate issued by a third-party signing authority. This option can be exercised by first generating a certificate signing request (CSR), having that CSR signed by the external signing authority, and then uploading that signed CA to Oracle Key Vault. You will then be required to perform a CA certificate rotation so that all certificates on board Oracle Key Vault (endpoint certificates as well as those used for communication between Oracle Key Vault multi-master cluster nodes) are re-issued by the new CA. In previous releases, the Oracle Key Vault CA certificate was always self-signed.
- **Ability to configure a validity period of Oracle Key Vault self-signed root CA certificate:** You can configure the certificate validity period of the Oracle Key Vault self-signed CA. The new validity period would take effect the next time a CA certificate rotation is performed. Previously, this value was fixed and unchangeable.
- **In multi-master cluster environments, the ability to set the order in which endpoints are rotated during the Oracle Key Vault CA certificate rotation process:** This enhancement enables you to configure the order in which endpoints are rotated during a CA certificate rotation. Starting in this release, the endpoints are, by default, rotated in order of endpoint certificate expiry (that is, those expiring soonest are rotated first). You can also choose to order the endpoint rotation by providing a cluster subgroup priority list before initiating a CA certificate rotation. Then, during the CA certificate rotation process, endpoints that belong to cluster subgroups higher in the priority list are rotated before those in lower-priority cluster subgroups. In previous releases, when a CA certificate rotation was performed, the endpoints were rotated in random order.
- **Ability to configure a batch number of endpoints rotated during an Oracle Key Vault CA certificate rotation:** You can configure the number of endpoints that can be in the `Updating to current certificate issuer` state at a given point in the CA certificate rotation process. You can configure this value based on the number of endpoints in the Oracle Key Vault configuration. Previously, this value was static and release dependent (for example, at most, 15 endpoints could be in this state in Oracle Key Vault release 21.3).
- **Ability to rotate Oracle Key Vault server and node certificates:** Starting in this release, the certificates that are used for communication between Oracle Key Vault systems (cluster nodes in a multi-master cluster environment, or primary and standby environments), and for communication between an Oracle Key Vault system and its endpoints are now known as server certificates (in standalone or primary-standby environments) and node certificates (in multi-master cluster environments). This enhancement provides greater operational flexibility, because you now can choose different validity periods for the Oracle Key Vault CA certificate and server and node certificates. You then can rotate the server and

node certificates as often as needed, without needing to go through the entire CA certificate rotation process.

Related Topics

- Managing Certificates

Support for Policy Based Automatic Purging of Old Oracle Key Vault Backups

Starting in Oracle Key Vault release 21.4, you can create a policy to schedule the removal of one or more remote backups.

You can now better manage the disk space consumed by Oracle Key Vault backups on remote backup destination servers without the need to manually delete them once they are deemed no longer needed. You can configure Oracle Key Vault to automatically purge older backups from a remote backup destination based on a policy. For example, you can configure and apply a policy to a remote backup destination to automatically purge backups that are older than 30 days unless the backup is among the 10 more recent backups. In addition, you can now manually delete a local Oracle Key Vault backup.

Related Topics

- Scheduling the Purging of Old Oracle Key Vault Backups

Support for Policy Based Automatic Purging of Old Oracle Key Vault Backups in RESTful Services Utility

Starting in Oracle Key Vault release 21.4, you can manually purge the local Oracle Key Vault backup or create a destination policy to purge one or more remote backups.

The following commands have been updated:

- `okv backup destination create`
- `okv backup destination update`

The following commands are new:

- `okv backup destination delete-backup`
- `okv backup destination-policy create`
- `okv backup destination-policy delete`
- `okv backup destination-policy get`
- `okv backup destination-policy list`
- `okv backup destination-policy list-purged-backups`
- `okv backup destination-policy update`
- `okv backup destination resume-policy`
- `okv backup destination suspend-policy`

Related Topics

- Backup, Schedule, and Restore Commands

Ability to Restrict Oracle Key Vault Administrative Role Grants

Starting in Oracle Key Vault release 21.4, you can control whether a grantee of an Oracle Key Vault administrative role can grant the role to other Oracle Key Vault users.

In previous releases, the Oracle Key Vault administrative roles (System Administrator, Key Administrator, and Audit Manager) could be granted to another Oracle Key Vault user by any user who currently has the role. Starting with this release, when an administrator grants the role to another user, the administrator can restrict how the grantee user can in turn grant the role to other users. This enhancement improves overall user security and helps to adhere to good least privileges practices.

Related Topics

- About Administrative Roles in Oracle Key Vault

Enhancements to Endpoint, Endpoint Group, and Wallet-Related RESTful Services Utility Commands

Starting in Oracle Key Vault release 21.4, additional commands are available to enable you to perform more operations with endpoints, endpoint groups, and wallets.

The new commands are as follows:

- `okv admin endpoint get`
- `okv admin endpoint list`
- `okv admin endpoint list-objects`
- `okv admin endpoint resume`
- `okv admin endpoint suspend`
- `okv manage-access endpoint-group get`
- `okv manage-access endpoint-group list`
- `okv manage-access wallet add-object`
- `okv manage-access wallet get`
- `okv manage-access wallet list`
- `okv manage-access wallet list-objects`
- `okv manage-access wallet remove-object`

The commands to list objects for an endpoint (`okv admin endpoint list-objects`) and a wallet (`okv admin wallet list-objects`) provide an option to show or hide the wallet membership of the objects. Omitting wallet membership information of objects can improve command's performance.

Related Topics

- *Oracle Key Vault RESTful Services Administrator's Guide*

Support for Updating the Configuration of Endpoints

Starting in Oracle Key Vault release 21.4, you can update the endpoint configuration parameters and endpoint settings for keys and secrets of an endpoint using the RESTful services utility command `okv admin endpoint update`.

The endpoint configuration parameters includes various PKCS#11 settings and endpoint settings for keys and secrets includes the `extractable` attribute setting for the new symmetric keys.

Related Topics

- *Oracle Key Vault RESTful Services Administrator's Guide*

RESTful Commands to Set Date and Time Accommodate ISO 8601 Standard

Starting in Oracle Key Vault release 21.4, the *`duration`* time interval settings will follow the ISO 8601 standard, and the fixed format for date and time settings are compatible with ISO 8601 when using RESTful commands.

