

## NOTE:

- A) MKPI DevOps team (#mkpiglidevopsengineering@mkpimail.com) has provisioned self service portal for creating “name service” in Hashicorp Vault. Self service portal will provide admin access to the name space as well. You may contact MKPI DevOps team for any issue with Hashicorp vault after opening an incident with them. Once you have the admin access, you should have Hashicorp vault applymation knowledge before following this document.
- B) This document is prepared by Unix Ops while doing Hashicorp integration with Ansible Tower and is not responsible if there is any deviation because of changes on Hashicorp Vault or Ansible Tower applymation.

- 1) On Hashicorp, enable below Secrets Engines on Hashicorp under assigned namespace  
Example Name Space: karsh-ymat-devops

Secret: KV

< kv < ansible

### ansible

<input type="checkbox"/> JSON	
Key	Value
ssh-private-key	  [REDACTED]
ssh-username	  [REDACTED]

Secret: SSH

- a) Generate private and public key for service account - pvc-ymat-tw-prd after logging into any server.

```
[kumar00@noloc21as127 ~]$ ssh-keygen
```

Generating public/private rsa key pair.

Enter file in which to save the key (/home/kumar00/.ssh/id\_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identifiymation has been saved in /home/kumar00/.ssh/id\_rsa.

Your public key has been saved in /home/kumar00/.ssh/id\_rsa.pub.

The key fingerprint is:

SHA256:pZAsZkSIDBPzT1iglkjvCOZI7oUX/6vY+mY9C8NJ4dE kumar00@noloc21as127

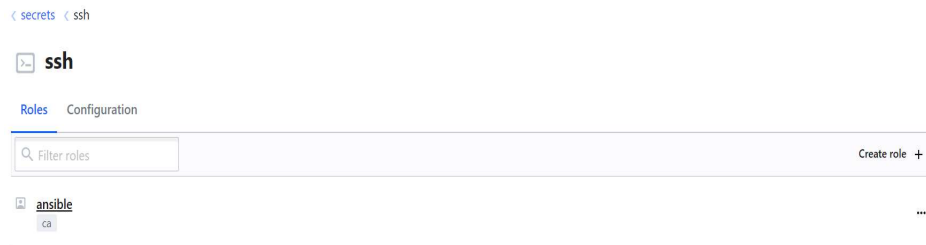
The key's randomart image is:

+---[RSA 2048]---+

```
| .o+oo      |
| ...X = ..   |
| o.+O.=o E.  |
| +.*o.++.oo  |
| o + o.+S    |
| . o o o     |
| . =..       |
|   oooo.     |
```

```
| o=+.oo |
+----[SHA256]-----+
[kumar00@noloc21as127 ~]$ ls -la .ssh/
total 20
drwxr-xr-x 2 kumar00 sysadmin 36 Jan 29 07:19 .
drwxr-xr-x 38 kumar00 sysadmin 8192 Jan 17 18:05 ..
-rw----- 1 kumar00 unixadm 1679 Jan 29 07:19 id_rsa
-rw-r--r-- 1 kumar00 unixadm 403 Jan 29 07:19 id_rsa.pub
[kumar00@noloc21as127 ~]$
```

b) Enable ssh secret and then create role ansible



c) Ensure ansible role having below setting

Role Name: ansible

Key Type: ca

Allow user certificates: Yes

Default user: pvc-ymat-tw-prd

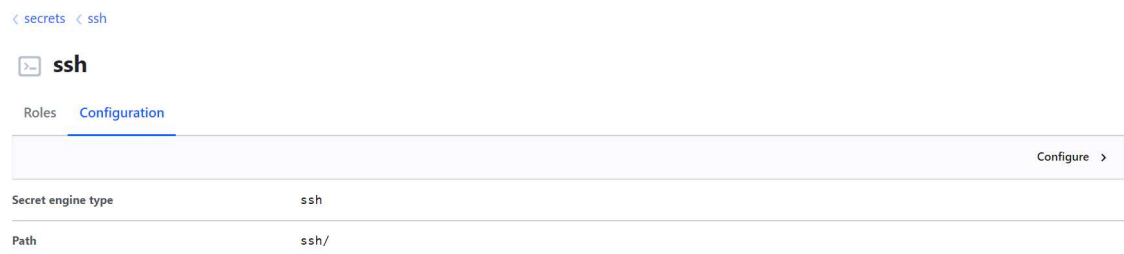
Allowed users: \*

Default Critical Options: {}

Default Extensions: {  
 "permit-pty": ""  
}

d) Generate the CA key in hashicorp using private and public key. This CA key will be copied to all the ansible managed servers.

