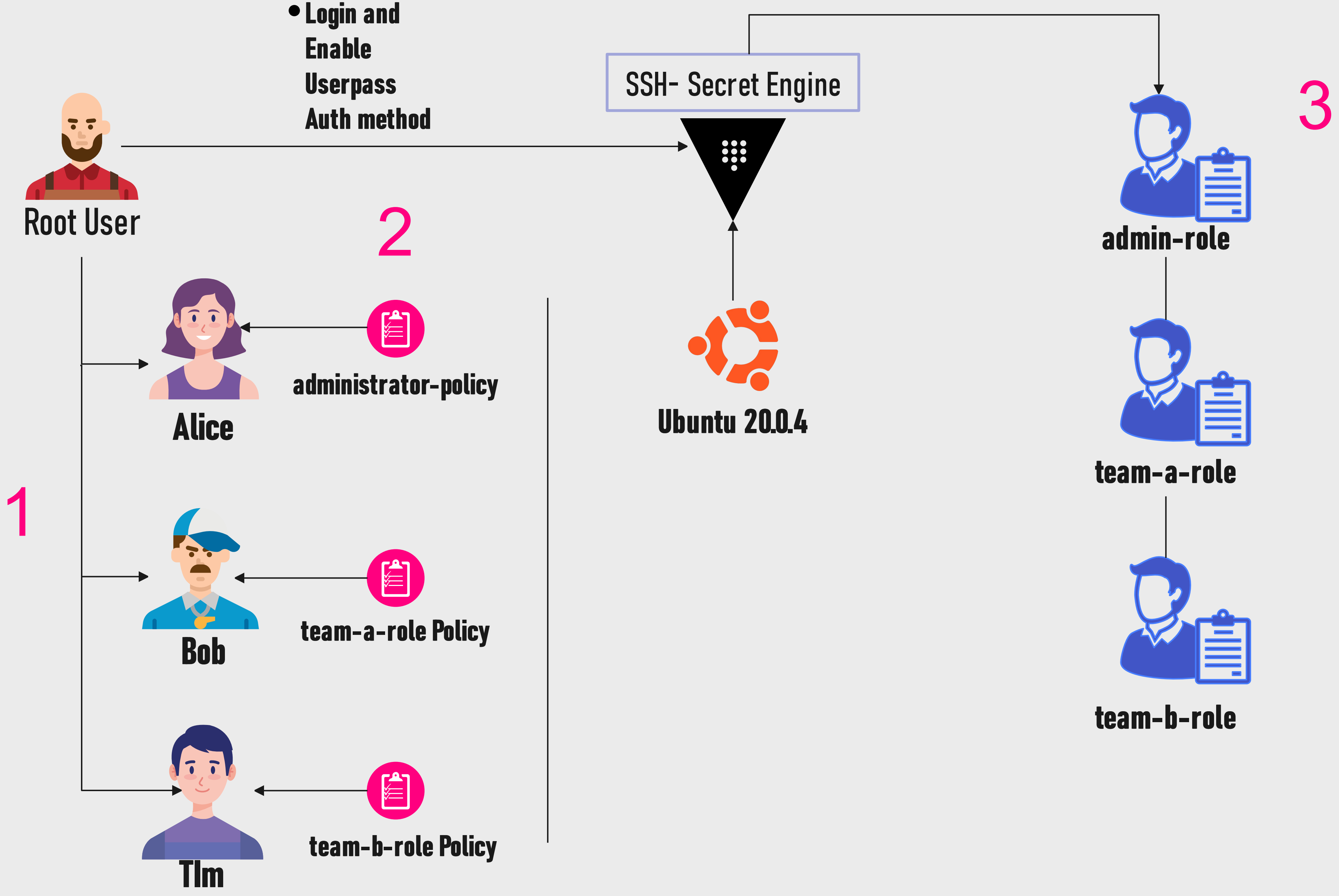
HashiCorp Vault

Hashicorp SSH-CA Engine setup Architecture



- Login and Enable Userpass Auth method

SSH- Secret Engine

Root User

1

2

3

Alice

administrator-policy

Bob

team-a-role Policy

TIm

team-b-role Policy

Ubuntu 20.0.4

admin-role

team-a-role

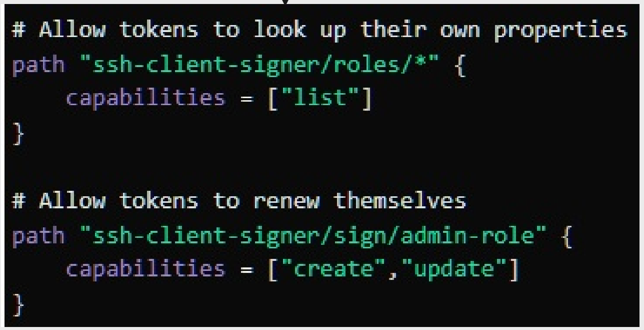
team-b-role

HashiCorp Vault

Hashicorp Vault SSH-CA Engine setup Architecture

Alice

administrator-policy

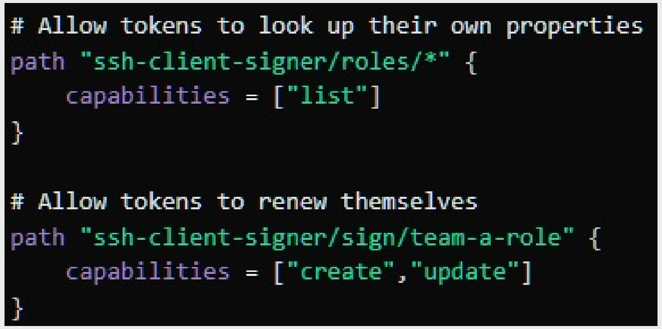


```
# Allow tokens to look up their own properties
path "ssh-client-signer/roles/*" {
    capabilities = ["list"]
}

# Allow tokens to renew themselves
path "ssh-client-signer/sign/admin-role" {
    capabilities = ["create","update"]
}
```

