ORACLE DATA SHEET

Oracle Key Vault

Security threats and increased regulation of personally identifiable information, payment card data, healthcare records, and other sensitive information have expanded the use of encryption 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 ecosystem, impacting both security and business continuity. Oracle Key Vault is a centralized key management platform that accelerates the deployment of encryption across the enterprise.

KEY FEATURES

- Manages keys, Oracle Wallets, Java Keystores, and credential files in a modern and robust key management platform
- Securely shares keys across authorized endpoints in an enterprise
- Manages key lifecycle stages including creation, rotation, and expiration
- Optimized for Transparent Data Encryption (TDE) master keys
- Easily enrolls and provisions endpoints
- Automates endpoint enrollment using protected RESTful interfaces
- Supports primary and standby for availability and disaster recovery
- Supports read-only restricted mode for server and persistent cache for endpoints to enhance endpoint availability
- Schedules automatic backup to a remote location
- Supports prior database versions without requiring database patching
- Supports Linux, Windows, Solaris, AIX, and HP-UX(IA) endpoint platform
- Supports Hardware Security Module (HSM) Integration
- Supports the OASIS KMIP standard

Introduction to Oracle Key Vault

Oracle Key Vault (OKV) enables customers to quickly deploy encryption and other security solutions by centrally managing encryption keys, Oracle Wallets, Java Keystores, and credential files; it is optimized for managing Oracle Advanced Security Transparent Data Encryption (TDE) master keys. The full-stack, security-hardened software appliance uses Oracle Linux and Oracle Database technology for security, availability, and scalability. OKV supports the OASIS KMIP (Key Management Interoperability Protocol) industry standard.

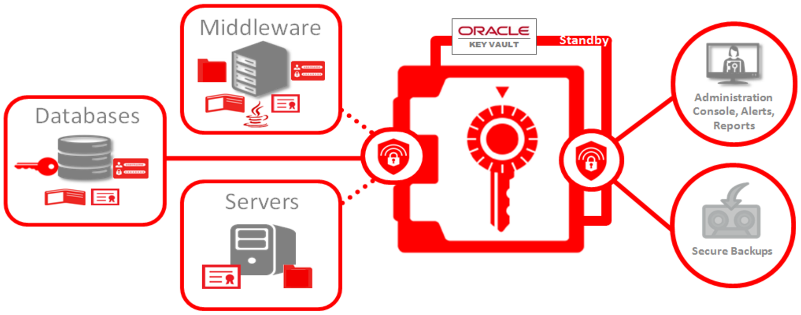

Figure. Oracle Key Vault Deployment Overview

Centrally Manage Oracle Wallets and Java Keystores

Oracle Wallets and Java Keystores are often distributed across servers and server clusters manually. Oracle Key Vault (OKV) itemizes and stores contents of these files in a master repository while allowing server endpoints to continue operating disconnected from OKV using their local copies. Once archived, wallets and keystores can be recovered back to servers if their local copies are mistakenly deleted or their passwords are forgotten. OKV streamlines sharing of wallets across database clusters such as Oracle RAC, Oracle Active Data Guard, and Oracle GoldenGate. Secure sharing of wallets also facilitates movement of encrypted data using Oracle DataPump and Oracle Transportable Tablespaces. OKV can be used with Oracle Wallets from all supported releases of Oracle Middleware and Oracle Database.