secrets -> ssh -> Configuration -> Configure





**Note:** Just click *Generate signing key* check box to get the *ca public key*, which will be generated internally by Hashicorp vault. Leave *Private key* and *Public Key* fields blank. *CA public key* should be copied on all the clients under `/etc/centrifydc/ssh/trusted-user-ca-keys.pem`

- e) Ensure Hashicorp team has correct algorithm **from ssh-rsa to rsa-sha2-256** within namespace. They should match configuration with any working name space for example: **KTC\_Ansible\_Tower**

You can use below Hashicorp vault command to correct algorithm, If any issue, please refer Hashicorp vault documentation or open ticket with DevOps team if any issue.

```

vault write -namespace="namespacename" ssh/roles/ansible
algorithm_signer=rsa-sha2-256 key_type=ca
allow_user_certifyates=true

```

Example:

```

vault write -namespace="mkpi-app-prod-dallas/mer-mettldevop-
mkpimail-mettl-vault-mettldevop" ssh/roles/ansible
algorithm_signer=rsa-sha2-256 key_type=ca
allow_user_certifyates=true

```

⇒ **Check hashicorp signed public key for ssh algorithm**

Example Name Space: KTC\_Ansible\_Tower  
 service account: ktc-db-automation-ansible-tower  
 pvc-tower.pub.sign2 -> Signed public key from HV.

```
[noloc21as553v ~]$ ssh-keygen -Lf .ssh/pvc-tower.pub.sign2
```

.ssh/pvc-tower.pub.sign2:

Type: ssh-rsa-cert-v01@openssh.com user certifymate

Public key: RSA-CERT SHA256:LkahltmvVLOs9reEGXLvSIUFK+iOdI0bw8+tIZeChII

Signing CA: RSA SHA256:1Tk4BdTY3GsDvegb+AmOH1yHOn2YKnd7EIMDI8uq0KY  
(using ssh-rsa) Key ID: "vault-ldap-u1231255-  
2e46a122d9ef54b3acf6b7841972ef4a55052be8b4765d1bc3cfad21911c8652"  
Serial: 7970660710892761685  
Valid: from 2022-01-27T23:51:46 to 2022-02-28T23:52:16  
Principals:  
pvc-dbs-tw-prd  
Critical Options: (none)  
Extensions:  
permit-pty

⇒ **Below example showing unsupported ssh algorithm - rsa-sha2-256 by Ansible**

```
[noloc21as553v ~]$ ssh-keygen -Lf .ssh/pvc-tower.pub.signed
.ssh/pvc-tower.pub.signed:
  Type: ssh-rsa-cert-v01@openssh.com user certifymate
  Public key: RSA-CERT SHA256:LkahltvVLOs9reEGXLvSIUFK+iOdI0bw8+tIZechll
  Signing CA: RSA SHA256:2/WofeM+zXsrl9EJZwJlaYRp4VF+FEY4rdJWGjY4C0w (using rsa-
sha2-256)
  Key ID: "vault-ldap-fyuan-
2e46a122d9ef54b3acf6b7841972ef4a55052be8b4765d1bc3cfad21911c8652"
  Serial: 532653045777859207
  Valid: from 2022-01-27T22:51:35 to 2022-02-28T22:52:05
  Principals:
    pvc-dbs-tw-prd
  Critical Options: (none)
  Extensions:
    permit-pty
```

## 2) On Ansible Tower, Create below credentials type

HashiCorp Vault Secret Lookup  
HashiCorp Vault Signed SSH  
Machine

Example:

Name:	Type
ansudoymat	Machine
Hashicorp Secrets lcat	HashiCorp Vault Secret Lookup
Hashicorp Vault ymat	HashiCorp Vault Signed SSH

### a) HashiCorp Vault Secret Lookup Setup

It is based on KV (Key Value) secret engine in Hashicorp and used to store key and its value.

