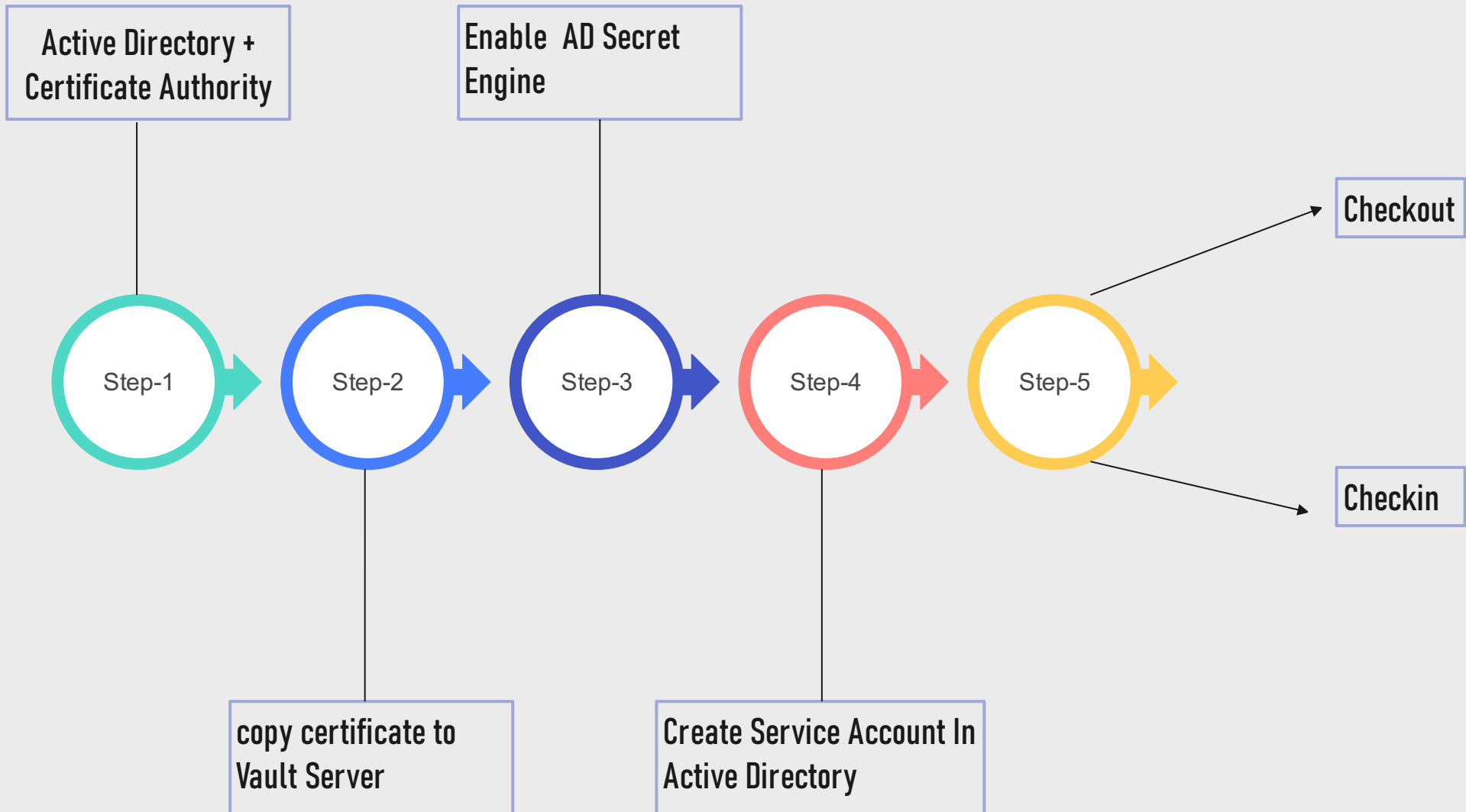




HashiCorp

**Vault**

# Active Directory Secret Engine



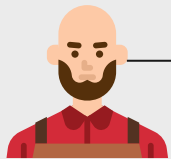


HashiCorp

# Vault Active Directory Secret Engine

1

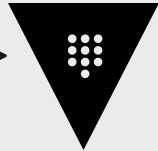
## Active Directory Secret Engine Architecture



Root User

I have taken root user to perform all the steps however you can make custom restrictive policy and perform same