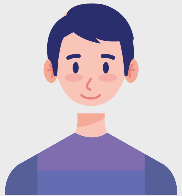
Bob

team-a-role Policy



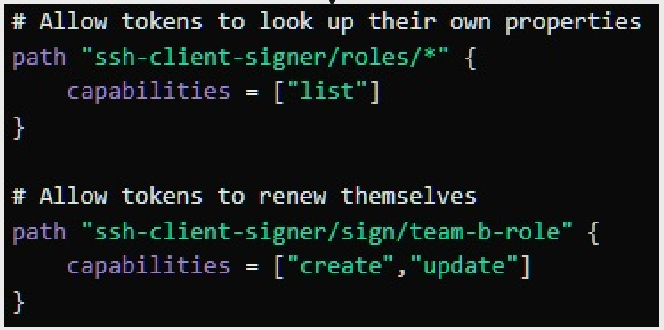
```
# Allow tokens to look up their own properties
path "ssh-client-signer/roles/*" {
    capabilities = ["list"]
}

# Allow tokens to renew themselves
path "ssh-client-signer/sign/team-a-role" {
    capabilities = ["create","update"]
}
```



TIm

team-b-role Policy

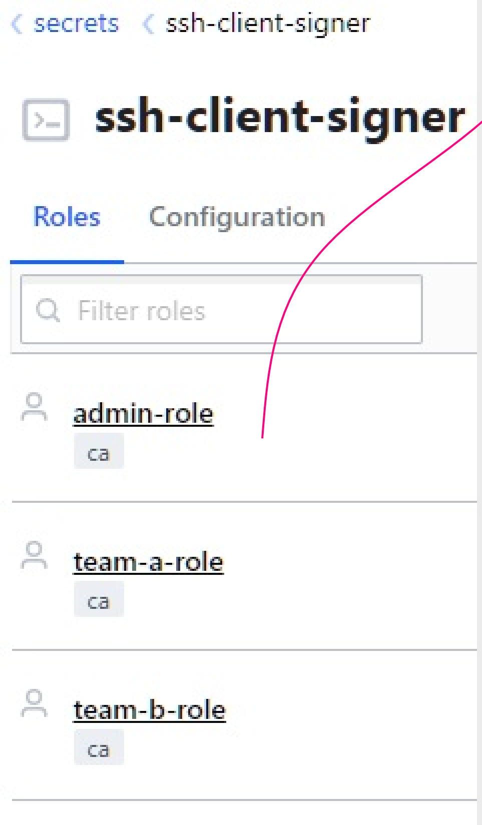


```
# Allow tokens to look up their own properties
path "ssh-client-signer/roles/*" {
    capabilities = ["list"]
}

# Allow tokens to renew themselves
path "ssh-client-signer/sign/team-b-role" {
    capabilities = ["create","update"]
}
```

Hashicorp Vault SSH-CA setup Architecture

SSH Role Creation

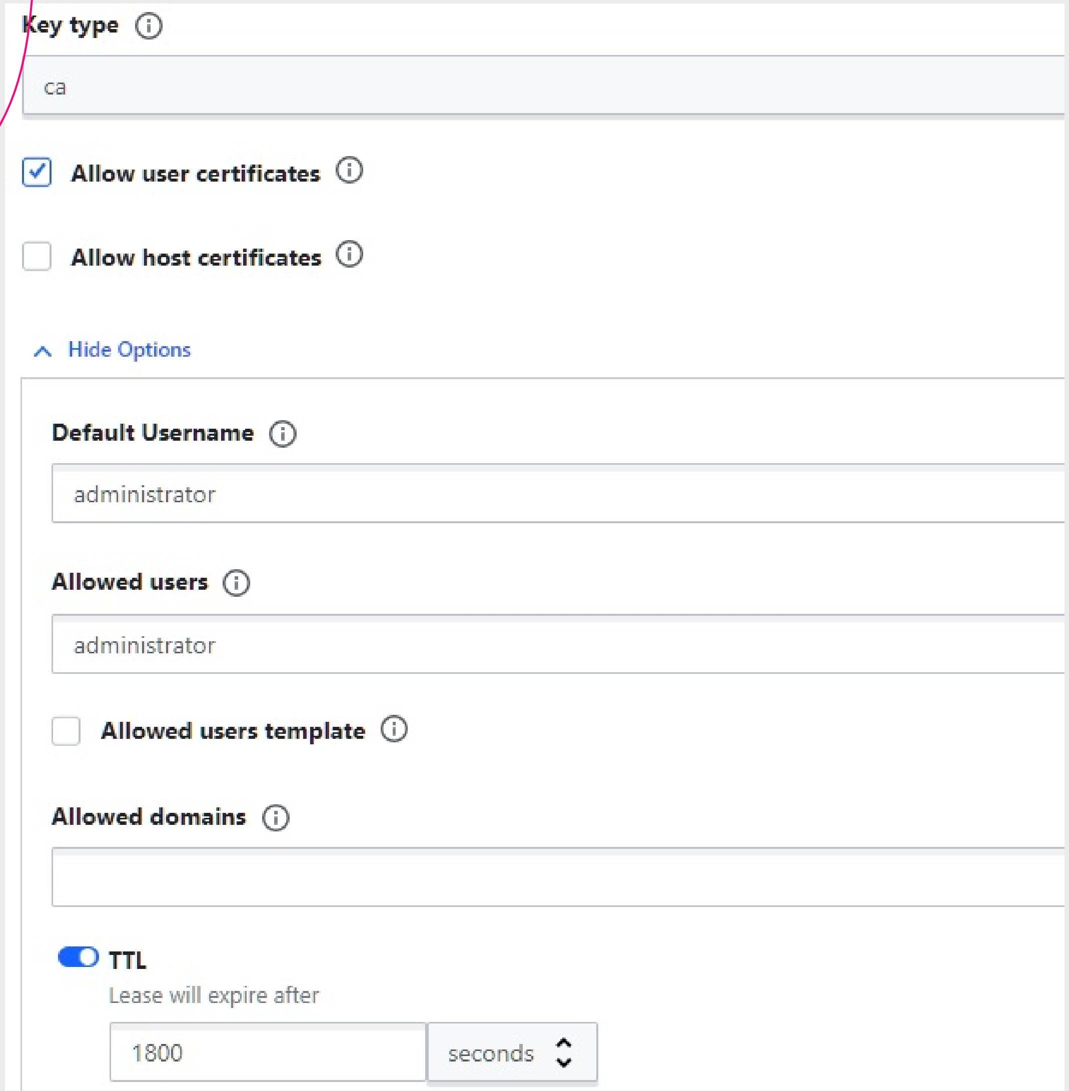


< secrets < ssh-client-signer

ssh-client-signer

- admin-role — ca
- team-a-role — ca
- team-b-role — ca

admin-role



Key type: ca

☑ Allow user certificates

□ Allow host certificates

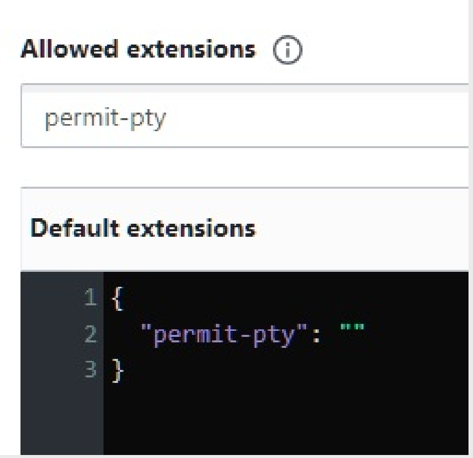
Default Username: administrator

Allowed users: administrator

□ Allowed users template

Allowed domains:

TTL: Lease will expire after 1800 seconds



Allowed extensions: permit-pty

Default extensions

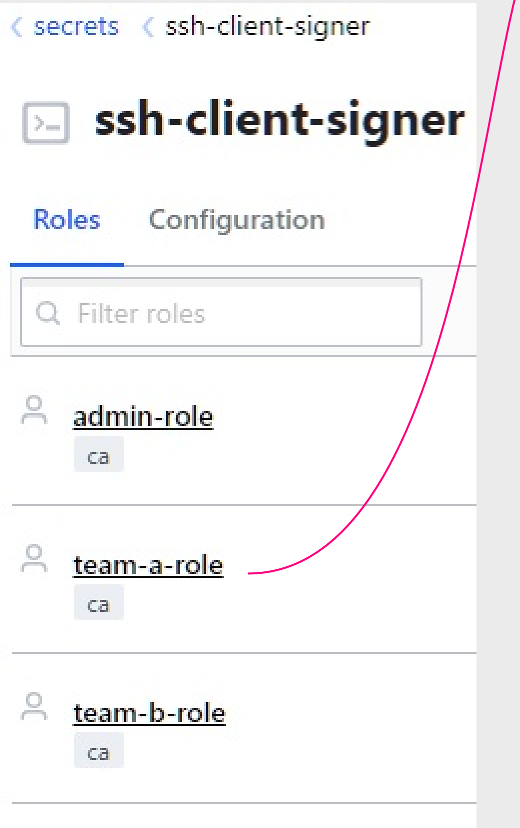
```
{
  "permit-pty": ""
}
```

Configure the parameter according to snap

HashiCorp Vault

Hashicorp Vault SSH-CA setup Architecture

SSH Role Creation



‹ secrets ‹ ssh-client-signer

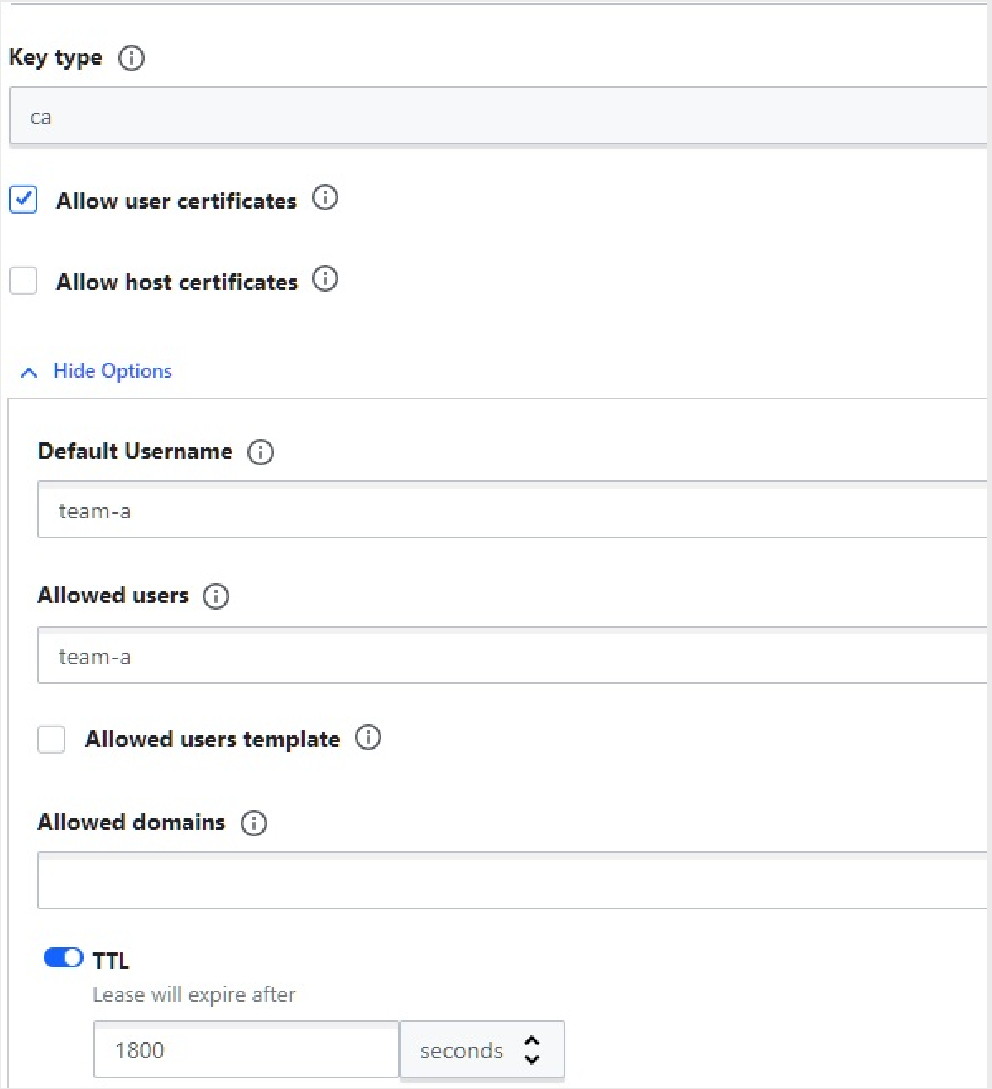
ssh-client-signer

Roles | Configuration

Filter roles

- admin-role ca
- team-a-role ca
- team-b-role ca

team-a-role



Key type ⓘ

ca

☑ Allow user certificates ⓘ

□ Allow host certificates ⓘ

Hide Options

Default Username ⓘ

team-a

Allowed users ⓘ

team-a

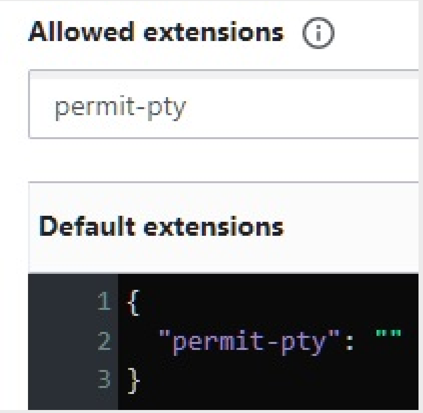
□ Allowed users template ⓘ

Allowed domains ⓘ

TTL

Lease will expire after

1800 seconds



Allowed extensions ⓘ

permit-pty

Default extensions

