Vaultive and SafeNet KeySecure KMIP Integration Guide v1.0

September 2016

Vaultive

Contents

Overview 4

Configure KMIP Server to Store Encryption Keys 6

Create a KMIP Server 6

Assign the KMIP Server to an HA Pool 8

Create the Encryption Key 8

Using Keys Stored on the KMIP Server 9

Overview

Vaultive

The Vaultive Cloud Data Security Platform encrypts cloud data at every potential point of cloud exposure—in transit, at rest, and in use—while organizations retain control and ownership of the encryption keys.

The Vaultive enterprise topology consists of the following:

- Vaultive deployments have one or more *sites* corresponding to corporate entities or locations. Sites are physically and logically separate.
- Within each site is one or more high availability (HA) *pools*.
- Each HA pool consists of one or more *nodes* that provide load balancing and failover, and share encryption keys.
- Within every HA pool, one node is set as the *pool master*, which distributes configuration changes to all nodes within the pool.
- Within the enterprise topology, one node is defined as the *configuration master*. The administrator configures all node settings on the configuration master, and the configuration master distributes all configuration changes, except encryption keys, to all pool masters. The pool masters then distribute the configurations to all other nodes.

You configure and manage the Vaultive deployment through the Vaultive Administration Console.

Note: *For details about configuring and managing the Vaultive deployment, see the* Vaultive 5.0 Administration and Configuration Guide.

SafeNet KeySecure

SafeNet KeySecure from Gemalto provides centralized key management for multiple key types from across departments and a variety of encryption products that support the OASIS Key Management Interoperability Protocol (KMIP) standard.

Note: *This guide assumes that the SafeNet KeySecure KMIP server is already installed and configured in your environment. For more information, refer to the* SafeNet KeySecure Appliance Installation and Configuration Guide.

The Integration

The Vaultive integration with SafeNet KeySecure provides organizations with the option to manage encryption keys using SafeNet KeySecure instead of storing them on the Vaultive data encryption virtual appliance. With SafeNet KeySecure in a Vaultive-protected environment, organizations can use a single, centralized key management platform to manage the encryption keys for Vaultive-protected data for KMIP-enabled SaaS applications across the enterprise.

You also manage the Vaultive/Gemalto integration through the Vaultive Administration Console.

Supported Deployment Options

The Vaultive integration with SafeNet KeySecure supports the following deployment options:

- Store keys using Virtual KeySecure, a FIPS 140-2 Level 1-validated, hardened virtual security appliance.
- Store keys using KeySecure with a FIPS 140-2 Level 3 internal hardware root of trust (RoT).
- Store keys using KeySecure with a FIPS 140-2 Level 3 hardware RoT using SafeNet Network HSM or Amazon Web Services (AWS) CloudHSM.

Note: *This integration was tested and verified using Vaultive 5.0 and SafeNet KeySecure 8.4.2.*

For More Information

For more information about Vaultive and Gemalto, visit these sites on the web:

https://www.vaultive.com/

https://www.safenet.gemalto.com/

Configure KMIP Server to Store Encryption Keys

Using the Vaultive Administration Console, you configure a KMIP server for each HA pool to store encryption keys, and then you assign the KMIP server to a pool. Each HA pool can only have one KMIP server.

Valid configurations for KMIP servers and HA pools are as follows:

- One KMIP server per HA pool.
- One KMIP server for multiple HA pools.
- Multiple KMIP servers for multiple HA pools; one server per pool.