You can specify the following formats:

- *`duration`* (follows the ISO 8601 standard)
- *`timestamp`* (is in a format that is compatible with the ISO 8601 standard)
- `now` (represents the current time when a command is run)

You can use these formats in the following combinations:

- *`timestamp`*
- `now`
- *`timestamp`* + *`duration`*
- `now` + *`duration`*

The *`timestamp`* format that has been used in previous releases is still supported.

The following commands have been updated for this enhancement:

- `okv backup schedule create`
- `okv backup schedule update`
- `okv managed-object attribute add`
- `okv managed-object attribute delete`
- `okv managed-object attribute modify`
- `okv managed-object certificate-request register`
- `okv managed-object key register`

- `okv managed-object object locate`
- `okv managed-object opaque register`
- `okv managed-object private_key register`
- `okv managed-object public-key register`
- `okv managed-object secret register`

Related Topics

- *Oracle Key Vault RESTful Services Administrator's Guide*

Support for Command Line Help for the RESTful Services Utility

Starting in Oracle Key Vault release 21.4, you can find the command line help information about the RESTful services utility commands.

This enhancement enables you to find the detailed help information about the various categories, resources, and actions that are supported for all Oracle Key Vault RESTful services utility commands. The help information shows the command's syntax, and definitions for the available categories, resources, and actions as well as the configuration parameters that are applicable to all the commands.

Related Topics

- *Oracle Key Vault RESTful Services Administrator's Guide*

Preferred KMIP Version Updated to 1.1 for Oracle Key Vault KMIP Server

Oracle Key Vault KMIP Server now uses KMIP protocol version 1.1 as its preferred version.

In prior releases of Oracle Key Vault, even though the KMIP server accepted and processed client requests with KMIP version 1.1, it always sent the server response with the KMIP version 1.0. Now, the KMIP server sends a response with the protocol version with which the KMIP request was made. The KMIP server is also enhanced to return an error for client requests that are made with unsupported KMIP version. Such error responses are returned using the server's preferred KMIP version which is currently set to 1.1.

Related Topics

- Support for OASIS Key Management Interoperability Protocol (KMIP)

Client IP Address in the Oracle Key Vault Audit Trail

Starting in Oracle Key Vault release 21.4, the Oracle Key Vault audit trail has one new field: `Client IP`.

The Oracle Key Vault audit trail contains fields to capture information such as the name and type of the entity that performed an operation, the time the operation was performed, the node in which an operation was performed, and the result of the operation. The addition of the `Client IP` field enables users to better find where operations were performed, particularly in Cloud environments.

Related Topics

- Oracle Key Vault Audit Trail

Client Endpoint File Updated When A KMIP Server Operation Is Executed Using SDK

The client endpoint file `okvclient.ora` is now updated when a KMIP server operation is executed using the SDK.

Prior to Oracle Key Vault release 21.4, the client endpoint file `okvclient.ora` was not updated whenever a KMIP server operation was performed using the SDK. Now, the client endpoint file `okvclient.ora` will be updated if there are any new endpoint updates whenever a KMIP server operation is performed using the Oracle Key Vault client SDK.

Support for Additional Monitoring Information Through SNMP

Starting in Oracle Key Vault release 21.4, additional monitoring information is available through the SNMP `nsExtendOutputFull` MIB base variable.

The `nsExtendOutputFull` MIB base variable now returns the following values:

- Fast recovery size, used and free space
- Tomcat server status
- Oracle Audit Vault agent status
- CA certificate expiration date
- Server certificate expiration date
- Server certificate subject alternative name (SAN)

Related Topics

- SNMP Management Information Base Variables for Oracle Key Vault

Changes for Oracle Key Vault Release 21.3

Oracle Key Vault release 21.3 introduces several new features.

- Ability to Configure Other HSMs for Oracle Key Vault
  Starting with Oracle Key Vault release 21.3, in addition to the Thales Luna Network HSM version 7000, Entrust nShield Connect + and XC models, and Utimaco's SecurityServer 4.31.1 HSMs, you can configure other HSMs that have been certified to work with Oracle Key Vault.
- Easier Oracle Audit Vault and Database Firewall Integration with Oracle Key Vault
  Starting in Oracle Key Vault release 21.3, steps in the integration of Oracle Audit Vault and Database Firewall (AVDF) with Oracle Key Vault have been automated.

- Enhancements for RESTful Services Utility Commands Used for Registration
  In Oracle Key Vault release 21.3, RESTful services utility commands that are used for the registration of managed objects will have additional attributes.
- Alert for Fast Recovery Area Space Utilization
  Starting in Oracle Key Vault release 21.3, an alert will be generated when the Fast Recovery Area Space utilization of the Oracle Key Vault's embedded database exceeds the configured threshold value.
- Cluster Redo Shipping Status Alert Message Change
  Starting in Oracle Key Vault release 21.3, the `Cluster Redo Shipping Status` alert notification message has changed.

Ability to Configure Other HSMs for Oracle Key Vault

Starting with Oracle Key Vault release 21.3, in addition to the Thales Luna Network HSM version 7000, Entrust nShield Connect + and XC models, and Utimaco's SecurityServer 4.31.1 HSMs, you can configure other HSMs that have been certified to work with Oracle Key Vault.

Those additional HSMs may or may not be already certified by the HSM vendor.

This feature gives you a much wider range of HSM products that you can use with Oracle Key Vault. The configuration is slightly different from the configuration of the Thales Luna Network HSM version 7000, Entrust nShield Connect + and XC models, and Utimaco's SecurityServer 4.31.1 HSMs in that you will need to work with your HSM vendor with regard to the requirements that they must fulfill in order for their HSM to work with Oracle Key Vault. After you have successfully integrated the HSM with Oracle Key Vault, you will be able to perform all the tasks that you normally perform with the Thales Luna Network HSM version 7000, Entrust nShield Connect + and XC models, and Utimaco's SecurityServer 4.31.1 HSMs, such as upgrade operations, backup and restore operations, and reverse migrations.

