Secure DevOps

Setting up a secure environment for Ansible

PRESENTED BY:

Joel Kirch

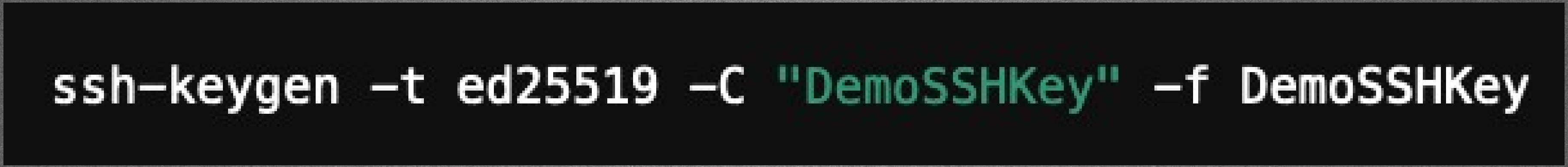
Today's Topics

- Many demos and tutorials skip over how to set up a secure environment for Ansible
  - SSH & GPG Keys, SSH-Agent, GPG-Agent
  - `pass` – The Unix Password Manager
  - Ansible Vault
- SSH Setup Demo
- Ansible Setup Demo
- Ansible Demo

SSH Setup Demo

Generate SSH Keys

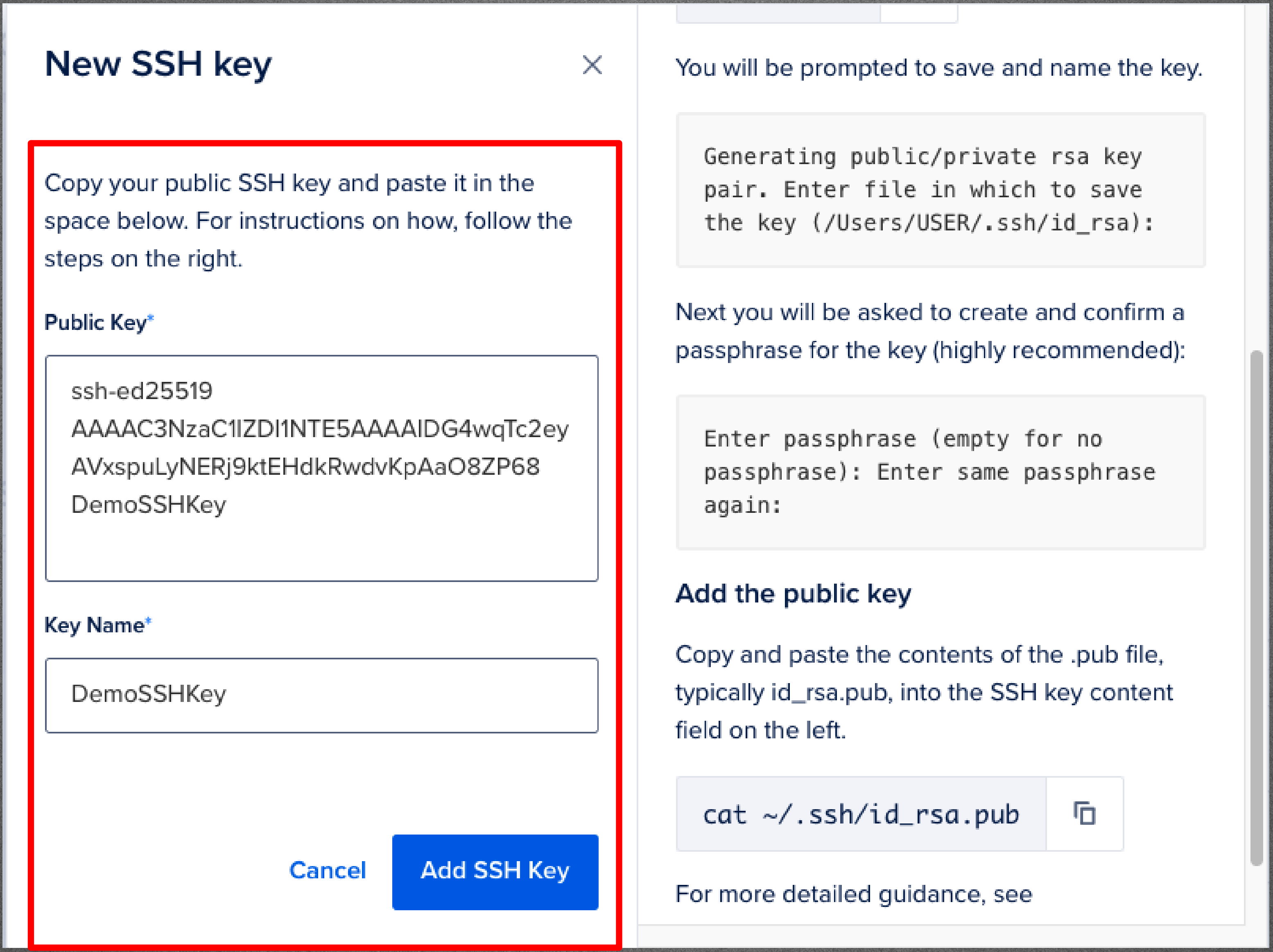
- Generate an ED25519 SSH key with the comment "DemoSSHKey" and save it using that same filename – USE A PASSWORD to protect your SSH Key.



```
ssh-keygen -t ed25519 -C "DemoSSHKey" -f DemoSSHKey
```

- This command breaks down as follows:
  - `-t ed25519`: Specifies the type of key to generate (ED25519).
  - `-C "DemoSSHKey"`: Adds the comment "DemoSSHKey" to the key
  - `-f DemoSSHKey`: Saves the private key to a file named `DemoSSHKey` and the public key to a file named `DemoSSHKey.pub`.
- After running this command, you’ll have two files:
- - DemoSSHKey (the private key)
- - DemoSSHKey.pub (the corresponding public key)

Upload SSH Public Key



New SSH key

Copy your public SSH key and paste it in the space below. For instructions on how, follow the steps on the right.

Public Key*

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDG4wqTc2ey
AVxspuLyNERj9ktEHdkRwdvKpAaO8ZP68
DemoSSHKey
```

Key Name*

DemoSSHKey

You will be prompted to save and name the key.

```
Generating public/private rsa key
pair. Enter file in which to save
the key (/Users/USER/.ssh/id_rsa):
```

Next you will be asked to create and confirm a passphrase for the key (highly recommended):

```
Enter passphrase (empty for no
passphrase): Enter same passphrase
again:
```

Add the public key

Copy and paste the contents of the .pub file, typically id_rsa.pub, into the SSH key content field on the left.

```
cat ~/.ssh/id_rsa.pub
```

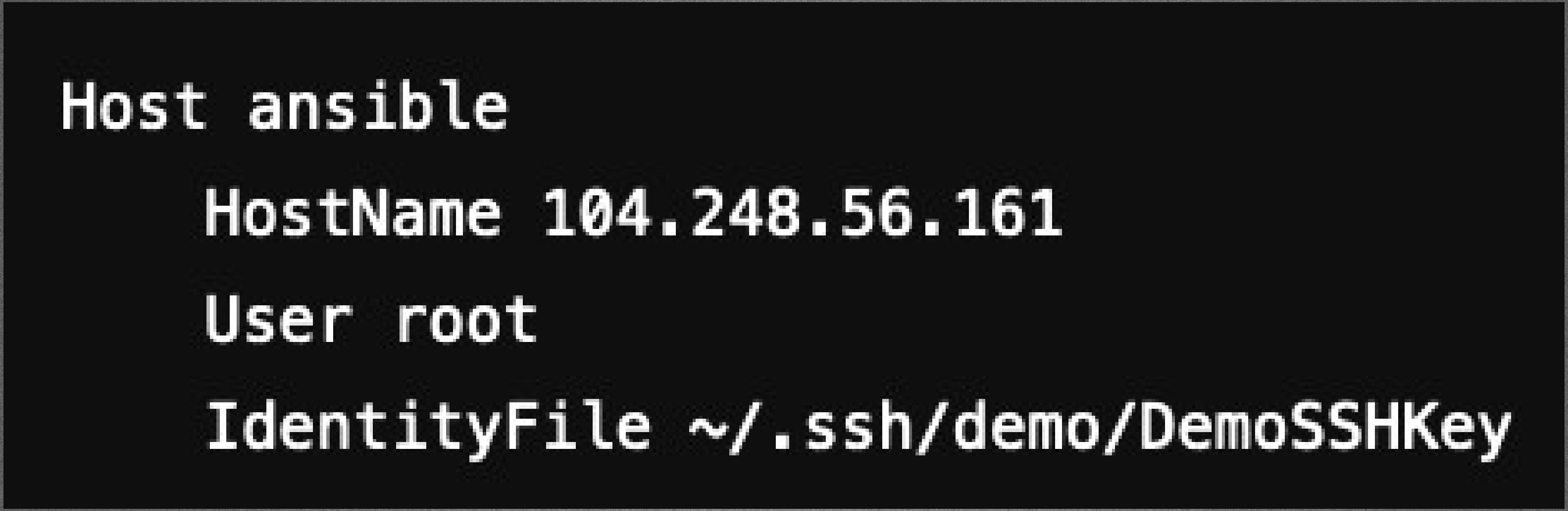
For more detailed guidance, see

RSA 4096 vs ED25519

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQDQ4kiiiQH2Avx4rzOsNffLvnEZAMuEF7C
A0cpg3L6BO1aFu6jEFvr/NonnL1tPN/
OwDoTeEMG4k7BN3dAXFFkgFAGAT+2RNvTnFb+nhyReeEkwZg+Iw9+stfxITrtvK
goNQ76n884P79FciMbn9QP6BmCXsTUQhMFMvWHP03rwYXFt9f/
pUgW6QCmpIw5i3fKgQf0WGFVsjPWXMCXrNiIDDk/
71VUqXg8FKFUvQUG1DGDcspPdel0gsJSXy14Wov4l4sSlViYqe6WQXKA6aIvsQG
k+DfZErKPWMg+20LCAYYQeD1+r4QiLbMHbHNK26WBmkjzv0pgkbEdBdrscRaTi8
AFCWelyqsoxxz4GEK0CG7NoBidl0KTf95OqDpmAnZcwRDTLWbYlLBxgL8+Pmjgk
u9Pnzhf2qipQs94A+teEgZiPlpIXSitqcBmJ0aamCTMrYE9BkylM7hvGkfx7QZY
WktQkgdPKKl8acKDM77nc1SWc1vQ2pHhq53xk08cNWrOMZaxqZaDMGncxp83GnO
EjkZhr6Xw9T5/
X27Ju5Egt5S7pXFydwCwCsb3yVQ0S0dstalf3cknJcAfZZ+SNekkXRTYO2H/
U+g5ELLmOo2LnQNP5DQG9IwW4JPF2sAOicO96ry8Wyy3ghLFXD+mdoleLaXgOWj
f9lyWmanETq/Eylw== Demo_SSH_RSA_Key
```

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDG4wqTc2eyAVxspuLyNERj9ktEHdkRwdvKpAaO
8ZP68 Demo_SSH_ED25519_Key
```

Configure SSH Client



