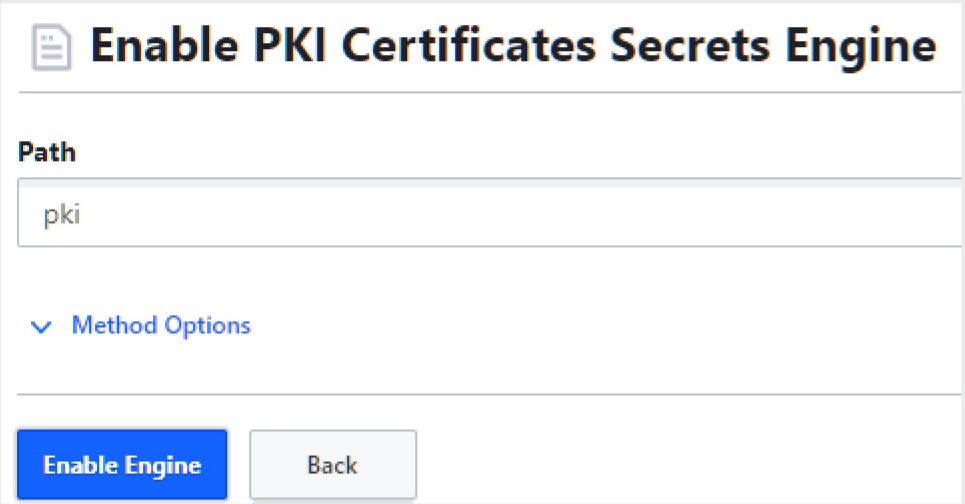
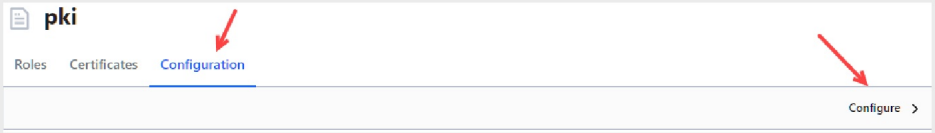
HashiCorp Vault Vault PKI Secret Engine