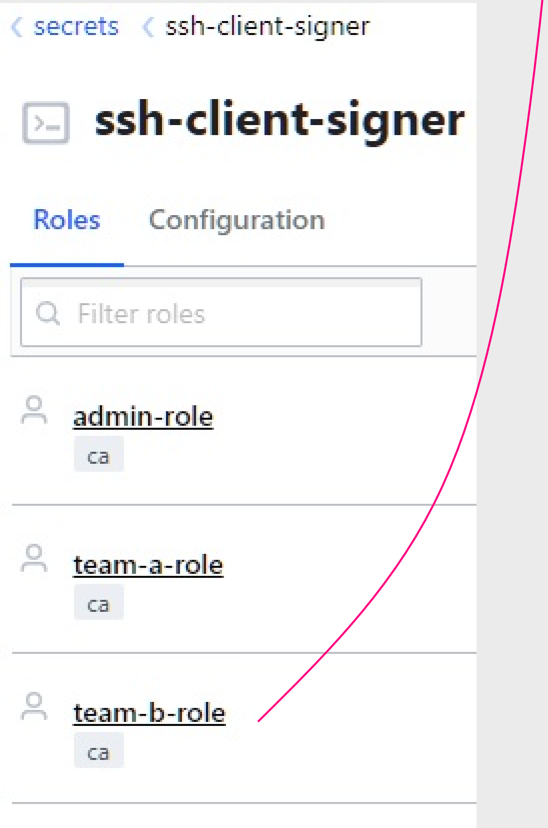
```
{
  "permit-pty": ""
}
```

Configure the parameter according to snap

HashiCorp Vault

Hashicorp Vault SSH-CA Architecture

SSH Role Creation



‹ secrets ‹ ssh-client-signer

ssh-client-signer

Roles | Configuration

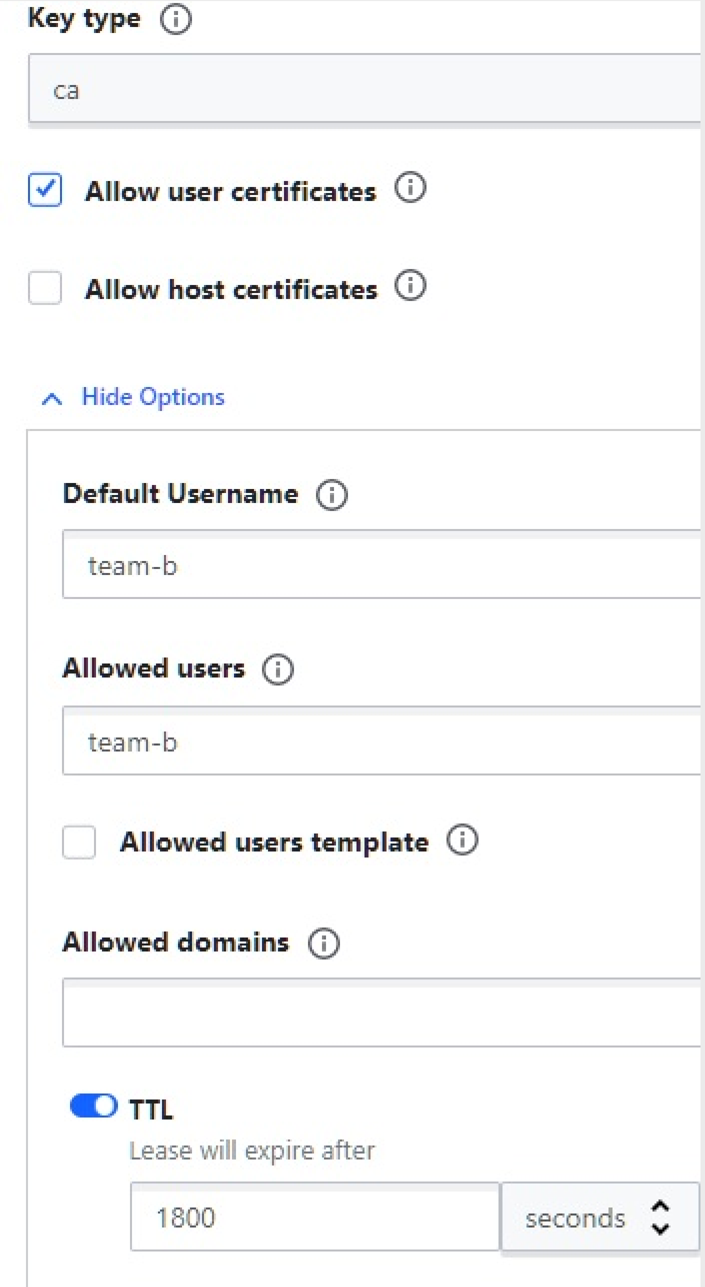
Filter roles

admin-role
ca

team-a-role
ca

team-b-role
ca

team-b-role



Key type ⓘ

ca

☑ **Allow user certificates** ⓘ

□ **Allow host certificates** ⓘ

Hide Options

Default Username ⓘ

team-b

Allowed users ⓘ

team-b

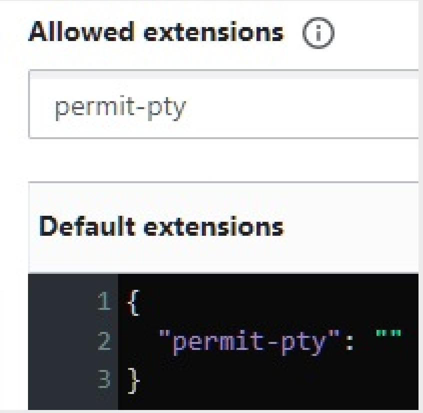
□ **Allowed users template** ⓘ

Allowed domains ⓘ

TTL

Lease will expire after

1800 seconds



Allowed extensions ⓘ

permit-pty

Default extensions

```
{
  "permit-pty": ""
}
```

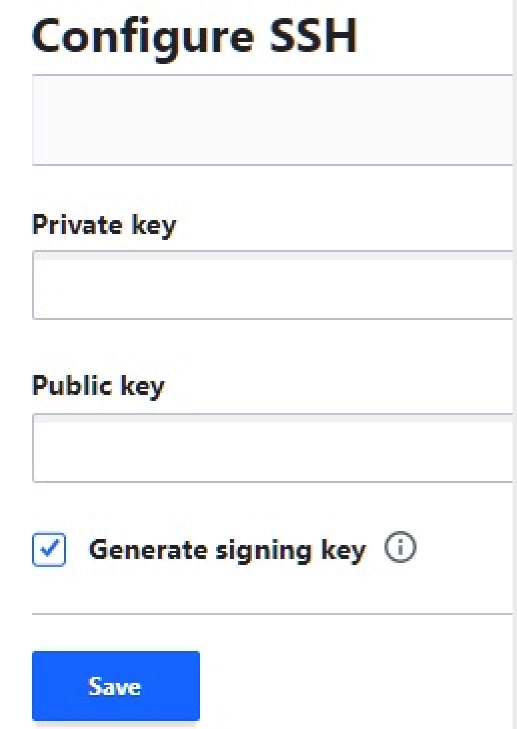
Configure the parameter according to snap