192.168.50.102



Active Directory

Certificate  
Authority

Service  
Accounts

192.168.50.106



HashiCorp

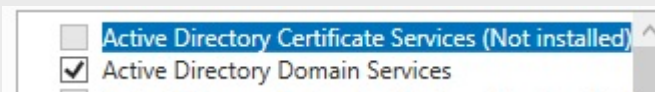
# Vault Active Directory Secret Engine

1

## Active Directory server setup

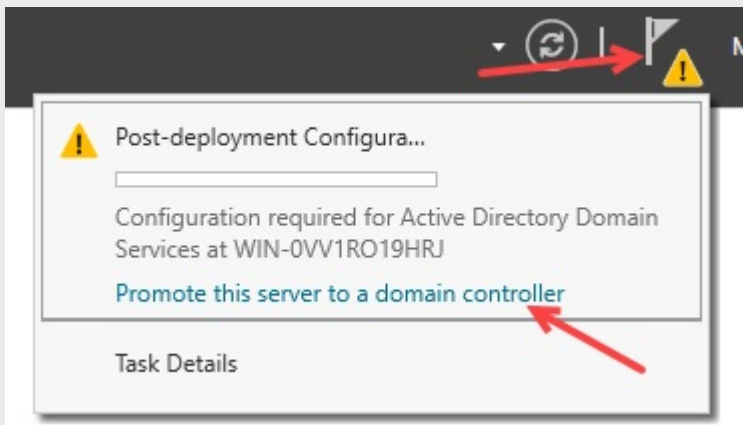
1

Server manager >> Add Role and Feature



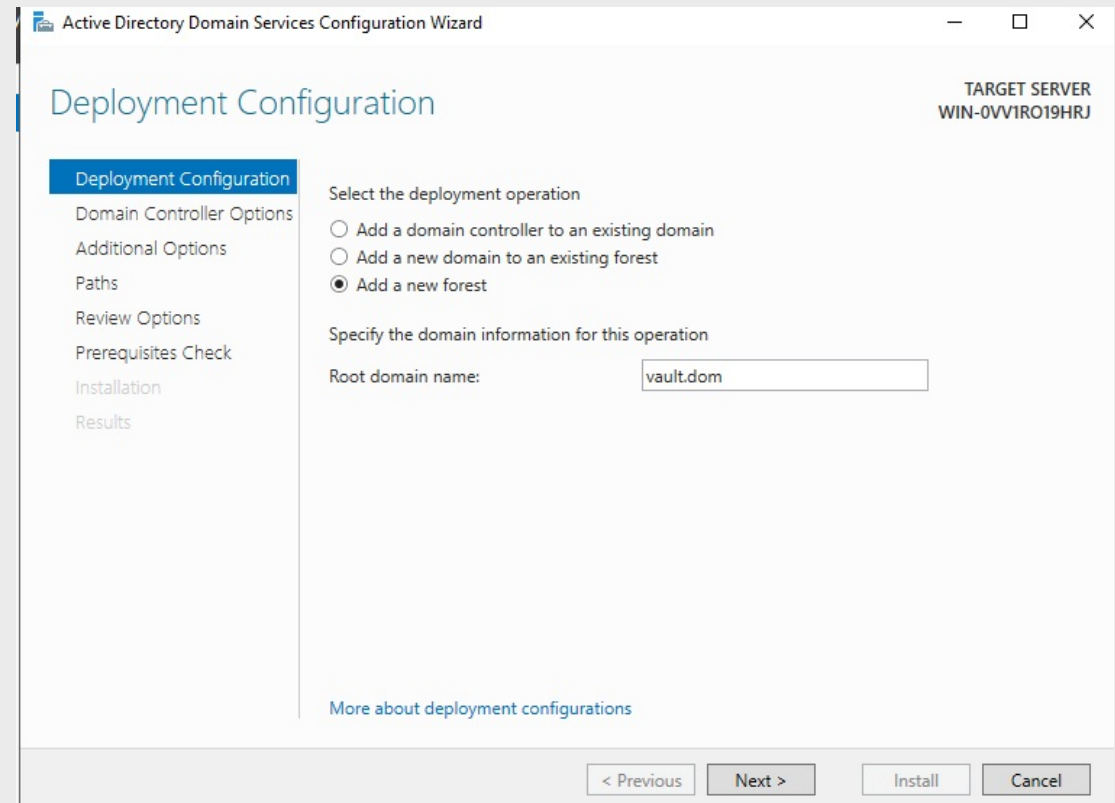
2

promote the server to domain controller



3

configure domain vault.dom



after step-3 accept default and enter password



HashiCorp

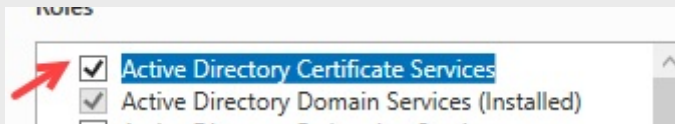
# Vault Active Directory Secret Engine

2

Active Directory certificate service install

1

Server manager >> Add Role and Feature



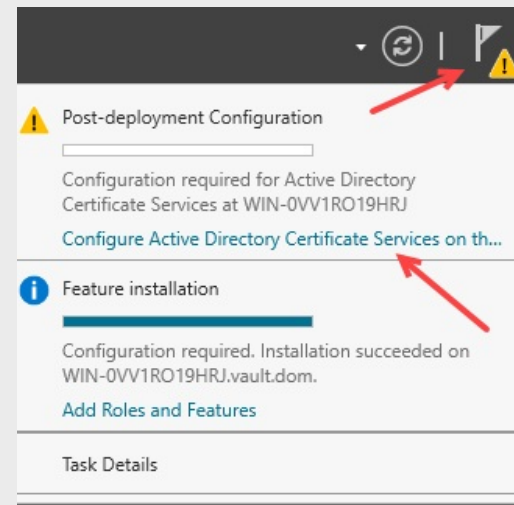
2

Select Certificate Authority



3

configure active directory certificate service



4

Select Certificate Authority





HashiCorp

# Vault Active Directory Secret Engine

2

## Active Directory certificate service install

5

## Select Enterprise CA

certificates.