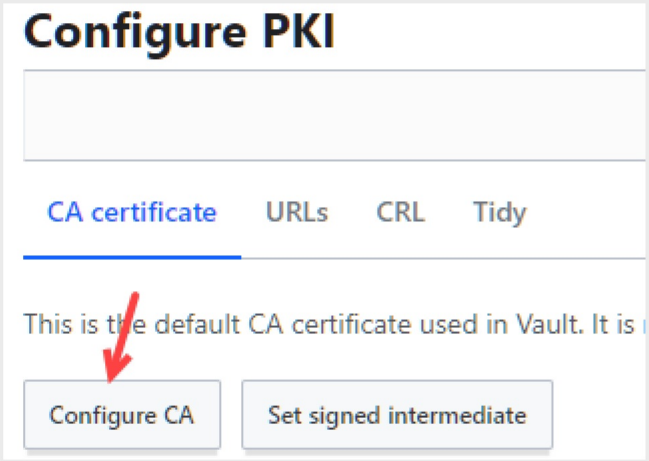
1 Enable the PKI Secret Engine

2 Enable the Engine



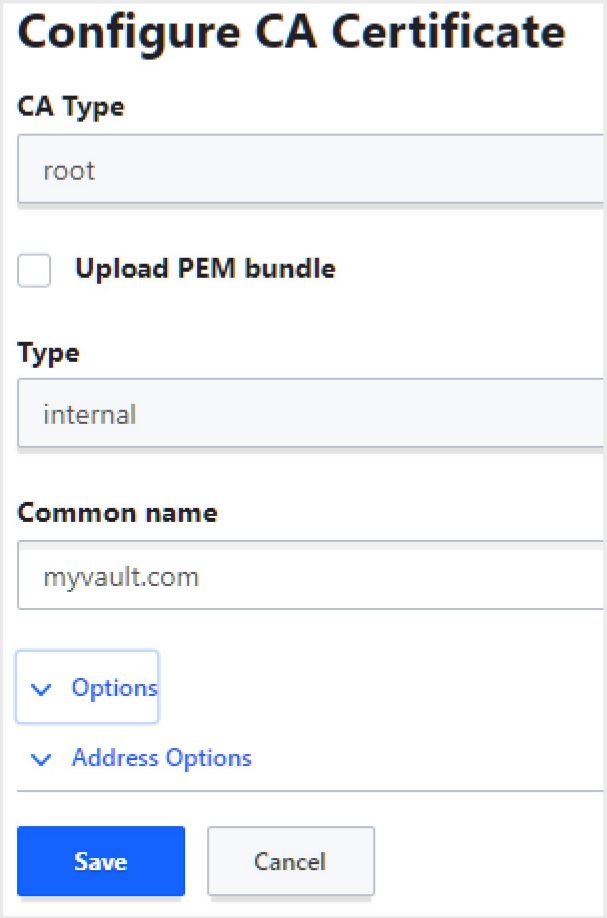
3 Configure the ROOT CA



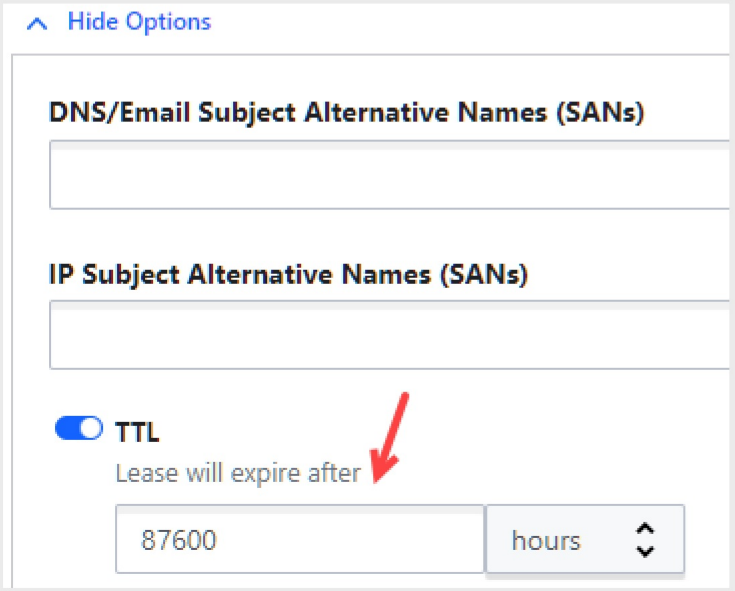


HashiCorp
Vault PKI Secret Engine

4 Configure CA Certificate

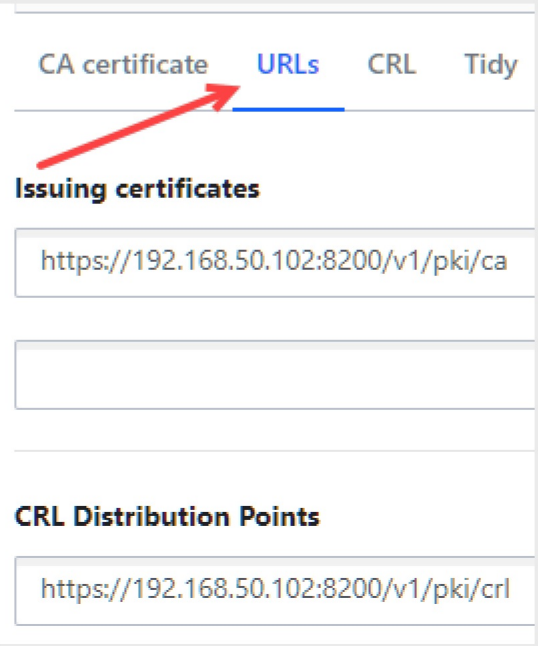


