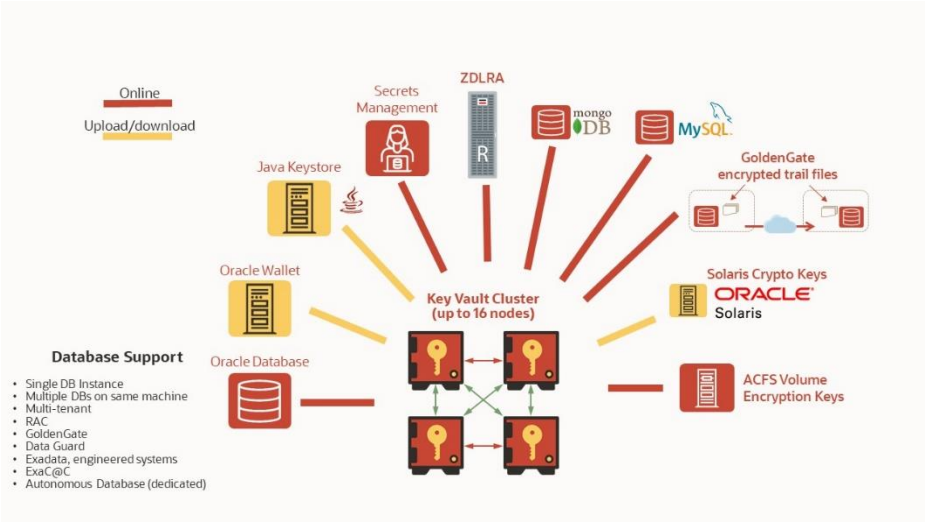
ORACLE

Oracle Key Vault

Security threats and increased regulations for handling sensitive information are driving the use of Oracle Transparent Data Encryption (TDE) and other encryption technologies in the data center. As a result, management of encryption keys, wallets, Java keystores and other secrets has become a vital part of the data center mission. Oracle Key Vault simplifies the deployment of TDE and other encryption technologies across the enterprise with scalable, highly-available key and secrets 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, credential files and other secrets. Oracle Key Vault supports a high-availability cluster deployment architecture to deliver continuous availability and geographic locality.



Oracle Key Vault delivers secure key management for mission-critical systems across the enterprise.

Manage TDE Master Keys

Many regulations and security best practices require that encryption keys be stored separately from the encrypted data. Oracle Key Vault addresses this requirement for Oracle TDE users by managing the keys securely in the service and as an alternative to using local wallet files. This 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 Databases running on-premises, on Exadata

Oracle Key Vault use cases

- Key management for Oracle Databases using TDE
- Key management for integrated Oracle products and solutions such as GoldenGate and ZDLRA
- Wallet, keystore, and credential file management for Oracle Databases and applications
- Secrets management for securing automation scripts
- Centralized key and secrets management for applications that process sensitive information
- KMIP compatibility for third-party key management support

Cloud@Customer, and Autonomous Database (Dedicated), and works with options such 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.

Secure Oracle Wallets, Java Keystores and Other Secrets

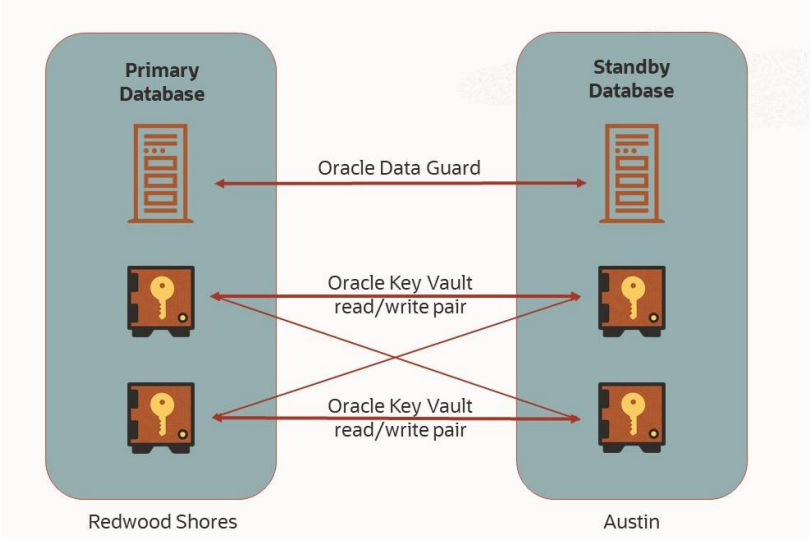
Administrators often copy Oracle wallets and Java keystores across servers and server clusters manually. Oracle Key Vault streamlines sharing of wallets across database clusters such as Oracle RAC, Oracle Data Guard, and Oracle GoldenGate. Secure sharing of wallets also facilitates movement of encrypted 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 files containing SSH keys, Kerberos keytab files, and system passwords are widely distributed without appropriate protective mechanisms. Oracle Key Vault securely stores these files, audits access to them, shares them across trusted endpoints and backs them up for long-term retention and recovery.

