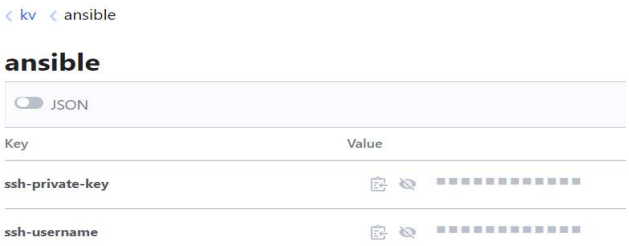
NOTE:

A) MKPI DevOps team (#mkpigldevopsengineering@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



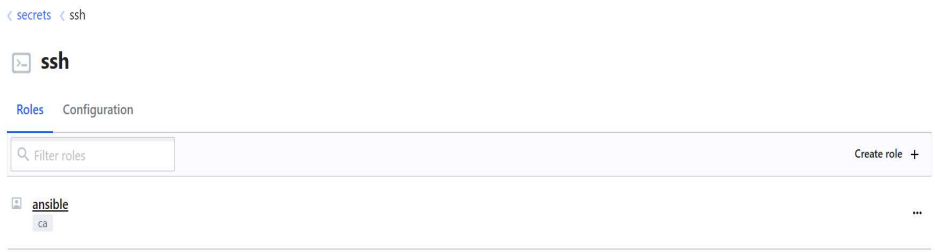
Secret: SSH

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 identifymation 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:pZAsZkSlDBPzT1iglkjvCOZl7oUX/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 certifymates: Yes

Default user: pvc-ymat-tw-prd

Allowed users: *

Default Critical Options: {}

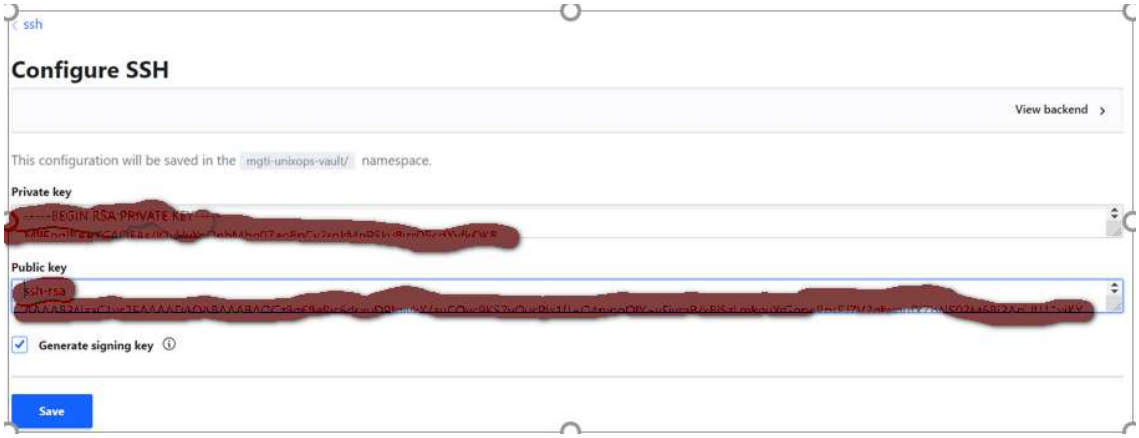
Default Extensions: {

“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_certifymates=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_certifymates=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:LkahItnvVLOs9reEGXLvSlUFK+i0dl0bw8+tIZEchlI

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:LkahItnvVLOs9reEGXLvSlUFK+i0dl0bw8+tIZEchlI
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

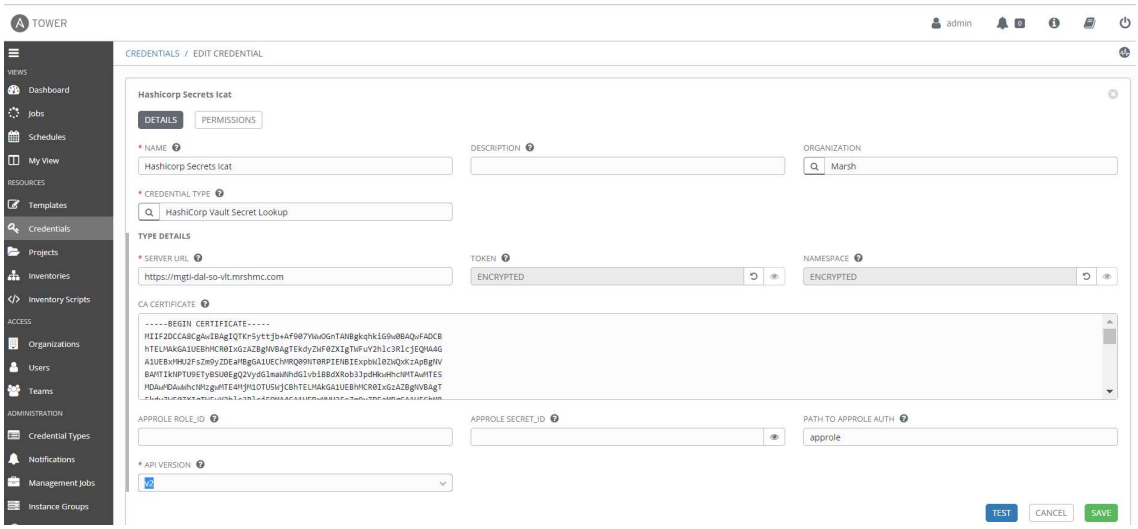
Example:

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.

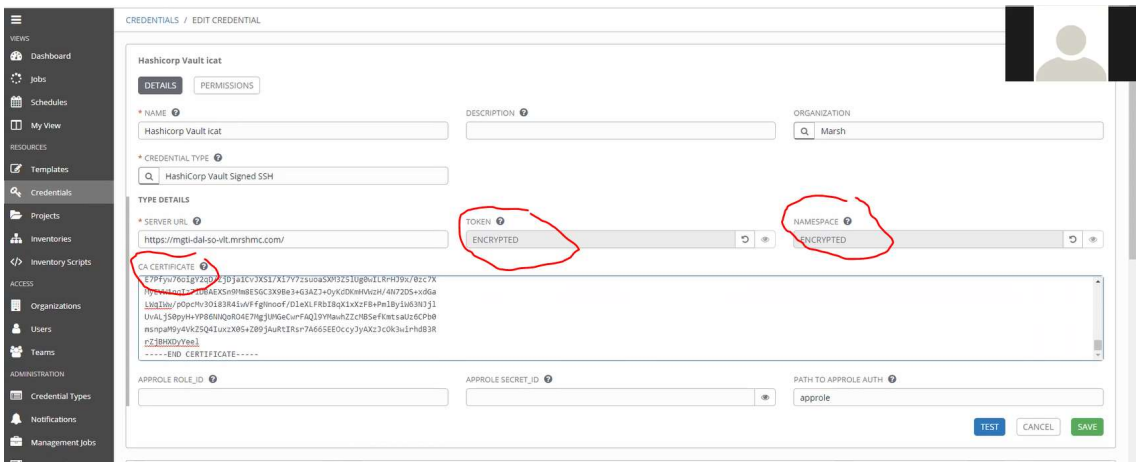
TOKEN: You can copy from Hashicorp
NAMESPACE: karsh-ymat-devops
CERTIFYMATE: Contact #mkpigldevopsengineering@mkpimail.com with incident number (an M Khan an.M.Khan@ktc.com, Hook matthook@ktc.com or chrola@ktc.com. Imran Khan (MKPI HashiCorp) to get certifymate

SAVE



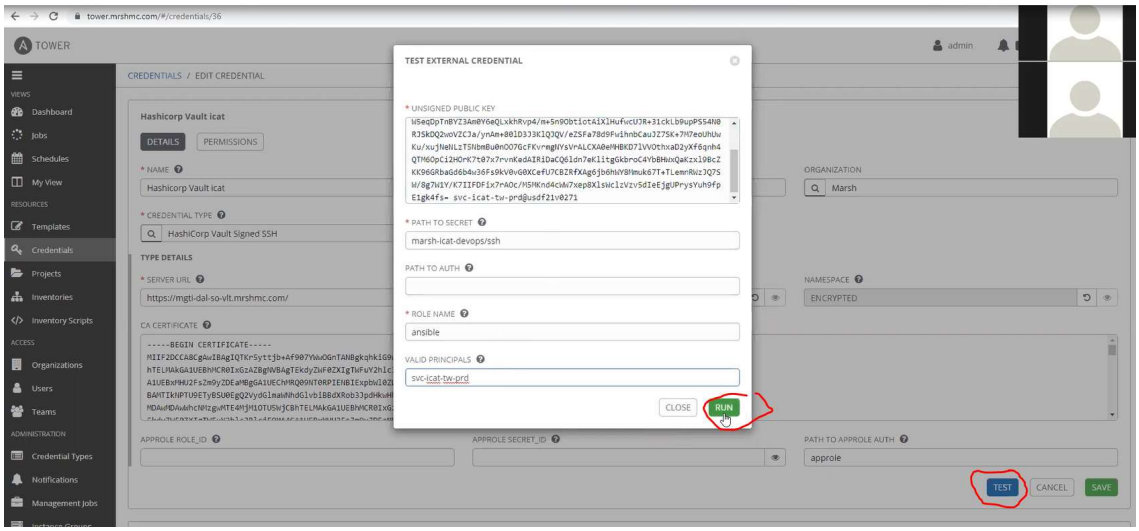
b) Hashicorp Vault Signed SSH Setup
You are using vault to sign your ssh key.

