Frequently Asked Questions

Oracle Key Vault

Oracle Key Vault (OKV) enables customers to easily deploy encryption and other security solutions by offering robust, central management of encryption keys, Oracle Wallets, Java Keystores, and credential files. This document describes frequently asked questions about Oracle Key Vault installation and deployment.

Features

Q: What kind of keys and secrets can I manage using Oracle Key Vault?

A: Oracle Key Vault enables you to centrally manage Oracle Advanced Security Transparent Data Encryption (TDE) master encryption keys, Oracle Wallets, Java Keystores, and credential files such as files containing SSH keys, and Kerberos keytab files. Additionally, Key Vault can also manage MySQL TDE master encryption key and ACFS (ASM Cluster File System) volumne keys.

Q: How does Oracle Key Vault facilitate sharing of keys, wallets, and keystores?

A: Oracle Key Vault administrators can define access control policies between a set of related server endpoints and a set of keys and secrets. A set of server endpoints is defined as an endpoint group. A set of keys and secrets in Oracle Key Vault is called a virtual “wallet”. When a virtual wallet is assigned to an endpoint group, all the server endpoints are able to access contents of the virtual wallet. This method of sharing is useful for clustered database or middleware servers.

Q: How does Oracle Key Vault manage Oracle Wallets?

Oracle database servers and clients use Oracle Wallets to store Oracle Advanced Security Transparent Data Encryption (TDE) master keys, certificates, server passwords, and connection strings. Oracle Wallet is a standard PKCS#12 file, encrypted with a password-derived key. Oracle Key Vault centrally stores and manages itemized contents of Oracle Wallets. It allows sharing of wallet contents across server clusters. It audits access to wallet contents.

Scale

Q: How many keys can Oracle Key Vault store and manage?

A: Oracle Key Vault can store and manage hundreds of thousands of keys.

Q: How many server endpoints can Oracle Key Vault manage?

A: As most endpoints connect only intermittently to the Oracle Key Vault appliance, more than thousand endpoints can be supported by Oracle Key Vault.

Upgrade to Oracle Key Vault 18

Q: Can I directly upgrade from Oracle Key Vault 12.x to 18?

A: Follow the instruction in the Release Notes for OKV 18 to confirm if an upgrade requires one or multiple steps.

Q: How can I upgrade to OKV 18 with minimal downtime for my database endpoints that are configured with ‘Online Master Key’?

A: It is highly recommended to go through a complete upgrade cycle in the test environment that matches the current production OKV version:

1) Set the Persistent Cache timeout to 3 days or more in the OKV Web GUI:
   a) Navigate to the “Endpoints” tab
   b) Select “Settings”
   c) On the “Global Endpoints Confguration Parameters”, click on “Save Default” to populate the text fields with the current default values.
   d) Change the "PKCS11 Persistent Cache Timeout" from 1,440 minutes to 4,320 minutes (= 3 days) or more
   e) Click “Safe”

   Each endpoint that is not using the global endpoint settings because they have individual settings saved should either revert to the global endpoint settings via the "Clear All" button on the Endpoint Details page or have its PKCS11 Persistent Cache Timeout set to 4,320 minutes (or more) as well.

2) All databases do a mandatory re-key operation to refresh the current master key in the Persistent Cache with the new "contract" (expiration time); DBAs confirm and report back to the OKV owner after validating all persistent caches have been updated (for example standby databases, non-lead-nodes in RAC)

3) OKV owner suspends all Endpoints.

4) If “Root-of-Trust” is configured, reverse migrate out of the HSM

5) OKV owner creates full backup with all keys included (no new keys can be created because suspended endpoints are forced to use their Persistent Cache).

6) If OKV runs in active primary/passive standby mode, break the HA configuration.

7) Old standby OKV is lost; install fresh OKV 18 onto this host (=> OKV02); in parallel, upgrade old primary OKV 12.2 to 18.1, **this becomes the Initial Node (OKV01) as it has all the keys**; optionally configure Root-of-Trust in all 18.1 OKVs **before** adding them to the cluster.

8) Follow the setup guide to connect the two stand-alone OKVs (from 7)) 18.1 to your first read-write pair OKV01 and OKV02.

9) Add OKV03 to the first pair as a read-only node.

10) Add OKV04 to the read-only node OKV03 as its read-write peer to make it the next read-write pair.

11) Continue to build up your cluster by adding a read-only node, then adding another node using that read-only node to create another read-write pair up to a maximum of 16 (read-write pairs and read-only nodes combined).

