Hashicorp Vault Setup

Here are steps for setting up a secrets store using Hashicorp Vault, on Ubuntu 24.

References

Lots of steps were taken from here: https://developer.hashicorp.com/vault/tutorials/secrets-management/pki-engine

Server Setup

Before installing Vault, perform steps from this page, to setup the server: Ubuntu Host Setup

Since a typical vault cluster has limited internet visibility, it may be necessary to map in the local NTP server, to keep each node in sync.

See this page for how to setup each host/VM to use the local private NTP server: Ubuntu: Use Private NTP Server

Install Vault

Here are three lines to install vault.

First, we will setup the package source keys...

```
sudo wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
```

Now, add the package source entry...

```
echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list
```

Now, install vault...

```
sudo apt update && sudo apt install vault
```

Vault User

The installer created a user called, vault, and the service runs under it.
But, the default keys are restricted to root permissions.
So, we need to fix access to certificates.

For this, we will create a group to make it easier to control and test access to certs and keys.

```
sudo groupadd pki
```

And, we will add the vault user to the group:

```
sudo usermod -a -G pki vault
```

Clustered Config

> NOTE: If you are standing up a single node vault, skip this section.

Work through the steps on this page, for clustering your vault servers: Clustering HashiCorp Vault

Vault Configuration

> NOTE: This is for a single vault node. If you are standing up a cluster, skip this section.

Edit the config file at: /etc/vault.d/vault.hcl

Specifically, you want to set the tls cert/key paths to your own domain certs.

As well, you may want to limit the listener to just a single address, since the default is for all adapters on the host.

Once done, save the config update.

Continue Setup

Once installed and configured, we need to enable and start the vault services, with these lines:

```
sudo systemctl daemon-reload
sudo systemctl enable vault
sudo systemctl start vault
sudo systemctl status vault
```

You should be able to verify that the vault service is active by call this:

https://<host-ip>:8200/v1/sys/seal-status

> NOTE: Use your VM’s fully-qualified name (or IP address), in the above.

If successful, the above call will return something like this:


```
{
  "type":"shamir",
  "initialized":false,
  "sealed":true,
  "t":0,
  "n":0,
  "progress":0,
  "nonce":"",
  "version":"1.17.6",
  "build_date":"2024-09-24T19:48:40Z",
  "migration":false,
  "recovery_seal":false,
  "storage_type":"file"
}
```


Cluster Unseal

If you're standing up a cluster, see this page: HashiCorp Vault Cluster Unseal

If you're standing up a single-node vault instance, see this page: Vault Single-Node Unseal

Administrative Setup

Once the vault is unsealed, you need to setup auditing and administrative policies.

See this page for how: Vault Administrative Setup

Creating Users (Access Tokens)

Once the vault cluster is setup, you need to establish some administrative users.

See this page for how to create admin and user tokens: Vault Token Administration

