Oracle Key Vault: Frequently Asked Questions

Enterprise key and secrets management

March, 2024 Version 21.8

Public

Table of contents

Overview

Oracle Key Vault securely stores encryption keys, Oracle Wallets, Java KeyStores, SSH key pairs, and other secrets in a scalable, fault-tolerant, highly-available cluster. Users can deploy Key Vault servers in Oracle Cloud Infrastructure (OCI), Microsoft Azure, Amazon AWS, and on-premises on dedicated hardware or in virtual machines. Key Vault supports the OASIS KMIP standard.

This document answers frequently asked questions about Oracle Key Vault features, use cases, and deployment.

Features

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

Oracle Key Vault lets you centrally manage the following:

- Oracle Advanced Security Transparent Data Encryption (TDE) master encryption keys
- SSH key pairs for remote server access control and centrally managed public key authentication
- Oracle Wallets
- Java KeyStores
- Kerberos keytab files
- GoldenGate trail file encryption master keys
- ACFS (ASM Cluster File System) volume encryption keys
- ZFS Storage Appliance master encryption keys
- MySQL TDE master encryption keys
- MongoDB master encryption keys
- Encryption keys for dbms_crypto

Can 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. An 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 the sharing of wallet contents across server clusters. It also audits access to wallet contents.

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

Oracle Key Vault administrators can define access control policies between related server endpoints and a set of keys and secrets. A set of keys and secrets in Oracle Key Vault is called a virtual wallet. When a virtual wallet is assigned to an endpoint, all the server endpoints can access the contents of the virtual wallet. This method of sharing is helpful for databases using Oracle Data Guard, Real Application Clusters (RAC), sharded databases, and middleware servers requiring Java keystores.

TDE online master encryption key management

What are the benefits of online TDE key management using Oracle Key Vault?

Centralizing TDE keys in Oracle Key Vault makes them easier to administer, particularly when users are running TDE across 100s or 1,000s of databases. Maintaining encryption keys separate from the servers hosting encrypted data is also essential for many compliance requirements. Centralizing key management in Oracle Key Vault facilitates secure key sharing across RAC instances and standby databases. Finally, centralized key management can provide better governance and security as keys can be managed, backed up, revoked, suspended, and recovered.

Which Oracle Databases does Oracle Key Vault support?

Oracle Key Vault provides online master encryption key management for all Oracle databases from version 12.1.0.2 to 23c, running on UNIX and Windows endpoint platforms. In addition to on-premises Oracle Databases, it works with databases running in virtual machines, compute instances on OCI, and third-party clouds. Oracle Key Vault supports Oracle Cloud at Customer databases (including ExaDB-C@C and ADB-C@C) and Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D and ExaDB-D@Azure). Please refer to the Oracle Key Vault documentation for information about supported endpoint platforms.

Do I need to maintain Oracle TDE master keys in an Oracle wallet after migrating them to Oracle Key Vault?

No; for Oracle Databases using Transparent Data Encryption (TDE), Oracle Key Vault can centrally manage TDE master keys as an alternative to local wallet files. After uploading the current and all retired keys from the wallet to OKV, you can easily migrate an encrypted database to Oracle Key Vault by running the "ADMINISTER KEY MANAGEMENT MIGRATE" SQL*Plus command. Please refer to the Oracle Key Vault documentation for further details.

Will Oracle Key Vault impact TDE encryption performance?

TDE master keys are accessed from Oracle Key Vault and used to decrypt the data encryption keys. Since the data encryption keys are obfuscated and cached in the database, using Oracle Key Vault does not impact TDE performance.

SSH Key Management

What are the advantages of using Oracle Key Vault to store and manage SSH keys?

Administrators use SSH keys to access servers and IT systems, and that use has exploded with the rise of cloud computing. Unmanaged SSH key pairs used for public key authentication are a security and management challenge. Oracle Key Vault helps organizations better manage their SSH keys in two ways:

- **Centralized access control** – Administering users' public keys for SSH hosts in Oracle Key Vault makes provisioning and revocation of access to systems by administrators easy to manage. Administrators can provision a user for access to a remote server by uploading the user's public key into a special SSH server wallet in Oracle Key Vault. To deny access to the remote servers, SSH administrators only need to remove the user's public keys from the SSH Server wallets. Centralizing the management of SSH public keys allows administrators to track and report on access attempts.