```
Host ansible
    HostName 104.248.56.161
    User root
    IdentityFile ~/.ssh/demo/DemoSSHKey
```

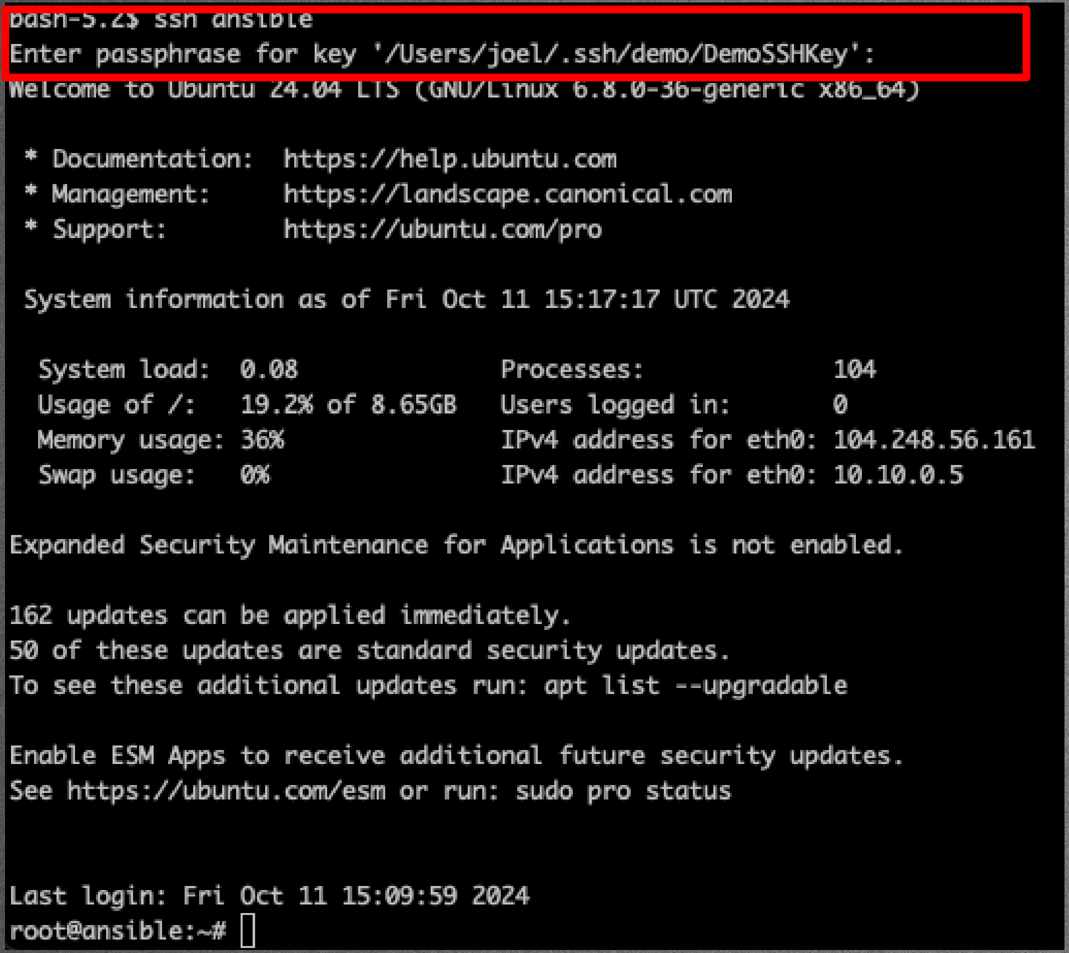
`Host ansible`: Creates an alias "ansible" for easy connection.

`HostName 104.248.56.161`: Sets the server’s IP address.

`User root`: Uses "root" as the default username.

`IdentityFile ~/.ssh/demo/DemoSSHKey`: Specifies the SSH key for secure login.

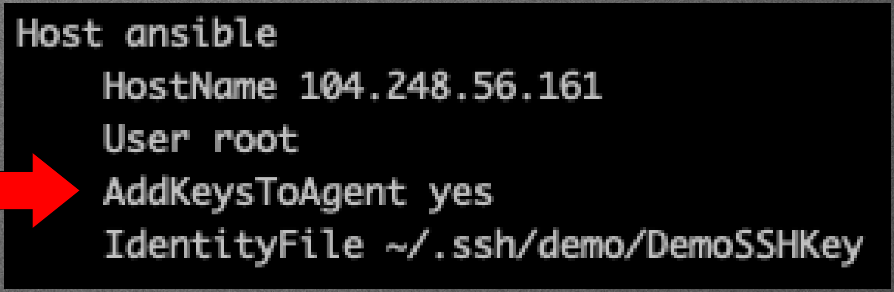
SSH to ansible, part 1



```
bash-5.2$ ssh ansible
Enter passphrase for key '/Users/joel/.ssh/demo/DemoSSHKey':
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Oct 11 15:17:17 UTC 2024

  System load:  0.08              Processes:             104
  Usage of /:   19.2% of 8.65GB   Users logged in:       0
  Memory usage: 36%               IPv4 address for eth0: 104.248.56.161
  Swap usage:   0%                IPv4 address for eth0: 10.10.0.5

Expanded Security Maintenance for Applications is not enabled.

162 updates can be applied immediately.
50 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Fri Oct 11 15:09:59 2024
root@ansible:~# 
```

- Notice that I have to enter a password to use my SSH key.
- Let’s fix that by using SSH agent
  - Add this line to your config file:

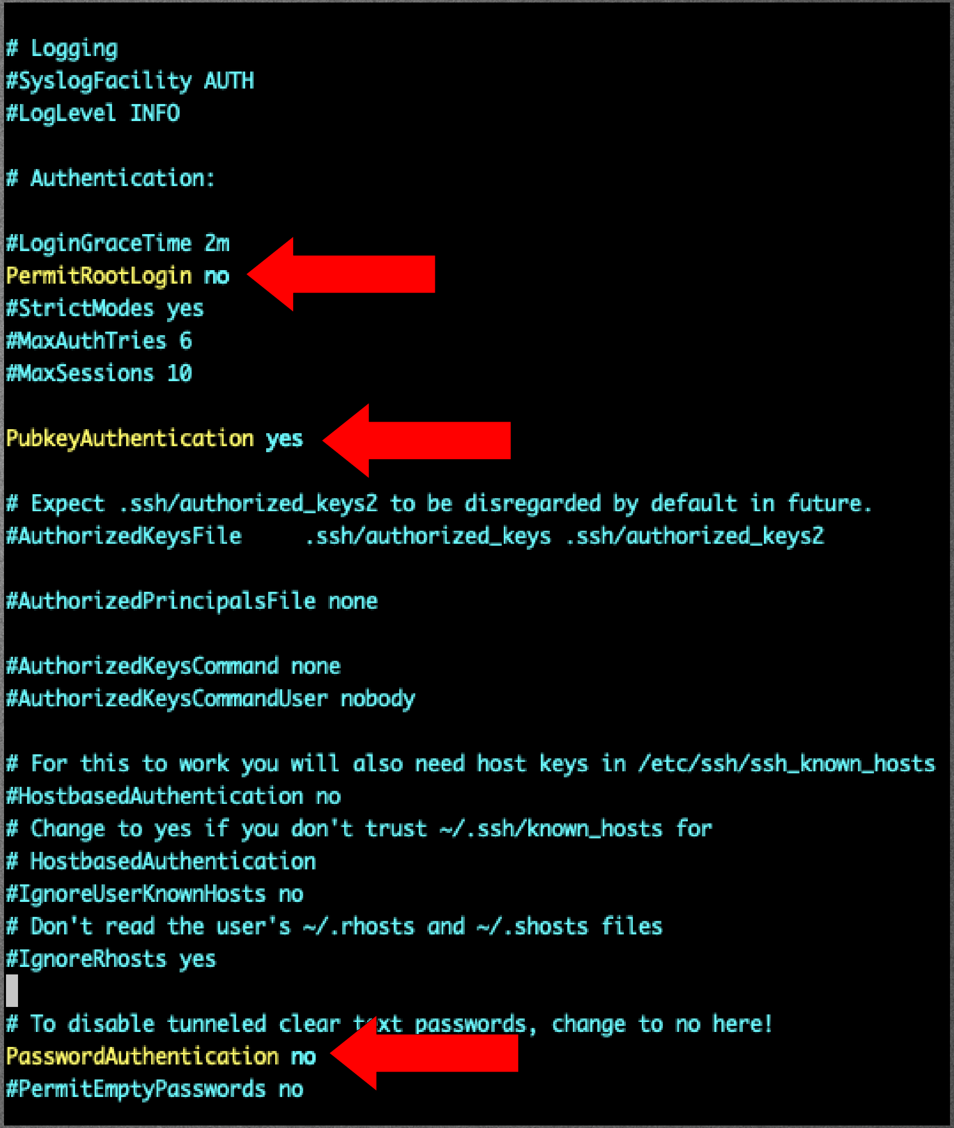
    `AddKeysToAgent yes`



```
Host ansible
    HostName 104.248.56.161
    User root
    AddKeysToAgent yes
    IdentityFile ~/.ssh/demo/DemoSSHKey
```

CyberSecurity Time

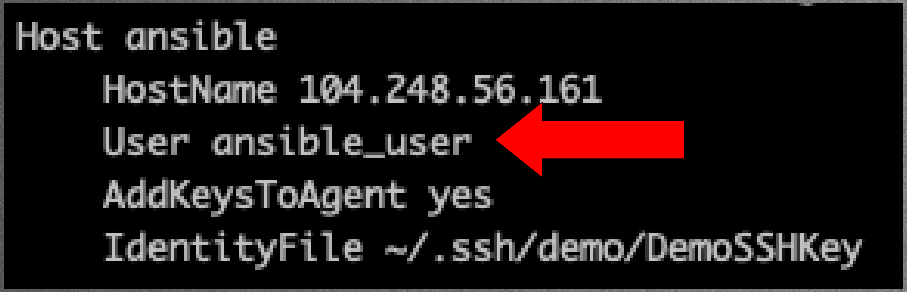
- Update the `sshd_config` on the ansible server
  - Disable root login: `PermitRootLogin no` ensures that root cannot access the server via SSH.
  - Enforce public key authentication: `PubkeyAuthentication yes` and `PasswordAuthentication no` require that all users authenticate with an SSH key.
  - Do not forget to restart SSHD: `systemctl restart ssh.service`



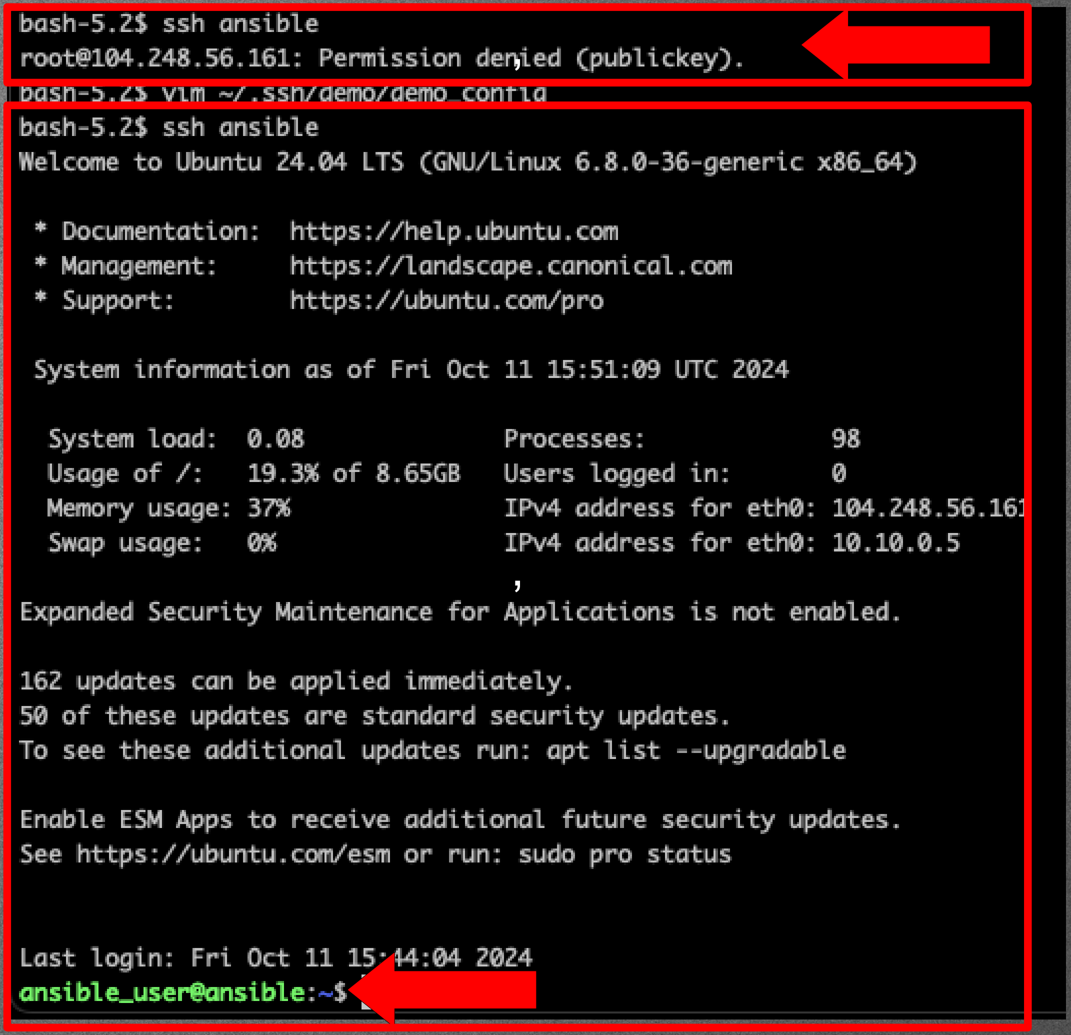
```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Update ssh config