After the servers have been installed, connected and configured, upgrade the OKV client software:

12) Backup the current OKV client 12.x installation (incl. the “/okv/$ORACLE_SID” sub-directory either under $ORACLE_BASE, $ORACLE_HOME, or $OKV_HOME).

13) Shutdown database

14) Clean out current OKV client 12.x installation (incl. the “/okv/$ORACLE_SID” sub-directory either under $ORACLE_BASE, $ORACLE_HOME, or $OKV_HOME).

15) Install the new OKV client software on the database hosts.

16) Restart database

17) In OKV, Resume the endpoints where the client software was upgraded.

Key Availability and Backup

Q: Can Oracle Key Vault (OKV) provide continuous key availability?

A: Group up to 16 Oracle Kay Vault instances together to form a key management cluster, potentially encompassing geographically distributed data centers. Within this cluster, there is always at least one other OKV that is updated immediately.

Q: How do I backup the Oracle Key Vault appliance?

A: Oracle Key Vault can be backed up either manually or automatically on a configurable schedule. The backup process executes the internal backup script, encrypts the backup file, and then automatically moves the encrypted backup file to a remote destination over a secure connection. Refer to the Oracle Key Vault documentation for further details.

Administration

Q: How do I administer and manage Oracle Key Vault?

A: A browser-based management console makes it easy to administer Oracle Key Vault, provision server endpoints, securely manage key groups, and report on access to keys. Key Vault also exposes command line interfaces to perform certain administrative functions such as upgrades and patches. Additionally, endpoint enrollment and provisioning can be automated using RESTful interfaces for mass deployment on premise or in the cloud.

Q: How does Key Vault provide administrative separation of duties?

A: Key Vault administrator roles can be divided into key, system, and audit management functions for separation of duties. Additional users with operation responsibilities for server endpoints can be granted access to their keys and wallets for ease of management.

Security

Q: How does Oracle Key Vault secure its stored keys and secrets?

A: Oracle Key Vault uses various Oracle database security technologies to secure its stored keys and secrets. These include Oracle Advanced Security Transparent Data

Encryption to encrypt the keys and secrets, Database Vault, and Virtual Private Database to prevent sensitive data exposure to privileged users.

Oracle Key Vault also audits all access to the stored keys and secrets. The audit logs can be forwarded to Oracle Audit Vault and Database Firewall for log consolidation.

Q: What protocol is used to securely transport the keys between Key Vault and the endpoints?

A: Endpoints such as database and middleware servers communicate with the Oracle Key Vault server using OASIS KMIP (Key Management Interoperability Protocol) over a mutually authenticated secure TLS transport over fixed port 5696.

The Oracle Key Vault browser-based management console uses HTTPS (fixed port 443). Browser-based management console supports third-party certificates.

Installation and Hardware Requirements

Q: Where can I download the software for Oracle Key Vault?

A: Oracle Key Vault can be downloaded from Oracle Software Delivery Cloud.

Go to https://edelivery.oracle.com;

Search Oracle Key Vault for product. Click *Continue* and select Oracle Key Vault, Platform Linux x86-64 to download.

Q: What are the recommended hardware specifications?

A: CPU: Minimum x86-64 16 cores, Recommended: 24-48 cores with cryptographic acceleration support (Intel® AES-NI)

Memory: Minimum 16 GB of RAM, Recommended: 32-64 GB

Disk: Minimum 2 TB, Recommended: 4 TB

Hardware Compatibility: Refer to the hardware compatibility list (HCL) for Oracle Linux Release 6 Update 9. The HCL is available at http://linux.oracle.com/pls/apex/f?p=117:1

Q: How is Oracle Key Vault installed?

A: Oracle Key Vault is packaged as a software appliance, which means it contains everything, including the operating system, needed to install the product on bare hardware.

During installation, the Key Vault installer completely takes over the hardware. In addition to partitioning and formatting the disks, it installs the base OS, user-space libraries, Oracle Database, and Oracle Key Vault software. It configures all software components (OS, networking, database) automatically and with minimal user involvement. It hardens the operating system, network configuration, and database according to hardening best practices. It also removes unnecessary packages and software and disables unused services and ports.

Q: Can I deploy the Oracle Key Vault on Windows or Solaris?

A: Oracle Key Vault can only be deployed on bare metal. Any existing OS including Windows or Solaris and software will be removed by the install process. Note that this applies only to the Oracle Key Vault and is independent of the OS for the server endpoint whose keys are being managed.

Q: Can I run Oracle Key Vault on Oracle Virtual Machine?

