ORACLE

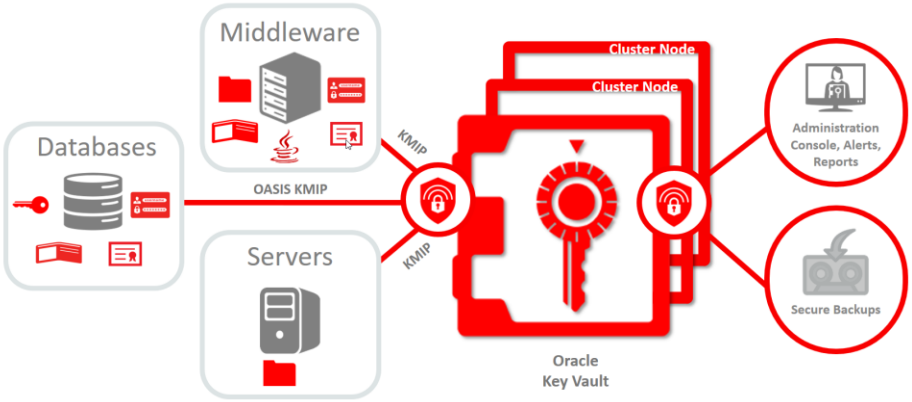
ORACLE KEY VAULT

Oracle Key Vault 18

Security threats and increased regulation of personally identifiable information, payment card data, healthcare records, and other sensitive information have expanded the use of Oracle Transparent Data Encryption (TDE) and other encryption technologies in the data center. As a result, management of encryption keys, Java keystores and other secrets has become a vital part of the data center mission. Oracle Key Vault simplifies the deployment of encryption across the enterprise with extremely scalable, fault-tolerant, continuously available key management.

INTRODUCTION

Oracle Key Vault enables customers to deploy encryption and other security solutions by centrally managing Transparent Data Encryption (TDE) database encryption keys, Oracle Wallets, Java Keystores, and credential files. Oracle Key Vault supports a high-availability cluster deployment architecture to deliver continuous key service availability and geographic coverage.



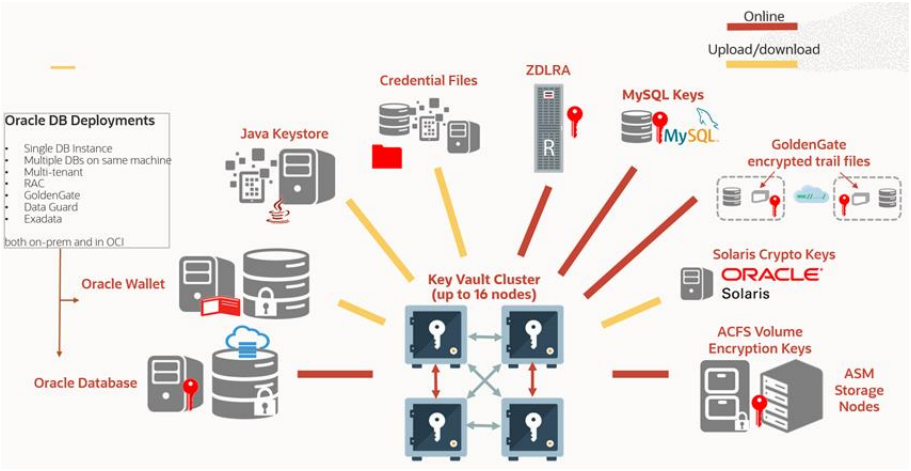
Oracle Key Vault Deployment Overview

Key Features

- Manages TDE master keys, Oracle Wallets, Java Keystores, and credential files
- Eliminates local key stores with on-line TDE master key management
- Can be provisioned into an OCI tenancy from the Oracle Cloud Marketplace in minutes
- Supports 16 read/write nodes for continuous availability
- Endpoints automatically select available nodes and transparently fail over in the event of any outage
- Automates endpoint enrollment with RESTful services utility
- Automates key creation, deactivation and key deletion with RESTful APIs
- Keeps the encrypted databases running even when network connections are down with optional persistent cache
- Migrates keys from Oracle Wallet to Oracle Key Vault
- Integrates with Hardware Security Modules (HSMs)
- Supports OASIS KMIP standard
- Simplifies deployment with pre-configured and secured software appliance
- Installs on a variety of supported hardware platforms or on Oracle Cloud Infrastructure from the Oracle Cloud Marketplace

TRANSPARENT DATA ENCRYPTION MASTER KEY MANAGEMENT

Oracle Key Vault provides physical separation between the encryption key and encrypted data often required for regulatory compliance. It centrally manages TDE master keys over a direct network connection as an alternative to using local wallet files. This also eliminates operational challenges of wallet file management such as periodic password rotation, backing up wallet files, and recovery from forgotten-password situations. Master key sharing supports Oracle Multitenant database instances as well as Oracle Real Application Clusters (RAC), Oracle Data Guard, and Oracle GoldenGate. Existing master keys used for encrypted data in Oracle databases can be easily migrated from Oracle Wallets to Oracle Key Vault.