- Update my ssh client config to use `ansible_user` instead of `root`



```
Host ansible
    HostName 104.248.56.161
    User ansible_user
    AddKeysToAgent yes
    IdentityFile ~/.ssh/demo/DemoSSHKey
```



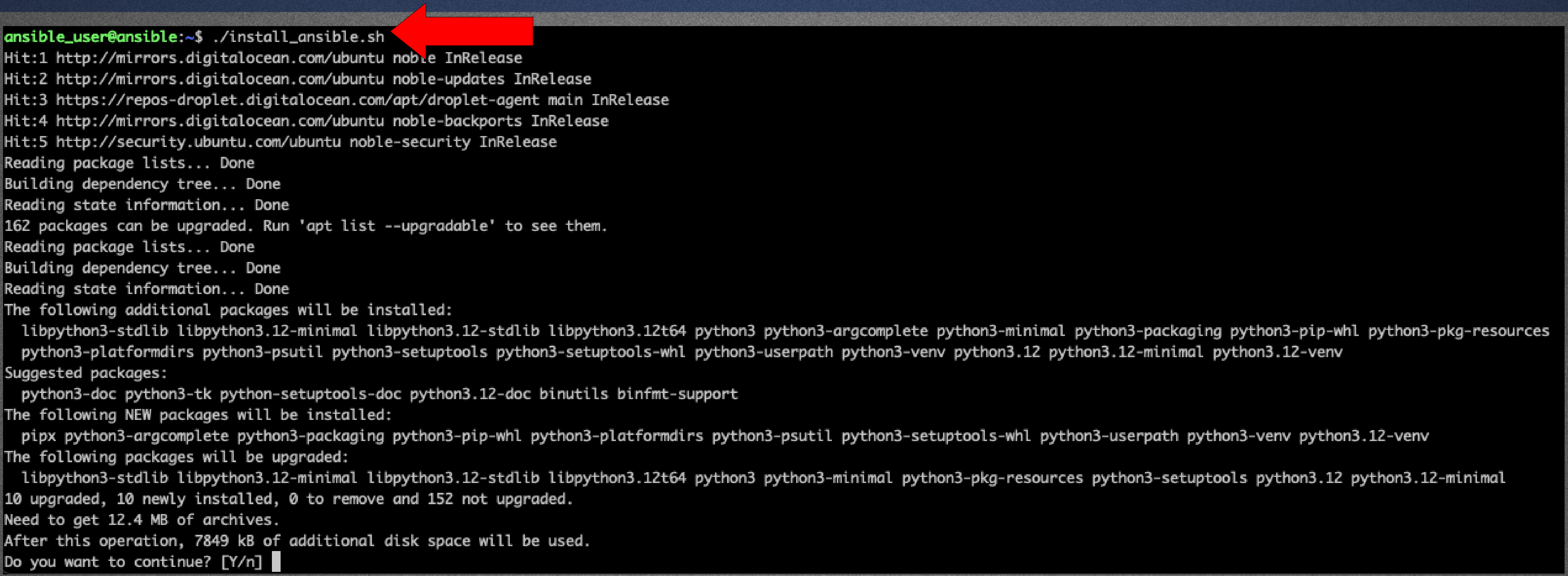
```
bash-5.2$ ssh ansible
root@104.248.56.161: Permission denied (publickey).
bash-5.2$ vim ~/.ssh/demo/demo_config
bash-5.2$ ssh ansible
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Oct 11 15:51:09 UTC 2024

  System load:  0.08              Processes:             98
  Usage of /:   19.3% of 8.65GB   Users logged in:       0
  Memory usage: 37%               IPv4 address for eth0: 104.248.56.161
  Swap usage:   0%                IPv4 address for eth0: 10.10.0.5

Expanded Security Maintenance for Applications is not enabled.

162 updates can be applied immediately.
50 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Fri Oct 11 15:44:04 2024
ansible_user@ansible:~$
```

SSH Setup Summary

- Created SSH keys, uploaded the public key to cloud provider
- Configured our client with to use SSH Agent with SSH keys
- Connected to our ansible server, using SSH keys
- Hardened SSHd on the ansible server
- Verified that our settings worked
- QUESTION: Are we doing DevOps?