A: For testing or proof of concept purposes, Oracle Key Vault can be run in Oracle Virtual Machine or Oracle VirtualBox. However, for production deployment, Oracle Key Vault should be installed on dedicated physical hardware; otherwise VM administrators may be able to gain access to underlying keys and secrets stored inside Oracle Key Vault.

Q: Can I install Oracle Key Vault on Oracle Database Appliance (ODA) or Oracle Exadata?

A: At this time Oracle Key Vault is not certified with the Oracle Database Appliance or Oracle Exadata. Oracle Key Vault can however be used to manage keys used by ODA or Oracle Exadata.

Integration with Target Endpoints

Q: How is the endpoint software downloaded and deployed?

A: Database servers, middleware servers, and systems that wish their keys and secrets to be managed are called endpoints. The Oracle Key Vault management console provides links to download and provision required endpoint software. The endpoint software package contains all necessary binaries and configuration files as well as TLS certificates for establishing a mutually authenticated secure connection between the endpoint and Oracle Key Vault.

When Key Vault system administrators register endpoints, Oracle Key Vault automatically generates a one-time enrollment token. Endpoint software is downloaded using this enrollment token by the endpoint administrators such as DBAs. Oracle Key Vault also supports self-enrollment in a test environment with minimal administrative involvement.

Q: Can I migrate Oracle TDE master key in Oracle Wallet to Oracle Key Vault?

A: For Oracle Databases using Transparent Data Encryption (TDE), Oracle Key Vault can centrally manage TDE master keys over a direct network connection as an alternative to using local wallet files. You can easily migrate an existing TDE master key from Oracle Wallet to Oracle Key Vault by running one of the SQL commands ALTER SYSTEM MIGRATE or ADMINISTER KEY MANAGEMENT MIGRATE. Refer to the Oracle Key Vault documentation for further details.

Q: Will Oracle Key Vault impact the performance of encryption at the endpoints?

A: Oracle Key Vault does not directly impact the performance of encryption.

Q: How much downtime should I plan for configuring and provisioning my endpoints?

A: Endpoints that upload Oracle Wallets or Java Keystores to Oracle Key Vault are not required to have any downtime. Oracle database endpoints migrating TDE master keys from Oracle Wallet to Oracle Key Vault requires closing and opening a wallet in standalone configuration and database restart in shared server configuration which requires planning for minimal downtime.

Feature Compatibility

Q: Which Oracle database and middleware versions are supported by Oracle Key Vault?

A: Oracle Key Vault supports upload and restore of Oracle Wallets from all supported releases of Oracle middleware and Oracle database on Oracle Linux, Red Hat Linux, Solaris Sparc, Solaris x64 , AIX, HP-UX and Windows. Direct connections between TDE and Oracle Key Vault are supported for Oracle Database 11*g*R2, 12.1, 12.2, 18 and 19 on Oracle Linux, Red Hat Linux, Solaris Sparc, Solaris x64 , AIX, HP-UX and Windows.

Q: What types of key storage files does Oracle Key Vault support?

A: Oracle Key Vault supports Oracle Wallet and Java Keystore (JKS and JCEKS) key storage files. Java Keystores using Oracle JDK 1.4, 1.5, 1.6, 7, and 8 have been tested.

Q: What types of credential files can Oracle Key Vault store?

A: Oracle Key Vault stores any credential files such as Kerberos keytabs and files containing SSH keys. Technically, a credential file can be any file that you want to manage centrally. Each credential file size must be under the 128 KB limit to be uploaded into Oracle Key Vault.

Q: Can Oracle Key Vault encrypt sensitive data?

A: Oracle Key Vault only manages keys and secrets for the endpoints that encrypt data. The data encryption responsibilities are left to the endpoints. Oracle Key Vault does encrypt its managed keys.

Q: Can Oracle Key Vault manage DBMS_CRYPTO keys?

Oracle Key Vault currently does not manage DBMS_CRYPTO keys.

Learn More!

Q: Where do I go to learn more?

A: Product collateral can be found at:

http://www.oracle.com/technetwork/database/options/key-management/index.html

Q: Where can I go for more training?

A: Resources and collateral for Oracle Key Vault including product datasheet, frequently asked questions, and videos are available on Oracle.com and Oracle Technology Network (OTN) web pages. Also, Oracle University offers a training course on Oracle Key Vault.

Q: Is there an external discussion forum?

A: The Oracle Key Vault OTN page under the Database Security category will be updated as soon as the discussion forum is created. Please refer to the Oracle key management blog at https://blogs.oracle.com/securityinsideout/advanced-security for announcements. You may leave comments or ask questions directly on the blog.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200