Related Topics

- Vendor Instructions for Integrating an HSM as the Root of Trust for Oracle Key Vault

Easier Oracle Audit Vault and Database Firewall Integration with Oracle Key Vault

Starting in Oracle Key Vault release 21.3, steps in the integration of Oracle Audit Vault and Database Firewall (AVDF) with Oracle Key Vault have been automated.

In previous releases, an Oracle Key Vault administrator had to manually perform steps such as downloading and installing the AVDF agent to perform this integration. Now, much of this integration work is built in to the Oracle Key Vault management console, enabling an administrator to perform the integration easily and quickly.

Enhancements for RESTful Services Utility Commands Used for Registration

In Oracle Key Vault release 21.3, RESTful services utility commands that are used for the registration of managed objects will have additional attributes.

The affected commands are as follows:

- `okv managed-object certificate register`
- `okv managed-object certificate-request register`
- `okv managed-object key register`
- `okv managed-object opaque register`
- `okv managed-object private-key register`
- `okv managed-object public-key register`
- `okv managed-object secret register`

In previous releases, these commands provided two attributes, `name` and `contactInfo`. In this release, in addition to these two attributes, the following new attributes are included:

- `activationDate`
- `deactivationDate`
- `processStartDate`
- `protectStopDate`

Related Topics

- Security Object Commands

Alert for Fast Recovery Area Space Utilization

Starting in Oracle Key Vault release 21.3, an alert will be generated when the Fast Recovery Area Space utilization of the Oracle Key Vault's embedded database exceeds the configured threshold value.

By default, the configured threshold value is 70 and the alert is available for standalone, multi-master cluster, and primary-standby environments. The new alert enables you to better monitor the Fast Recovery Area space usage of the Oracle Key Vault's embedded database.

Related Topics

- About Configuring Alerts

Cluster Redo Shipping Status Alert Message Change

Starting in Oracle Key Vault release 21.3, the `Cluster Redo Shipping Status` alert notification message has changed.

In previous releases, users were alerted only when the redo-shipping status was active (up) or inactive (down). The message now, in addition to this information, indicates whether the node in the cluster is operating in read-only mode or is no longer in read-only mode.

Related Topics

- Oracle Key Vault Administrator's Guide

Changes for Oracle Key Vault Release 21.2

Oracle Key Vault release 21.2 introduces new features that are related to installation and upgrade operations.

- Certificate and Secret Objects Expiration Alerts
  Starting with this release, you can configure alert notifications for the expiration of certificate and secret objects.
- New C and Java SDK APIs for Certificates, Certificate Requests, Private Keys, and Public Keys
  In Oracle Key Vault release 21.2, new APIs enable you to perform operations such as registering and fetching objects, and adding attributes to those objects (for example, length, type, ID, subject, issuer, and algorithm).
- New and Changed RESTful Services Utility Commands
  Several new and changed `okv managed-object` RESTful services utility commands are available starting with this release.
- Changes in the Oracle Key Vault Management Console
  In Oracle Key Vault release 21.2, the Oracle Key Vault management console user interface has had minor changes throughout.

Certificate and Secret Objects Expiration Alerts

Starting with this release, you can configure alert notifications for the expiration of certificate and secret objects.

In previous releases, expiration alerts for all managed objects shared a common configuration under the `Key Rotations` alert. Starting with this release, you can separately configure the expiration alerts for certificate and secret objects. The expiration alerts for the certificate and secret objects are no longer reported as `Key Rotations` alerts. Similar to alerts such as those for cluster components or user password expiration, you can set this type of alert to notify users when the deactivation date for a certificate or secret object is within its threshold value.

The new alerts for certificate and secret objects are as follows:

- `Certificate Object Expiration`
- `Secret Object Expiration`

The object expiration alerts are now raised only when the object is in the `PRE-ACTIVE` or `ACTIVE` state. Previously, they were raised regardless of the object state.

The object expiration alerts are now deleted when an object is revoked or destroyed. Previously, they were deleted when object was destroyed.

Related Topics

- Oracle Key Vault Administrator's Guide

New C and Java SDK APIs for Certificates, Certificate Requests, Private Keys, and Public Keys

In Oracle Key Vault release 21.2, new APIs enable you to perform operations such as registering and fetching objects, and adding attributes to those objects (for example, length, type, ID, subject, issuer, and algorithm).

C SDK APIs

Registration and fetch operations are as follows:

- `okvGetCertificate`
- `okvGetCertificateRequest`
- `okvGetPrivateKey`
- `okvGetPublicKey`
- `okvRegCertificate`
- `okvRegCertificateRequest`
- `okvRegPrivateKey`
- `okvRegPublicKey`

Attribute operations are as follows:

- `okvAttrAddCertLen`
- `okvAttrAddCertType`
- `okvAttrAddDigitalSignAlgo`
- `okvAttrAddX509CertId`
- `okvAttrAddX509CertIss`
- `okvAttrAddX509CertIssAltName`
- `okvAttrAddX509CertSubj`
- `okvAttrAddX509CertSubjAltName`
- `okvAttrGetCertLen`
- `okvAttrGetCertType`
- `okvAttrGetDigitalSignAlgo`
- `okvAttrGetX509CertId`
- `okvAttrGetX509CertIdIssuerLen`
- `okvAttrGetX509CertIdSerialNoLen`
- `okvAttrGetX509CertIss`
- `okvAttrGetX509CertIssAltName`
- `okvAttrGetX509CertIssAltNameLen`

- okvAttrGetX509CertIssDNLen
- okvAttrGetX509CertSubj
- okvAttrGetX509CertSubjAltName
- okvAttrGetX509CertSubjAltNameLen
- okvAttrGetX509CertSubjDNLen

Java SDK APIs

Registration and fetch operations are as follows:

- okvGetCertificate
- okvGetCertificateRequest
- okvGetPrivateKey
- okvGetPublicKey
- okvRegCertificate
- okvRegCertificateRequest
- okvRegPrivateKey
- okvRegPublicKey

Attribute operations are as follows:

- okvAttrAddArchiveDate
- okvAttrAddCertLen
- okvAttrAddCertType
- okvAttrAddDigitalSignAlgo
- okvAttrAddInitialDate
- okvAttrAddLastChangeDate
- okvAttrAddState
- okvAttrAddX509CertId
- okvAttrAddX509CertIss
- okvAttrAddX509CertIssAltName
- okvAttrAddX509CertSubj
- okvAttrAddX509CertSubjAltName
- okvAttrGetCertLen
- okvAttrGetCertType
- okvAttrGetDigitalSignAlgo
- okvAttrGetX509CertId

- `okvAttrGetX509CertIss`
- `okvAttrGetX509CertIssAltName`
- `okvAttrGetX509CertSubj`
- `okvAttrGetX509CertSubjAltName`

Related Topics

- Oracle Key Vault Developer's Guide

New and Changed RESTful Services Utility Commands

Several new and changed `okv managed-object` RESTful services utility commands are available starting with this release.