Khan ( MKPI HashiCorp) to get certifymate

TOWER
admin

VIEWS

- [Dashboard](#)
- [Jobs](#)
- [Schedules](#)
- [My View](#)

RESOURCES

- [Templates](#)
- [Credentials](#)
- [Projects](#)
- [Inventories](#)
- [Inventory Scripts](#)

ACCESS

- [Organizations](#)
- [Users](#)
- [Teams](#)

ADMINISTRATION

- [Credential Types](#)
- [Notifications](#)
- [Management Jobs](#)
- [Instance Groups](#)

## CREDENTIALS / EDIT CREDENTIAL

Hashicorp Secrets Icat

DETAILS

PERMISSIONS

\* NAME ⓘ

Hashicorp Secrets Icat

DESCRIPTION ⓘ

ORGANIZATION

Q Marsh

\* CREDENTIAL TYPE ⓘ

Q HashiCorp Vault Secret Lookup

TYPE DETAILS

\* SERVER URL ⓘ

https://mgtdal-so-vlrmshmc.com

TOKEN ⓘ

ENCRYPTED

NAMESPACE ⓘ

ENCRYPTED

CA CERTIFICATE ⓘ

-----BEGIN CERTIFICATE-----  
MIIFZDCCABGwIIBAgIQKTrSyttJb+AFB87YwUoGTAN@ghkqhI69u0BAQiFADCB  
HTELWAGA1UEBHMCRo1xgZA2BgHnBagTEkdyZHFOZXIgtfUvZVz1CjRlClEQH4AG  
AUBehvKIZfStayZDEahlgGA1UECHMQRm90OTtPNTNBIExpbmI0ZWxzqAZBglnv  
RAITTEIMPUYSyTysyngdygdzmauhpRcIvSI8J0X0ob3JjdmluawCMITMTES  
MDluIDBlawhChguITeLhY1SDTUSUjGBTELWAGA1UEBHMCRo1xgZA2BgHnBagTE  
kdyZHFOZXIgtfUvZVz1CjRlClEQH4AG

APPROLE ROLE\_ID ⓘ

APPROLE SECRET\_ID ⓘ

PATH TO APPROLE AUTH ⓘ

approve

\* API VERSION ⓘ

v0

TEST CANCEL SAVE

SAVE

You can test external credential as per below screenshot. It should show “Test Pass” when you click “RUN”.

#### UNSIGNED PUBLIC KEY:

It is public key generated for service account - pvc-yamat-tw-prd using as above

ROLE NAME: ansible # This role is created under ssh secret engine.

HashiCorp ssh secret showing ansible role

c) Machine credential setup

Credentials -> New Credentials

**Credential Type: Machine**

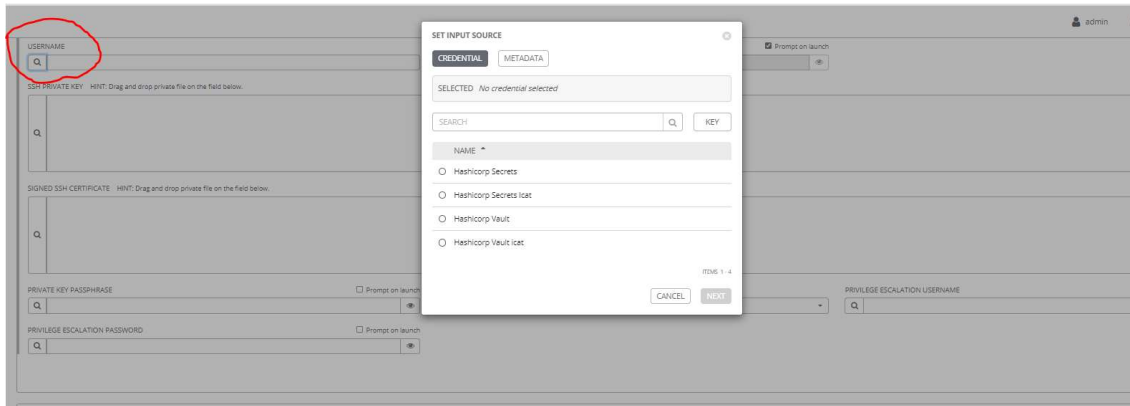
The screenshot shows the 'NEW CREDENTIAL' form in Ansible Tower. The 'CREDENTIAL TYPE' is set to 'Machine'. The 'NAME' field is empty, and the 'ORGANIZATION' dropdown is set to 'SELECT AN ORGANIZATION'. The 'DESCRIPTION' field is empty. The 'TYPE DETAILS' section includes 'USERNAME' and 'PASSWORD' fields, both with search icons. Below these are two large text areas for 'SSH PRIVATE KEY' and 'SIGNED SSH CERTIFICATE', both with search icons. At the bottom, there are fields for 'PRIVATE KEY PASSPHRASE', 'PRIVILEGE ESCALATION METHOD', and 'PRIVILEGE ESCALATION USERNAME', each with a search icon. The 'CANCEL' and 'SAVE' buttons are at the bottom right.

