CAA 2024

Laboratoire #1

September 2024 - Nathan Rayburn

Abstract

Vault is a secure platform developed by HashiCorp to manage secrets and protect sensitive data. It is designed to store, access, and control secrets and credentials such as passwords, API keys, and certificates in a highly secure way. Vault leverages encryption and a multi-step unseal process, providing strong data protection through Shamir's Secret Sharing, where decryption keys are distributed among trusted security officers. This design ensures that sensitive information remains inaccessible even if the storage backend is compromised. Vault is highly extensible and supports various authentication methods, making it versatile for multiple use cases. Overall, Vault significantly improves data confidentiality and access control for organizations handling critical secrets.

1 Run the script

To run the script just execute the setup file. All of the policies and configuration files are situated in the script. Create a folder with the script inside, because the files will be stored in the current folder of the script.

```
./setup_vault_script.sh
```

Listing 1: Executing the script.

2 Questions

2.1 What is the goal of the unseal process? Why are there more than one unsealing key?

The unseal process in Vault is required to initialize the Vault server after it has been started or restarted. Vault encrypts data that is stored and not actively being processed or transmitted. Vault uses Shamir's Secret Sharing scheme, and these shared keys are distributed to security officers.

The unseal process reconstructs the master key from key shares, which allows Vault to decrypt its data and operate.

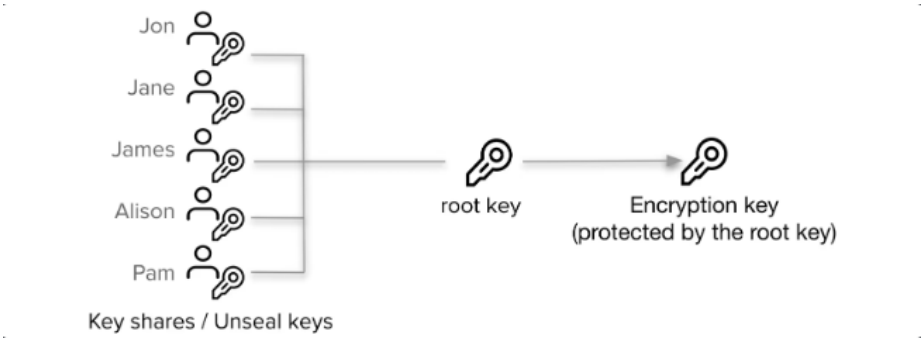

Figure 1: Unseal process scheme

2.2 What is a security officer? What do you do if one leaves the company?

A security officer is responsible for overseeing information security, cybersecurity, and IT risk management programs. In the context of Vault, a security officer is an individual who holds one of the keys required to unseal the Vault. They are typically trusted members of the company. Like one of our 6 members.

If a security officer leaves the company, the Vault would need to be re-keyed, which involves generating a new set of unseal keys. This process can be done while the Vault is still running.

The ‘operator rekey‘ command generates a new set of unseal keys. This process can optionally change the total number of key shares or the required threshold of those key shares to reconstruct the root key. This operation is zero downtime, but it requires that Vault is unsealed and that a quorum of existing unseal keys are provided.

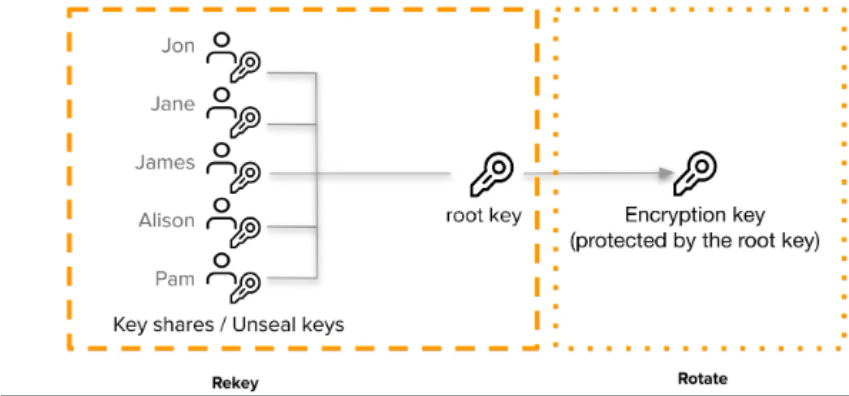

Figure 2: Rekey and key rotation

2.3 Why is it recommended to store the root certificate private key outside of Vault (we did not do this here) ?

The root certificate private key is highly sensitive because it's the top-most in a PKI hierarchy. If compromised, it would compromise the entire PKI. Storing it outside Vault, typically in a secure offline location, minimizes the risk of exposure.

2.4 Where would you typically store the root certificate private key?

Typically, the root certificate private key would be stored in a Hardware Security Module (HSM). Which offers enhanced security by being isolated from the network and any network attacks.

2.5 What do you need to do in Vault to store the root certificate private key outside of Vault?

To store the root certificate private key outside Vault, you need to export the private key and move it to a secure location such as an HSM. Ensure that Vault can still manage certificate lifecycles through the intermediate CAs that will sign the leaf certificates using PKI secrets engine. The private key remains secured externally.

2.6 How is the intermediate certificate private key secured?

The intermediate certificate private key is secured through Vault's encryption-at-rest mechanisms. Vault encrypts the data in the storage backend using a master key, ensuring that even if someone gains access to the storage backend, the intermediate certificate remains secure.

2.7 In the certificate for intra.heig-vd.ch, what is its duration of validity? What is the name of its issuer?

The certificate for intra.heig-vd.ch has a validity of **24 hours**. The issuer of the certificate is likely "HEIG-VD Intermediate CA" or a similar entity.