The new `okv managed-object` RESTful services commands, which add support for `get` and `register` operations for certificate requests, private keys, and public keys, are as follows:

- `okv managed-object certificate-request get`
- `okv managed-object certificate-request register`
- `okv managed-object private-key get`
- `okv managed-object private-key register`
- `okv managed-object public-key get`
- `okv managed-object public-key register`

The changed `okv managed-object` RESTful services commands are as follows:

- `okv managed-object certificate register`
- `okv managed-object object locate`

Related Topics

- Security Object Commands

Changes in the Oracle Key Vault Management Console

In Oracle Key Vault release 21.2, the Oracle Key Vault management console user interface has had minor changes throughout.

These changes are the result of modified terms, updates to the current release, and enhancements for better usability. The overall interface has not had major changes.

Changes for Oracle Key Vault Release 21.1

Oracle Key Vault release 21.1 introduces several new features.

- Dual NIC Network Interface Support

  Starting with this release, Oracle Key Vault supports the use of two network interfaces, referred to as dual NIC configuration.

- LDAP User Authentication and Authorization in Oracle Key Vault
  Starting with this release, you can configure authentication and authorization of Oracle Key Vault users to be centrally managed in a Microsoft Active Directory.
- RESTful Services Utility Command-Line Interface for Appliance Management
  In Oracle Key Vault release 21.1, the RESTful services utility command-line interface has been expanded and redesigned to provide more functionality.
- Support for SFTP to Transfer External Backups
  Oracle Key Vault now supports the use of SSH Secure File Transfer Protocol (SFTP) for the transfer of (scheduled) external backups to remote backup destinations.
- Development Using the Java SDK
  This release introduces a new Java language software development kit that you can use to integrate custom endpoints with the Oracle Key Vault server.
- Development Using the C SDK
  This release introduces a new C language software development kit that you can use to integrate custom endpoints with the Oracle Key Vault server.

Dual NIC Network Interface Support

Starting with this release, Oracle Key Vault supports the use of two network interfaces, referred to as dual NIC configuration.

In a dual NIC configuration, Oracle Key Vault combines the two network interfaces into a single logical interface using the Linux NIC bonding mechanism to provide redundancy at the network layer. The dual NIC configuration maintains the network availability of an Oracle Key Vault in case one of the interfaces becomes unavailable. Depending upon the dual NIC configuration mode, load balancing of the network traffic may also be achieved.

This type of configuration is particularly useful in large Oracle Key Vault deployments where need for operational continuity is higher despite physical or software failures. Configuring a dual NIC network interface helps to avoid the scenario where, for example, a network interface associated with an Oracle Key Vault server becomes unavailable, which can result in a loss of communication between the Oracle Key Vault nodes and between endpoints and Oracle Key Vault server.

In previous releases, Oracle Key Vault supported only one network interface. When you install and configure Oracle Key Vault in this release, you have the option of using a single network interface (Classic mode) or using dual NIC mode.

LDAP User Authentication and Authorization in Oracle Key Vault

Starting with this release, you can configure authentication and authorization of Oracle Key Vault users to be centrally managed in a Microsoft Active Directory.

This feature benefits large deployment environments where enterprise users are centrally managed in a Microsoft Active Directory. Centrally managing users, as opposed to creating user accounts in different systems and applications, is not only easier and more efficient for administrators, it improves compliance, control, and security. You enable the Microsoft Active Directory users to authenticate with Oracle

Key Vault through the use of their directory credentials. You manage the authorization of the directory users in Oracle Key Vault through mapping definitions between Microsoft Active Directory groups and Oracle Key Vault administrative roles or user groups. When a directory user successfully logs in to Oracle Key Vault the first time, Oracle Key Vault automatically creates an Oracle Key Vault user account for this user.

RESTful Services Utility Command-Line Interface for Appliance Management

In Oracle Key Vault release 21.1, the RESTful services utility command-line interface has been expanded and redesigned to provide more functionality.

This redesign includes the following:

- Structured and simplified command-line interface with the following format:

  ```
  okv category resource action configuration-options command-options
  ```

- Profile support in configuration file to centrally administer multiple Oracle Key Vault endpoints.
- JSON support for command input and output.
- New commands to support system management tasks and monitoring of deployments, in addition to the enhancements for the current functionality for endpoints, wallets, and security objects.

In previous releases, the RESTful command-line interface covered only endpoint, wallet, and security object management commands. The addition of system management commands, which include commands for backup operations and server operations for standalone, multi-master, and primary-standby environments, benefits large deployments where the automation of these types of configuration is needed.

The previous RESTful services APIs are still supported.

Support for SFTP to Transfer External Backups

Oracle Key Vault now supports the use of SSH Secure File Transfer Protocol (SFTP) for the transfer of (scheduled) external backups to remote backup destinations.

SFTP enables the use of ZFS Storage Appliance as a backup destination. The use of Secure Copy Protocol (SCP) is also supported.

Development Using the Java SDK

This release introduces a new Java language software development kit that you can use to integrate custom endpoints with the Oracle Key Vault server.

The Java SDK enables developers to create their own custom endpoint integration solutions for Oracle Key Vault.

Development Using the C SDK

This release introduces a new C language software development kit that you can use to integrate custom endpoints with the Oracle Key Vault server.

The C SDK allows developers to create their own custom endpoint integration solutions for Oracle Key Vault.

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 21.9.0.0.0** or click the **+Add to Cart** button next to the **Oracle Key Vault 21.9.0.0.0**.