TOKEN: You can copy from Hashicorp
NAMESPACE: karsh-ymat-devops
CERTIFYMATE: Contact #mkpigldevopsengineering@mkpimail.com with incident number (Imran M Khan Imran.M.Khan@ktc.com, Matthew Hook matthew.hook@ktc.com or chris.rempola@ktc.com. Imran Khan (MKPI HashiCorp) to get certifymate
SAVE

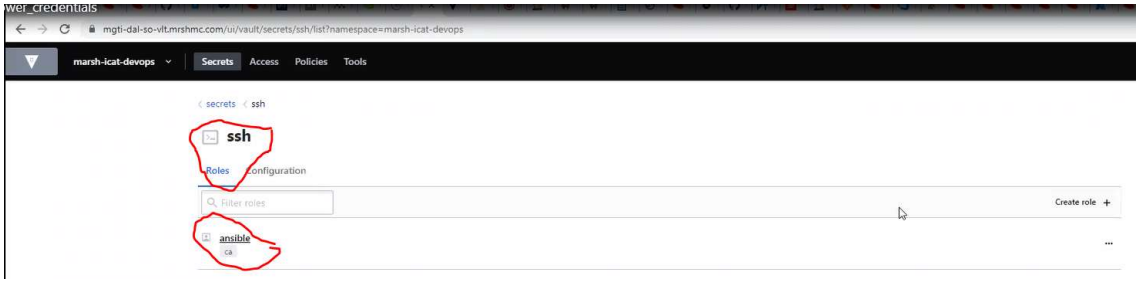


You can test external credential as per below screenshot. It should show “Test Pass” when you click “RUN”.

UNSIGNED PUBLIC KEY:
It is public key generated for service account - pvc-ymat-tw-prd using as above
ROLE NAME: ansible # This role is created under ssh secret engine.



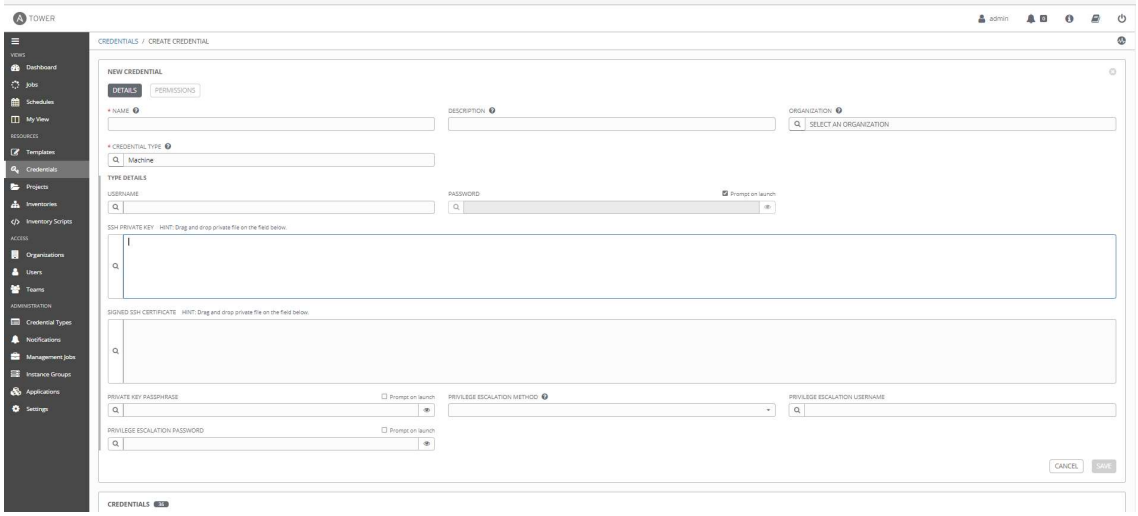
HashiCorp ssh secret showing ansible role