Hashicorp Vault SSH-CA setup Architecture

Generate Trusted CA Keys

1 ssh-client-signer »Configuration » Configure

2



Configure SSH

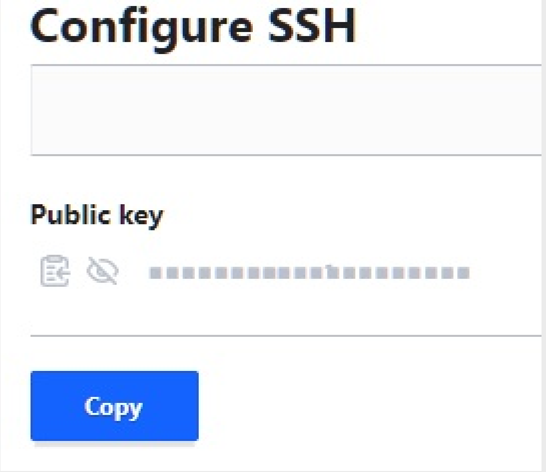
Private key

Public key

☑ Generate signing key ⓘ

Click on save without doing anything

3



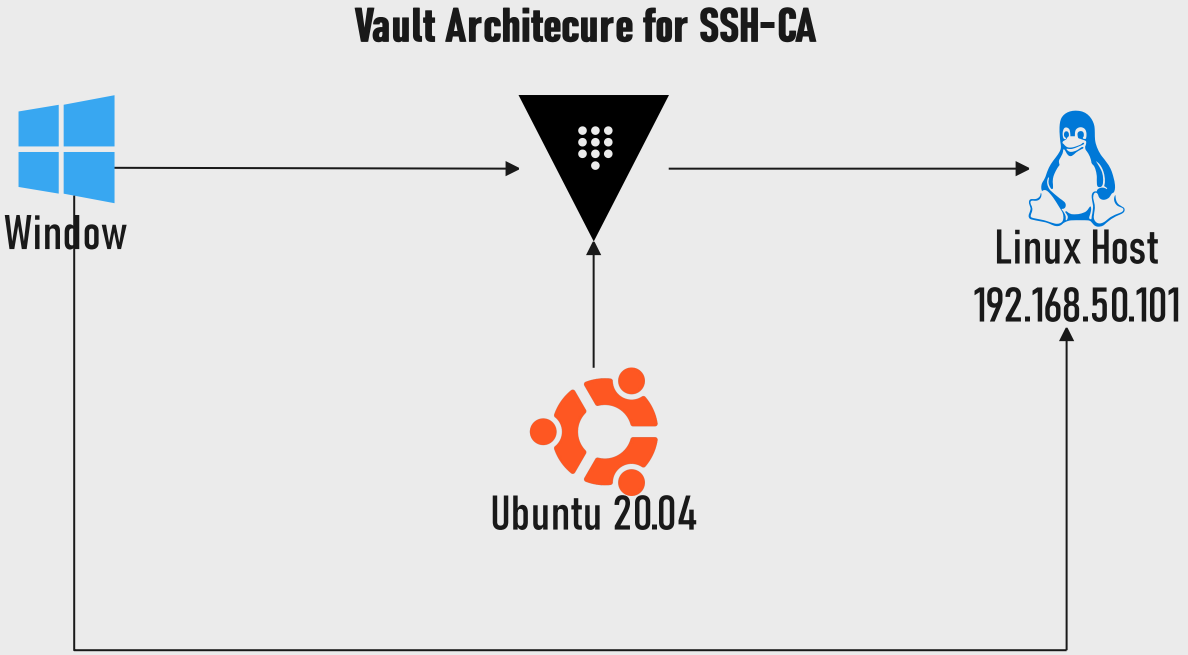
Configure SSH

Public key

copy key

HashiCorp Vault

Hashicorp Vault SSH-CA setup Architecture

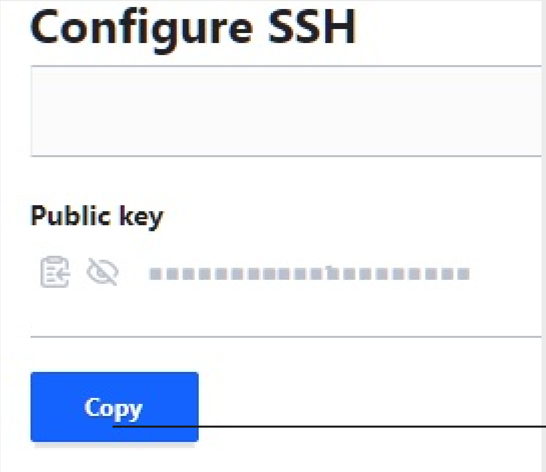


Configure the parameter according to snap

Hashicorp Vault SSH-CA setup Architecture

Configure SSH Host [this step perform on Host Machine Not on vault server

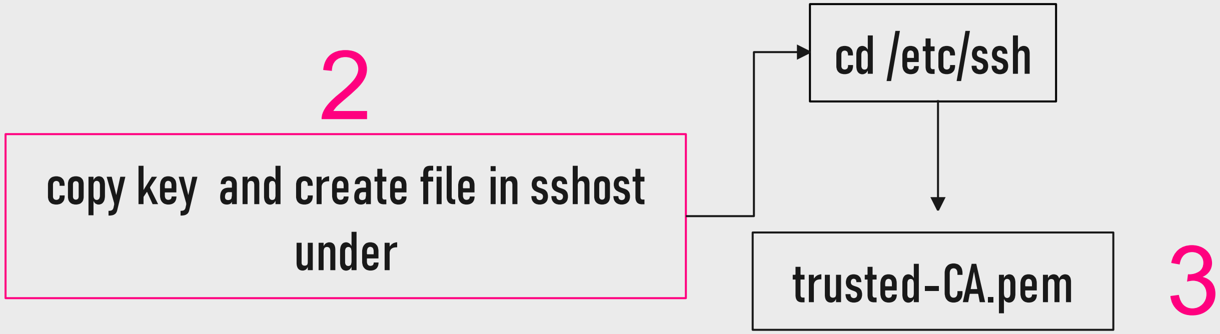
1 ssh-client-signer »Configuration » Configure



Configure SSH

Public key

••••••••••••••••••••••



2

copy key and create file in sshost under

cd /etc/ssh

trusted-CA.pem

3

4

```
cd /etc/ssh

mkdir auth_principals/

sudo echo 'administrator' > admin
sudo echo 'team-a' > appadmin
sudo echo 'team-b' > appadmin
```

5 configure these parameter Under /etc/ssh/sshd_config

```
AuthorizedPrincipalsFile /etc/ssh/auth_principals/%u
ChallengeResponseAuthentication no
PasswordAuthentication no
TrustedUserCAKeys /etc/ssh/trusted-CA.pem
```

6

```
sudo service ssh restart
```

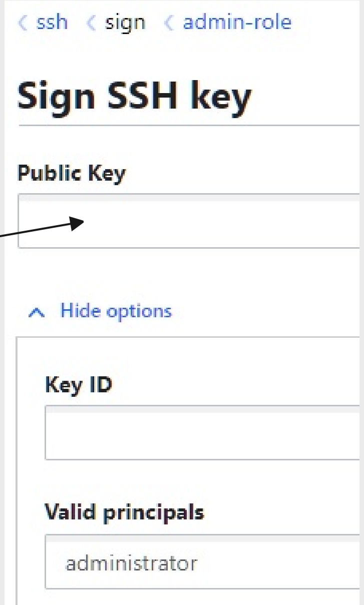
HashiCorp Vault

Hashicorp Vault SSH-CA setup Architecture

1 Generate the Key-pair on client machine In these scenario it is windows machine

```
ssh-keygen -f c:\Users\%USERNAME%\.ssh\alice-key
```

alice-key alice-key.pub



ssh < sign < admin-role

Sign SSH key

Public Key

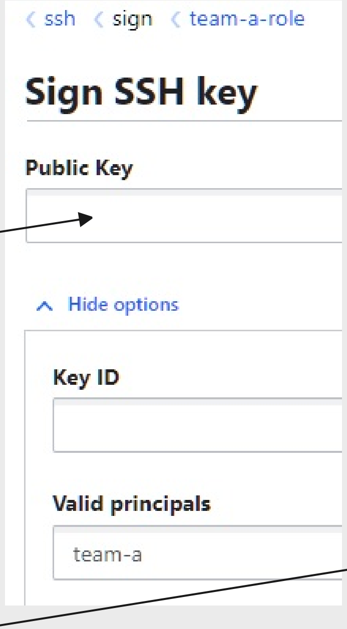
^ Hide options

Key ID

Valid principals: administrator

```
ssh-keygen -f c:\Users\%USERNAME%\.ssh\bob-key
```