   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 file:

   - *Vpart_number*`.iso` (Oracle Key Vault 21.9.0.0.0)
8. To the right of the **Print** button, click **View Digest Details**.

The listing for the ISO file expands to display the SHA-1 and SHA-256 checksum reference number for the ISO file.

9. Copy the SHA-256 checksum reference number and store it for later reference.
10. Click **Download** and select a location to save the ISO file.
11. Click **Save**.

    The size of the ISO file 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 file is downloaded to the specified location, verify the SHA-256 checksums of the downloaded file:

    ```
    $ sha256sum V<part_number>.iso
    ```

    Ensure that the checksum matches the value that you copied from the **File Download** dialog box in step 9.
13. Optionally, burn the `V<part_number>.iso` file to a DVD-ROM disc and then label the discs:

    ```
    OKV 21.9
    ```

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 21.9 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
- Software Development Kit Issues

General Issues

This section describes general Oracle Key Vault issues.

Certificate Attributes Will Not Get Uploaded By okvutil For Windows Endpoints Using 11.2.0.4 DB

Issue: When you upload an object containing certificates to the Oracle Key Vault server from a Windows endpoint system that has Oracle Database release 11.2.0.4, the cryptographic algorithm and cryptographic length will not be displayed on the management console for such certificates uploaded.

Workaround: If you wish the cryptographic algorithm and cryptographic length to be displayed for certificates, then consider uploading such objects from a different combination of endpoint platform or Oracle Database version.

Bug Number: 32855953

KMIP Daemon May Stop Servicing Endpoints Until the Server is Rebooted

Issue: It has been observed that the KMIP daemon, which services endpoint requests, may stop working on an Oracle Key Vault server due to database bug 33846119. This was observed during a CA certificate rotation operation. Because endpoints must have their certificates rotated by specific nodes, this may result in certain endpoints getting stuck. On the Endpoint Details page of the management console, the endpoint will be

seen as having the **Common Name of Certificate Issuer** stuck on **Updating to current certificate issuer** and not transitioning to the new CA certificate's common name, despite repeated successful endpoint operations to other nodes. In standalone and primary-standby configurations, this may result in endpoints failing to fetch objects from the server. In multi-master cluster environments, the endpoints will be able to fetch objects from other nodes, but not the affected node.

Workaround: Rebooting the server will resolve the issue.

Bug Number: 33846151

KMIPD May Be Stopped At The Same Time On Multiple Nodes During Certificate Rotation

Issue: During certificate rotation, the `kmip` and `kmipus` daemons are restarted several times, with downtime of a few minutes each. It is possible that this restart can happen on multiple nodes at the same time. Especially in smaller clusters, this means it is possible, although unlikely, that all of the `kmip` daemons in the cluster are unable to respond to endpoint requests, potentially leading to downtime.

Workaround: Turn on or increase the in-memory cache timeout, persistent cache timeout, and persistent cache refresh window values prior to certificate rotation in order to avoid endpoint downtime.

Bug Number: 31311978

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

Oracle Key Vault 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

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

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

Update Client Endpoint Software With Latest Scan List, Config Params, and Certificate Rotation Updates When a KMIP Server Operation Is Executed Using REST

Issue: Whenever a server operation is performed using the RESTful utility, the configuration file `okvclient.ora` does not get updated with the latest state. The configuration file remains static as it is when the endpoint software is installed. For example, if there is a new node added to the Oracle Key Vault cluster, the client configuration file `okvclient.ora` will not get updated with the new node information whenever a server operation is performed using the RESTful utility.

Workaround: In order to have an updated `okvclient.ora` after a change in configuration, perform an operation using `okvutil` or the Oracle Key Vault SDK.

Bug Number: 29492842

Oracle Key Vault Integration with Oracle Audit Vault 20.8 Fails

Issue: Integrating Oracle Key Vault with Oracle Audit Vault 20.8 fails with the following error:

Failed to get client software from Audit Vault server, ensure Public Host Key and 'support' user password are valid

This is due to a change in permissions of Oracle Audit Vault client jar files that are required for the integration process.

Workaround: Before integrating Oracle Key Vault with Oracle Audit Vault 20.8, the following commands need to be run on the **Oracle Audit Vault 20.8 server**:

1. Log into the **Oracle Audit Vault 20.8 server** as user support through ssh:

   $ ssh support@*AV_instance_ip_address*

2. Switch to user root:
   $ su – root

3. Check the permissions of the `/var/lib/oracle/dbfw/av/jlib/agent.jar` and `/var/lib/oracle/dbfw/av/jlib/avcli.jar` files. They should be similar to the below:

   ```
   # ls -l /var/lib/oracle/dbfw/av/jlib/agent.jar

   -rw-r-----. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
   dbfw/av/jlib/agent.jar

   # ls -l /var/lib/oracle/dbfw/av/jlib/avcli.jar

   -rw-r-----. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
   dbfw/av/jlib/avcli.jar
   ```

4. Take a backup of these files (using /bin/cp -p below preserves file permissions):

   ```
   # /bin/cp -p /var/lib/oracle/dbfw/av/jlib/agent.jar /var/lib/oracle/
   dbfw/av/jlib/agent.jar.bkp

   # /bin/cp -p /var/lib/oracle/dbfw/av/jlib/avcli.jar /var/lib/oracle/
   dbfw/av/jlib/avcli.jar.bkp

   # ls -l /var/lib/oracle/dbfw/av/jlib/agent.jar /var/lib/oracle/
   dbfw/av/jlib/agent.jar.bkp
   ```

   Check that the file permissions and ownership of the original files and their backups are identical:

   ```
   -rw-r-----. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
   dbfw/av/jlib/agent.jar

   -rw-r-----. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
   dbfw/av/jlib/agent.jar.bkp

   # ls -l /var/lib/oracle/dbfw/av/jlib/avcli.jar /var/lib/oracle/
   dbfw/av/jlib/avcli.jar.bkp

   -rw-r-----. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
   dbfw/av/jlib/avcli.jar
   ```

```
-rw-r-----. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/avcli.jar.bkp
```

5. Update the permissions of `/var/lib/oracle/dbfw/av/jlib/agent.jar` and `/var/lib/oracle/dbfw/av/jlib/avcli.jar`:

```
# /bin/chmod 644 /var/lib/oracle/dbfw/av/jlib/agent.jar

# /bin/chmod 644 /var/lib/oracle/dbfw/av/jlib/avcli.jar
```