To add a KMIP server, steps in the overall process are as follows:

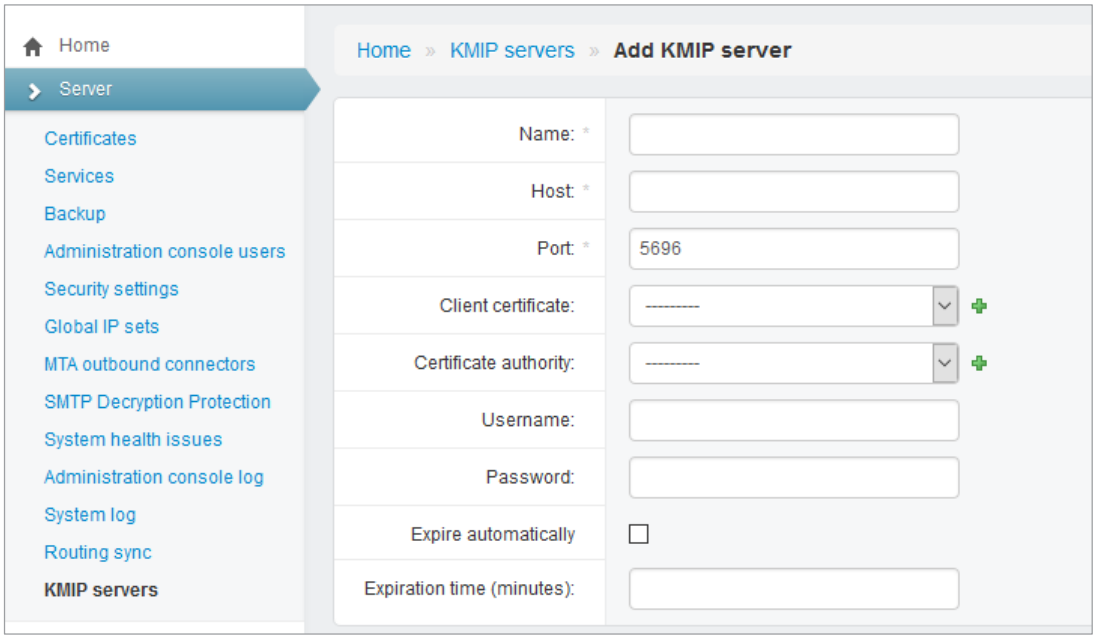
1. Create the KMIP server.
2. Assign the KMIP server to an HA pool.
3. Create the encryption key.

You can repeat these steps to add multiple KMIP severs.

Create a KMIP Server

Procedure

1. Log into the Vaultive Administration Console on the configuration master node for the HA pool.
2. Go to **Server** > **KMIP servers**.
3. Click **Add**.



4. Complete the following required properties:
   - **Name** – Enter the name by which Vaultive identifies the KMIP server.
   - **Host** – Specify the KMIP host to which Vaultive connects.
   - **Port** – Specify the port Vaultive uses to connect to the KMIP server.
5. Specify at least one of the following authentication methods to connect to the KMIP server:
   - Client certificate and certificate authority (CA)
     a. Select or upload a **Client certificate** that Vaultive sends, which the KMIP server uses to validate Vaultive as a legitimate client, and to identify the user.
     b. Select or upload a **Certificate authority** that Vaultive uses to verify the certificate that the KMIP server sends, which identifies the server as legitimate.

     Note: *For information about creating the client certificate, refer to the* SafeNet KeySecure Appliance Installation and Configuration Guide.
   - Username and password
     a. Enter a **Username** that identifies the client (Vaultive) to the KMIP server.
     b. Enter the **Password** for logging into the KMIP server. `
6. Specify whether the encryption key expires.
   - Leave the **Automatically expire** option unselected (the default) to specify that the key never expires. This means that after Vaultive connects with the KMIP server and retrieves the key, it remains available in memory (never on disk) for services to use each time it is needed, without needing to reconnect with the KMIP server.

     In this case, Vaultive retrieves the key only when services restart—either manually or when services reload.
   - Select **Automatically expire** to automatically expire the key after a specified number of minutes. In the **Expiration time (minutes)** field, enter the number of minutes before the key expires.

     In this case, Vaultive must reconnect to the KMIP server and retrieve the key each time it expires—not just when services restart.
7. Click **Test** to verify that the configuration master node can connect to the KMIP server.

