Configure HashiCorp Vault

You can configure a HashiCorp Vault to use with Tessera.

The private/public key pairs used by Tessera can bestored in andretrieved from the Vault, without the need to store the keys locally.

TheHashiCorp Vault documentation provides the information you need to get started. The following section goes over some additional considerations when running Tessera with Vault.

Configure the vault

TLS

When running Tessera with HashiCorp Vault in production settings, we recommend configuring the Vault server for two-way (mutual) TLS communication. Tessera also supports one-way TLS and unsecured (no TLS) communications with a Vault server.

The following is an example configuration for the Vault listener to use two-way TLS. This can be included as part of the.hcl used when starting the Vault server.

listener "tcp" { tls_min_version = "tls12" tls_cert_file = "/path/to/server.crt" tls_key_file = "/path/to/server.key" tls_require_and_verify_client_cert = "true" tls_client_ca_file = "/path/to/client-ca.crt" }

Auth methods

Tessera supports theAppRole auth method. If required, other auth methods can be used by logging in outside of Tessera (for example, using the HTTP API) and providing the resulting vault token to Tessera. SeeEnabling Tessera to use the vault for more information.

When using AppRole, Tessera assumes the default auth path isapprole . You canconfigure this value .

Policies

Tessera requires the following policy capabilities to be able to carry out all possible interactions with a Vault:["create", "update", "read"] . You can configure a subset of these capabilities if some functionality is not required.

Secret engines

Tessera can read and write keys to theKey/Value version 2 secrets engine.

The secrets engine supports storing multiple versions of secrets. The number of versions stored can be configured as part of the Vault configuration process.

Enable Tessera to use the vault

Environment variables

Tessera requires certain environment variables to be set depending on theauth method used.

If using the AppRole auth method, set:

- HASHICORP_ROLE_ID
- HASHICORP_SECRET_ID

You can get these credentials as outlined in theAppRole documentation . Tessera uses these credentials to authenticate with Vault.

If using the root token, or if you already have a token due to authorizing with an alternative method, set:

- HASHICORP_TOKEN

note If using TLS, additional environment variables must be set.

Dependencies

Unpackhashicorp-key-vault-.zip|tar andcp hashicorp-key-vault-/lib/* tessera-dist/lib/ . Edit this page Last updatedonOct 9, 2023 bydependabot[bot] Previous Configure Azure Key Vault Next Servers