Check the file permissions and ownership of the original files and their backups again:

```
# ls -l /var/lib/oracle/dbfw/av/jlib/agent.jar /var/lib/oracle/
dbfw/av/jlib/agent.jar.bkp
-rw-r--r--. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/agent.jar

-rw-r-----. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/agent.jar.bkp

# ls -l /var/lib/oracle/dbfw/av/jlib/avcli.jar /var/lib/oracle/
dbfw/av/jlib/avcli.jar.bkp

-rw-r--r--. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/avcli.jar

-rw-r-----. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/avcli.jar.bkp
```

Notice that `/var/lib/oracle/dbfw/av/jlib/agent.jar` and `/var/lib/oracle/dbfw/av/jlib/avcli.jar` now have additional permissions when compared to their backup.

You can now proceed to integrate Oracle Key Vault with Oracle Audit Vault 20.8 using the normal process.

After the integration has been successfully completed, the permissions on the Oracle Audit Vault 20.8 files can be restored to their original values. To do so:

1. SSH into the **Oracle Audit Vault 20.8 server** as user support.
```
$ ssh support@AV_instance_ip_address
```
2. Switch to user root:

```
$ su - root
```

3. Check the permissions of the `/var/lib/oracle/dbfw/av/jlib/agent.jar` and `/var/lib/oracle/dbfw/av/jlib/avcli.jar` files.
They should be similar to the below:

```
# ls -l /var/lib/oracle/dbfw/av/jlib/agent.jar /var/lib/oracle/
dbfw/av/jlib/avcli.jar
-rw-r--r--. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/agent.jar

-rw-r--r--. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/avcli.jar
```

4. Restore the files to their backups:

```
# /bin/cp -pf /var/lib/oracle/dbfw/av/jlib/agent.jar.bkp /var/lib/
oracle/dbfw/av/jlib/agent.jar

# /bin/cp -pf /var/lib/oracle/dbfw/av/jlib/avcli.jar.bkp /var/lib/
oracle/dbfw/av/jlib/avcli.jar
```

5. Check permissions again. This time, the files should be identical in permissions and ownership to the backups:

```
# ls -l /var/lib/oracle/dbfw/av/jlib/agent.jar /var/lib/oracle/
dbfw/av/jlib/agent.jar.bkp

-rw-r-----. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/agent.jar

-rw-r-----. 1 oracle oinstall 36212863 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/agent.jar.bkp

# ls -l /var/lib/oracle/dbfw/av/jlib/avcli.jar /var/lib/oracle/
dbfw/av/jlib/avcli.jar.bkp

-rw-r-----. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/avcli.jar

-rw-r-----. 1 oracle oinstall 30091681 Sep 29 09:28 /var/lib/oracle/
dbfw/av/jlib/avcli.jar.bkp
```

   The same workaround must be applied when deleting Oracle Key Vault integration with Oracle Audit Vault 20.8.

Oracle Key Vault Endpoint Utility Displays an Error on Uploading a Java KeyStore Containing a Key with Password Different from the KeyStore Password

Issue: Oracle Key Vault endpoint utility `okvutil` supports to upload keys stored in a Java KeyStore to the Oracle Key Vault server. If a Java KeyStore contains a key protected with a password different from the KeyStore password, the utility shows an error "`Error: Cannot Invoke JKS Method`" and fails to upload the objects stored in the KeyStore.

Workaround: A workaround is to set the same password for Java KeyStore and all of the password protected keys stored in the KeyStore, upload the KeyStore to the Oracle Key Vault server using `okvutil`, and then reset the passwords if you require them to be different.

To change the keystore password:

1. *$ keytool -storepasswd -keystore keystorename*
2. Enter keystore password: <*old password*>
3. New keystore password: <*new password*>
4. Re-enter new keystore password: <*new password*>

To change an individual key password:

1. *$keytool -keypasswd -keystore keystorename -alias <alias>*

2. Enter keystore password: *<keystore password>*
3. Enter key password for *<alias>* *<old key password>*
4. New key password for *<alias>: <new key password>*
5. Re-enter new key password for *<alias>: <new key password>*
   If the passwords cannot be changed, then the workaround is to upload the entire keyStore as an 'OTHER' type object instead of 'JKS' using `okvutil`. Following this approach stores the KeyStore as an opaque object on the server and requires to track the passwords by some other mechanism. It enables to store the KeyStore in a centralized repository for backup and distribution, however losing the ability to manage keys and certificate at an object-level granularity.

   Bug Number: 22818588

RESTful Services Utility Commands May Not Work As Intended When Using client_wallet Parameter in okvrestcli.ini

Issue: In Oracle Key Vault release 21.9, when `okvrestcli.ini` profiles are configured with `client_wallet` parameter, the RESTful services utility commands may not function as intended in certain uncommon scenarios when multiple Oracle Key Vault administrators share the same RESTful services utility installation. You may encounter one or more of these errors depending upon your configuration:

1. RESTful services utility commands from the `managed-object` category may unexpectedly prompt for a user password.
2. RESTful services utility commands to add a user's credentials to an existing client wallet may ask for the password twice.
3. RESTful services utility commands may fail with `Invalid Login Credentials` error.
4. RESTful services utility commands may fail with an exception.

RESTful services utility installation used by a single Oracle Key Vault administrator

- Use the `client_wallet` and `user` parameters in a single profile only.

RESTful services utility installation used by multiple Oracle Key Vault administrators

Patch 36843467 is available with the fix for the Bug 36843335. Oracle recommends that you apply this patch on your Oracle Key Vault release 21.9 deployment if you are using RESTful services utility. Alternatively, use the workaround described below.

Workaround: Ensure that you use a separate profile for each administrator, with each profile containing the `client_wallet` and user parameters of the respective administrator.

Other considerations:

1. Do not specify the `client_wallet` and `user` parameters in the `[Default]` profile. You may specify other parameters such as `server`, `log_property`, and `okv_client_config` in the `[Default]` profile.

2. Ensure that the valid user credentials are available in the corresponding client wallet.
3. Do not specify the `user` or `client_wallet` as the command line options.