c) Machine credential setup

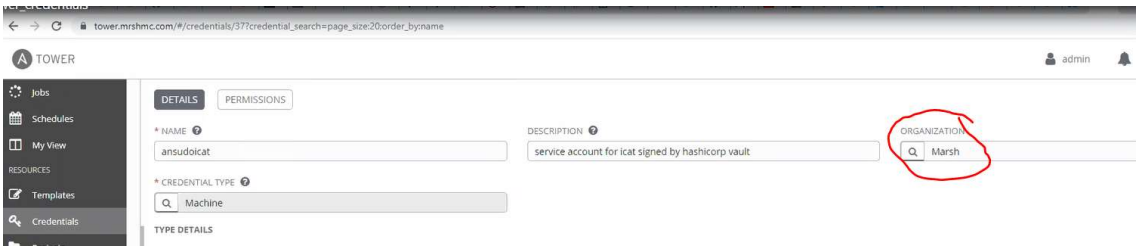
Credentials -> New Credentials

Credential Type: Machine

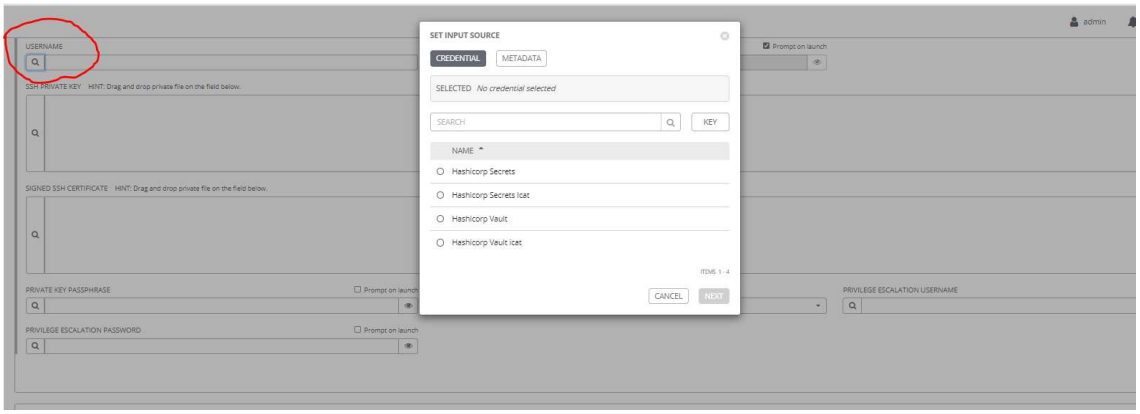


NAME: Give the credential name

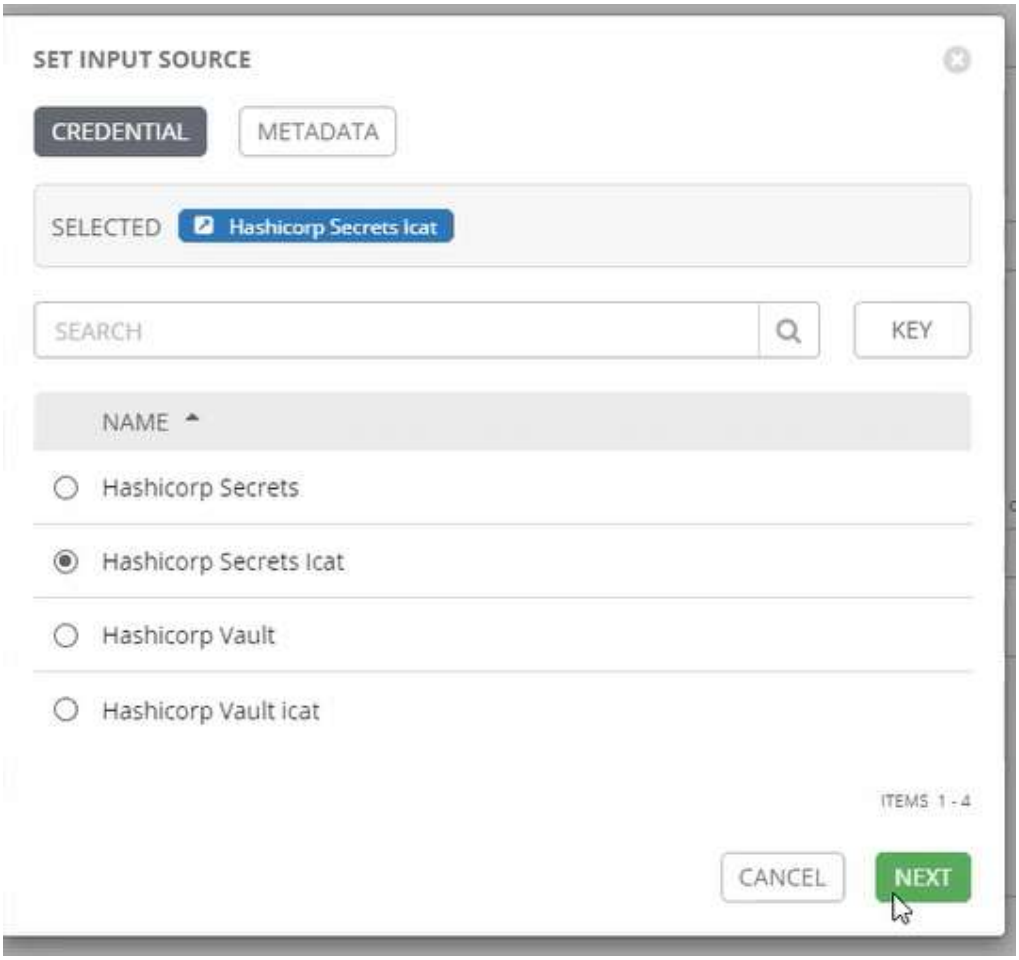