Oracle Key Vault provides online master key management without the need for local wallets.

MANAGE ORACLE WALLETS, JAVA KEYSTORES, AND CREDENTIAL FILES

Administrators often copy Oracle wallets and Java keystores across servers and server clusters manually. Oracle Key Vault streamlines sharing of wallets across database clusters such as Oracle RAC, Oracle Data Guard, and Oracle GoldenGate. Secure sharing of wallets also facilitates movement of encrypted data using Oracle DataPump and Oracle Recovery Manager (RMAN). Oracle Key Vault securely archives these files and allows recovery of wallets and keystores when they are mistakenly deleted or if their passwords are forgotten.

In many enterprises credential files containing SSH keys, Kerberos keytab files, and similar credential files are also widely distributed without appropriate protective mechanisms. Oracle Key Vault backs up credential files for long-term retention and recovery. Oracle Key Vault easily recovers these files when needed, audits access to them, and shares them across trusted endpoints.

CONTINUOUSLY AVAILABLE AND SCALABLE CLUSTER ARCHITECTURE

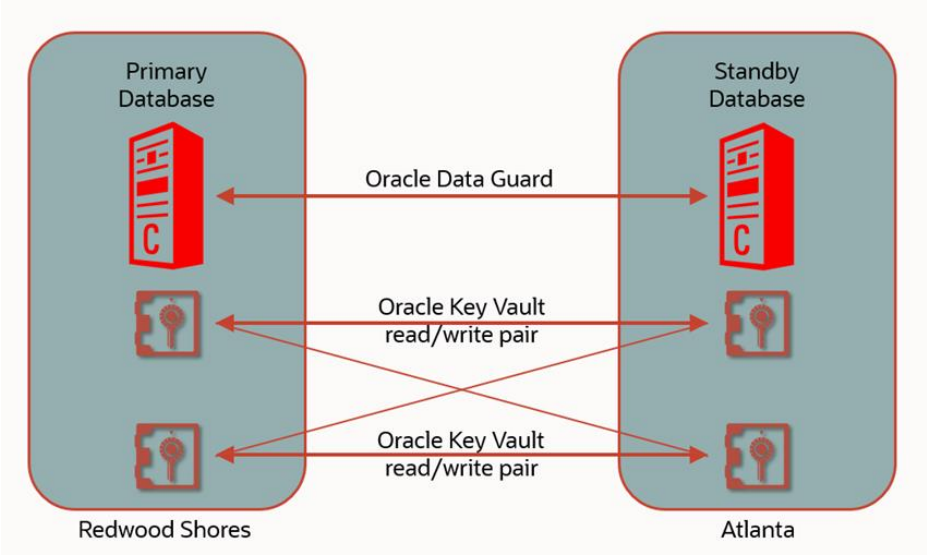
Oracle Key Vault nodes deploy as part of a cluster to provide continuous availability and geographic coverage. Oracle Key Vault supports up to 16 nodes in a cluster, automatically synchronizing any changes made at one node across the entire cluster.

Each database endpoint transparently maintains its own list of available nodes and is continuously aware of changes to the cluster. If the current node becomes

Key Business Benefits

- Provides separation between the key and encrypted data required for compliance
- Reduces risk and cost by consolidating key stores
- Protects keys or credentials from inadvertent loss or theft
- Ensures continuous key availability when software, hardware or network fails
- Scales to thousands of databases across data centers
- Lowers hardware cost with no idle nodes
- Full accountability of key management life cycle with auditing

unavailable, the endpoint transparently fails over to another nearby node. To further increase resilience for network outages, Oracle Key Vault allows the optional creation of a persistent cache on the database servers so databases remain fully functional should network connectivity to all nodes be down.



Database endpoints transparently fail over to a nearby node when the preferred node becomes unavailable.