bob-key bob-key.pub



ssh < sign < team-a-role

Sign SSH key

Public Key

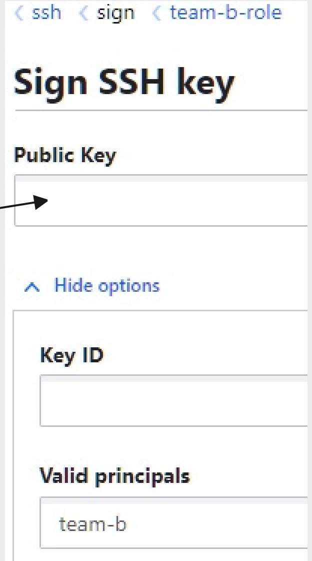
^ Hide options

Key ID

Valid principals: team-a

```
ssh-keygen -f c:\Users\%USERNAME%\.ssh\tim-key
```

tim-key tim-key.pub



ssh < sign < team-b-role

Sign SSH key

Public Key

^ Hide options

Key ID

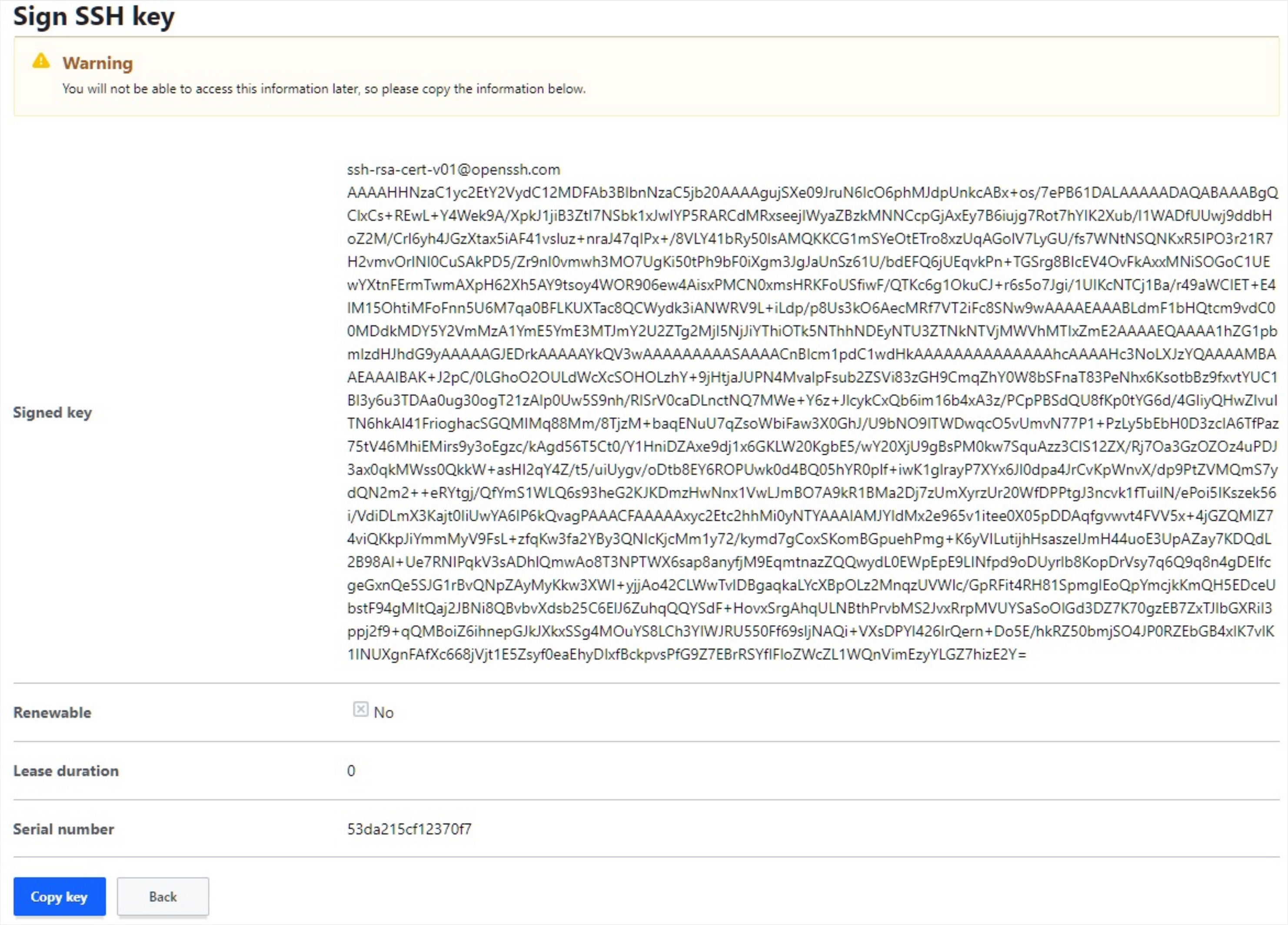
Valid principals: team-b

Click on Sign will generate signed public key

HashiCorp Vault

Hashicorp Vault SSH-CA setup Architecture

1 copy generated signed key using Copy button and save it in your machine alice-signed-key.pub



Sign SSH key

Warning

You will not be able to access this information later, so please copy the information below.