**NAME:** Give the credential name

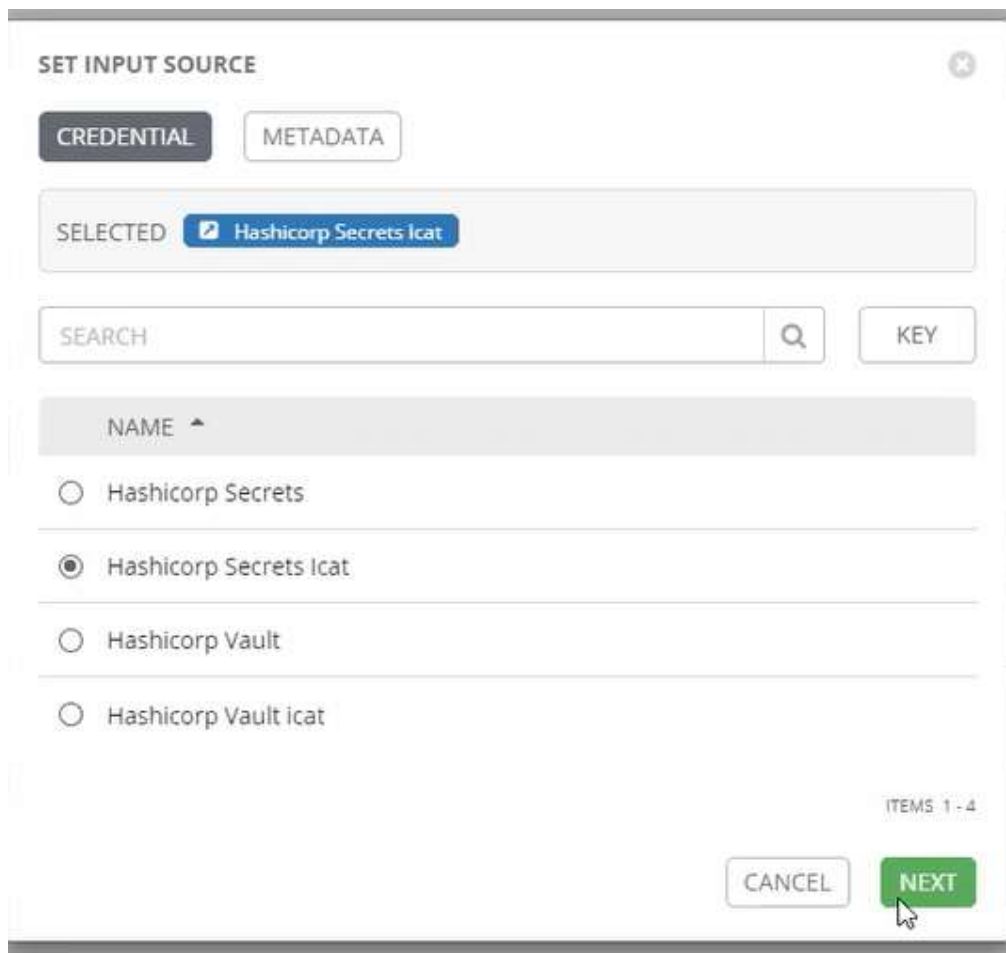
**ORGANIZATION:** Select your organisation

The screenshot shows the 'DETAILS' view of a credential named 'ansudoicat'. The 'DESCRIPTION' is 'service account for icat signed by hashicorp vault'. The 'ORGANIZATION' dropdown is set to 'Marsh', which is circled in red. The 'CREDENTIAL TYPE' is 'Machine'. The 'TYPE DETAILS' section is partially visible at the bottom.