Ansible Setup Demo

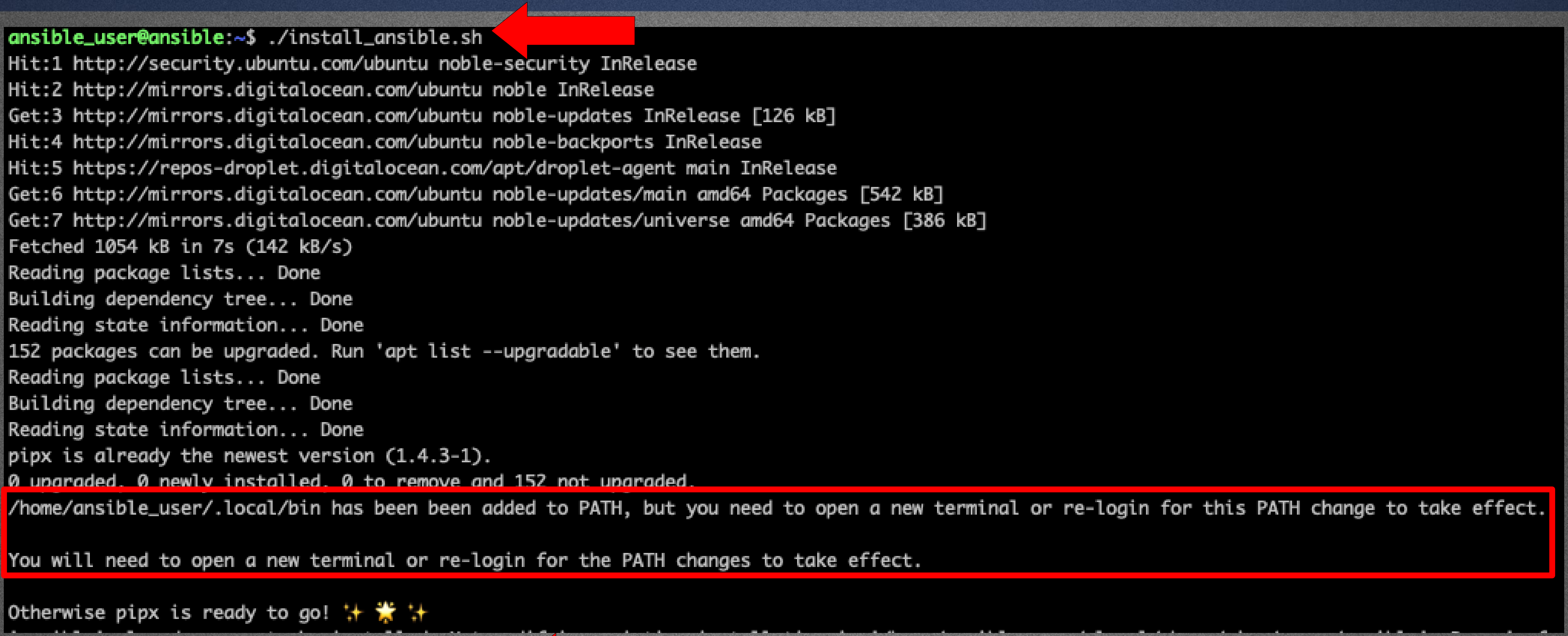
Install Ansible



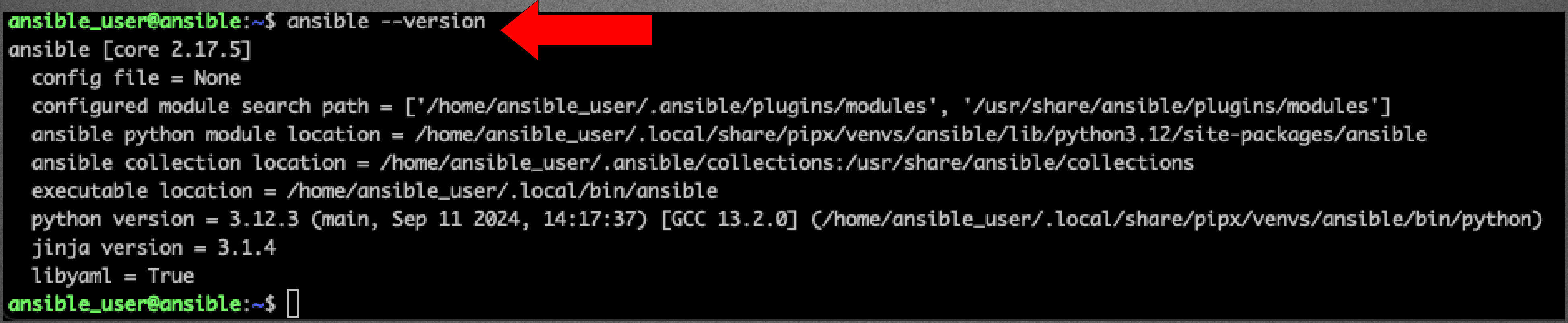
```
ansible_user@ansible:~$ ./install_ansible.sh
Hit:1 http://mirrors.digitalocean.com/ubuntu noble InRelease
Hit:2 http://mirrors.digitalocean.com/ubuntu noble-updates InRelease
Hit:3 https://repos-droplet.digitalocean.com/apt/droplet-agent main InRelease
Hit:4 http://mirrors.digitalocean.com/ubuntu noble-backports InRelease
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
162 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython3-stdlib libpython3.12-minimal libpython3.12-stdlib libpython3.12t64 python3 python3-argcomplete python3-minimal python3-packaging python3-pip-whl python3-pkg-resources
  python3-platformdirs python3-psutil python3-setuptools python3-setuptools-whl python3-userpath python3-venv python3.12 python3.12-minimal python3.12-venv
Suggested packages:
  python3-doc python3-tk python-setuptools-doc python3.12-doc binutils binfmt-support
The following NEW packages will be installed:
  pipx python3-argcomplete python3-packaging python3-pip-whl python3-platformdirs python3-psutil python3-setuptools-whl python3-userpath python3-venv python3.12-venv
The following packages will be upgraded:
  libpython3-stdlib libpython3.12-minimal libpython3.12-stdlib libpython3.12t64 python3 python3-minimal python3-pkg-resources python3-setuptools python3.12 python3.12-minimal
10 upgraded, 10 newly installed, 0 to remove and 152 not upgraded.
Need to get 12.4 MB of archives.
After this operation, 7849 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

- Use `git` to download the install script
- `chmod +x install_ansible.sh`
- `./install_ansible.sh`

Logout & Login

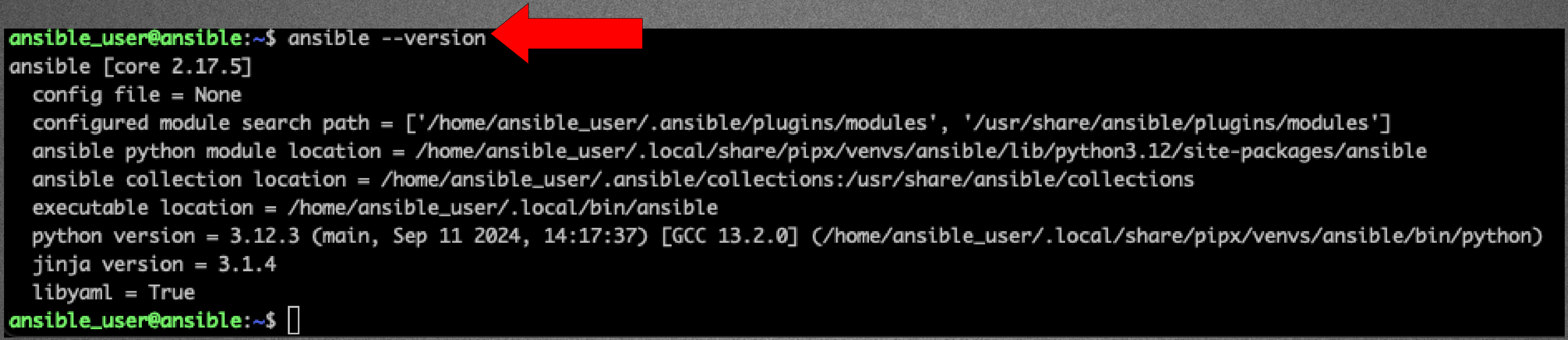


```
ansible_user@ansible:~$ ./install_ansible.sh
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://mirrors.digitalocean.com/ubuntu noble InRelease
Get:3 http://mirrors.digitalocean.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://mirrors.digitalocean.com/ubuntu noble-backports InRelease
Hit:5 https://repos-droplet.digitalocean.com/apt/droplet-agent main InRelease
Get:6 http://mirrors.digitalocean.com/ubuntu noble-updates/main amd64 Packages [542 kB]
Get:7 http://mirrors.digitalocean.com/ubuntu noble-updates/universe amd64 Packages [386 kB]
Fetched 1054 kB in 7s (142 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
152 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
pipx is already the newest version (1.4.3-1).
0 upgraded, 0 newly installed, 0 to remove and 152 not upgraded.
/home/ansible_user/.local/bin has been been added to PATH, but you need to open a new terminal or re-login for this PATH change to take effect.

You will need to open a new terminal or re-login for the PATH changes to take effect.

Otherwise pipx is ready to go! ✨ 🌟 ✨
```



```
ansible_user@ansible:~$ ansible --version
ansible [core 2.17.5]
  config file = None
  configured module search path = ['/home/ansible_user/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /home/ansible_user/.local/share/pipx/venvs/ansible/lib/python3.12/site-packages/ansible
  ansible collection location = /home/ansible_user/.ansible/collections:/usr/share/ansible/collections
  executable location = /home/ansible_user/.local/bin/ansible
  python version = 3.12.3 (main, Sep 11 2024, 14:17:37) [GCC 13.2.0] (/home/ansible_user/.local/share/pipx/venvs/ansible/bin/python)
  jinja version = 3.1.4
  libyaml = True
ansible_user@ansible:~$
```

Ansible Installed

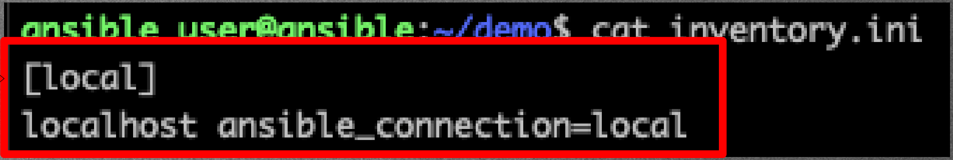


```
ansible_user@ansible:~$ ansible --version
ansible [core 2.17.5]
  config file = None
  configured module search path = ['/home/ansible_user/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /home/ansible_user/.local/share/pipx/venvs/ansible/lib/python3.12/site-packages/ansible
  ansible collection location = /home/ansible_user/.ansible/collections:/usr/share/ansible/collections
  executable location = /home/ansible_user/.local/bin/ansible
  python version = 3.12.3 (main, Sep 11 2024, 14:17:37) [GCC 13.2.0] (/home/ansible_user/.local/share/pipx/venvs/ansible/bin/python)
  jinja version = 3.1.4
  libyaml = True
ansible_user@ansible:~$
```

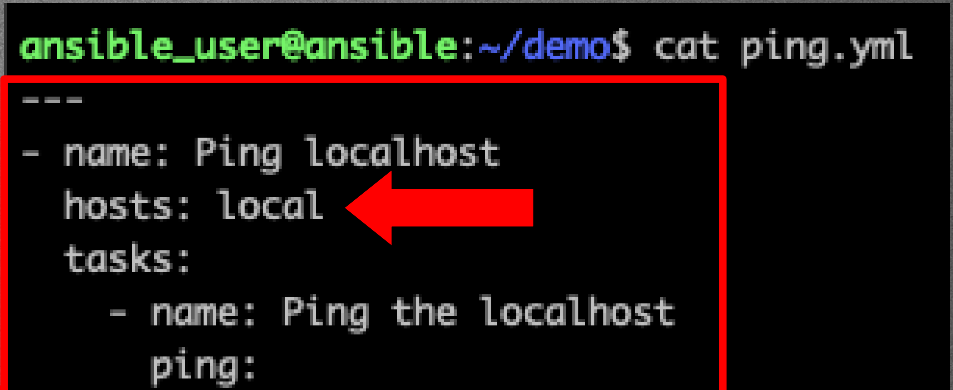
Ansible Demo

Our First Ansible Playbook

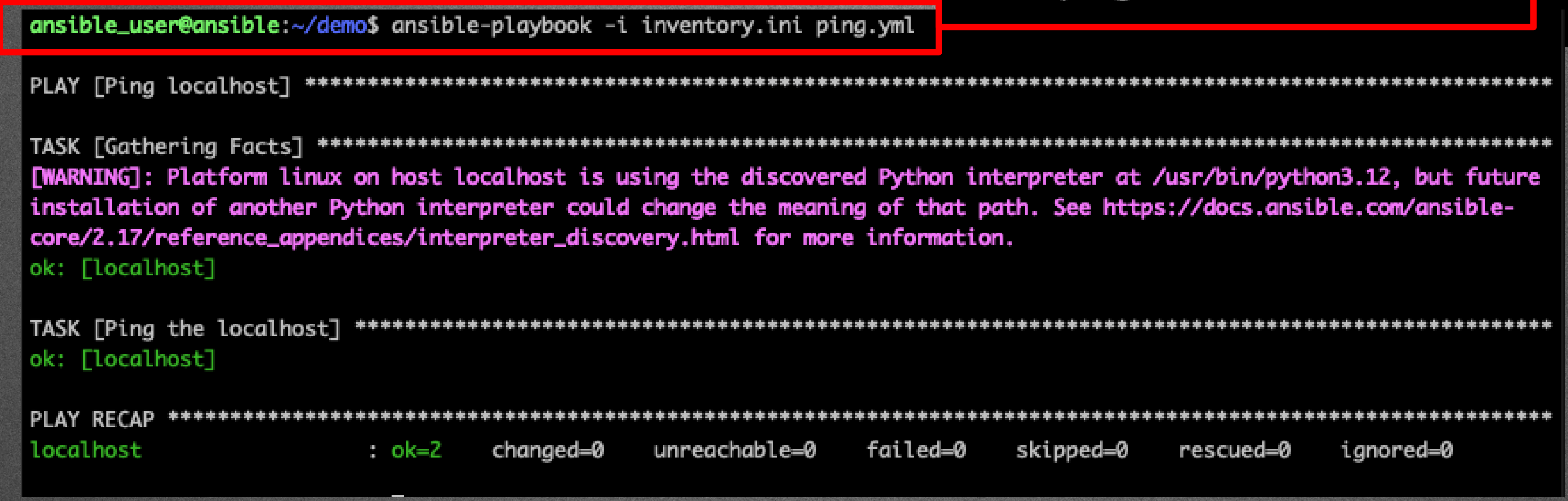
- Create an inventory file
- Write a playbook
- Run the playbook



```
ansible_user@ansible:~/demo$ cat inventory.ini
[local]
localhost ansible_connection=local
```

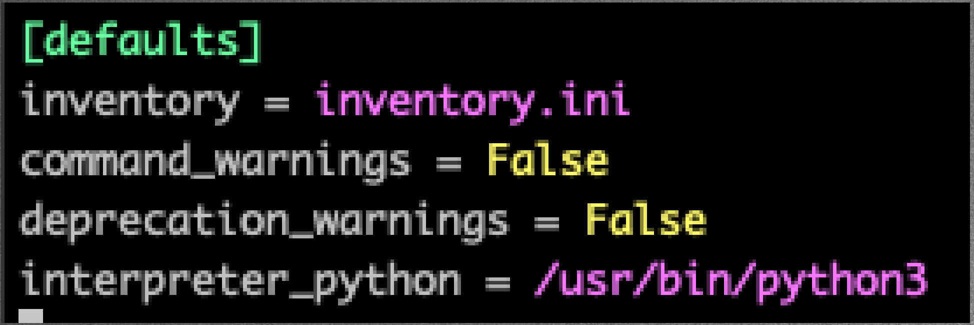


```
ansible_user@ansible:~/demo$ cat ping.yml
---
- name: Ping localhost
  hosts: local
  tasks:
    - name: Ping the localhost
      ping:
```



```
ansible_user@ansible:~/demo$ ansible-playbook -i inventory.ini ping.yml

PLAY [Ping localhost] **************************************************************************************

TASK [Gathering Facts] *************************************************************************************
[WARNING]: Platform linux on host localhost is using the discovered Python interpreter at /usr/bin/python3.12, but future
installation of another Python interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-
core/2.17/reference_appendices/interpreter_discovery.html for more information.
ok: [localhost]

TASK [Ping the localhost] **********************************************************************************
ok: [localhost]

PLAY RECAP *************************************************************************************************
localhost                  : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