Bug Number: 36843335

After a Certificate Rotation Password-Protected Endpoints May Fail to Connect to Oracle Key Vault with Server Connect Failed Errors

Issue: After an Oracle Key Vault 21.9.0.0.0 endpoint is rotated and has received its new certificate, it may fail to connect to Oracle Key Vault and return `Server Connect Failed` errors. This issue is likely to be seen in Oracle Key Vault multi-master cluster deployments when an endpoint receives its certificate when you run the `okvutil` command.

A fix is available for this issue in Bug **37006283**. Apply the patch for bug **37006283** to all the Oracle Key Vault systems in your deployment using the steps detailed in the patch README before initiating a certificate rotation. Oracle recommends that you apply this patch to all systems in the Oracle Key Vault deployment immediately after you upgrade to release 21.9.0.0.0 but before you upgrade the endpoint software. Use the workaround provided for any endpoints (at version 21.9.0.0.0) that have already encountered this issue.

Workaround: Apply the patch for Bug **37006283** to all systems in the Oracle Key Vault 21.9.0.0.0 deployment. Reenroll any endpoints that have already encountered this issue after a certificate rotation. Follow the instructions in the patch README for all other scenarios.

Bug Number: 37006283

Endpoints Cannot be Enrolled When CA Certificate Rotation is In-Progress

Issue: In Oracle Key Vault release 21.9.0.0.0, enrolling a new endpoint when a CA certificate rotation is in progress fails.

Workaround: Complete the CA certificate rotation before you register and enroll new endpoints. During a CA certificate rotation, if there are any endpoints in the REGISTERED state that hinder the progress of the rotation, then consider deleting or suspending such endpoints until the CA certificate rotation process is complete.

Bug Number: 37335254

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
- Primary-Standby Upgrade from Oracle Key Vault 21.1 and 21.2 to 21.6 or 21.7 Fails When Upgrading Primary Server

- Upgrade to Oracle Key Vault 21.9.0.0.0 Misconfigures Internal Oracle GoldenGate Process Settings, Causing Upgrade to 21.0.0.0 to Fail

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

Primary-Standby Upgrade from Oracle Key Vault 21.1 and 21.2 to 21.6 or 21.7 Fails When Upgrading Primary Server

Issue: When upgrading the Oracle Key Vault primary-standby deployment from releases 21.1 and 21.2 to 21.7, the upgrade of the primary server fails.

Workaround: Oracle recommends that you upgrade the Oracle Key Vault primary-standby deployment to a multi-master cluster. Oracle Key Vault primary-standby deployment is now deprecated.

The steps for upgrading from Oracle Key Vault release 21.1 or 21.2 primary standby deployment to Oracle Key Vault release 21.6 are described below. The same steps apply for upgrading to Oracle Key Vault release 21.7 also.

To upgrade an Oracle Key Vault release 21.1 or 21.2 primary-standby deployment to a multi-master cluster, follow these steps for the upgrade:

- First unpair the primary-standby Oracle Key Vault servers
- After the two servers are unpaired, the primary and standby servers will operate in standalone mode. To prevent endpoints from connecting to the old standby (now standalone) Oracle Key Vault server, you must take the old standby off the network.
- Upgrade the standalone server (old primary) to Oracle Key Vault release 21.6.
- Convert the Oracle Key Vault standalone server to a multi-master cluster. You cannot add the old standby as the new node of the cluster. You must install a new standalone Oracle Key Vault server with release 21.6 and then add it to the cluster.

If you choose to continue to use the Oracle Key Vault primary-standby deployment after the upgrade to release 21.6 , follow these steps for the upgrade:

- First unpair the primary-standby Oracle Key Vault servers.
- After the two servers are unpaired, the primary and standby servers will operate in standalone mode. To prevent endpoints from connecting to the old standby (now standalone) Oracle Key Vault server, you must take the old standby off the network.
- Upgrade the standalone server (old primary) to Oracle Key Vault release 21.6.
- Install a new standalone server with the Oracle Key Vault release 21.6.
- Pair the upgraded server with the new server in the primary-standby mode. You cannot add the old standby as the new standby server after upgrade.

Bug Number: 35394085

Upgrade to Oracle Key Vault 21.9.0.0.0 Misconfigures Internal Oracle GoldenGate Process Settings, Causing Upgrade to 21.0.0.0 to Fail

Issue: After you upgrade to Oracle Key Vault release 21.9.0.0.0, some Oracle GoldenGate processes on the Oracle Key Vault system may operate with misconfigured settings, which is not recommended. This happens when you upgrade any Oracle Key Vault system to 21.9.0.0.0. Upgrading such a system from release 21.9.0.0.0 to 21.10.0.0 fails with the following error:

```
/usr/local/okv/bin/okv_ogg_service_config Cannot add cipherSuites to config
/usr/local/okv/bin/okv_ogg_monitor OKV OGG Set OGG Config: Failed to update the
recvsrvr
```

Workaround : After you upgrade the Oracle Key Vault deployment to 21.9.0.0.0, apply the patch for bug 37492574 to correct the configuration for the internal GoldenGate processes and to prevent future upgrades from failing.

Bug Number: 37492574

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
- Failover Issues When Primary OKV Experiences a Controlled Shutdown
- HA Setup Succeeds with Different Primary & Standby RO Restricted Mode Config
- Re-pair After Un-pair from HA 12.2 BP5 to new OKV Server Still Shows Standalone
- SSH Tunnel Status Shows as Disabled on Failover Case in Primary-Standby
- DNS Update on Primary Not Reflected in Standby
- okvclient.ora Not Properly Updated After a Failover of Primary-Standby

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

Issue: 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

Failover Issues When Primary OKV Experiences a Controlled Shutdown

Issue: Periodically, the primary Oracle Key Vault node in a primary-standby pair may have 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.

Note that failover still occurs in other situations, such as power loss on the primary or database failure.

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

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

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

DNS Update on Primary Not Reflected in Standby

Issue: DNS updates are specific to each Oracle Key Vault server and hence any DNS updates for Primary are not automatically reflected on the Standby.

Workaround: It is recommended to set the same DNS values on both primary and standby servers before pairing them into a Primary-Standby configuration.