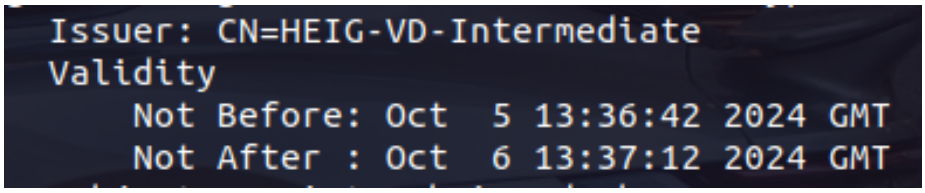

Figure 3: Validity date

2.8 What do you need to do concretely for the intra.heig-vd.ch certificate to be accepted by browsers?

For the intra.heig-vd.ch certificate to be accepted by browsers, we need to import the HEIG-VD root certificate into the browser's trusted certificate store. This will allow the browser to recognize the certificate chain as trusted and also verify/validate the chain of certificates.

2.9 What is a wildcard certificate? What are its advantages and disadvantages?

A wildcard certificate is a certificate that can be used to secure multiple subdomains under a single domain (e.g., *.heig-vd.ch). Anything that contains .heig-vd.ch will be a valid certificate.

Advantages: - We can use one certificate for multiple and potentially a lot of subdomains. - It reduces administrative overhead and costs for managing individual certificates.

Disadvantages: - If the wildcard certificate's private key is compromised, all subdomains are exposed. - Maybe some features, like having an Extended Validation , may not be supported for wildcard certificates.

2.10 How is the root key and the encryption key used to secure Vault?

Vault uses the root key to encrypt and secure the master encryption key. The master encryption key is then used to encrypt the data stored in the Vault. The root key is split into unseal keys, which are needed to reconstruct the root key and unseal the Vault.

2.11 What is key rotation and when is it done?

Key rotation is the process of generating new encryption keys to replace the old ones. It is performed periodically to ensure security or when a key compromise is suspected.

2.12 What can you say about the confidentiality of data in the storage backend? How is it done?

Vault ensures the confidentiality of data in the storage backend by encrypting the data using the encryption key derived from the master key. This guarantees that even if the storage backend is compromised, the data cannot be read without access to the encryption keys stored securely in Vault. The vault uses AES-256-GCM as the encryption algorithm using a 96 bits nonce.

2.13 What can you say about the security of Vault against an adversary that analyzes the memory of the server that runs Vault?

Vault's security model does not protect against attacks involving memory analysis of the running Vault server. If an adversary can inspect the memory state of a Vault instance, the confidentiality of the data in memory may be compromised. This is a known limitation, and Vault's threat model excludes protection against this type of attack.Reference : Vault Security Model

2.14 Try doing admin tasks with the toto user and show a screenshot of what happens.

Executing the following command as 'toto':

```
1 vault list pki_int/roles
```

Listing 2: Attempt to list roles in the PKI secrets engine as the user toto

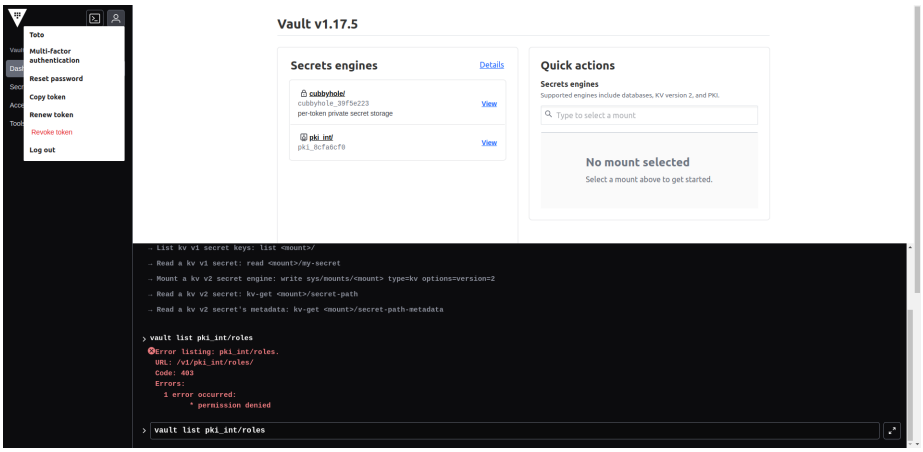

Figure 4: Refused access as Toto

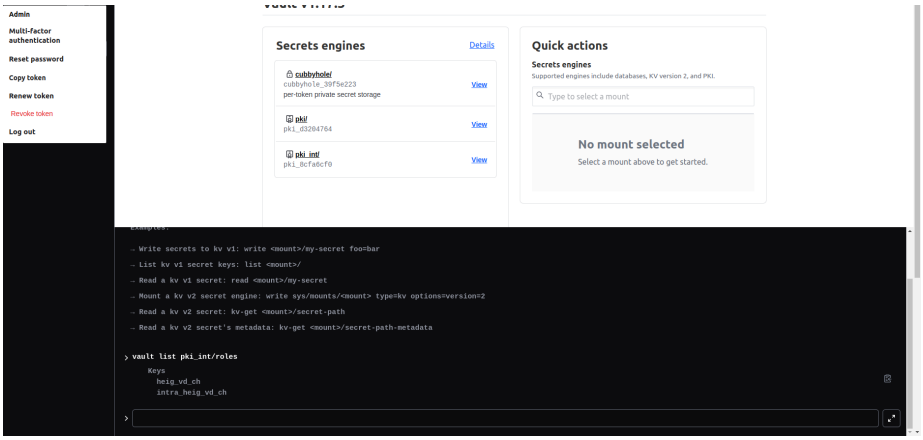

Figure 5: Access granted as Admin