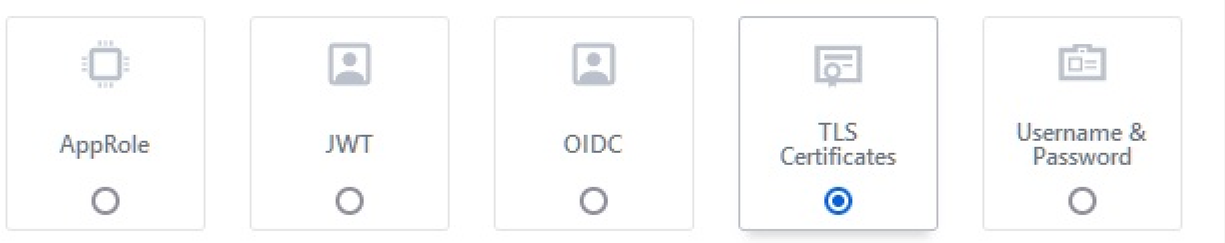
HashiCorp Vault TLS Auth Method

1 enable the tls auth method



AppRole ○

JWT ○

OIDC ○

TLS Certificates ●

Username & Password ○

2 create the App Policy for the certificate

```
path "secret/app" {
  capabilities = ["read", "create", "update"]
}
path "secret/data/app" {
  capabilities = ["read", "create", "update"]
}
```

3 create the web policy

```
path "secret/web" {
  capabilities = ["read", "create", "update"]
}
path "secret/data/web" {
  capabilities = ["read", "create", "update"]
}
```

HashiCorp

Vault TLS Auth Method

4 Create the Certificate using openssl

https://github.com/vijayendrar/devsecops/tree/main/Hashicorp/Vault/Vault-TLS-Auth

5 Create certs for App

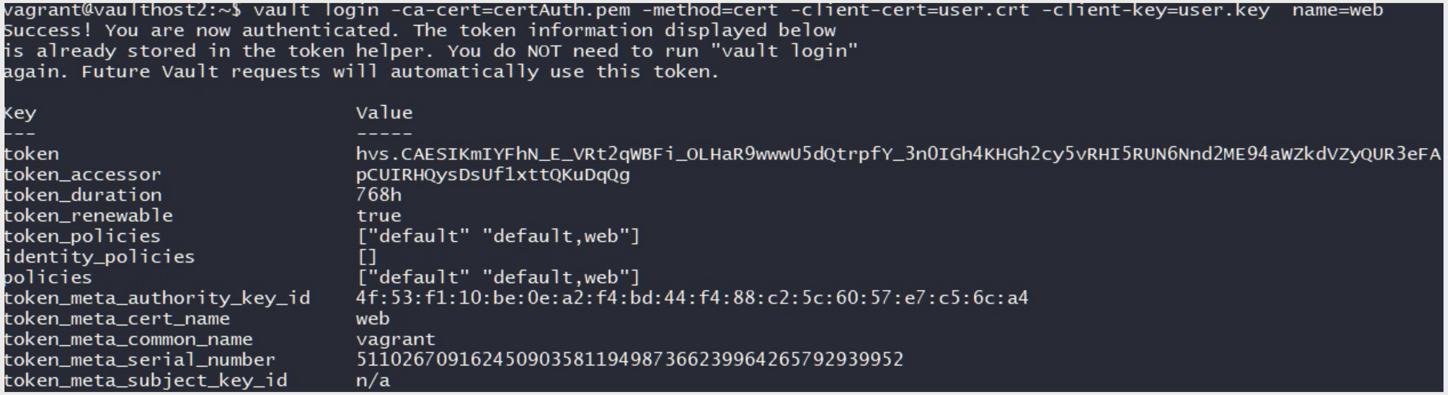
```
vault write auth/cert/certs/app
display_name=appcert policies=default,app
certificate=@certAuth.pem ttl=3600
```

6 create the cert for Web

```
vault login -ca-cert=certAuth.pem -
method=cert -client-cert=user.crt -client-
key=user.key  name=web
```

