Initializing Vault

PW

Owned by Paul Wilson

Oct 27, 2022 • 4 min read • 3 people viewed

Vault config and initialization

When you deploy the OpenStack model with juju Vault will need to be initialized. once initialized the keys must be saved in source control to ensure access to systems but additionally, the systems will all be secured by the vault system

To initialize

On the management PC the vault client must be added to interact with vault. (typically done from the maas CLI)

```
sudo snap install vault
```

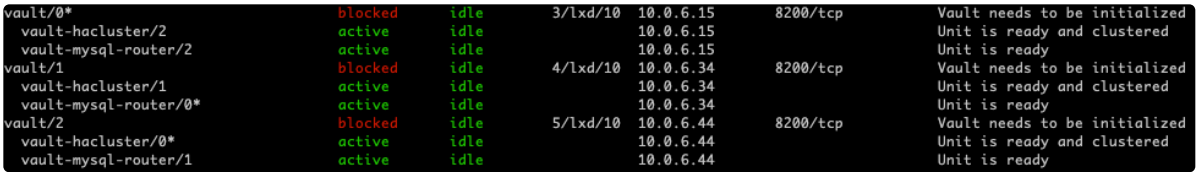
Copy

To connect to each vault you must export the vault address and use the IP of the vault you want to connect to. this must be done with each vault to “open them”

```
export VAULT_ADDR="http://%vault-address%:8200"
```

Copy

The address is available by looking at the juju status command as it will show the IP of each vault container



So for example, if we wanted to initialize the leader vault in this scenario you would select the IP for the one labeled as the leader (*) and run the following command

```
export VAULT_ADDR="http://10.0.6.15:8200"
```

Copy

once selected, you must initialize with the following command to generate 5 unseal keys and a threshold of required keys to unseal. in this case, we will make 5 keys and require 3 to unseal the vault.

```
vault operator init -key-shares=5 -key-threshold=3
```

Copy

This will give you an output that must be saved in source control to ensure the ability to unseal the vault.

```
Unseal Key 1: %Key1%
Unseal Key 2: %Key2%
Unseal Key 3: %Key3%
Unseal Key 4: %Key4%
Unseal Key 5: %Key5%

Initial Root Token: %root-token%

Vault initialized with 5 key shares and a key threshold of 3. Plea
distribute the key shares printed above. When the Vault is re-seal
restarted, or stopped, you must supply at least 3 of these keys to
before it can start servicing requests.

Vault does not store the generated master key. Without at least 3
reconstruct the master key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a qu
existing unseal keys shares. See "vault operator rekey" for more i
```

Copy

The following will need to be done 3 times for each vault to "Unseal" the vault. use one unseal key each time and they must be different

EX: first run use key 1, 2nd run use key 2 etc.

```
vault operator unseal
```

Copy

the return after entering the key will look like this:

after you do this with 3 keys the sealed value will change like this:

the vault selected is now unsealed and can assign and allocate keys and certificates.

When the leader vault is first initialized and unsealed you can now generate a token that will authorize the charm

first export the vault token

```
export VAULT_TOKEN=%root-token%
```

Copy

Then you will generate a new token

```
vault token create -ttl=10m
```

Copy

this will give an output similar to this:

```
Key                  Value
---                  -----
token                %new-token%
token_accessor       dUufLMDcAGvZvMomEHbQxhPl
token_duration       10m
token_renewable      true
token_policies       ["root"]
identity_policies    []
policies             ["root"]
```

Copy

with the new token you will authorize the charm with the following command:

```
juju run-action --wait vault/leader authorize-charm token=%new-toke
```

Copy

once completed it will show completed and vault is now available to generate a new CA certificate.

```
unit-vault-0:
  UnitId: vault/0
  id: "2"
  results:
    Stdout: |
      lxc
      lxc
      active
```

```
    status: completed
    timing:
      completed: 2022-01-19 19:22:58 +0000 UTC
      enqueued: 2022-01-19 19:22:48 +0000 UTC
      started: 2022-01-19 19:22:52 +0000 UTC
```

Copy

now to generate the certificate

```
juju run-action --wait vault/leader generate-root-ca
```

Copy

this will output a certificate value, once the certificate value is populated then just allow the model to settle. also, unseal the other vaults.

Additional resources

https://learn.hashicorp.com/tutorials/vault/rekeying-and-rotating?in=vault/operations

+ Add label

Be the first to add a reaction