5 Configure the TTL



After TTL Configuration click on save

6 Configure the URL

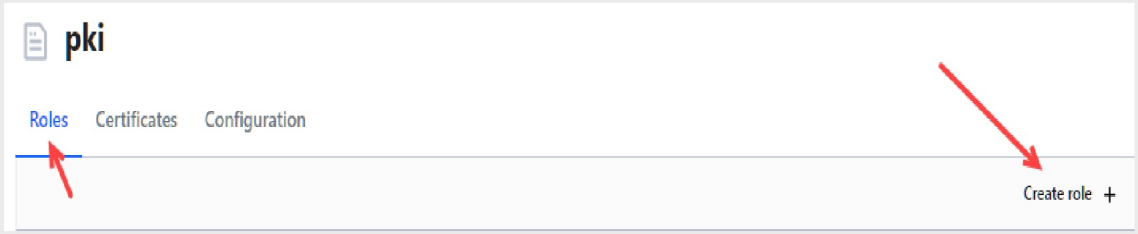


enter the your vault server ip address

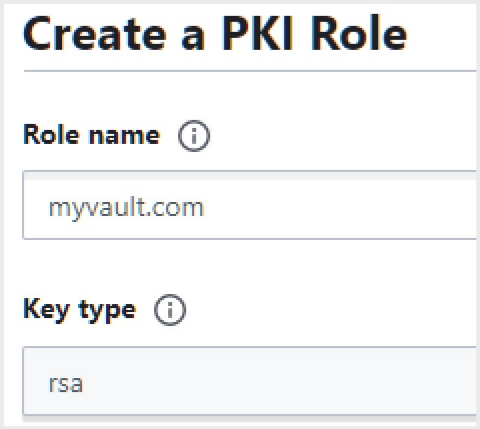
HashiCorp

Vault PKI Secret Engine

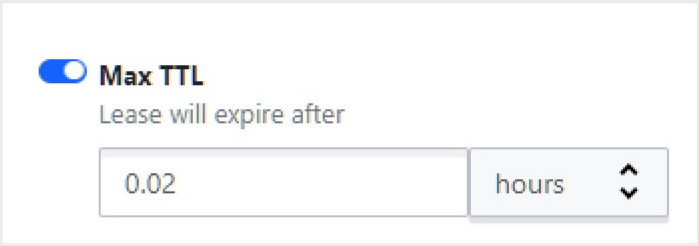
7 create role