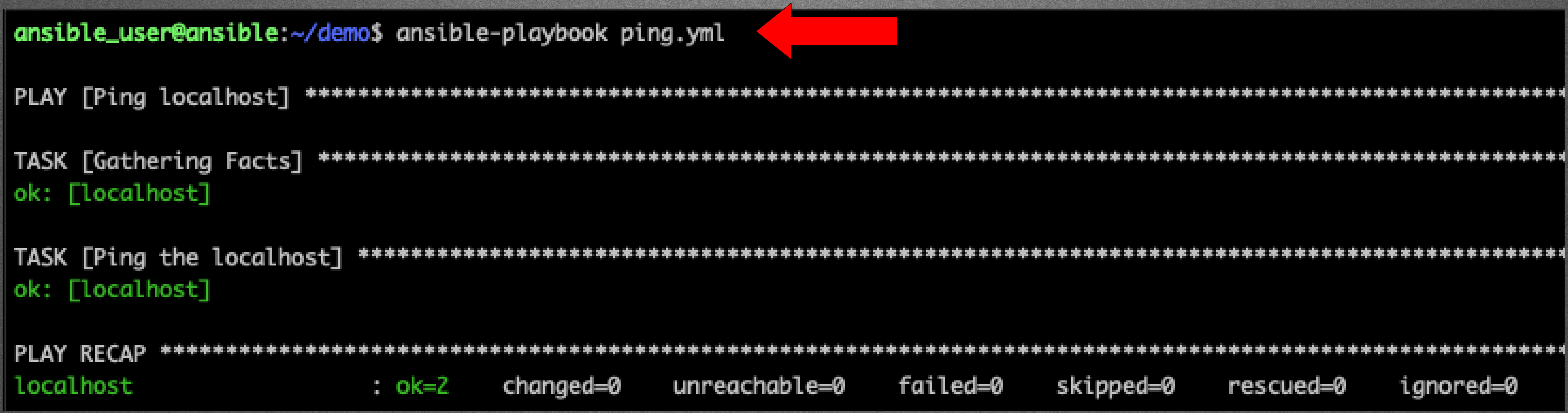
ansible.cfg



```
[defaults]
inventory = inventory.ini
command_warnings = False
deprecation_warnings = False
interpreter_python = /usr/bin/python3
```

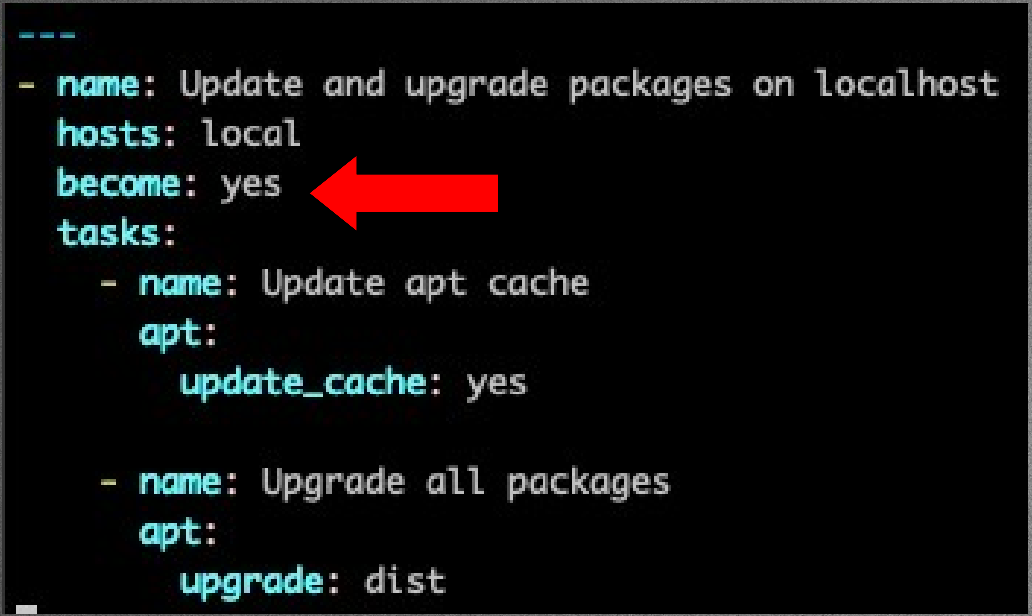
Add the inventory location and turn off those warnings

Now you don’t have to pass the `-i inventory.ini` each time you run a playbook



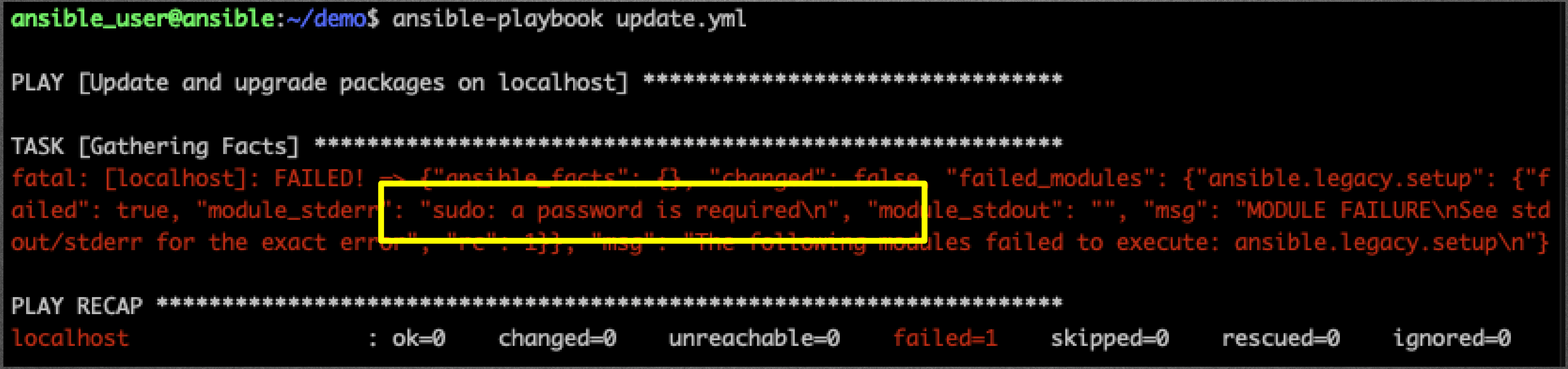
```
ansible_user@ansible:~/demo$ ansible-playbook ping.yml

PLAY [Ping localhost] ******************************************************************

TASK [Gathering Facts] *****************************************************************
ok: [localhost]

TASK [Ping the localhost] **************************************************************
ok: [localhost]

PLAY RECAP *****************************************************************************
localhost                  : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Update ansible with Ansible



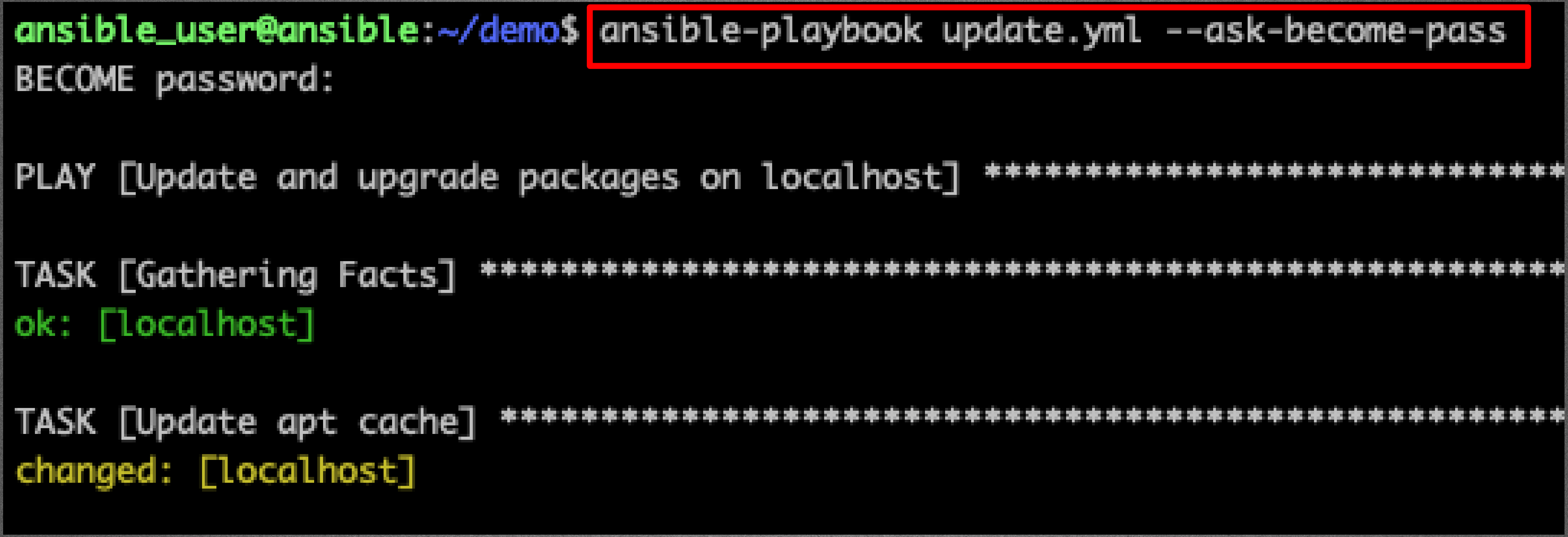
```
---
- name: Update and upgrade packages on localhost
  hosts: local
  become: yes
  tasks:
    - name: Update apt cache
      apt:
        update_cache: yes

    - name: Upgrade all packages
      apt:
        upgrade: dist
```

- Notice that we are using `become` to use `sudo`
- It failed?
- Why?



```
ansible_user@ansible:~/demo$ ansible-playbook update.yml

PLAY [Update and upgrade packages on localhost] *********************************

TASK [Gathering Facts] *********************************************************
fatal: [localhost]: FAILED! => {"ansible_facts": {}, "changed": false, "failed_modules": {"ansible.legacy.setup": {"f
ailed": true, "module_stderr": "sudo: a password is required\n", "module_stdout": "", "msg": "MODULE FAILURE\nSee std
out/stderr for the exact error", "rc": 1}}, "msg": "The following modules failed to execute: ansible.legacy.setup\n"}

PLAY RECAP *********************************************************************
localhost                  : ok=0    changed=0    unreachable=0    failed=1    skipped=0    rescued=0    ignored=0
```

Ansible with sudo



```
ansible_user@ansible:~/demo$ ansible-playbook update.yml --ask-become-pass
BECOME password:

PLAY [Update and upgrade packages on localhost] *****************************

TASK [Gathering Facts] ******************************************************
ok: [localhost]

TASK [Update apt cache] *****************************************************
changed: [localhost]
```

- It worked!
- Typing passwords each time you run a playbook is no good.
- Let’s fix that.

Storing Secrets in Ansible

- Ansible can store secrets in a “vault”
  - Uses AES 256 to encrypt the data
  - Needs to be unlocked before using

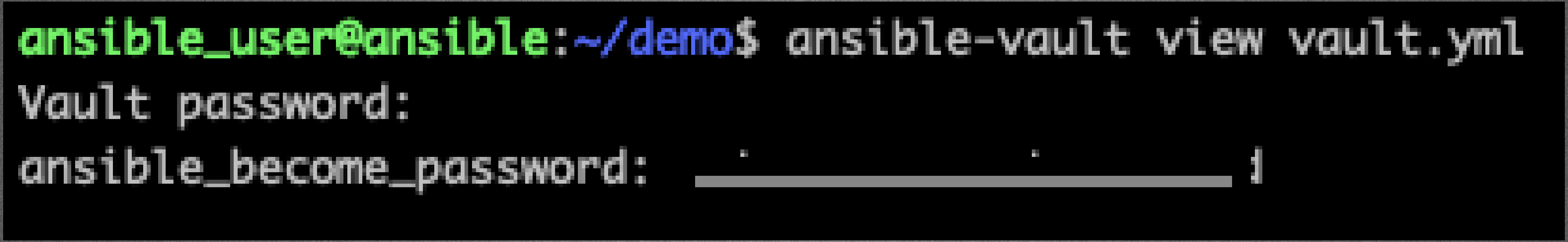
- You could store the ansible_user password for sudo in the vault and run the playbook:

  ```
  ansible-playbook update.yml –ask-vault-pass
  ```

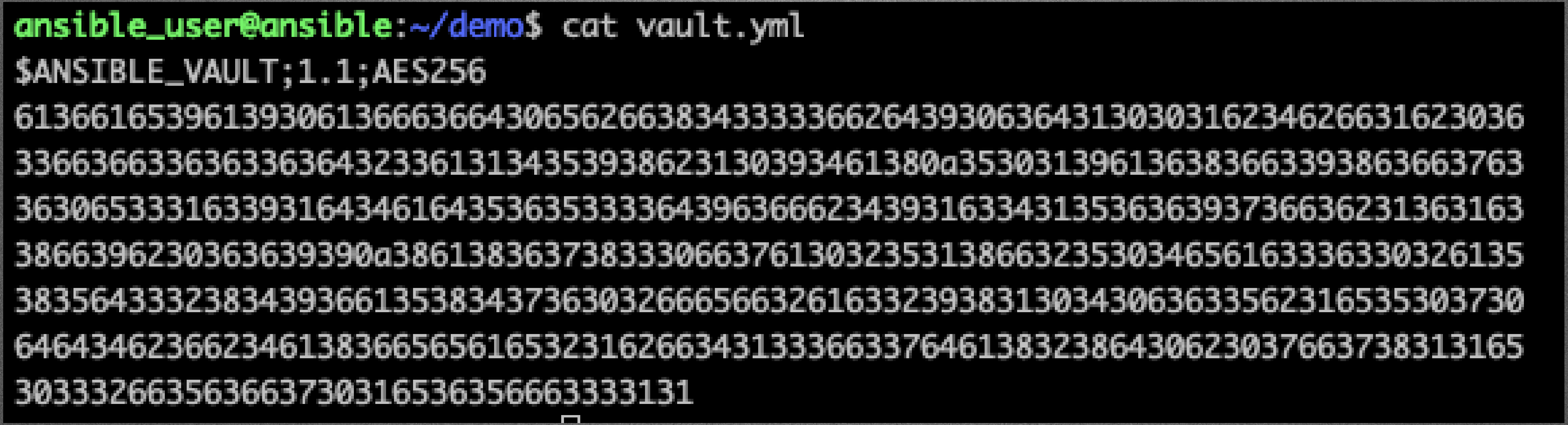
- Not much better than just running:

  ```
  ansible-playbook update.yml --ask-become-pass
  ```

Ansible Vault

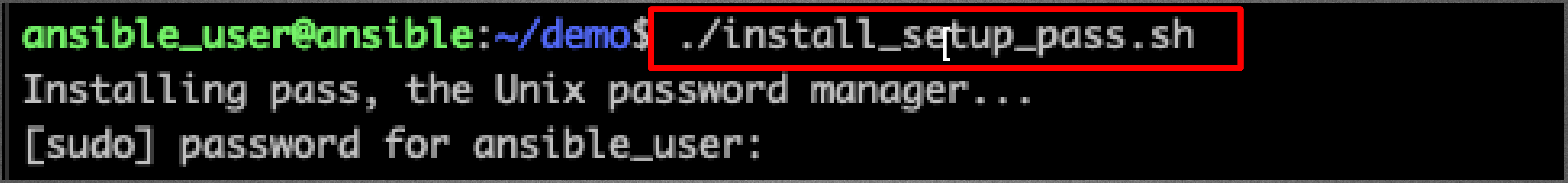


```
ansible_user@ansible:~/demo$ ansible-vault view vault.yml
Vault password:
ansible_become_password: [redacted]
```

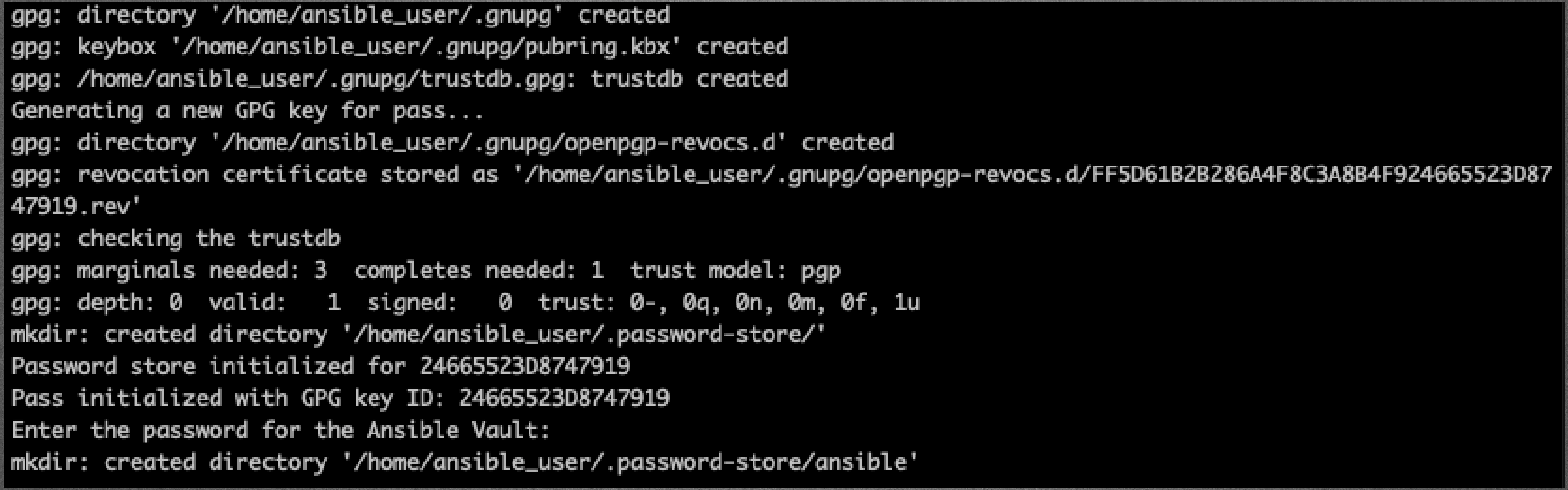


```
ansible_user@ansible:~/demo$ cat vault.yml
$ANSIBLE_VAULT;1.1;AES256
61366165396139306136663664306562663834333336626439306364313030316234626631623036
33663663363633363643233613134353938623130393461380a353031396136383663393863663763
36306533316339316434616435363533336439636662343931633431353636393736636231363163
3866396230363639390a38613836373833306637613032353138663235303465616333363330326135
38356433323834393661353834373630326665663261633239383130343063633562316535303730
64643462366234613836656561653231626634313336633764613832386430623037663738313165
303332663563663730316536356663333131
```

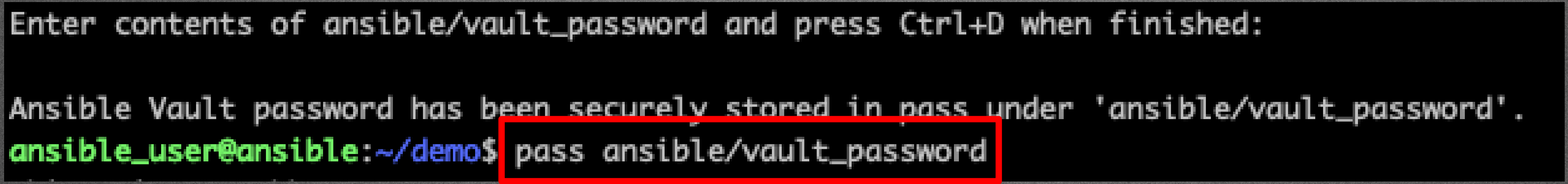
Lets use pass



```
ansible_user@ansible:~/demo$ ./install_setup_pass.sh
Installing pass, the Unix password manager...
[sudo] password for ansible_user:
```



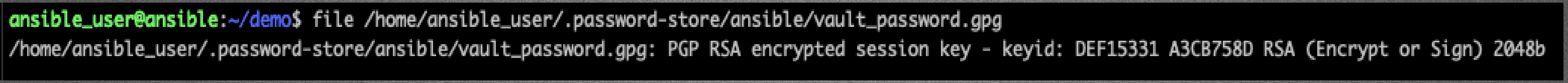
```
gpg: directory '/home/ansible_user/.gnupg' created
gpg: keybox '/home/ansible_user/.gnupg/pubring.kbx' created
gpg: /home/ansible_user/.gnupg/trustdb.gpg: trustdb created
Generating a new GPG key for pass...
gpg: directory '/home/ansible_user/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/ansible_user/.gnupg/openpgp-revocs.d/FF5D61B2B286A4F8C3A8B4F924665523D87
47919.rev'
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
mkdir: created directory '/home/ansible_user/.password-store/'
Password store initialized for 24665523D8747919
Pass initialized with GPG key ID: 24665523D8747919
Enter the password for the Ansible Vault:
mkdir: created directory '/home/ansible_user/.password-store/ansible'
```



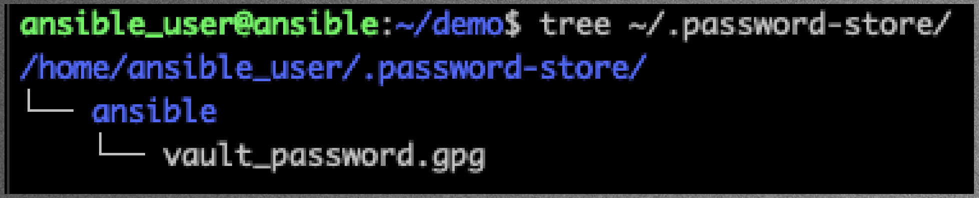
```
Enter contents of ansible/vault_password and press Ctrl+D when finished:

Ansible Vault password has been securely stored in pass under 'ansible/vault_password'.
ansible_user@ansible:~/demo$ pass ansible/vault_password
```

pass uses GPG

pass uses GPG to encrypt/decrypt passwords

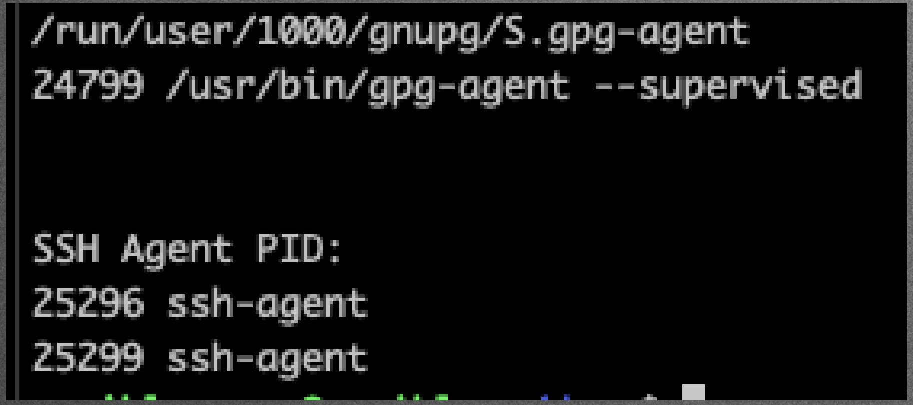


```
ansible_user@ansible:~/demo$ file /home/ansible_user/.password-store/ansible/vault_password.gpg
/home/ansible_user/.password-store/ansible/vault_password.gpg: PGP RSA encrypted session key - keyid: DEF15331 A3CB758D RSA (Encrypt or Sign) 2048b
```

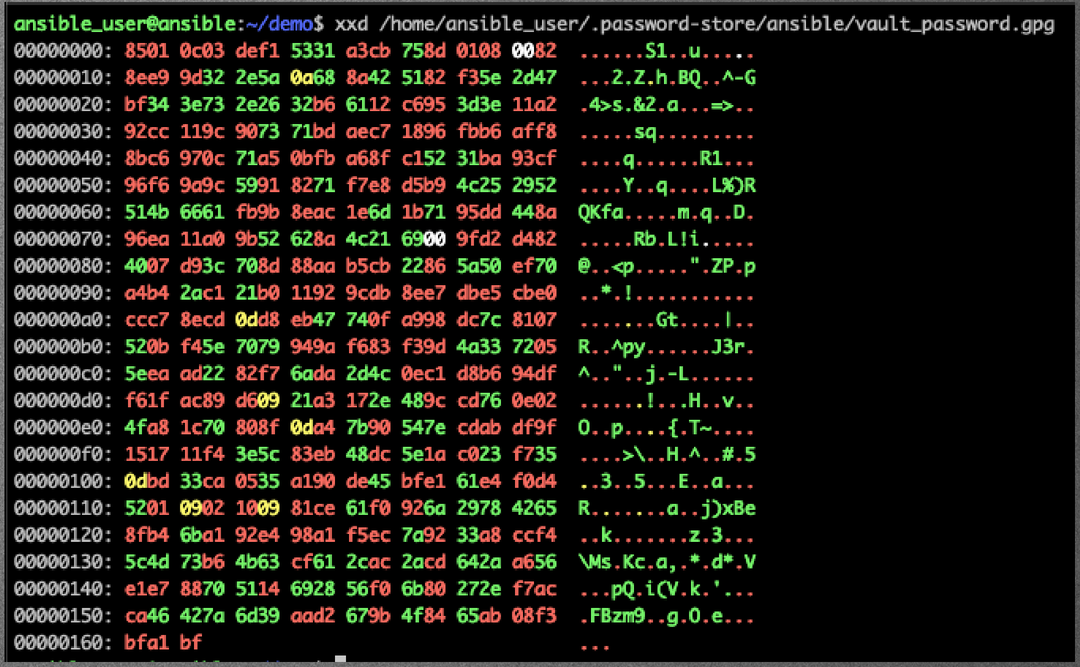


```
ansible_user@ansible:~/demo$ tree ~/.password-store/
/home/ansible_user/.password-store/
└── ansible
    └── vault_password.gpg
```

pass just stores each entry as its own gpg encrypted file



```
/run/user/1000/gnupg/S.gpg-agent
24799 /usr/bin/gpg-agent --supervised


SSH Agent PID:
25296 ssh-agent
25299 ssh-agent
```

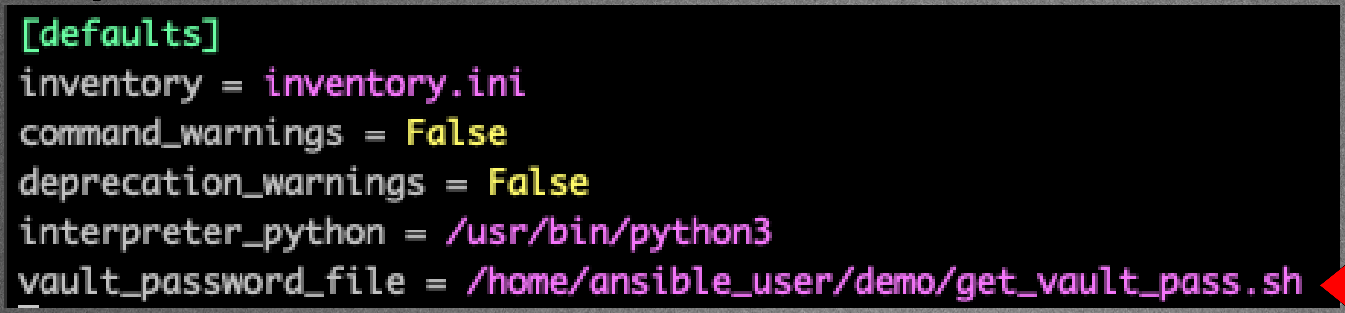


```
ansible_user@ansible:~/demo$ xxd /home/ansible_user/.password-store/ansible/vault_password.gpg
00000000: 8501 0c03 def1 5331 a3cb 758d 0108 0082  ......S1..u.....
00000010: 8ee9 9d32 2e5a 0a68 8a42 5182 f35e 2d47  ...2.Z.h.BQ..^-G
00000020: bf34 3e73 2e26 32b6 6112 c695 3d3e 11a2  .4>s.&2.a...=>..
00000030: 92cc 119c 9073 71bd aec7 1896 fbb6 aff8  .....sq.........
00000040: 8bc6 970c 71a5 0bfb a68f c152 31ba 93cf  ....q......R1...
00000050: 96f6 9a9c 5991 8271 f7e8 d5b9 4c25 2952  ....Y..q....L%)R
00000060: 514b 6661 fb9b 8eac 1e6d 1b71 95dd 448a  QKfa.....m.q..D.
00000070: 96ea 11a0 9b52 628a 4c21 6900 9fd2 d482  .....Rb.L!i.....
00000080: 4007 d93c 708d 88aa b5cb 2286 5a50 ef70  @..<p.....".ZP.p
00000090: a4b4 2ac1 21b0 1192 9cdb 8ee7 dbe5 cbe0  ..*.!...........
000000a0: ccc7 8ecd 0dd8 eb47 740f a998 dc7c 8107  .......Gt....|..
000000b0: 520b f45e 7079 949a f683 f39d 4a33 7205  R..^py......J3r.
000000c0: 5eea ad22 82f7 6ada 2d4c 0ec1 d8b6 94df  ^.."..j.-L......
000000d0: f61f ac89 d609 21a3 172e 489c cd76 0e02  ......!...H..v..
000000e0: 4fa8 1c70 808f 0da4 7b90 547e cdab df9f  O..p....{.T~....
000000f0: 1517 11f4 3e5c 83eb 48dc 5e1a c023 f735  ....>\..H.^..#.5
00000100: 0dbd 33ca 0535 a190 de45 bfe1 61e4 f0d4  ..3..5...E..a...
00000110: 5201 0902 1009 81ce 61f0 926a 2978 4265  R.......a..j)xBe
00000120: 8fb4 6ba1 92e4 98a1 f5ec 7a92 33a8 ccf4  ..k.......z.3...
00000130: 5c4d 73b6 4b63 cf61 2cac 2acd 642a a656  \Ms.Kc.a,.*.d*.V
00000140: e1e7 8870 5114 6928 56f0 6b80 272e f7ac  ...pQ.i(V.k.'...
00000150: ca46 427a 6d39 aad2 679b 4f84 65ab 08f3  .FBzm9..g.O.e...
00000160: bfa1 bf                                  ...
```

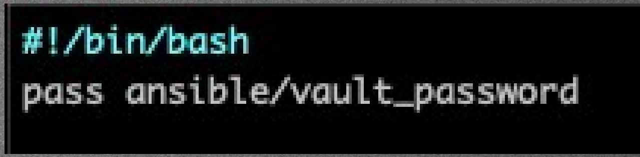
GPG uses an agent, just like the SSH Agent

Update `ansible.cfg` for `pass`

- Update the ansible.cfg to call a script to use pass to unlock our vault



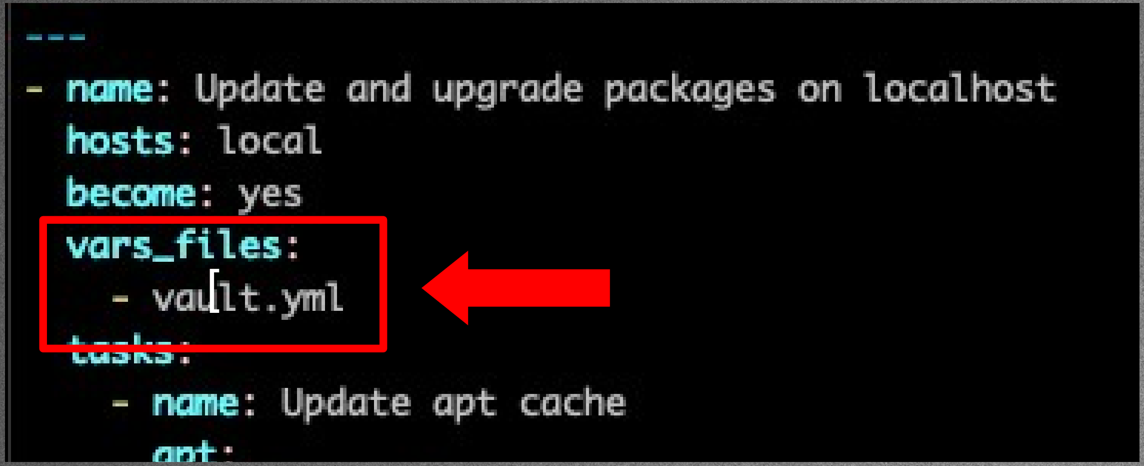
```
[defaults]
inventory = inventory.ini
command_warnings = False
deprecation_warnings = False
interpreter_python = /usr/bin/python3
vault_password_file = /home/ansible_user/demo/get_vault_pass.sh
```



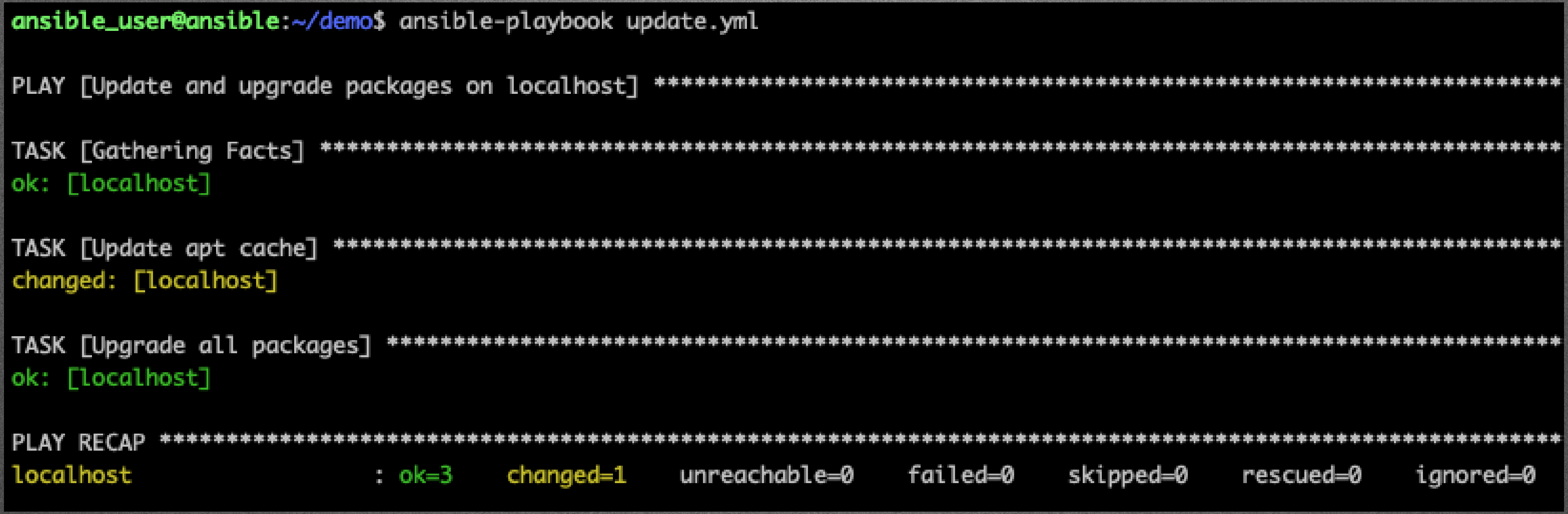
```
#!/bin/bash
pass ansible/vault_password
```

- Wait, what were we doing again?
- Updating the packages on the ansible server, securely using NO PLAINTEXT passwords.

Update our `update.yml`