Signed key

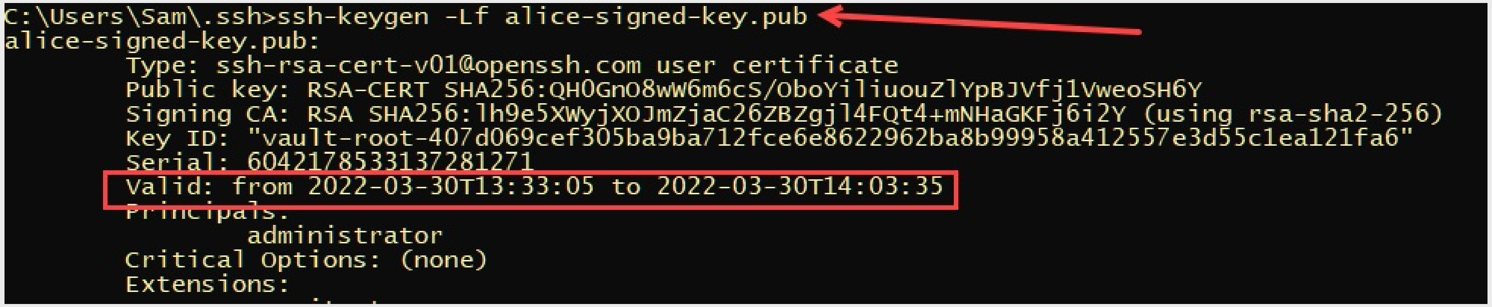
```
ssh-rsa-cert-v01@openssh.com
AAAAHHNzaC1yc2EtY2VydC12MDFAb3BlbnNzaC5jb20AAAAgujSXe09JruN6lcO6phMJdpUnkcABx+os/7ePB61DALAAAAADAQABAAABgQ
ClxCs+REwL+Y4Wek9A/XpkJ1jiB3Ztl7NSbk1xJwlYP5RARCdMRxseejlWyaZBzkMNNCcpGjAxEy7B6iujg7Rot7hYIK2Xub/l1WADfUUwj9ddbH
oZ2M/Crl6yh4JGzXtax5iAF41vsluz+nraJ47qlPx+/8VLY41bRy50lsAMQKKCG1mSYeOtETro8xzUqAGolV7LyGU/fs7WNtNSQNKxR5lPO3r21R7
H2vmvOrlNl0CuSAkPD5/Zr9nl0vmwh3MO7UgKi50tPh9bF0iXgm3JgJaUnSz61U/bdEFQ6jUEqvkPn+TGSrg8BlcEV4OvFkAxxMNiSOGoC1UE
wYXtnFErmTwmAXpH62Xh5AY9tsoy4WOR906ew4AisxPMCN0xmsHRKFoUSfiwF/QTKc6g1OkuCJ+r6s5o7Jgi/1UlKcNTCj1Ba/r49aWClET+E4
lM15OhtiMFoFnn5U6M7qa0BFLKUXTac8QCWydk3iANWRV9L+iLdp/p8Us3kO6AecMRf7VT2iFc8SNw9wAAAAEAAABLdmF1bHQtcm9vdC0
0MDdkMDY5Y2VmMzA1YmE5YmE3MTJmY2U2ZTg2MjI5NjJiYThiOTk5NThhNDEyNTU3ZTNkNTVjMWVhMTIxZmE2AAAAEQAAAA1hZG1pb
mlzdHJhdG9yAAAAAGJEDrkAAAAAYkQV3wAAAAAAAAASAAAACnBlcm1pdC1wdHkAAAAAAAAAAAAAAAhcAAAAHc3NoLXJzYQAAAAMBA
AEAAAIBAK+J2pC/0LGhoO2OULdWcXcSOHOLzhY+9jHtjaJUPN4MvalpFsub2ZSVi83zGH9CmqZhY0W8bSFnaT83PeNhx6KsotbBz9fxvtYUC1
Bl3y6u3TDAa0ug30ogT21zAlp0Uw5S9nh/RlSrV0caDLnctNQ7MWe+Y6z+JlcykCxQb6im16b4xA3z/PCpPBSdQU8fKp0tYG6d/4GliyQHwZlvul
TN6hkAl41FrioghacSGQMlMq88Mm/8TjzM+baqENuU7qZsoWbiFaw3X0GhJ/U9bNO9lTWDwqcO5vUmvN77P1+PzLy5bEbH0D3zclA6TfPaz
75tV46MhiEMirs9y3oEgzc/kAgd56T5Ct0/Y1HniDZAxe9dj1x6GKLW20KgbE5/wY20XjU9gBsPM0kw7SquAzz3ClS12ZX/Rj7Oa3GzOZOz4uPDJ
3ax0qkMWss0QkkW+asHI2qY4Z/t5/uiUygv/oDtb8EY6ROPUwk0d4BQ05hYR0plf+iwK1glrayP7XYx6Jl0dpa4JrCvKpWnvX/dp9PtZVMQmS7y
dQN2m2++eRYtgj/QfYmS1WLQ6s93heG2KJKDmzHwNnx1VwLJmBO7A9kR1BMa2Dj7zUmXyrzUr20WfDPPtgJ3ncvk1fTuiIN/ePoi5IKszek56
i/VdiDLmX3Kajt0IiUwYA6lP6kQvagPAAACFAAAAAxyc2Etc2hhMi0yNTYAAAIAMJYldMx2e965v1itee0X05pDDAqfgvwvt4FVV5x+4jGZQMIZ7