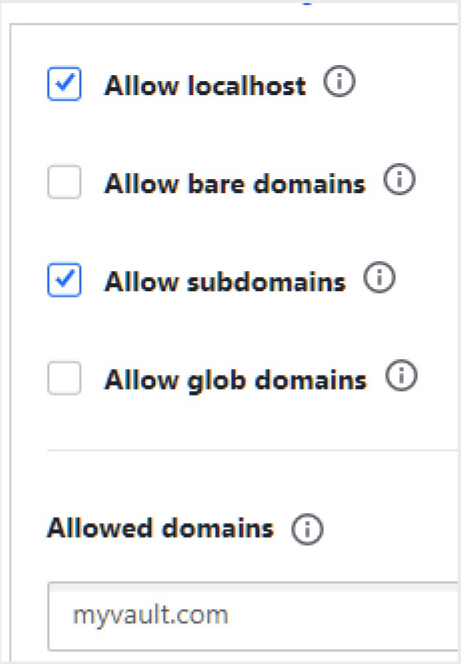
7.1



7.2



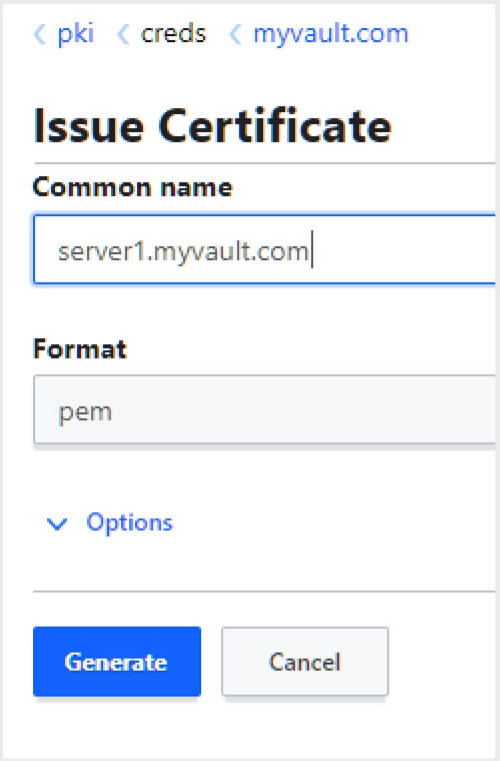
7.3



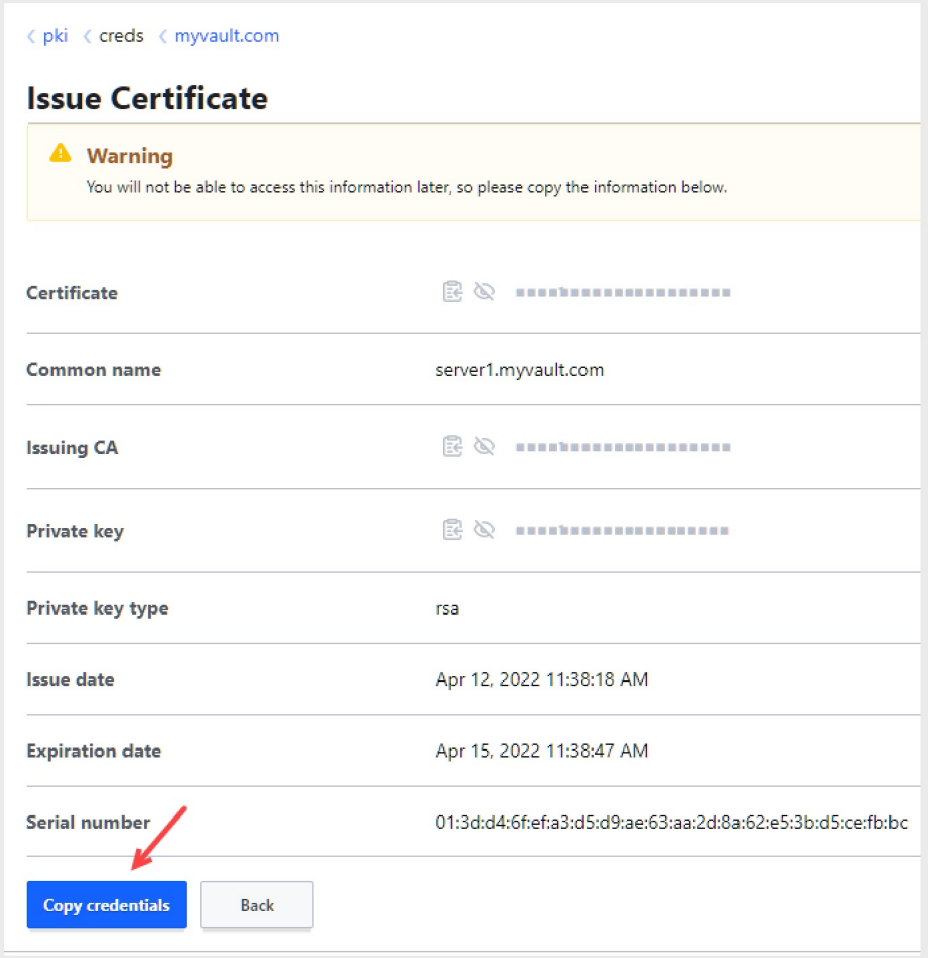
HashiCorp
Vault PKI Secret Engine

8 Generate Certificate

8.1

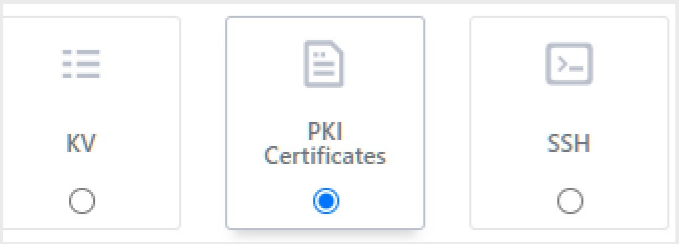


8.2

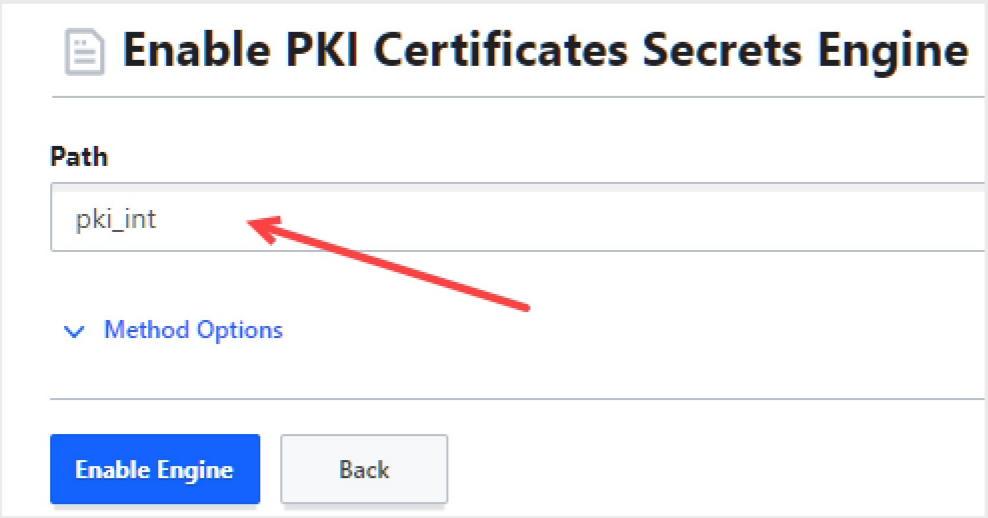


HashiCorp