**Select USERNAME**

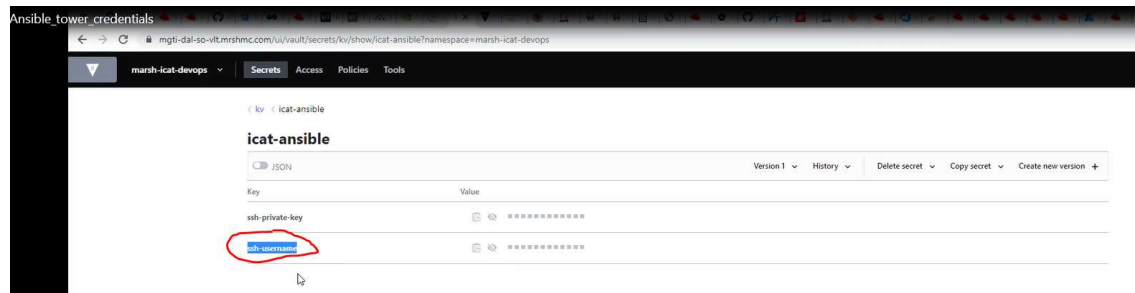


Click your Hashicorp secret and then Next



Provide details from Hashicorp namespace ( below screenshot from Hashicorp namespace )





**SET INPUT SOURCE**

**CREDENTIAL** **METADATA**

NAME OF SECRET BACKEND ?

PATH TO SECRET ?

PATH TO AUTH ?

\* KEY NAME ?

SECRET VERSION (V2 ONLY) ?

TEST CANCEL OK

vm.title

After test successful, select "OK"

## SSH PRIVATE KEY

Click on SSH PRIVATE KEY "Search"

SSH PRIVATE KEY HINT: Drag and drop private file on the field below.

Q

SET INPUT SOURCE

CREDENTIAL

METADATA

SELECTED 

Hashicorp Secrets Icat

SEARCH

Q

KEY

NAME ▲

☐ Hashicorp Secrets

☒ Hashicorp Secrets Icat

☐ Hashicorp Vault

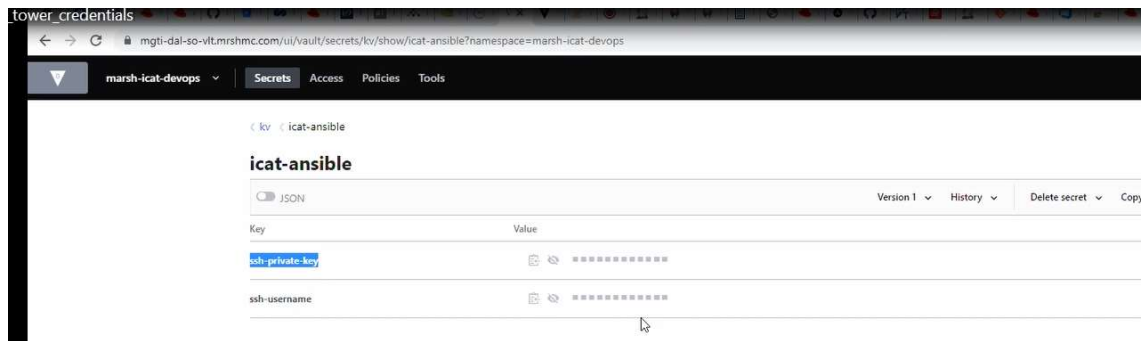
☐ Hashicorp Vault icat

ITEMS 1 - 4

CANCEL

NEXT

Ssh-private-key is stored in Hashicorp Vault as shown below.



**SET INPUT SOURCE**

NAME OF SECRET BACKEND ?