4viQKkpJiYmmMyV9FsL+zfqKw3fa2YBy3QNlcKjcMm1y72/kymd7gCoxSKomBGpuehPmg+K6yVILutijhHsaszelJmH44uoE3UpAZay7KDQdL
2B98Al+Ue7RNIPqkV3sADhlQmwAo8T3NPTWX6sap8anyfjM9EqmtnazZQQwydL0EWpEpE9LINfpd9oDUyrlb8KopDrVsy7q6Q9q8n4gDElfc
geGxnQe5SJG1rBvQNpZAyMyKkw3XWI+yjjAo42CLWwTvIDBgaqkaLYcXBpOLz2MnqzUVWlc/GpRFit4RH81SpmglEoQpYmcjkKmQH5EDceU
bstF94gMltQaj2JBNi8QBvbvXdsb25C6ElJ6ZuhqQQYSdF+HovxSrgAhqULNBthPrvbMS2JvxRrpMVUYSaSoOlGd3DZ7K70gzEB7ZxTJlbGXRiI3
ppj2f9+qQMBoiZ6ihnepGJkJXkxSSg4MOuYS8LCh3YIWJRU550Ff69sIjNAQi+VXsDPYI426lrQern+Do5E/hkRZ50bmjSO4JP0RZEbGB4xlK7vlK
1lNUXgnFAfXc668jVjt1E5Zsyf0eaEhyDlxfBckpvsPfG9Z7EBrRSYflFloZWcZL1WQnVimEzyYLGZ7hizE2Y=
```

Renewable	☒ No
Lease duration	0
Serial number	53da215cf12370f7

HashiCorp Vault

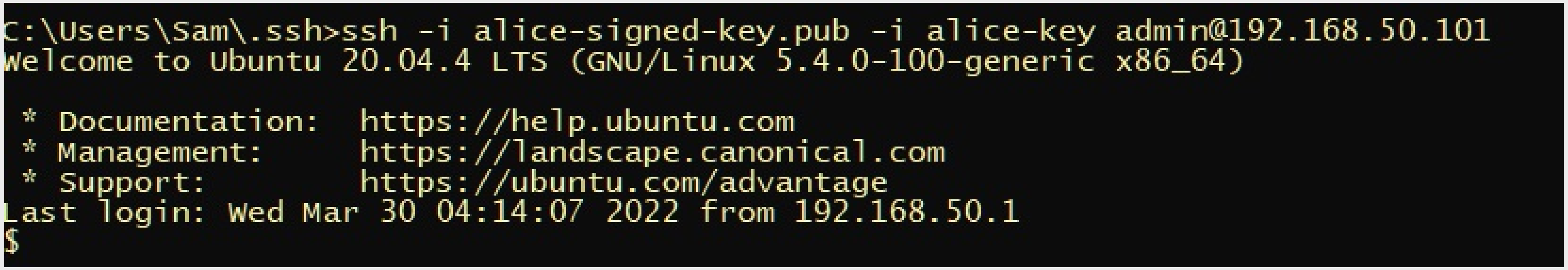
Hashicorp Vault SSH-CA setup Architecture

1 verify the sigend public-key [note: it is vailid only for 30 minute



```
C:\Users\Sam\.ssh>ssh-keygen -Lf alice-signed-key.pub
alice-signed-key.pub:
        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key: RSA-CERT SHA256:QH0GnO8wW6m6cS/OboYiliuouZlYpBJVfj1VweoSH6Y
        Signing CA: RSA SHA256:lh9e5XWyjXOJmZjaC26ZBZgjl4FQt4+mNHaGKFj6i2Y (using rsa-sha2-256)
        Key ID: "vault-root-407d069cef305ba9ba712fce6e8622962ba8b99958a412557e3d55c1ea121fa6"
        Serial: 6042178533137281271
        Valid: from 2022-03-30T13:33:05 to 2022-03-30T14:03:35
        Principals:
                administrator
        Critical Options: (none)
        Extensions:
```

2 now try to login with signed and private key



```
C:\Users\Sam\.ssh>ssh -i alice-signed-key.pub -i alice-key admin@192.168.50.101
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-100-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Wed Mar 30 04:14:07 2022 from 192.168.50.1
$
```

3 verify user

```
$ whoami
admin
$
```