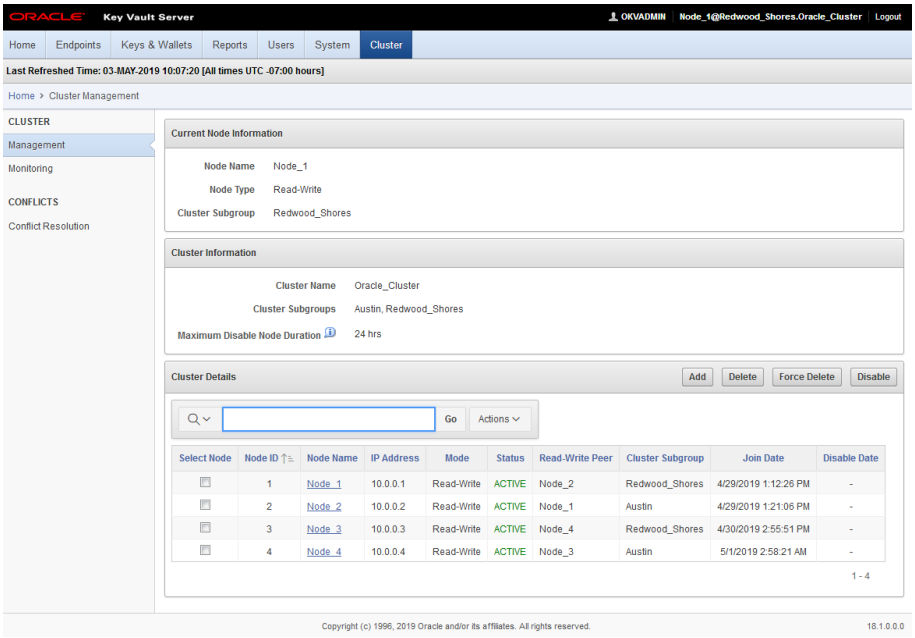
Oracle Key Vault's unique cluster deployment architecture is highly scalable. Customers can deploy pairs of read-write nodes across data centers to help ensure endpoints have access to a local node for both read and write operations. In addition, the cluster architecture supports deployment of additional read-only nodes to provide a local key service presence for smaller data centers. Finally, each Oracle Key Vault server deploys on commodity hardware platforms that can be sized to meet the most demanding service loads. The result is a key service which can support thousands of databases deployed around the world, with extreme availability and high service levels.

ADMINISTRATION

A browser-based management console makes it easy to administer Oracle Key Vault servers, manage clusters, provision server endpoints, securely manage key groups, and report on access to keys. Administrators receive email alerts for important status updates and system activities such as upcoming password and key expirations. Endpoint enrollment and provisioning can be automated using protected RESTful interfaces for mass deployment to databases.

SECURITY

Security is a critical requirement for enterprise scale deployment. Oracle Key Vault addresses security at multiple layers including infrastructure, administration, and operations. Oracle Key Vault is delivered as an ISO image and installs as a pre-configured and secured software appliance. It uses various Oracle database security technologies to protect keys and secrets stored inside Oracle Key Vault. For example, Oracle Key Vault uses Transparent Data Encryption to encrypt keys stored in the embedded Oracle Database. It also uses Oracle Database Vault to restrict unauthorized privileged user access.



Oracle Key Vault management console simplifies tasks such as adding or removing nodes from the cluster.

Administrator roles can be divided into key, system, and audit management functions for separation of security duties. Oracle Key Vault audits all critical operations including key access and key life cycle changes. The audit data can be forwarded to Oracle Audit Vault and Database Firewall (AVDF) or to a syslog server for record retention and reporting. Oracle Key Vault supports SNMP v3 for remote monitoring.

Oracle Key Vault can integrate with hardware security modules (HSMs) to provide additional security for keys, certificates, and other security artifacts during patching and upgrades. In this case, the HSM serves as a root of trust, protecting 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 mitigates the risk of administrators potentially extracting keys and credentials from systems they can physically access.

For organizations that need to conform to the Federal Information Processing Standard (FIPS), Oracle Key Vault installs with a FIPS 140–2 compliant option. Selecting this option performs all required changes during the installation to ensure that only FIPS 140–2 compliant libraries are used for the Key Vault server's operating system, embedded Oracle Database, and other components. In addition, a FIPS 140–2 certified HSM deployed as a root of trust can be used to further help meet these compliance requirements.

INSTALLATION ON HARDWARE AND ON THE ORACLE CLOUD

Oracle Key Vault is easy to install and can be deployed on compatible x86-64 hardware of users' choice. It is also available from the Oracle Cloud Marketplace and can be deployed in an OCI tenancy within minutes, providing fault-tolerant, continuous key management services to on-premises, hybrid, or multi-cloud database deployments. Oracle Key Vault supports endpoints on common enterprise platforms including Oracle Linux, Red Hat Linux, Solaris SPARC, Solaris x64, IBM AIX, HP-UX (IA) and Microsoft Windows.

Related Products

Oracle Key Vault is an important database security control. Related Oracle Database Security products include:

- Oracle Advanced Security
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting
- Oracle Audit Vault and Database Firewall

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