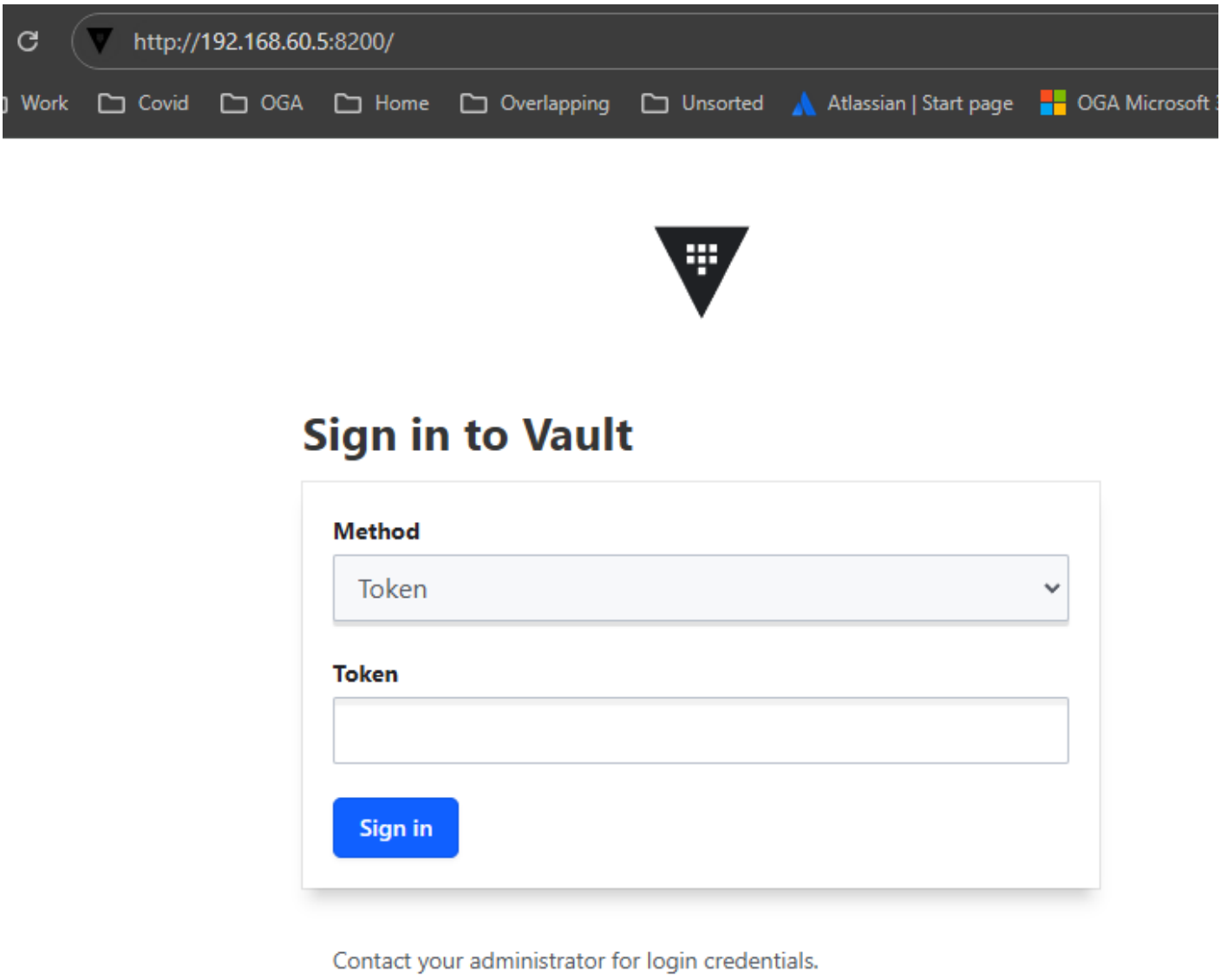
To protect tokens in transit, see this page for Response-Wrapped Tokens: Vault Wrapping Token