ORGANIZATION: Select your organisation



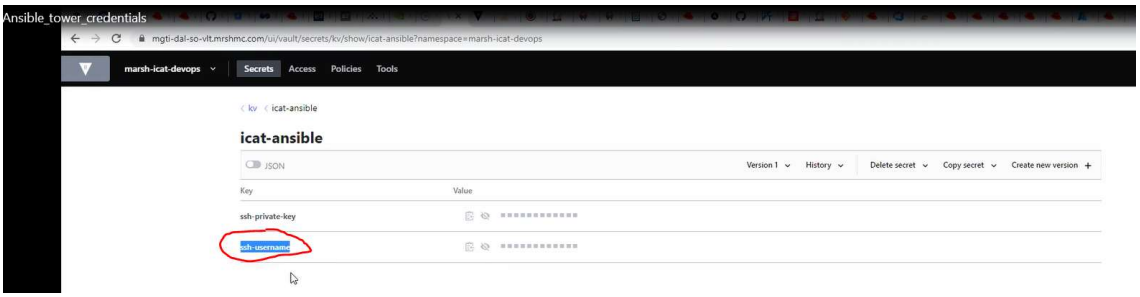
Select USERNAME



Click your Hashicorp secret and then Next



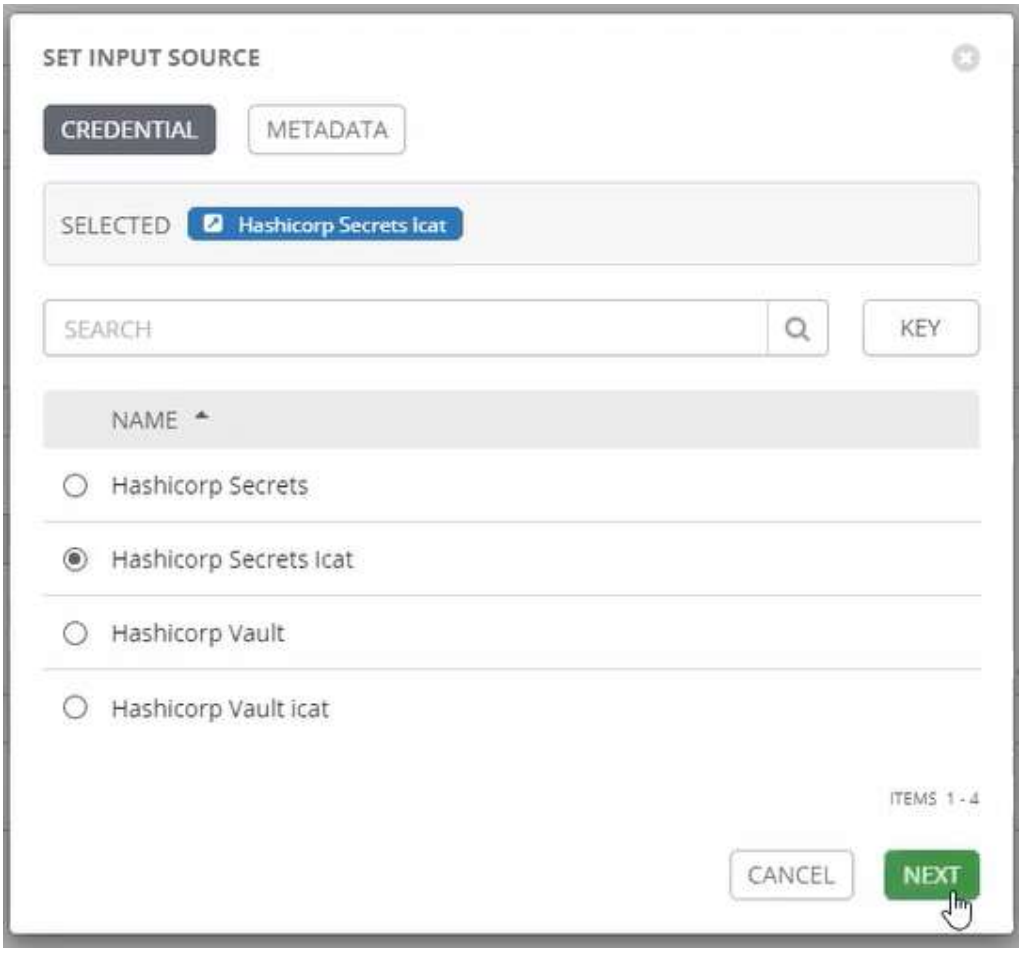
Provide details from Hashicorp namespace (below screenshot from Hashicorp namespace)