☒ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

**These Option Only Come if you logged as Domain Administrator**

6

## Server ROOT CA

☒ Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

7

## create the Private Key

☒ Create a new private key

Use this option if you do not have a private key or want to create a new private key.

8

## Encryption

Select a cryptographic provider:

RSA#Microsoft Software Key Storage Provider

Key length:

2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256

after these step select all default parameter



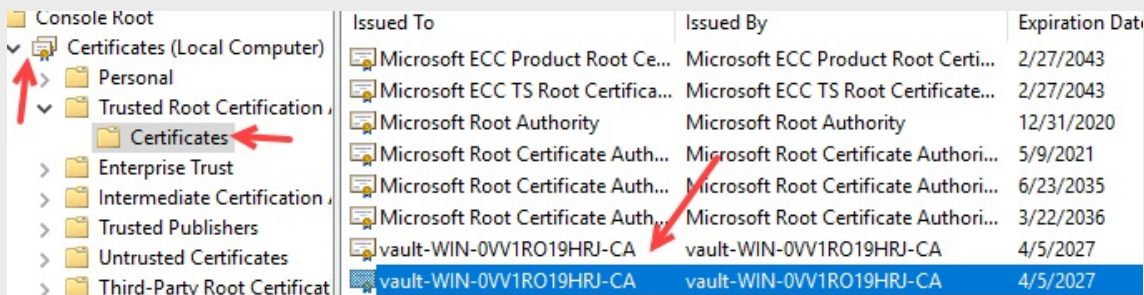
HashiCorp

# Vault Active Directory Secret Engine

2

export the certificate

## 1 Run mmc console and select add/remove Snap In



## 2 right Click Export Certificate

Select the format you want to use:

- ☐ DER encoded binary X.509 (.CER)
- ☒ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

## 3 save it windows machine and then transfer to vault server

File name:

C:\Users\administrator\Desktop\AD.cer

Browse...



HashiCorp

# Vault Active Directory Secret Engine

3

Configure the Vault server

1

Configure the Domain controller FQDN in /etc/hosts

```
vagrant@vaulthost2:~$ cat /etc/hosts
192.168.50.106 win-0vv1ro19hrj.vault.dom
```

2

Configure the Environment Variable

```
export USERNAME='CN=vagrant,CN=Users,DC=vault,DC=dom'
export PASSWORD=vagrant
export ADSERVER=ldaps://WIN-0VV1R019HRJ.vault.dom:636
export USERDN='DC=vault,DC=dom'
export INSECURTLS="true"
export VAULT_ADDR=https://192.168.50.102:8200
export VAULT_SKIP_VERIFY=true
```

3

Login into vault

vault login << i used root token however you can use policy based token

4

enable AD secret Engine

vault secrets enable ad

5

Write the configuration Details

```
vault write ad/config \
  binddn=$USERNAME \
  bindpass=$PASSWORD \
  url=$ADSERVER \
  insecure_tls=$INSECURTLS \
  userdn=$USERDN \
  certificate=@AD.cer
```

6

create service account in Active Directory

 fizz	User
 buzz	User



4

configure service account

1



## Create library for Service Account

```
vault write ad/library/accounting-team \  
  service_account_names=fizz@vault.dom,buzz@vault.dom \  
  ttl=10h \  
  max_ttl=20h \  
  disable_check_in_enforcement=false
```

2

## Verify the status

```
vagrant@vaulthost2:~$ vault read ad/library/accounting-team/status  
Key      Value  
---      -  
buzz@vault.dom  map[available:true]  
fizz@vault.dom  map[available:true]
```

 fizz	User
 buzz	User





HashiCorp

# Vault Active Directory Secret Engine

5

## Account Check-in/check-out

1

### Account Checkout

`vault write -f ad/library/accounting-team/check-out`

```
vagrant@vaulthost2:~$ vault write -f ad/library/accounting-team/check-out
Key                               Value
---                               -
lease_id                         ad/library/accounting-team/check-out/UVwtYbph01CTmraPc4y1DQY
lease_duration                   10h
lease_renewable                  true
password                         ?@09AZF4LVudZkentYqPXfKe6htgi3K9rSp1PFcfbUsFMSrAAIkjr04wYyw5WU5b
service_account_name             fizz@vault.dom
```

2

### Check Ins

`vault write ad/library/accounting-team/check-in service_account_names=fizz@vault.dom`