Vault PKI Secret Engine

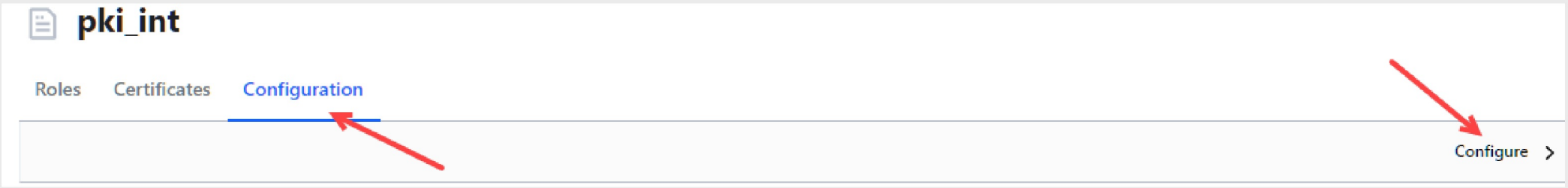
9 Configure the Intermediate CA



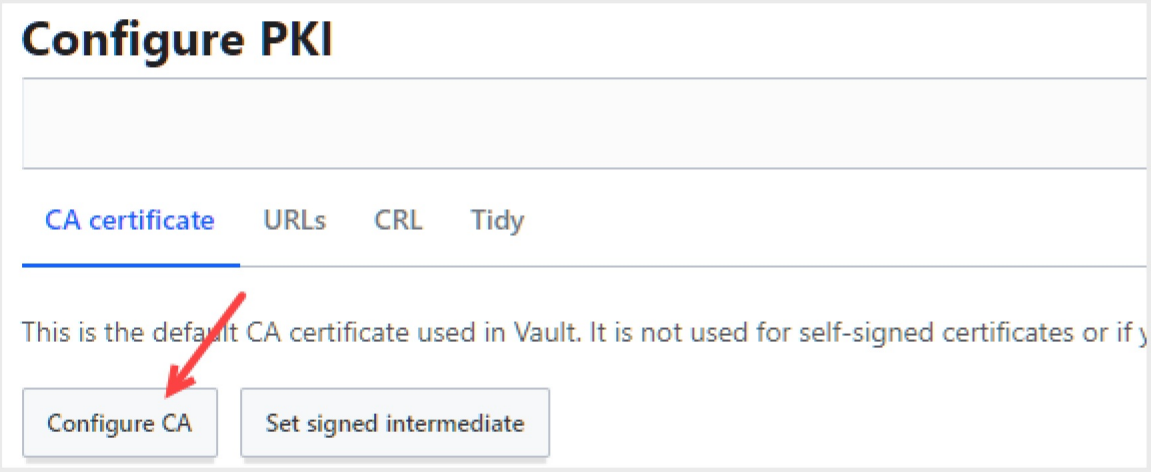
9.1



9.2



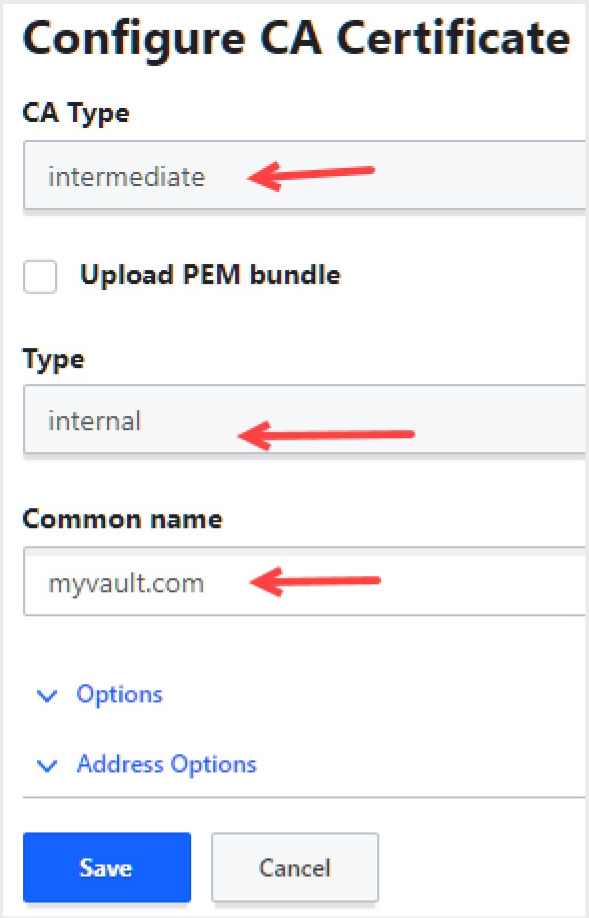
9.3



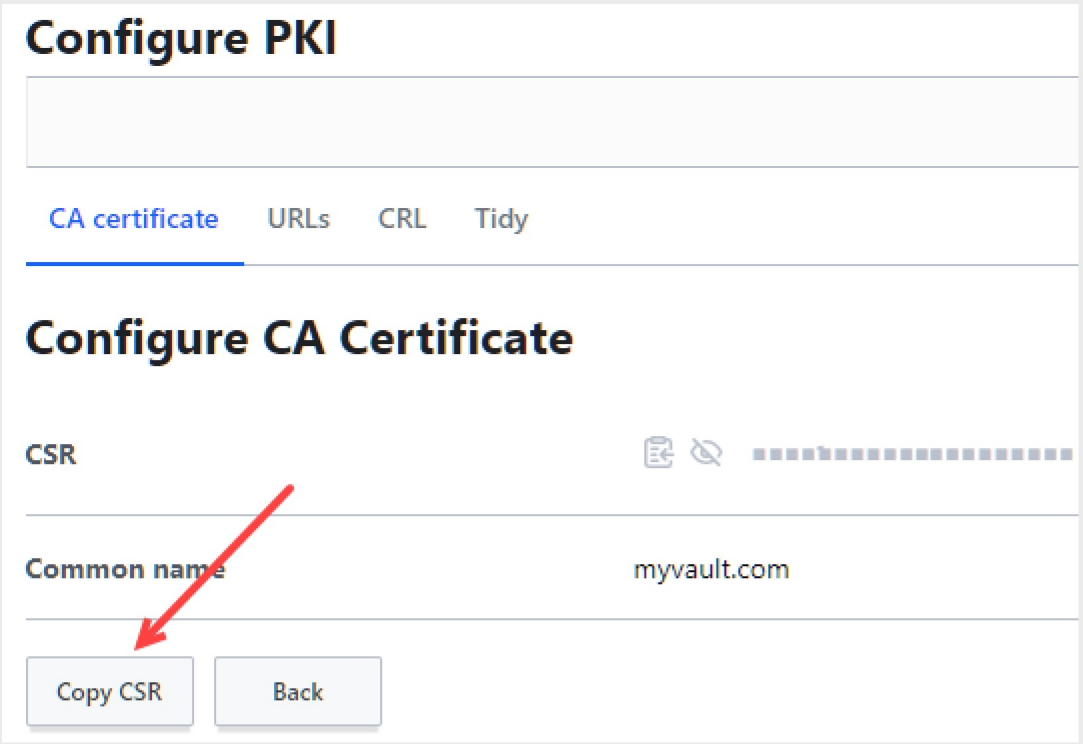
HashiCorp Vault

PKI Secret Engine

9.4 Configure the Intermediate CA