   Important: *Do not skip this step.*

   A message will confirm that the KMIP server connection is successful. Otherwise, the message will indicate a possible cause to assist you in troubleshooting the connection.
8. Click **Save** to complete the KMIP server configuration.

Assign the KMIP Server to an HA Pool

Note: *For multiple HA pools, you can add a single KMIP server for multiple HA pools, or one KMIP server per HA pool, but each HA pool can only have one KMIP server.*

Procedure

1. Go to **Topology** > **HA pools**, and click the HA pool to associate with the KMIP server.
2. From the **KMIP server** drop-down list, select the KMIP server that you configured for this pool.

Create the Encryption Key

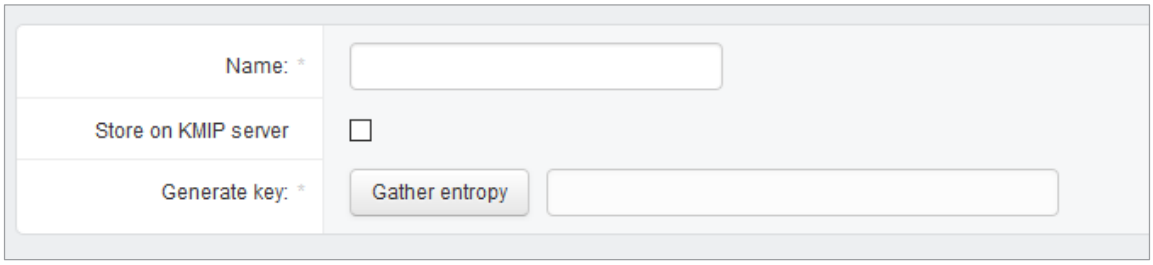
Encryption keys can be stored either locally with the Vaultive appliance, or remotely in the pool's KMIP server.

Requirements for hosting a key on a KMIP server are as follows:

- The KMIP server must already be configured on the HA pool on which the key is generated
- You must select the option to store the key on KMIP server as part of key creation—you cannot edit a key to change this option later.

Procedure

1. Log into the Vaultive Administration Console connected to the node on which to generate the key.
2. Go to **Tenants** > **Keys**.
3. On the **Keys** page, click **Add Key**.



4. In the **Name** field (required), enter a name for the key.
5. Select **Store on KMIP server** to store the key on the KMIP server.

   If this option remains unselected (the default), the key is stored in Vaultive.

   Note: *You cannot change the* ***Store on KMIP server*** *setting after the key is created.*

6. To generate the encryption key, click **Gather entropy**, and then move your mouse to generate and collect entropy, or random data.

   As your mouse moves, the encryption key is generated based on the random movement of your mouse.
7. When the **Entropy** bar is full, click **Save**.

   The new key uploads to the KMIP server associated with the HA pool in which it is created.

Using Keys Stored on the KMIP Server

After the encryption key is stored on the KMIP server:

- The configuration master node synchronizes the key's metadata to all nodes in the pool.
- From any node in an HA pool, you can only export keys from the KMIP server if they reside on the KMIP server used by the node.
- If you export a key from one pool, and import it through another pool, the key is stored on that pool's configured KMIP server. For instructions on importing encryption keys, see the *Vaultive 5.0 Administration and Configuration Guide*.
- If a key is created on a node that is not the configuration master, you must import its metadata to the configuration master node.

In the Vaultive Administration Console:

- Under **Encryption settings** for a partition (**Tenants** > **Partitions**), you can select the KMIP-stored encryption key from the list of encryption keys for setting the encryption and decryption keys for the HA pool.
- The list of encryption keys (**Tenants** > **Keys**) identifies where keys are stored—either locally or on the KMIP server.

Note: *Vaultive does not back up KMIP server-stored encryption keys.*

See the *Vaultive 5.0 Administration and Configuration Guide* for information about the following:

- Exporting and importing encryption keys.
- Exporting and importing key metadata.
- Encryption settings for a partition.