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 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 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.

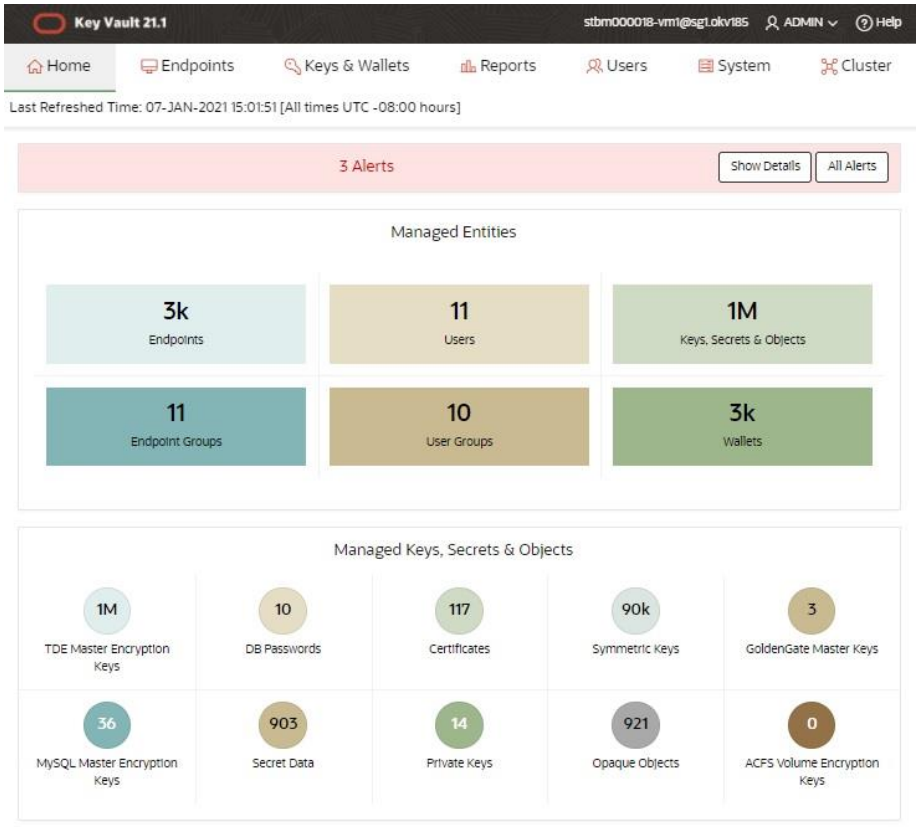
Key Features

- Manages TDE master keys, Oracle Wallets, Java Keystores, and credential files
- Eliminates local key stores with on-line TDE master key management
- Provisions 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
- Complete set of RESTful services to automate key lifecycle management, endpoint enrollment, and Oracle Key Vault administration
- in-memory and persistent cache options keep encrypted systems running even when network connections are down
- Integrates with Hardware Security Modules (HSMs) as root of trust
- Supports OASIS KMIP standard

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.

Easy 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.



Oracle Key Vault management console allows users to understand at a glance the various security objects under management.

Secure Software Appliance

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

Key Business Benefits

- Provides separation between the key and encrypted data required for compliance
- Reduces risk and cost by consolidating key stores
- Protects keys and secrets from inadvertent loss or theft
- Ensures continuous key and secret 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

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.

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.

Deploys on-Premises and in 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
- Oracle Data Safe cloud service