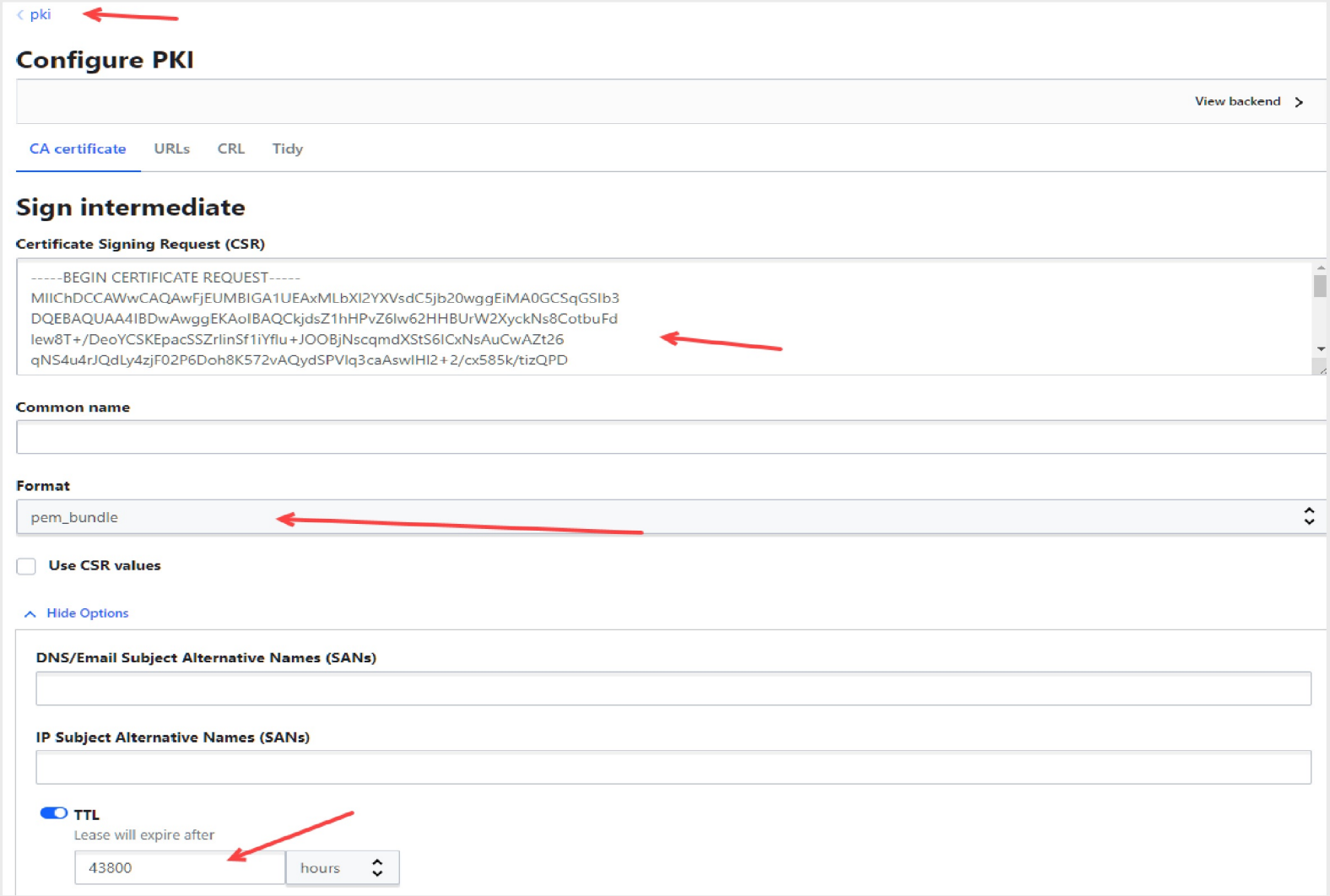
9.5 Copy CSR



HashiCorp

Vault PKI Secret Engine

10 copy CSR and visit root CA and paste CSR

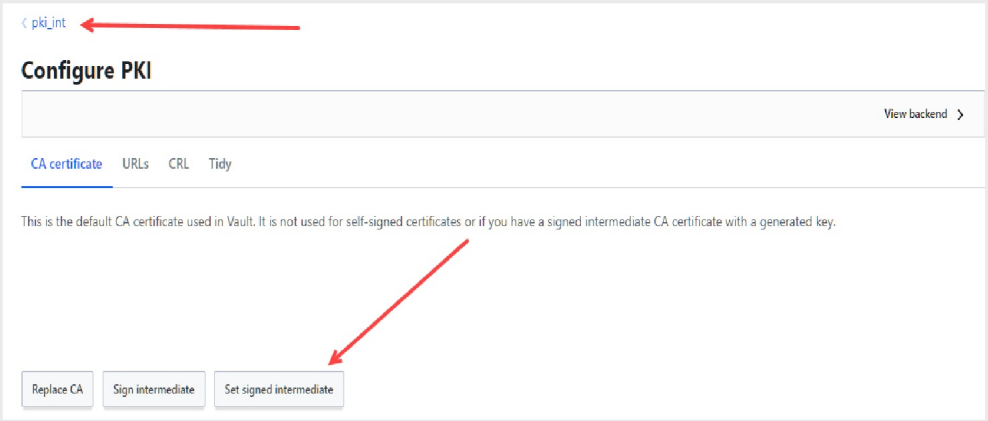


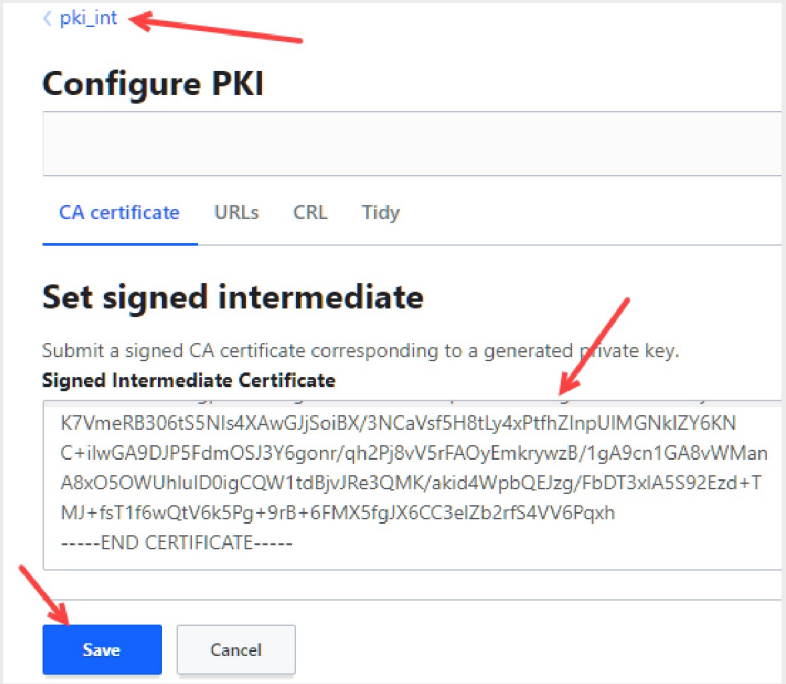
after these steps one more certificate generate please copy it sign the intermediate