Login

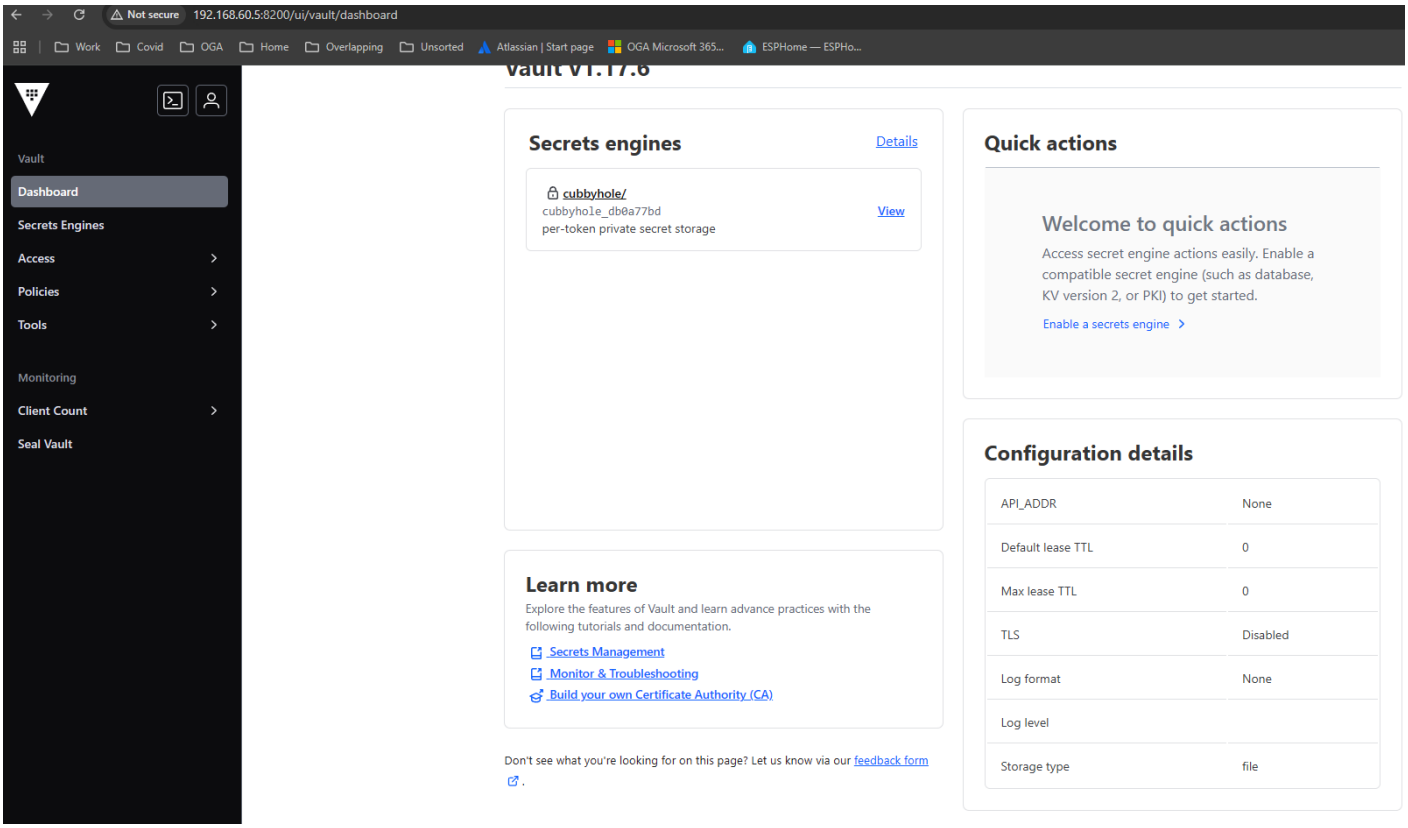
Once your vault is unsealed, you can log into its UI.

Log into its UI, here: http://<host-ip>:8200/

You will be prompted to enter your root token, here:

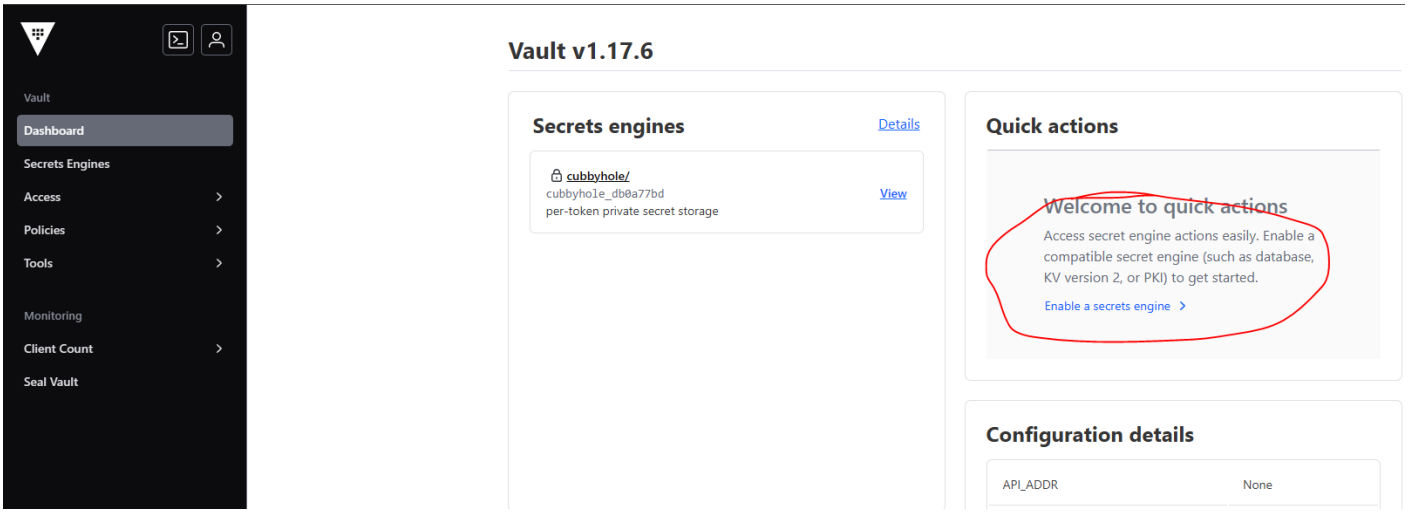


If successful, you will see the root user’s dashboard:



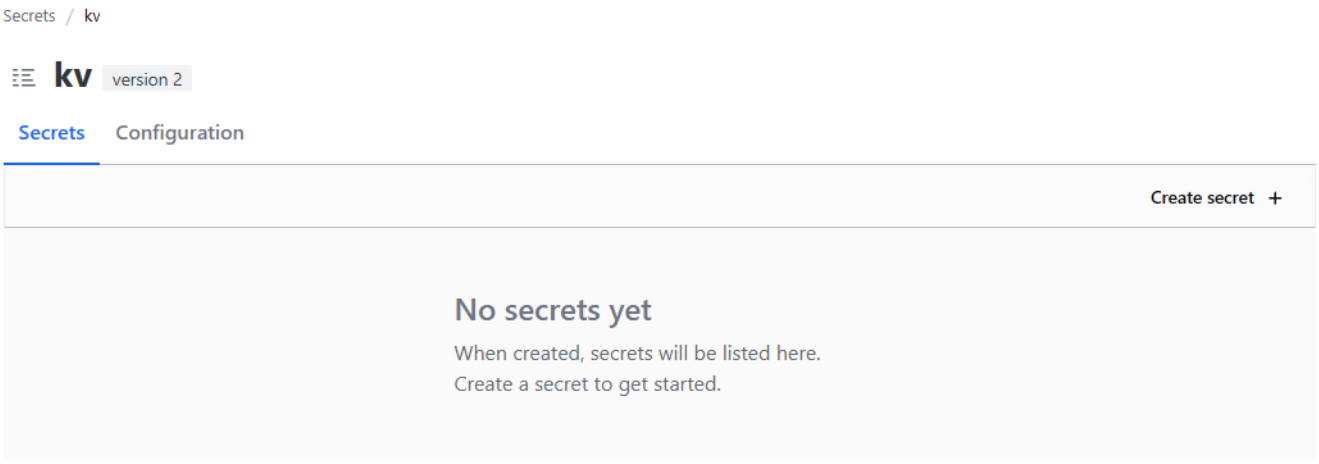
Creating the First Secret Store

Now, you should create a secrets engine, to store things.
The one that makes the most sense, first, is to make a KV store.
You should be able to make a kv secrets store (actually, a kv-v2 store) from the dashboard:



The above will create the secrets store at the path: /kv
You can change this if needed.

Once created, you will see the new empty store:



Using Vault as a CA

Follow steps on this page, to setup a vault instance as a Root CA: Vault as Root CA

> NOTE: You never want to directly sign certificates with a Root CA.
> If you do, there is no way to revoke the root CA, without collapsing all PKI chains (by revoking the root CA certificate).
> However. You can create an Intermediate CA that does signings.
> And, that Intermediate CA can be revoked, without losing the root CA certificate.

> So, we will create an Intermediate CA, to do actual signings.
> And, the Intermediate CA's certificate will be signed by the Root CA, just before offlining the Root CA.

Once a root CA is setup, you can follow this page, to setup an Intermediate CA,
that will do actual signings: Vault as Intermediate CA

See this page for how to generate certificates: Generate Certificates with Hashicorp Vault

---

Revision #13
Created 1 September 2025 01:40:34 by glwhite
Updated 4 September 2025 05:08:23 by glwhite