\* PATH TO SECRET ?

PATH TO AUTH ?

\* KEY NAME ?

SECRET VERSION (V2 ONLY) ?

After test successful, select "OK"

## SIGNED SSH CERTYMATE

Click "Search"

SIGNED SSH CERTIFICATE HINT: Drag and drop private file on the field below.

SET INPUT SOURCE

CREDENTIAL

METADATA

SELECTED

Hashicorp Vault icat

SEARCH

Q

KEY

NAME

Hashicorp Secrets

Hashicorp Secrets icat

Hashicorp Vault

Hashicorp Vault icat

ITEMS 1 - 4

CANCEL

NEXT

Click "NEXT"

Enter unassigned public key of the service account (key generated using sshd-keygen )

SET INPUT SOURCE

CREDENTIAL

METADATA

\* UNSIGNED PUBLIC KEY

W5eqDpTnBYZ3Am0Y6eQLxkhRvp4/m+5n90btiotAiX1HufwcUJR+31ckLb9upPS54N0  
RJSkDQ2woVZCJa/ynAm+801D3J3K1QJQV/eZSFa78d9FwihnbCauJZ7SK+7M7eoUhUw  
Ku/xujNeNLzT5NbmBu0n007GcFKvrmgNYsVrALCXA0eMHBKD71VV0thxaD2yXf6qnh4  
QTM6OpCi2HOrK7t07x7rvnKedAIRiDaCQ6ldn7eKlitgGkbroC4YbBHwxQaKzx19BcZ  
KK96GRBaGd6b4w36Fs9kV0vG0XCefU7CBZRfXAg6jb6hWY8Mmuk67T+TLemnRWzJQ7S  
W/8g7w1Y/K7IIFDFix7rAOc/M5MKnd4cWw7xep8XlswclzVzv5dIeEjgUPrysYuh9fp  
E1gk4fs= svc-icat-tw-prd@usdf21v0271

\* PATH TO SECRET ?

marsh-icat-devops/ssh

PATH TO AUTH ?

\* ROLE NAME ?

ansible

VALID PRINCIPALS ?

svc-icat-tw-prd

TEST

CANCEL

OK

After successful TEST, press "OK"

- 3) Provide Signed Hashicorp CA key (pem file) to Unix Ops, so they can add to sshd\_config on unix server for service account to login
- 4) Test ssh access manually from ansible server. It is optional step and need Unix Ops team involvement if you want to do this.
  - a. Login to usbrs21as50vcn1
  - b. \$ id -a  
uid=662853682(kumar00) gid=9999(unixadm)  
groups=9999(unixadm),64920(cloudops),6  
4976(enavusr),64977(enavadm)  
\$ /usr/share/centrifydc/bin/ssh-keygen  
Generating public/private rsa key pair.

Enter file in which to save the key (/home/kumar00/.ssh/id\_rsa):  
 Enter passphrase (empty for no passphrase):  
 Enter same passphrase again:  
 Your identification has been saved in /home/kumar00/.ssh/id\_rsa  
 Your public key has been saved in /home/kumar00/.ssh/id\_rsa.pub  
 The key fingerprint is:  
 SHA256:8d6fpsczjtLmJj/4idM4E2WgKCHWC7W8KknBL6ZlkZw  
 kumar00@usbrs21as50vcn1  
 The key's randomart image is:

+---[RSA 3072]-----+

```
| o.      |
|..++o.   |
| +Eooo ... |
| o.o.. .o o |
| +o... S.o |
| ++..    |
| +.     *. |
| .      O.*+. |
|        .%B*+o |
```

+----[SHA256]-----+

\$ cd .ssh

\$ ls -latr

total 12

-rw-r--r-- 1 kumar00 unixadm 1519 Sep 29 03:41 known\_hosts

drwx----- 3 kumar00 unixadm 162 Sep 29 03:58 ..

-rw-r--r-- 1 kumar00 unixadm 578 Jan 28 15:23 id\_rsa.pub

-rw----- 1 kumar00 unixadm 2610 Jan 28 15:23 id\_rsa

drwx----- 2 kumar00 unixadm 57 Jan 28 15:23 .