- **Improved SSH key governance** – Centralizing both private and public keys in a fault-tolerant, scalable, and continuously available key management system allows for enhanced key governance. With centralized key management, organizations can enforce corporate security policies such as required key length and algorithm, periodic key rotations, and key usage reporting and auditing. Furthermore, administrators can quickly restrict all remote access in case of an ongoing security incident. Security for SSH keys can be enhanced by generating a private/public SSH key pair on-board Key Vault and by making the private key non-extractable so it cannot leave Key Vault's cluster boundary. Copying the user's public key into the SSH Server wallet in Key Vault provides the user with server access. The end-user who attempts to access a remote server can do so as long as a) the public key is in the remote server's SSH wallet and b) the user has access to the matching private key in Key Vault. Managing keys in Key Vault mitigates risks associated with disk-based private keys, including key theft, unauthorized copying and sharing of keys, and key loss.

How does SSH user management work with Oracle Key Vault?

Key administrators can use standard SSH commands to create SSH key pairs in Oracle Key Vault for SSH users. One-time installation of Oracle Key Vault's PKCS-11 libraries enables the SSH clients to leverage Oracle Key Vault's sign and verify functionality to provide access to SSH hosts with no need for storing the private keys on the client.

How does SSH access management work with Oracle Key Vault?

Oracle Key Vault administrators can create virtual wallets in Oracle Key Vault for each SSH host user. The one-time installation of the endpoint software and configuration of the SSH daemon on the SSH host enables these hosts to access their virtual wallets dynamically on Oracle Key Vault at the time of an SSH connection request. An SSH user can be provisioned to access an SSH host simply by adding their public key to the host's virtual wallet. Managing SSH users' public keys in a virtual wallet in Oracle Key Vault enables centralized provisioning/de-provisioning/suspending users' access to SSH hosts and enhanced access and activity reporting capabilities. Managing private and public keys in Oracle Key Vault allows key administrators to rotate SSH keys without SSH user or client software intervention.

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?

Most endpoints connect intermittently to the Oracle Key Vault appliance, so an Oracle Key Vault cluster can support thousands of endpoints. Users can deploy additional Key Vault servers to an existing cluster to scale to more endpoints and provide high levels of availability and locality.

Key availability and backup

How does Oracle Key Vault provide continuous key availability?

Users can deploy up to 16 Oracle Key Vault instances to form a key management cluster, potentially encompassing geographically distributed on-premises and cloud data centers. Keys are shared across all nodes in the cluster, and endpoints may access any available node to access their keys.

How does Oracle Key Vault mitigate the potential for lost keys?

Each Oracle Key Vault cluster has at least one synchronous pair of Key Vault nodes. When an endpoint writes a new key to one of the nodes in the pair, the update operation is not complete until it is updated on the node's synchronous partner node. Distributing these synchronous pairs across regions or data centers helps ensure that key updates are recorded even if hardware or facility fails.

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 and keep them private, Database Vault to prevent sensitive data exposure to privileged users, and Virtual Private Database for user-level access control. Oracle Key Vault audits all access to the stored keys and secrets and can forward audit logs to Oracle Audit Vault and Database Firewall for analysis and consolidation.

How are keys transported between Oracle 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 1.2 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 supports installation in FIPS 140–2 mode. Selecting the option to install with FIPS 140–2 mode 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 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 documentation.

Installation and hardware requirements

How is Oracle Key Vault delivered?

Oracle Key Vault is packaged as a software appliance containing everything needed to install the product on dedicated hardware or as a virtual machine, including the operating system. During installation, the Key Vault installer partitions and formats the disks, 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.

  Oracle Key Vault supports 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 is from the Oracle Cloud Marketplace.

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

Customers running Oracle databases in 3rd party 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 automate cluster creation, node additions, and node removals.

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.

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 Databases 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 online TDE key management for Oracle Database 12.1.0.2 to 23c on Oracle Linux, Red Hat Linux, SuSE Linux Enterprise Server, Solaris Sparc, Solaris x64, AIX, HP-UX, and Windows. Oracle Key Vault supports uploading and restoring Oracle Wallets from all supported releases of Oracle middleware and Oracle Databases on Oracle Linux, Red Hat Linux, SuSE Linux Enterprise Server, Solaris Sparc, Solaris x64, AIX, HPUX, 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. Oracle Key Vault has been tested with Java keystores using Oracle JDK 1.4, 1.5, 1.6, 7, and 8.

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 manages keys and secrets for the endpoints that encrypt data. It also supports sign and verify operations on data. While Oracle Key Vault encrypts managed data such as keys and secrets, the data encryption responsibilities are left to the endpoints.

Can Oracle Key Vault manage DBMS_CRYPTO keys?

Yes. The product includes Java and C language SDKs that enable users to integrate their DBMS_CRYPTO applications with Oracle Key Vault.

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. The page has links to helpful information, including the data sheet, white paper, customer references, and product documentation. If you want to try Oracle Key Vault, visit Oracle LiveLabs.

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