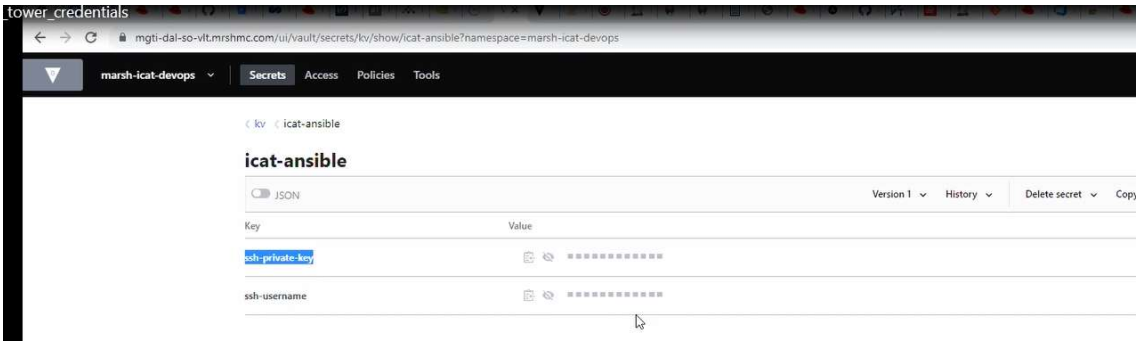
After test successful, select “OK”

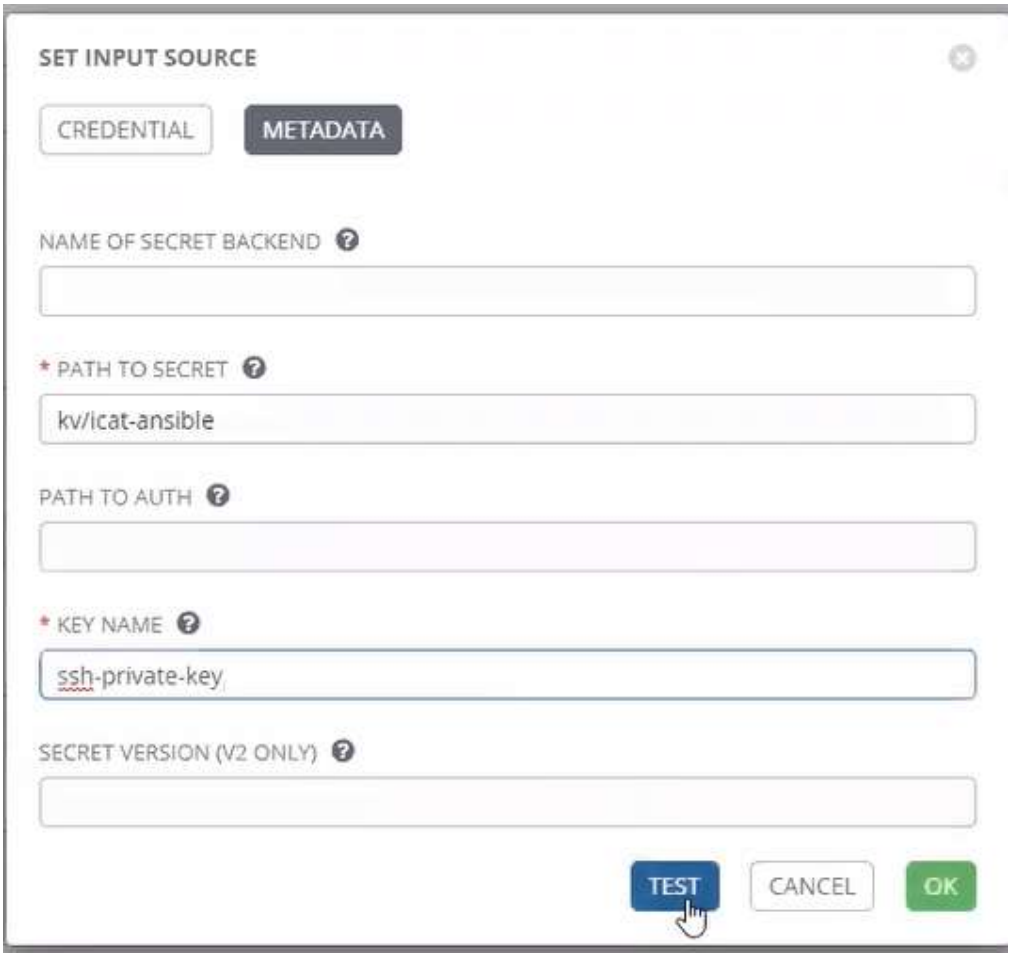
SSH PRIVATE KEY

Click on SSH PRIVATE KEY “Search”