\$ cat id\_rsa.pub

ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQgQDDYMh67LE/UPKUryW+SEiKOib7bFZTLESb2  
 UvO00u8

7CFxZnodLmWcmrhOXD7z38LsmhIOVJmsOsV+5XljjznRQ9w3krdf/HKZJTHmjsr/6n33n  
 jLSMPZiMnmO

wuk1pRj03ScGY/QqRX2FT2n7S5UCCs0zr9wYq0y4DZ3ahmDX+tpv6HIwSk7qzDNhhfb  
 GphkEhCRVnpx2

LfzQj7Ykb7NyPnDGoL0txl8eb+fQ7pX7EwuZVHaolWQPvDjwJF7Ri14gMcIAy5VK0aJ92  
 fSWU3BhmsvG

E9VDUT8xXR+7gq6fj0YcvZ1AXn37p0SG0s3qZa7/IJ7Epmzhycf3lhsav236mjGxehSuQE  
 +eZLoHTCCX

6zvumcybjablCtg0o+KuPpvznv+AVoMKbRnIRKD/1a5auB/WQKKIKzZ/u1hnVhm25V0p  
 IOyanSciQKiU

z+H6O8fUNpPFbk1QohDlyTCXoyDqoSGsh1ITBkG6itPL8EreLxp9oMcGdzZVXhqWqCf+  
 UBc= kumar0  
 0@usbrs21as50vcn1

- c. Get your public key signed from hashicorp vault and then copy as rsa.pub.signed

\$ vi id\_rsa.pub.signed

```
$ ssh -i
$
$ pwd
/home/kumar00/.ssh
$ cd ..
```

- d. Remote login to target server ( ansible managed server )

```
$ ssh -i .ssh/id_rsa -i .ssh/id_rsa.pub.signed pvc-dbs-tw-prd@usbrs23db35vcn2
```

The authenticity of host 'usbrs23db35vcn2 (192.168.29.78)' can't be established.

ECDSA key fingerprint is

SHA256:wc9R/pG3gYPicWkgVNBj/Jo7pCATMDqzW9QgTGcfUJI.

-----

```
#####
# *** This Server is using Centrify          *** #
# *** Remember to use your Active Directory account    *** #
# *** password when logging in          *** #
#####
```

Last login: Fri Jan 28 16:13:26 2022

```
$
```

5. Test credential by running any playbook on ansible managed server.

Note: Ensure managed server having hashicorp CA key and sudo root access configured. Contact Unix Ops.

## MISC

### How to generate public key from private key

Copy the private key in a file (say id\_rsa) on Linux server and then execute

```
ssh-keygen -y -f ~/.ssh/id_rsa > ~/.ssh/id_rsa.pub
```

### How Ansible - Hashicorp Integration works

Private key is stored in HV. Public key is in Ansible. When ssh connection is initiated, ansible will take public key from its vault, read private key from HV, HV will provide signed public key to the ssh connection, which then will be authenticated by trusted CA key in sshd configuration.

Client Config:

sshd\_config file:

```
TrustedUserCAKeys /etc/centrifydc/ssh/trusted-user-ca-keys.pem
```

```
Match User svc-ansible,svc-user1,svc-user2
```

```
    PasswordAuthentication no
```

Public Key:

```
[root@ausyd24as05v ssh]# cat /etc/centrifydc/ssh/trusted-user-ca-keys.pem
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCvM= svc-ansible@ansibletower
```

```
[root@ausyd24as05v ssh]# ls -l /etc/centrifydc/ssh/trusted-user-ca-keys.pem
```

```
-rw-r--r-- 1 root root 1327 Feb 10 16:34 /etc/centrifydc/ssh/trusted-user-ca-keys.pem
```

```
[root@ausyd24as05v ssh]#
```

Sudo access

```
[root@ausyd24as05v ssh]# cat /etc/sudoers.d/ansible
```

```
svc-ansible    ALL=(ALL)    NOPASSWD: ALL
```

```
[root@ausyd24as05v ssh]# ls -l /etc/sudoers.d/ansible
```

```
-rw-r--r-- 1 root root 49 Aug 18 2021 /etc/sudoers.d/ansible
```