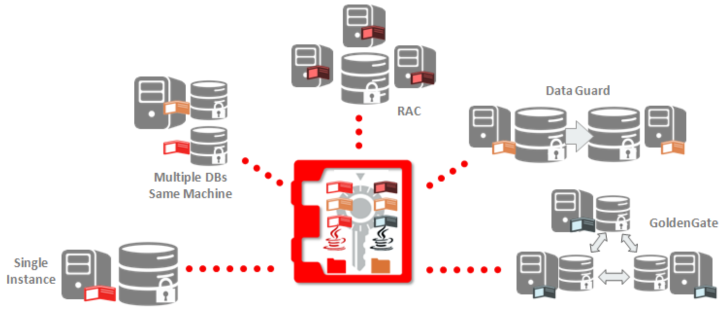

Figure. Oracle Key Vault Wallet Management Scenario

Online Transparent Data Encryption Master Key Management

For Oracle databases using Transparent Data Encryption (TDE), OKV centrally manages TDE master keys over a direct network connection as an alternative to using local wallet files. This eliminates operational challenges of wallet files management such as periodic password rotation, backing up wallet files, and recovery from forgotten-password situations. This also provides physical separation between the encryption key and encrypted data often mentioned in regulatory compliance. The master keys stored in OKV can be made available for decrypting tablespace keys or table keys across databases according to endpoint access control settings. This method of sharing keys without local wallet copies is useful when TDE is running on database clusters such as Oracle RAC, Oracle Active Data Guard, and Oracle GoldenGate. Existing master keys used for encrypted data in Oracle databases can be easily migrated from Oracle Wallet to OKV as part of the initial setup. Direct network connections between TDE and OKV are supported for Oracle Database 11*g*R2, Oracle Database 12*c,* and Oracle Database 18c without requiring database patching.

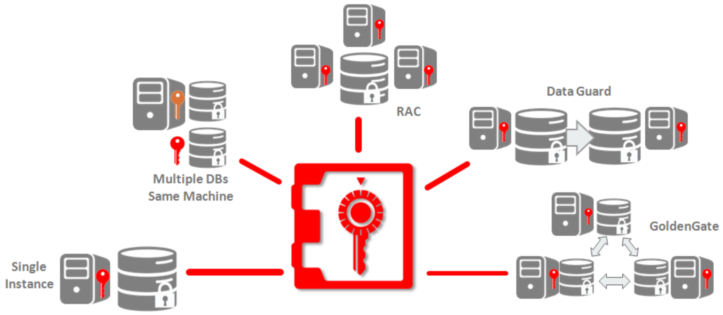

Figure. Oracle Key Vault Online TDE Master Key Scenario

Centrally Backup Credential Files

Credential files containing SSH keys, Kerberos keytab files, and similar credential files are also widely distributed without appropriate protective mechanisms. Oracle Key

ORACLE KEY VAULT

RELATED PRODUCTS

Oracle Key Vault is an important control in the Oracle Database Security suite. 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

Vault (OKV) backs up credential files for long-term retention and recovery. OKV easily recovers these files when needed, audits access to them, and shares them across trusted endpoints.

Oracle Key Vault Administration

A browser-based management console makes it easy to administer Oracle Key Vault (OKV), provision server endpoints, securely manage key groups, and report on access to keys. 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. Administrators receive email alerts for important status updates and system activities such as upcoming password and key expirations.

Security is a critical aspect for enterprise scale deployment. OKV uses various Oracle database security technologies to protect keys and secrets stored inside OKV. For example, OKV 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, and it audits all critical operations including key access and key life cycle changes. OKV audit data can be forwarded to Oracle Audit Vault and Database Firewall (AVDF) or to a syslog server for audit consolidation. OKV can be monitored remotely via SNMP v3.

Oracle Key Vault Deployment

Oracle Key Vault (OKV) is packaged as an ISO image and is delivered as a pre-configured and secured software appliance. The appliance is easy to install and can be deployed on compatible x86-64 hardware of users' choice depending on the scale of deployment.

OKV supports endpoints on common enterprise platforms including Linux, Windows, Solaris, AIX, and HP-UX (IA). Endpoint enrollment and provisioning can be automated using protected RESTful interfaces for mass deployment on premise or in the cloud. Oracle Key Vault is typically deployed in a primary and standby configuration for increased availability.

Oracle Key Vault protects keys and secrets for an enterprise while simplifying and centralizing management of keys, Oracle Wallets, Java Keystores, and secrets.

ORACLE

CONTACT US

For more information about Oracle Key Vault, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

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

Hardware and Software, Engineered to Work Together

Oracle is committed to developing practices and products that help protect the environment