HashiCorp Vault TLS Auth Method

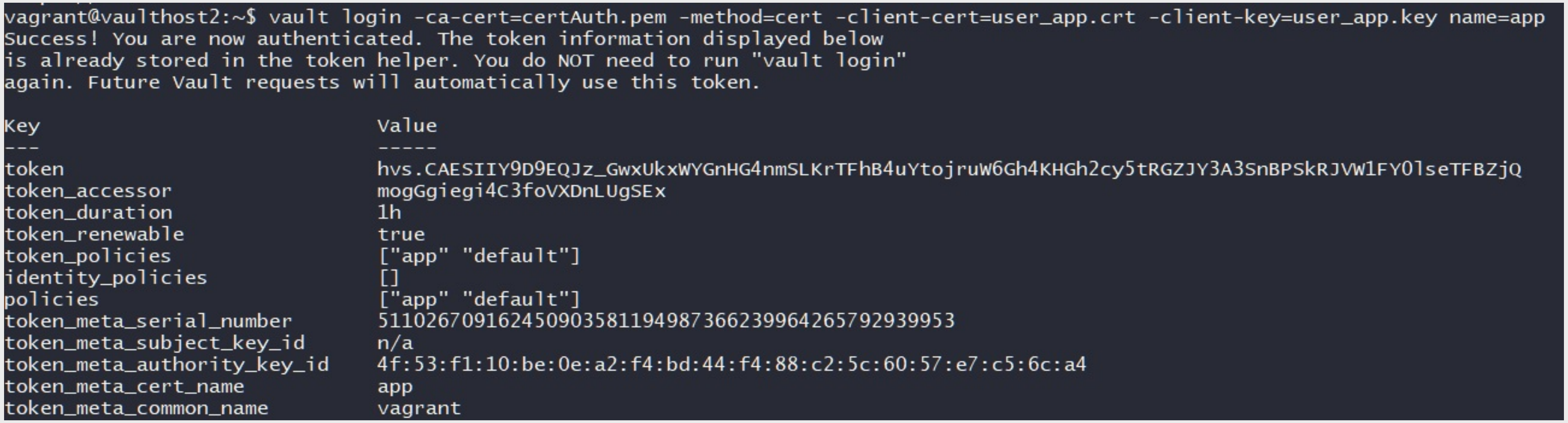
7 Testing Certificate web



```
vagrant@vaulthost2:~$ vault login -ca-cert=certAuth.pem -method=cert -client-cert=user.crt -client-key=user.key  name=web
Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.

Key                            Value
---                            -----
token                          hvs.CAESIKmIYFhN_E_VRt2qWBFi_OLHaR9wwwU5dQtrpfY_3n0IGh4KHGh2cy5vRHI5RUN6Nnd2ME94aWZkdVZyQUR3eFA
token_accessor                 pCUIRHQysDsUf1xttQKuDqQg
token_duration                 768h
token_renewable                true
token_policies                 ["default" "default,web"]
identity_policies              []
policies                       ["default" "default,web"]
token_meta_authority_key_id    4f:53:f1:10:be:0e:a2:f4:bd:44:f4:88:c2:5c:60:57:e7:c5:6c:a4
token_meta_cert_name           web
token_meta_common_name         vagrant
token_meta_serial_number       511026709162450903581194987366239964265792939952
token_meta_subject_key_id      n/a
```

8 Testing Certificate for App



```
vagrant@vaulthost2:~$ vault login -ca-cert=certAuth.pem -method=cert -client-cert=user_app.crt -client-key=user_app.key name=app
Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.

Key                            Value
---                            -----
token                          hvs.CAESIIY9D9EQJz_GwxUkxWYGnHG4nmSLKrTFhB4uYtojruW6Gh4KHGh2cy5tRGZJY3A3SnBPSkRJVW1FY0lseTFBZjQ
token_accessor                 mogGgiegi4C3foVXDnLUgSEx
token_duration                 1h
token_renewable                true
token_policies                 ["app" "default"]
identity_policies              []
policies                       ["app" "default"]
token_meta_serial_number       511026709162450903581194987366239964265792939953
token_meta_subject_key_id      n/a
token_meta_authority_key_id    4f:53:f1:10:be:0e:a2:f4:bd:44:f4:88:c2:5c:60:57:e7:c5:6c:a4
token_meta_cert_name           app
token_meta_common_name         vagrant
```