ORACLE

Oracle Key Vault: Frequently Asked Questions

Enterprise key and secrets management

August, 2023 Version 21.6

ORACLE

Table of contents

ORACLE

Overview

Oracle Key Vault securely stores encryption keys, Oracle Wallets, Java KeyStores, SSH key pairs, and other secrets in a scalable, fault-tolerant cluster that supports the OASIS KMIP standard and deploys in Oracle Cloud Infrastructure (OCI), Microsoft Azure, and Amazon AWS as well as on-premises.

This document answers frequently asked questions about Oracle Key Vault installation and deployment.

Features

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

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 SSH keys and Kerberos keytab files. Key Vault can also manage MySQL TDE master encryption key and ACFS (ASM Cluster File System) volume keys.

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

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 can access the contents of the virtual wallet. This method of sharing is useful for databases using Data Guard or Real Application Clusters (RAC) or middleware servers requiring Java Keystores.

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.

What sign and verify operations are supported?

Oracle Key Vault supports sign and verify operations using the keys stored in Oracle Key Vault. PL/SQL, Java, or C applications can encrypt, decrypt, sign, and verify using keys stored in Oracle Key Vault. Users can also download the public keys and use external tools like openssl to verify the signatures. Oracle Key Vault can sign raw data or its message digest using nonextractable private keys. The fact that these keys never leave the Oracle Key Vault cluster helps maintain their secrecy and security.

Scale

How many keys can Oracle Key Vault store and manage?

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

How many server endpoints can Oracle Key Vault manage?

As most endpoints connect only intermittently to the Oracle Key Vault appliance, Oracle Key Vault can support more than a thousand endpoints.

ORACLE

Key availability and backup

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

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

How do I back up the Oracle Key Vault appliance?

Oracle Key Vault can be backed up 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

How do I administer and manage Oracle Key Vault?

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 contains a command line interface to perform administrative functions such as upgrades and patching. Additionally, endpoint enrollment and provisioning can be automated using RESTful interfaces for mass deployment on-premises or in the cloud.

How does Oracle Key Vault support centralized users?

The Oracle Key Vault console users can be managed locally or centrally through integration with Microsoft Active Directory. The console also supports user authentication using SAML tokens to provide a seamless single sign-on experience for users authenticated to federated identity providers, such as Azure Active Directory (AD) or Active Directory Federation Services (ADFS).

How does Key Vault provide administrative separation of duties?

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

Security

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

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.

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

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. Can I enable FIPS mode in Oracle Key Vault? Oracle Key Vault release 18.1 installation is FIPS 140–2 compliant. Selecting the option to install with FIPS 140–2 compliance performs all required changes during the installation.

FIPS 140-2 mode can also be enabled after the installation. Can I integrate Oracle Key Vault with my corporate HSM? Yes. When a Hardware Security Module (HSM) is deployed with Oracle Key Vault, the Root of Trust (RoT) remains in the HSM. The HSM RoT protects the wallet password, which protects the TDE master key, which in turn protects all the encryption keys, certificates, and other security artifacts managed by the Oracle Key Vault server. This three-tier hierarchy mitigates the risk of administrators potentially extracting keys and credentials from systems they can physically access. In this RoT usage scenario, the HSM does not store any customer encryption keys. Customer keys are stored and managed directly by the Oracle Key Vault server. For more information on certified HSMs for Oracle Key Vault Root of Trust, please refer to the "Oracle Key Vault Integration with HSM" guide.

Installation and hardware requirements

How is Oracle Key Vault delivered?

Oracle Key Vault is packaged as a software appliance containing 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 turns off unused services and ports.

What are the recommended hardware specifications for Oracle Key Vault on dedicated hardware?

The minimum hardware requirements for deploying the Oracle Key Vault software appliance are:

- CPU: Minimum: x86-64 16 cores. Recommended: 24-48 cores with cryptographic acceleration support (Intel AESNI).
- Memory: Minimum 16 GB of RAM. Recommended: 32–64 GB.
- Disk: Minimum 2 TB. Recommended: 6 TB.
- Both BIOS and UEFI boot mode. For a system with a disk size greater than 2 TB, Oracle Key Vault supports booting in UEFI mode only.
- Note: Oracle Key Vault does not support fiber channel storage with multipath for the boot disk.

Refer to the Oracle Key Vault documentation for a complete list of requirements.

Can I deploy Oracle Key Vault on OCI?

Yes. The easiest way to deploy Oracle Key Vault on your Oracle Cloud infrastructure if from the Oracle Cloud Marketplace.

Can I deploy Oracle Key Vault on third-party clouds?

Customers running Oracle databases in multiple clouds can minimize network latency by deploying one or more Oracle Key Vault nodes alongside their databases. You can deploy Key Vault on compute nodes in Microsoft Azure and Amazon Web Services (AWS), delivering the same fault-tolerant, highly scalable, and highly available keys and secret management solution. Up to 16 Key Vault nodes can operate as part of a single cluster and can be deployed in OCI, on-premises data centers, or a combination based on customer requirements.

Where can I download the software for Oracle Key Vault?

Download Oracle Key Vault from the Oracle Software Delivery Cloud: Go to https://edelivery.oracle.com; Search for "Oracle Key Vault". Click Continue and select Oracle Key Vault, Platform Linux x86-64 to download the .iso image.

What features are available to support the deployment of Oracle Key Vault on virtual machines?

Oracle Key Vault supports cloned templates. This capability allows users to add more Oracle Key Vault nodes for high availability or local access for databases spread across multiple data centers. Users can clone an Oracle Key Vault template and then use a few REST commands to add nodes to an Oracle Key Vault cluster in minutes. They can also integrate cluster creation, node additions, and node removals in infrastructure-as-code (IAC) tools like Terraform.

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

Currently, Oracle Key Vault installation is not certified in 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

How is the endpoint software downloaded and deployed?

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, configuration files, and 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. The endpoint administrators then download endpoint software using this enrollment token. Oracle Key Vault also supports self-enrollment in a test environment with minimal administrative involvement.

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

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 local wallet files. You can easily migrate an existing TDE master key from Oracle Wallet to Oracle Key Vault by running the SQL command ADMINISTER KEY MANAGEMENT MIGRATE. Please refer to the Oracle Key Vault documentation for further details.

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

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

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

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 require no downtime.

Feature compatibility

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

Oracle Key Vault supports uploading and restoring Oracle Wallets from all supported releases of Oracle middleware and Oracle database on Oracle Linux, Red Hat Linux, Solaris Sparc, Solaris x64, AIX, HPUX and Windows. Direct connections

between TDE and Oracle Key Vault are supported for Oracle Database 12.1.0.2 to 23c on Oracle Linux, Red Hat Linux, Solaris Sparc, Solaris x64, AIX, HP-UX and Windows.

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

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.

What types of credential files can Oracle Key Vault store?

Oracle Key Vault stores any credential files such as Kerberos keytabs and files containing SSH keys. A credential file can be any file you want to manage centrally. Each credential file size must be under the 128 KB limit to be uploaded into Oracle Key Vault. Can Oracle Key Vault encrypt sensitive data? 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.

Can Oracle Key Vault manage DBMS_CRYPTO keys?

Oracle Key Vault currently does not manage DBMS_CRYPTO keys.

More information

Where can I find more information on Oracle Key Vault?

For more information, please see the Oracle Key Vault page on Oracle.com. Various helpful information is available online, including the data sheet, white paper, customer references, end-user documentation, and a discussion forum. If you want to try Oracle Key Vault, visit Oracle LiveLabs.

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle