How Do I Setup Jump Server / Bastion Host To Use With Ansible Engine / Ansible Tower ?

Issue

Issue

Setting up Jump Server / Bastion Host to use with Ansible Engine / Tower.

Resolution

Red Hat Ansible Engine:

- Check whether the Jump Server / Bastion Host is reachable from Ansible control machine.
- Create a SSH `config` file on the Ansible control machine and place it in `/home/user/.ssh/` with the below details:

```
Host jumpserver
    Hostname 10.11.X.X
    User username
    IdentityFile ~/.ssh/jumpserver.pem
    StrictHostKeyChecking no

Host 10.*
    Proxycommand ssh -W %h:%p username@jumpserver
```

- The `Host 10.*` line indicates that all hosts in that subnet will use the settings defined in that block, specifically all hosts will be accessed using the `ProxyCommand` setting and connect through `jumpserver`.
- You can also specify the private key file path using `IdentityFile` keyword to connect those hosts as shown in the above example.
- Make sure to change the permission and ownership of the SSH config and private key file as below. Here user is the filesystem user that you are using.

```
-rw-------. 1 user user  186 Jul 16 10:06 config
-rw-------. 1 user user  1679 Jul 16 09:47 jumpserver.key
```

- The `Host jumpserver` combines settings for acting as an SSH jump Server / Bastion Host with settings for using SSH multiplexing (the StrictHostKeyChecking, ControlMaster and ControlPersist settings).
- Finally, execute a ansible ad-hoc command and to verify whether the SSH traffic is tunneled through jump server to target node, SSH into the jump server and also to target node and run `journalctl -f` to monitor sshd trace or run tail -f /var/log/secure

- The above config method is applied for all the hosts from the inventory which are managed by Ansible but if you want to route SSH traffic for a single / specific set of hosts to use Jump Host / Bastion Server you can add the below variable to inventory `host_vars` or `group_vars`.

Raw

```
ansible_ssh_common_args='-o ProxyCommand="ssh -i ~/.ssh/jumpserver.pem
-o StrictHostKeyChecking=no -W %h:%p -q username@jumpserver"'
```

Red Hat Ansible Tower:

- Normally Ansible Tower jobs are launched by `awx` user, so to configure Jump Sever with Ansible Tower place a SSH private keyfile in the awx user's /var/lib/awx/.ssh directory and add it to the SSH config like below:

```
# vim /var/lib/awx/.ssh/config

Host jumpserver
    Hostname 10.11.X.X
    User username
    IdentityFile ~/.ssh/jumpserver.pem
    StrictHostKeyChecking no

Host 10.*
    Proxycommand ssh -W %h:%p username@jumpserver
```

- Make sure to change the permission and ownership of the SSH config and private key file to `awx` user.

```
# chown awx:awx /var/lib/awx/.ssh/config
# chown awx:awx  /var/lib/awx/.ssh/jumpserver.pem
```

- Credentials supplied by Tower will not flow to the Jump Host / Bastion Server via ProxyCommand. They are only used for the end-node once the tunneled connection is set up.
- You can also add a Jump Host to your Tower instance through Inventory variables. These variables can be set at either the inventory, group, or host level. To add this, navigate to your inventory and in the variables field of whichever level you choose, add the following variable:

```
ansible_ssh_common_args: '-o ProxyCommand="ssh -i ~/.ssh/jumpserver.pem
-o StrictHostKeyChecking=no -W %h:%p -q username@jumpserver"'
```

https://access.redhat.com/solutions/3824661