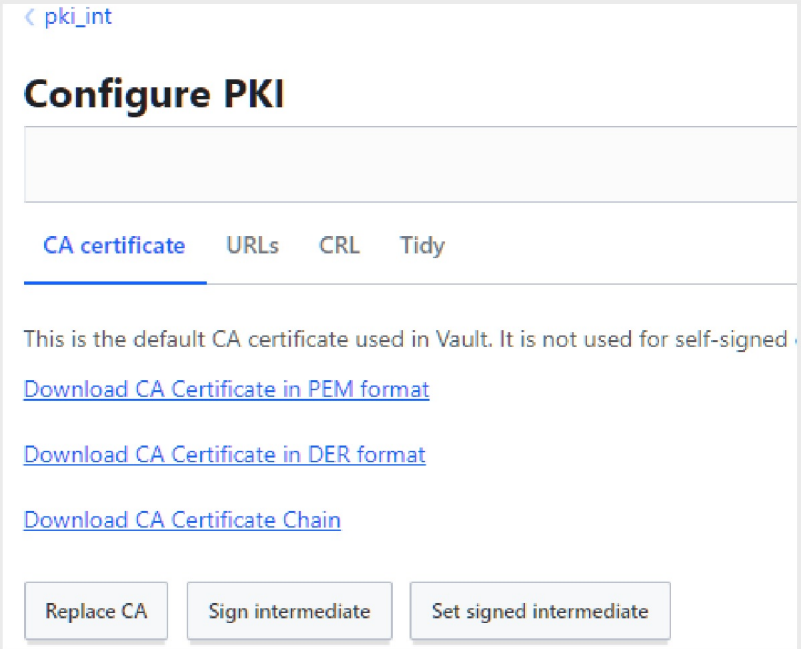
HashiCorp

Vault PKI Secret Engine

10.2 Set Signed Intermediate







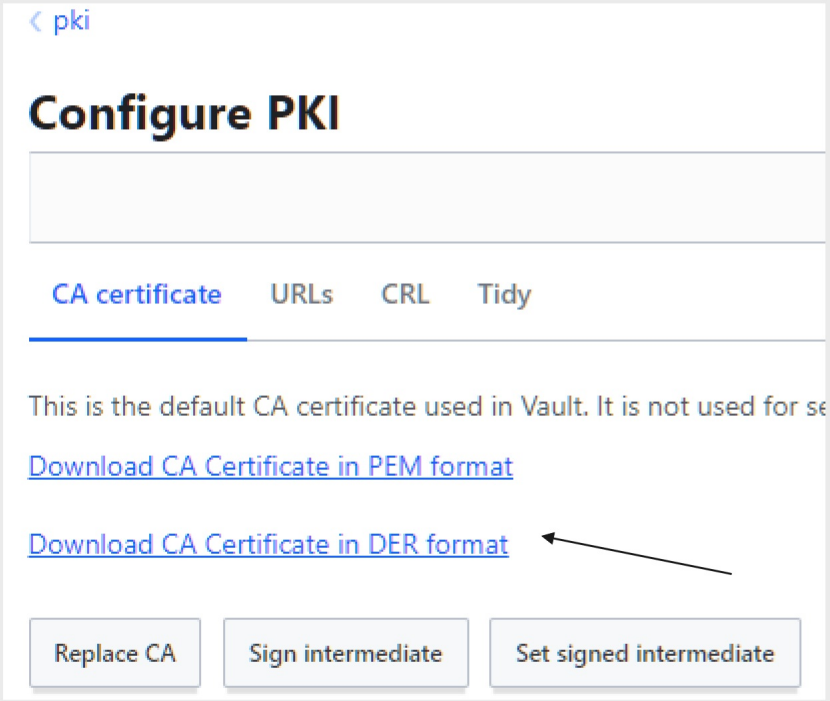
Certifcate are generated

Add your text here

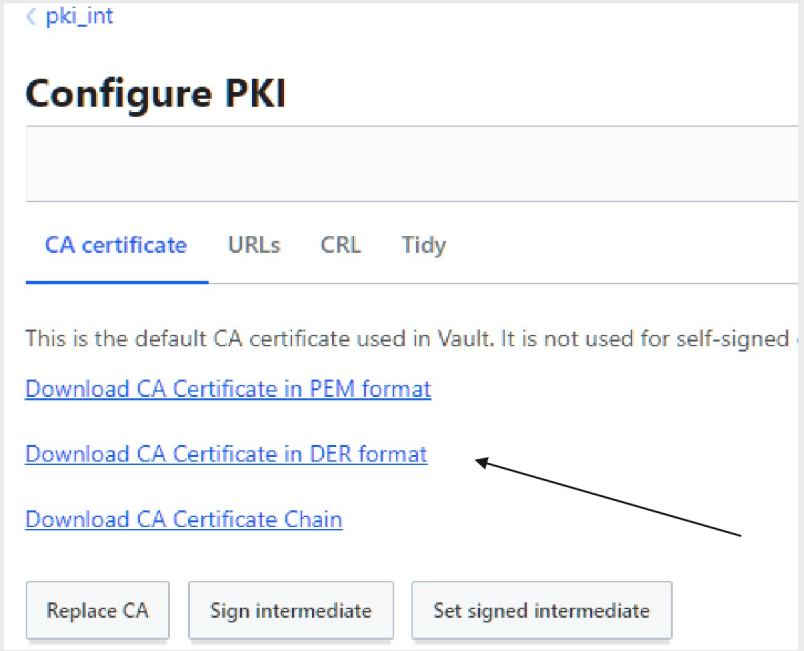
HashiCorp
Vault PKI Secret Engine

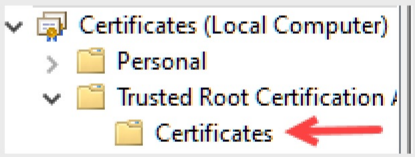
11 Download ROOT CA and Intermediate CA Certficate In Import to ROOT and Intermediate Authority

ROOT CA Certificate

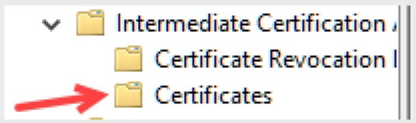


Intermediate Certificate



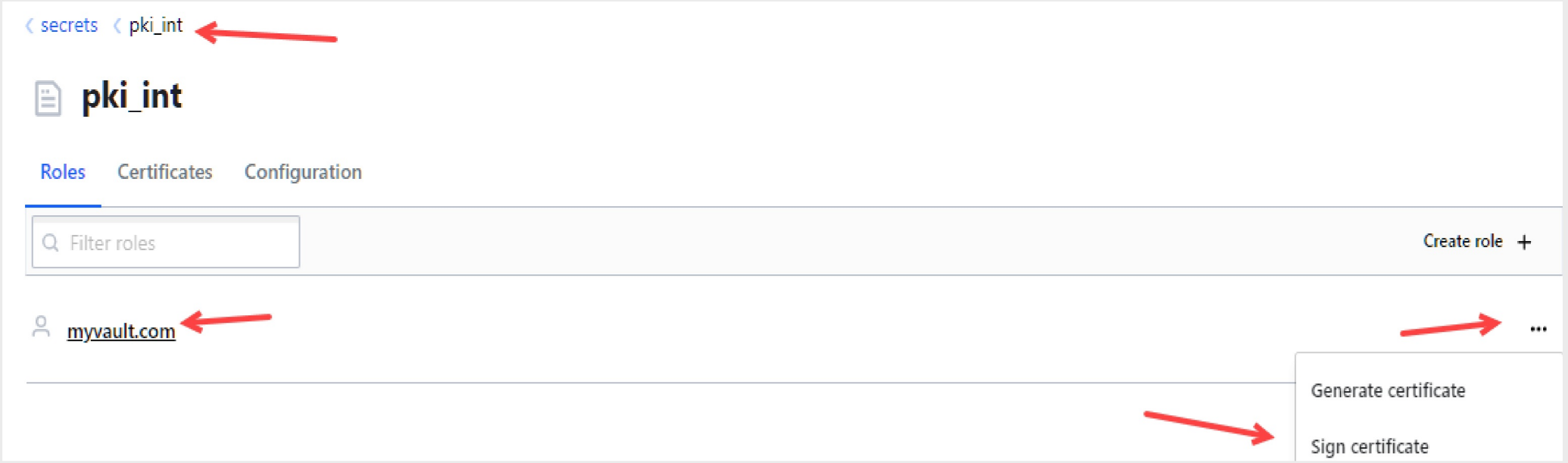


Import In window Certifcate store



HashiCorp Vault PKI Secret Engine

12 Visit pki_int/role click on generate certificate



Rolename

HashiCorp
Vault PKI Secret Engine

13 Generate the Certificate for the Website

```
vault write pki_int/issue/myvault.com ttl=31556952 common_name="server1.myvault.com" ip_sans="192.168.50.106"  -format=json > client_certs.json
```