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

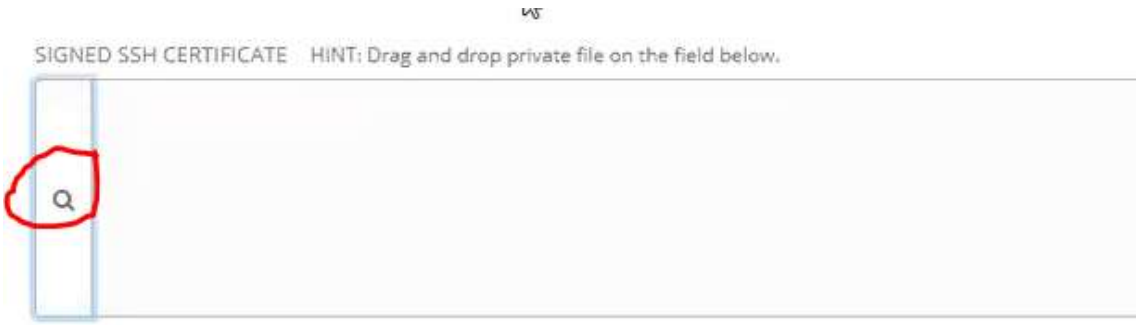


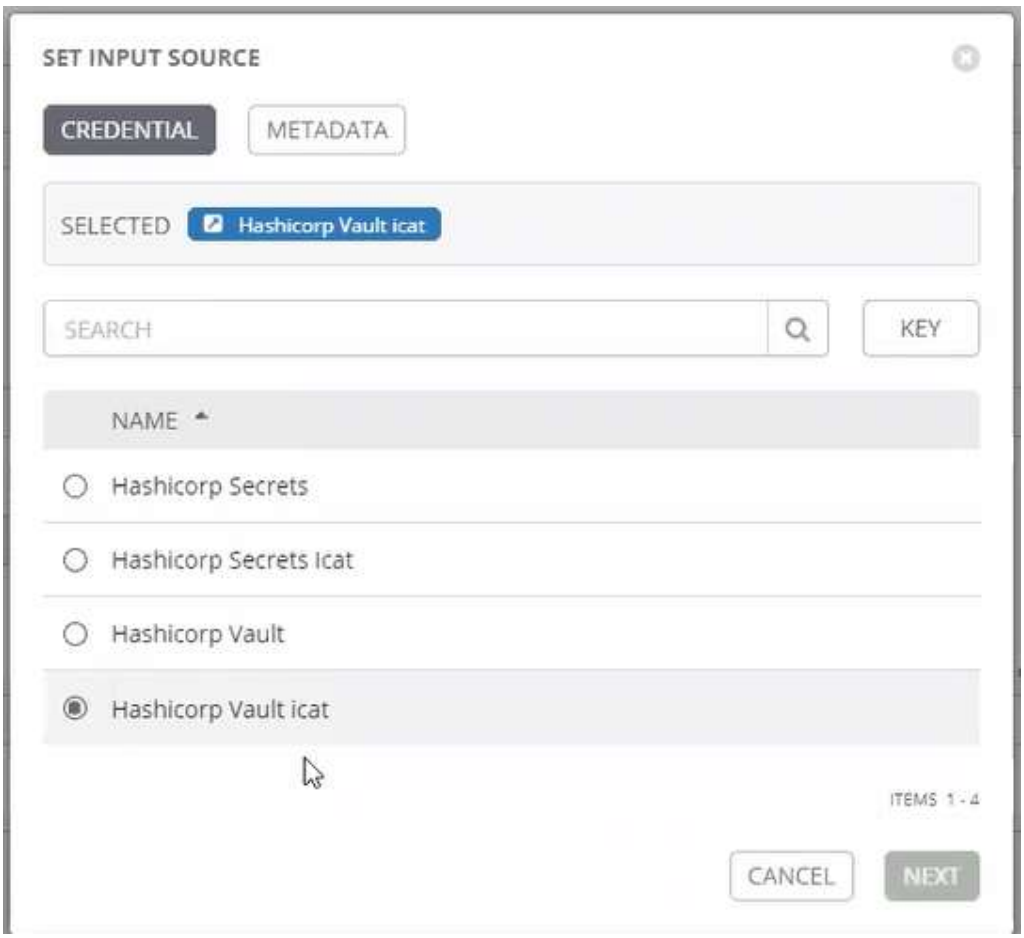


After test successful, select “OK”

