Frequently Asked Questions

Oracle Key Vault Hybrid Cloud Key Management

Oracle Key Vault (OKV) enables customers to easily deploy encryption and other security solutions by offering robust, central management of encryption keys, Oracle Wallets, Java Keystores, and credential files. OKV now supports key management for both on-premises as well as cloud endpoints. This document answers frequently asked questions about OKV hybrid cloud key management.

Hybrid Cloud Key Management

Q: What is hybrid cloud key management?

A: Hybrid Cloud Key Management is a deployment topology for cloud encryption solutions where data is encrypted in the cloud while the encryption key is managed from on-premise Oracle Key Vault.

On-premises Oracle Key Vault now manages Oracle Advanced Security TDE master encryption keys for Oracle Database Cloud Service (DBCS) in addition to managing TDE master encryption keys for on-premises Oracle databases. Hybrid cloud key management enables customers maintain control and visibility of master encryption keys used in Oracle Cloud as well as for on-premises Oracle databases.

Q: What are the benefits of hybrid cloud key management?

A: Utilizing an on-premise centralized key management infrastructure for both on-premise and cloud database endpoints offers many advantages which include maintaining control and visibility of keys irrespective of the location of the endpoints, consistent key management policies, shared resources between on-premise and cloud, and lower TCO.

Q: Does hybrid key management apply only to master keys or also to wallets and other credential files that are stored in Oracle Key Vault?

A: Hybrid Cloud Key Management only supports online TDE master key management for DBCS instances. This does not apply to managing wallets or credential files for resources in Oracle Cloud.

Q: When should I suspend TDE master keys for DBCS instances?

A: Suspending access to TDE master key should be done only in very serious conditions such as when you think that there is an unauthorized intrusion at the OS level. Suspending access to keys allows you time to investigate the intrusion and collect evidence, while at the same time removing all access to your sensitive data. Suspending TDE master keys means that the Oracle database can no longer access any encrypted data in the database, and in such cases any access to that data would get an ORA-28353: “failed to open wallet” error.

Q: How do I suspend TDE master keys for DBCS instances?

A: To suspend access, Key Vault system administrator can click “suspend” button corresponding to the DBCS instance from Oracle Key Vault management console. Clicking the “suspend” button for an endpoint temporarily removes access to the encryption key, such that the encrypted data is not accessible both to the application and the administrators in cloud. If you are satisfied with your investigation, clicking “resume” button resumes the access to the keys. Temporary removal of access to the encryption keys by clicking “suspend” button on an endpoint is also applicable to on-premise Oracle Database endpoint.

Q: Can on-premises OKV manage TDE master keys for Oracle Databases in non-Oracle cloud environments?

A: OKV can manage TDE master keys for Oracle Databases in any cloud as long as network connectivity exists

ORACLE

between OKV server and Oracle Databases (11gR2 and above).

Hybrid Cloud Key Management Deployment

Q: At a high level, how do I setup hybrid cloud deployment using DBCS with on-premise OKV?

A: If OKV is already installed on-premise, upgrade to OKV 12.2 BP1 (or higher), else install and configure OKV 12.2.0.1 (or higher) on-premise. Through the OKV administration UI, setup a SSH tunnel between DBCS instances (using TDE) and the primary OKV server. Follow usual procedures to enroll and provision the DBCS database instance as OKV endpoint as per the Oracle Key Vault documentation.

Q: Which version of OKV supports Hybrid Cloud deployments?

A: Hybrid Cloud Key Management is supported from OKV 12.2.0.1.0 (12.2 BP1) onwards.

Q: Which Oracle Database Cloud Services are supported by OKV hybrid cloud key management?

A: OKV hybrid cloud key management supports Oracle Database as a Service (DBaaS).

Q: What happens if on-premise primary OKV server fails over to the standby OKV server?

A: When primary OKV server fails over to the standby server, the standby server will automatically establish SSH tunnels to all active database cloud service endpoints.