Note You Must install jq before execute command make Seperate folder and do these step to avoid confustion

```
cat client_certs.json | jq -r '.data.certificate' > client-cert.pem
cat client_certs.json | jq -r '.data.private_key' > client-key.pem
cat client_certs.json | jq -r '.data.issuing_ca' >  ca.pem
cat client_certs.json | jq -r '.data.ca_chain[]' > ca_chain.pem
```

Generate the pfx for windows server

```
openssl pkcs12 -export -in client-cert.pem -inkey client-key.pem -out certificate.pfx -certfile ca_chain.pem
```

Generate the pfx for windows server

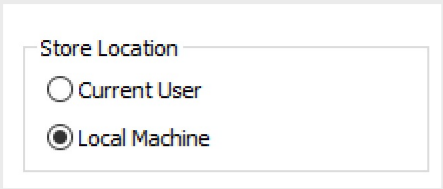
copy generated pfx to windows server

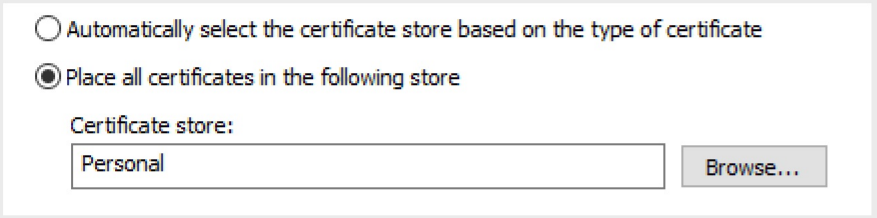
HashiCorp

Vault PKI Secret Engine

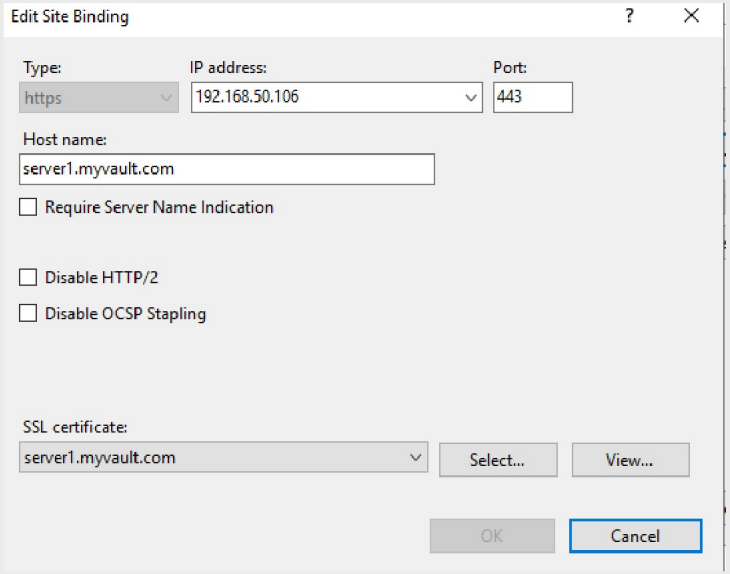
13 Bind the certificate in the IIS server

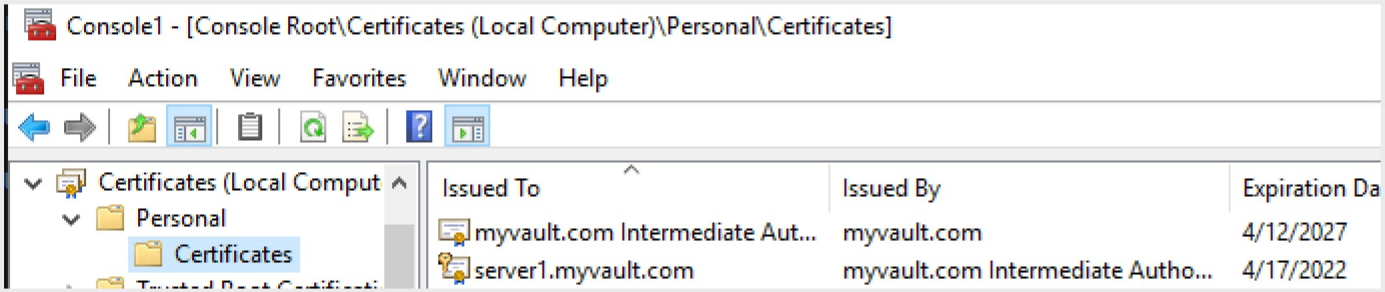
13.1 Install the certificate.pfx by double click





13.2 Bind the certificate in IIS





Make Entry in etc/hosts 192.168.50.106 server.nyvault.com

HashiCorp

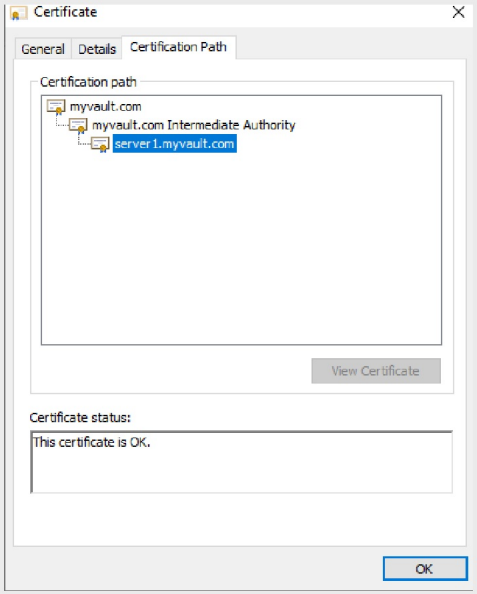
Vault PKI Secret Engine

13 Bind the certificate in the IIS server

13.3 entry in /etc/hosts

Make Entry in etc/hosts 192.168.50.106 server.myvault.com

machine which try to access the website should have ROOT CA and Intermediate CA Certificate Imported According to Page Number 9



13.4 Access the Website