SIGNED SSH CERTYMATE

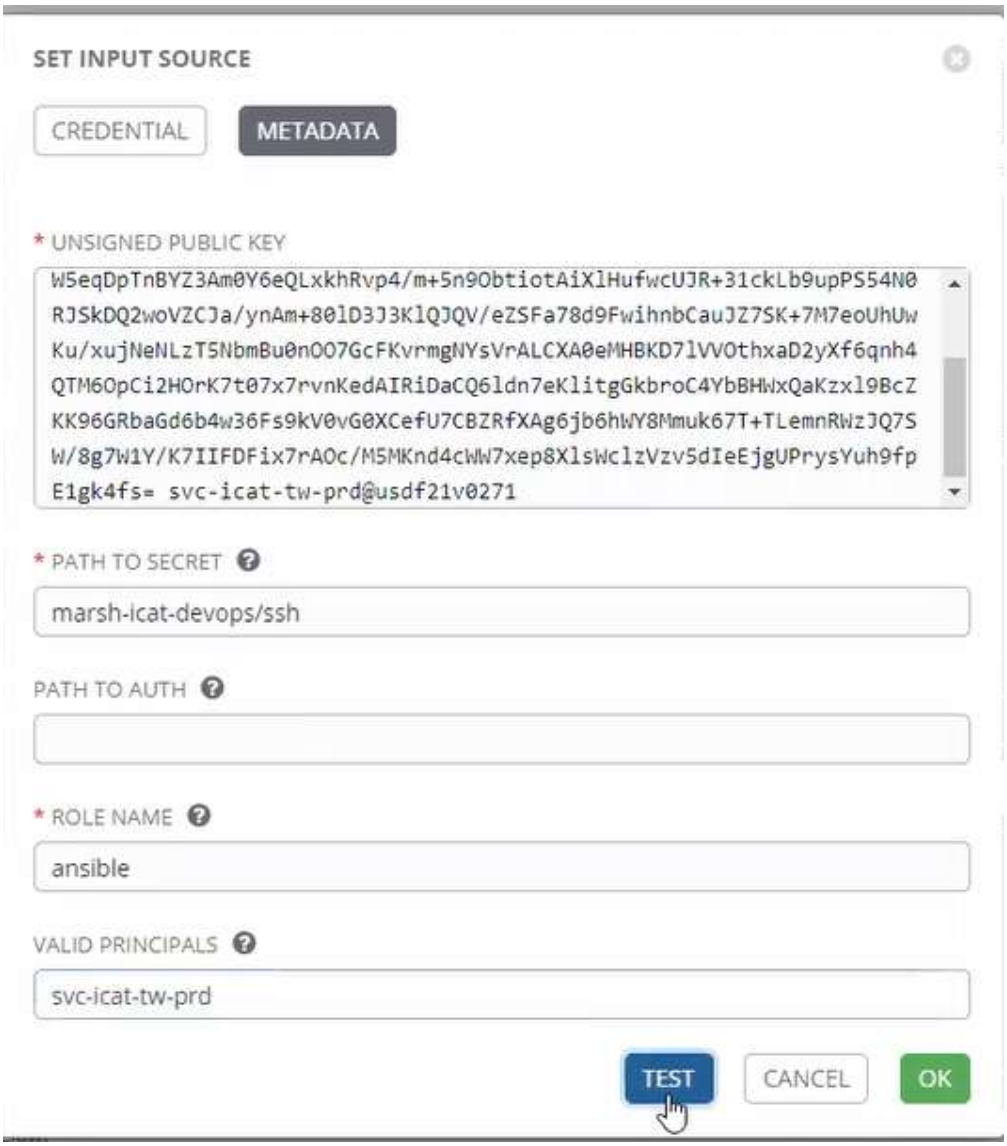
Click “Search”





Click “NEXT”

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



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 identifymation 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
AAAAB3NzaC1yc2EAAAADAQABAAABgQDDYMh67LE/UPKUryW+SEiKOib7bFZTLESb2
UvO00u8
7CFxZnodLmWcmrhOXD7z38LsmhlOVJmsOsV+5XIjiznrQ9w3krdf/HKZJTHmjsr/6n33n
jLSMPZiMnmO
wuk1pRj03ScGY/QqRX2FT2n7S5UCCs0zr9wYq0y4DZ3ahmDX+tvp6HIwSk7qzDNhhfb
GphkEhCRVnpx2
LfzQj7Ykb7NyPnDGoL0txl8eb+fQ7pX7EwuZVHaolWQPvDjwJF7Ri14gMcJAy5VK0aJ92
fSWU3BhmsvG
E9VDUT8xXR+7gq6fj0YcvZ1AXn37p0SG0s3qZa7/IJ7EpmzhycF3lhsav236mjGxehSuQE
+eZLoHTCCX
6zvumcybjablCtg0o+KuPpvznv+AVoMKbRnlRKD/1a5auB/WQKKIKzZ/u1hnVhm25V0p
IOyanSciQKiU
z+H6O8fUNpPFbk1QohDIyTCXoyDqoSGsh1ITBkG6itPL8EreLxp9oMcGdzZVXhqWqCf+
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 authentymated 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 AAAAB3NzaC1yc2EAAAADAQABAAABgQCvM= 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