Bug Number: 26618613

okvclient.ora Not Properly Updated After a Failover of Primary-Standby

Issue: After a Primary-Standby failover, the endpoint configuration file `okvclient.ora` does not update immediately when the endpoint client communicates with the Oracle Key Vault server.

Workaround: The configuration file `okvclient.ora` gets updated during the periodic updates. The periodic updates are prepared at 1 hour interval and are sent from Oracle Key Vault server to the endpoint whenever the endpoint client communicates with the Oracle Key Vault server after the period interval.

Bug Number: 31372732

Multi-Master Cluster Issues

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

- 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
- Cannot Create A Key On The Upgraded Nodes In A Cluster That Is Not Fully Upgraded
- Certificate Must Be Rotated Before Converting To Cluster If Upgrading From 12.2 BP4 or Older

- Cluster Service Status Is Down After Rotating Server Certificate
- OGG Bug 32079454 Causes Intermittent Distribution Path Failures Causing Replication to Break
- Oracle Key Vault Should Prevent Enabling From Finishing If It Takes Longer Than MDND
- Read/Write Nodes in Read-Only Restricted Mode After a Reboot
- RMAN Automatically Cleans Up Archivelogs Still Necessary for OGG
- System Settings Changed on an OKV Node After Conversion to a Candidate Node Do Not Reflect On The Controller Node

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

Cannot Create A Key On The Upgraded Nodes In A Cluster That Is Not Fully Upgraded

Issue: When a multi-master cluster is in the process of upgrading to Oracle Key Vault release 21.4 or higher version, the symmetric key creation operations fail on the cluster nodes that have been upgraded. The symmetric key creation operations continue successfully on the nodes that have not yet been upgraded. While upgrading the last read/write pair of the cluster, you cannot create a new symmetric key in a multi-master cluster. During the upgrade, operations such as database re-key or enrolling a new database will fail. Once the upgrade of the multi-master cluster completes, symmetric key create or register operations will resume.

Workaround: If you are upgrading a multi-master cluster with more than 2 nodes, you can ensure that symmetric key create or register operations continue to be available on upgraded read/write nodes by applying the patch for Bug 33974435, which is applied to each cluster node after upgrading it, but before enabling the node back into the cluster.

Bug Number: 33974435

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

Issue: If you upgrade from Oracle Key Vault 12.2 BP4 or older and do not generate a new certificate before converting the upgraded Oracle Key Vault server to a cluster node, 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

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

OGG Bug 32079454 Causes Intermittent Distribution Path Failures Causing Replication to Break

Issue: Due to Oracle GoldenGate bug 32079454, distribution paths will intermittently encounter SSL errors that cause them to fail and not automatically restart. This can cause replication between non-read/write peer nodes to break. Other side effects are objects that transition from `PENDING` to `ACTIVE` status to be stuck in `PENDING` status. You will also get replication lag alerts. You can see if a distribution path has potentially failed by checking the **Monitoring** page under the **Cluster** tab, and looking for red, downward arrows in the **Cluster Link State** section.

Workaround: If restarting the cluster link on the **Monitoring** page under the **Cluster** tab does not resolve the issue, restart the node and verify that there are no red, downward arrows on the **Monitoring** page afterward.

Bug Number: 32079491

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

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/`. If replication has broken because of this issue, take a remote backup of the node and then force delete it from the cluster. Note that you may

need to make sure that any keys or other objects created on that node are also on all other nodes in the cluster, and manually re-upload them if they are not.

Bug Number: 30558372

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. Abort the pairing process on both the controller and candidate nodes. Change the system settings on the candidate node as desired, then re-attempt the pairing process.

Bug Number: 29430349

Software Development Kit Issues

The Oracle Key Vault Software Development Kit (SDK) has the following issues when working with Oracle Key Vault server.

- If multiple single instance attributes are added to request TTLV, then no error will be thrown and the first value will get added.

  APIs impacted are: `okvCreateKey`, `okvRegKey`, `okvRegSecretData`, `okvRegOpaqueData`, `okvRegTemplate`, `okvRegPrivateKey`, `okvRegPublicKey`, `okvRegCertificateRequest`, `okvRegCertificate`

- The objects created using SDK are not downloadable by `okvutil` as of today. Attempting to run the `okvutil download` command may show the warning

  ```
  WARNING: Could not store <Unique Identifier of the object>.
  ```

  This warning can be safely ignored as we are skipping the download of keys, secrets & objects created through SDK (if found) to the given wallet. Support for the same will be provided in future releases.

- When a certificate, using SHA-DSA as the signature algorithm, is uploaded to Oracle Key Vault using CSDK, the certificate will be uploaded to Oracle Key Vault without any attributes. If a secret object containing such a certificate is uploaded using `okvutil`, the certificate will be uploaded without the cryptographic algorithm and cryptographic length attributes. If all attributes of such a certificate are required, the workaround will be to use JSDK to upload the certificate to Oracle Key Vault.

Oracle Key Vault Considerations

Below are details and changes of behavior of this release of Oracle Key Vault.

- 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.

For setting up a TDE-enabled Oracle database with Oracle Key Vault, several steps are required for smooth transition with the minimum interruption to your application availability. See Configuring TDE and Oracle Key Vault in an Oracle Data Guard Environment for single instance, multi-tenant Data Guard and Configuring TDE and Oracle Key Vault for Oracle RAC in a Multitenant Environment for 2-node RAC in the *Oracle Database Advanced Security Guide*.

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 this release of Oracle Key Vault:

- Oracle DB 12.1.0.2 with the compatible parameter set to 11.2 or 12.1
- Oracle DB 12.2.0.1
- Oracle DB 18c
- Oracle DB 19c
- Oracle DB 21c

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.

Critical Patch Updates Included in Release 21.9

Oracle Key Vault release 21.9 updated the underlying infrastructure to incorporate the April 2024 Release Update for Oracle Database (19.23 DB RU) - April Release Update. Please sign in for full details.

https://www.oracle.com/security-alerts/cpuapr2024.html

Oracle Key Vault release 21.9 also includes security and stability fixes for Java and Oracle Linux 8.9 operating system.

Oracle Key Vault Release Notes, Release 21.9
F96296-03