Q: What are the availability considerations? Would my database hang if OKV is not available, or is slow due to internet access issues?

A: Oracle Database endpoints caches keys in memory for a configured time interval. By default, the time interval is 5 minutes so that the database can handle brief network outages. Customers can change this cache value to meet their business and security needs.

Q: Can I integrate my OKV with on-premise HSM?

A: On-premise Key Vault can be integrated with an on-premise HSM as a “root-of-trust” for the key hierarchy that protects encrypted data stored in Key Vault. This root-of-trust is generated within the HSM and never leaves the HSM. Integration with an on-premise HSM is supported only on a new installation of Key Vault 12.2.0.1 and later.

For further details refer to the Key Vault HSM Integration guide.

Network and SSH Tunnel Deployment

Q: Do I need to poke a hole in my network firewall?

A: Typically, no changes are required to your network firewall. However, if your firewall does not already allow outbound SSH connections, the outbound SSH port (22) needs to be unblocked. Refer to the Oracle Key Vault documentation for further details regarding setting up SSH between Oracle Key Vault and DBCS instances.

Q: How does hybrid model handle temporary network glitches?

A: Cloud database PKCS#11 library caches the TDE master key for a short duration to prevent disruption of access to encrypted data for brief network glitches. For any network outage that disrupts the SSH tunnel, OKV will automatically reestablish the SSH tunnel.

Q: How is the traffic encrypted between DBCS database instance and on-premise OKV server?

A: Communication between on-premise OKV and DBCS instances use encrypted SSH tunnels. In addition, all OKV endpoints communicate with the Oracle Key Vault server using OASIS KMIP (Key Management Interoperability Protocol) over a mutually authenticated secure TLS transport.

Q: How do I setup SSH tunnel between on-premises OKV and DBCS instances?

A: SSH tunnel setup for OKV hybrid cloud key management uses standard key-based authentication.

First, copy the public key from primary OKV server management console to the DBCS instance via the DBCS admin UI interface for SSH key setup. Then, as system administrator for OKV, log on to the management console and create the SSH tunnel by providing the public IP address for DBCS instance and port number. Refer to the Oracle Key Vault documentation for further details.

Q: Do I need to setup SSH tunnel for each Oracle database instance in Oracle Cloud?

A: OKV supports two scenarios. You can setup individual SSH tunnel between each Oracle DBCS instance and primary OKV server. Alternatively, you can designate a DBCS instance (or any other host on the cloud) as an OKV

gateway through which all the SSH traffic is routed to the DBCS instances.

The choice of whether to use OKV gateway is based on the number of expected cloud endpoints, dependence on a gateway, and the required network isolation between cloud endpoints. In either case, the KMIP communication is protected end-to-end by TLS 1.2 which means that the communication is not visible to any intermediary and cannot be tampered by any intermediary.

Q: Do I need a SSH tunnel if I have network connectivity from OKV to the endpoints in the cloud?

A: No. SSH tunnel is only required if a direct connection from OKV to the cloud endpoint is unavailable.

Product Licensing and Support

Q: Is Hybrid Cloud Key Management for Key Vault a separately licensed feature?

A: No, Oracle Key Vault hybrid cloud key management does not require a separate license. Licensing Oracle Key Vault allows users to manage keys for on-premise and DBCS endpoints.

Q: Who do I contact if I have issues with OKV hybrid cloud key management?

A: Please contact My Oracle Support at https://support.oracle.com

Learn More!

Q: Where can I get more information about deploying OKV hybrid cloud key management?

A: Refer to the Oracle Key Vault 12.2 administration guide at Key Vault online documentation site. Also refer to Oracle Key Vault OTN page for further details.

Q: Where can I find more information about Oracle Key Vault in general?

A: Product collateral including Datasheet, FAQ, and product documentation links can be found at OTN page for OKV.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200