```
---
- name: Update and upgrade packages on localhost
  hosts: local
  become: yes
  vars_files:
    - vault.yml
  tasks:
    - name: Update apt cache
      apt:
```



```
ansible_user@ansible:~/demo$ ansible-playbook update.yml

PLAY [Update and upgrade packages on localhost] *******************************************************************

TASK [Gathering Facts] ********************************************************************************************
ok: [localhost]

TASK [Update apt cache] *******************************************************************************************
changed: [localhost]

TASK [Upgrade all packages] ***************************************************************************************
ok: [localhost]

PLAY RECAP ********************************************************************************************************
localhost                  : ok=3    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Okay...

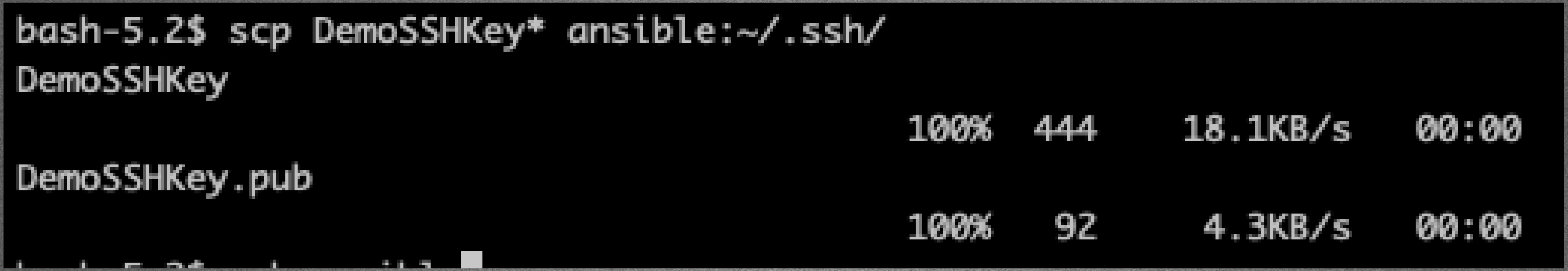
- Couldn’t I have just run:

```
apt update && apt upgrade -y
```

- Yes, but that’s not DevOps
  - It doesn’t scale to dozens / hundreds / thousands of machines
  - Error prone
  - You don’t get “infrastructure as code”

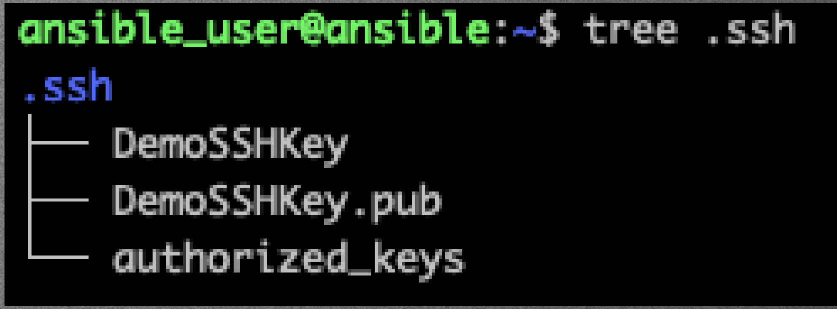
Let’s spin up more machines

- We are going to need our SSH Keys for this

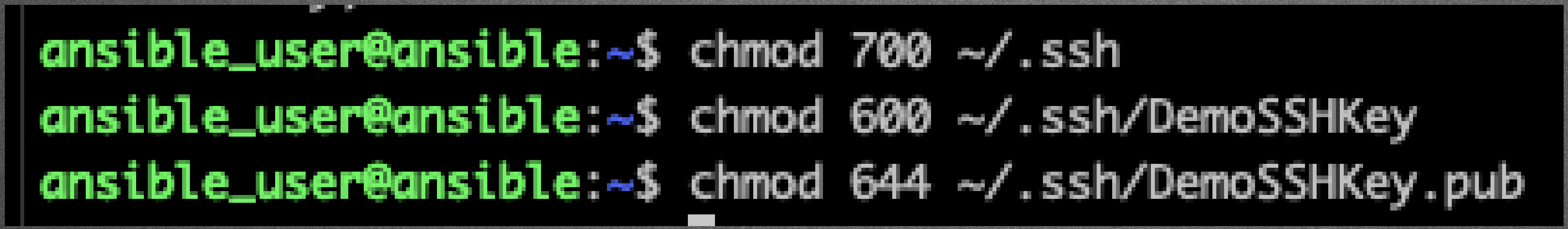


```
bash-5.2$ scp DemoSSHKey* ansible:~/.ssh/
DemoSSHKey
                                                 100%  444     18.1KB/s   00:00
DemoSSHKey.pub
                                                 100%   92      4.3KB/s   00:00
```

- SCP my keys to the ansible machine
- Set the permissions to be secure

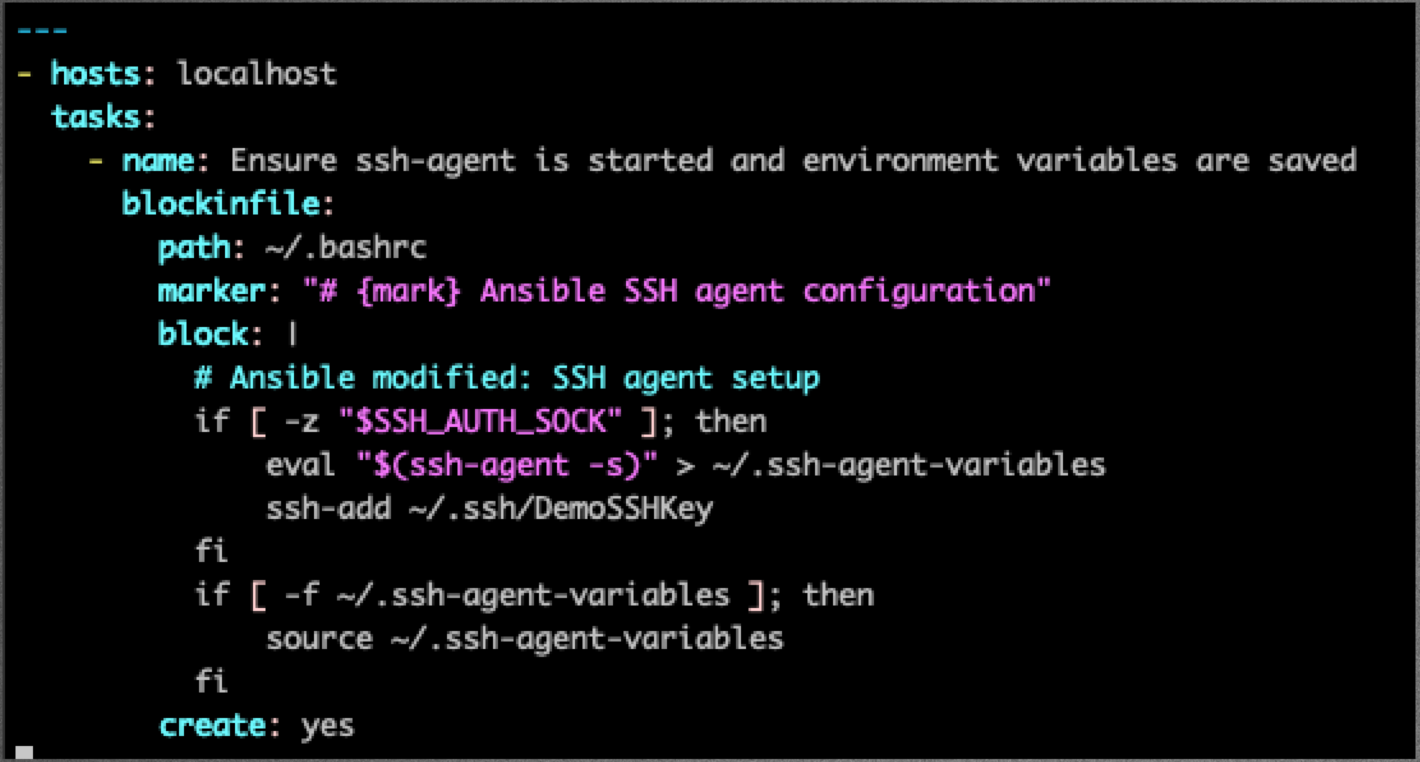


```
ansible_user@ansible:~$ tree .ssh
.ssh
├── DemoSSHKey
├── DemoSSHKey.pub
└── authorized_keys
```



```
ansible_user@ansible:~$ chmod 700 ~/.ssh
ansible_user@ansible:~$ chmod 600 ~/.ssh/DemoSSHKey
ansible_user@ansible:~$ chmod 644 ~/.ssh/DemoSSHKey.pub
```

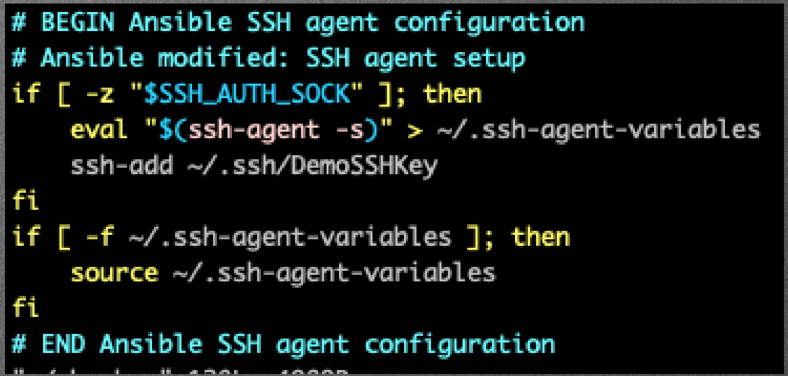
Ansible to update `.bashrc`



```
---
- hosts: localhost
  tasks:
    - name: Ensure ssh-agent is started and environment variables are saved
      blockinfile:
        path: ~/.bashrc
        marker: "# {mark} Ansible SSH agent configuration"
        block: |
          # Ansible modified: SSH agent setup
          if [ -z "$SSH_AUTH_SOCK" ]; then
              eval "$(ssh-agent -s)" > ~/.ssh-agent-variables
              ssh-add ~/.ssh/DemoSSHKey
          fi
          if [ -f ~/.ssh-agent-variables ]; then
              source ~/.ssh-agent-variables
          fi
        create: yes
```

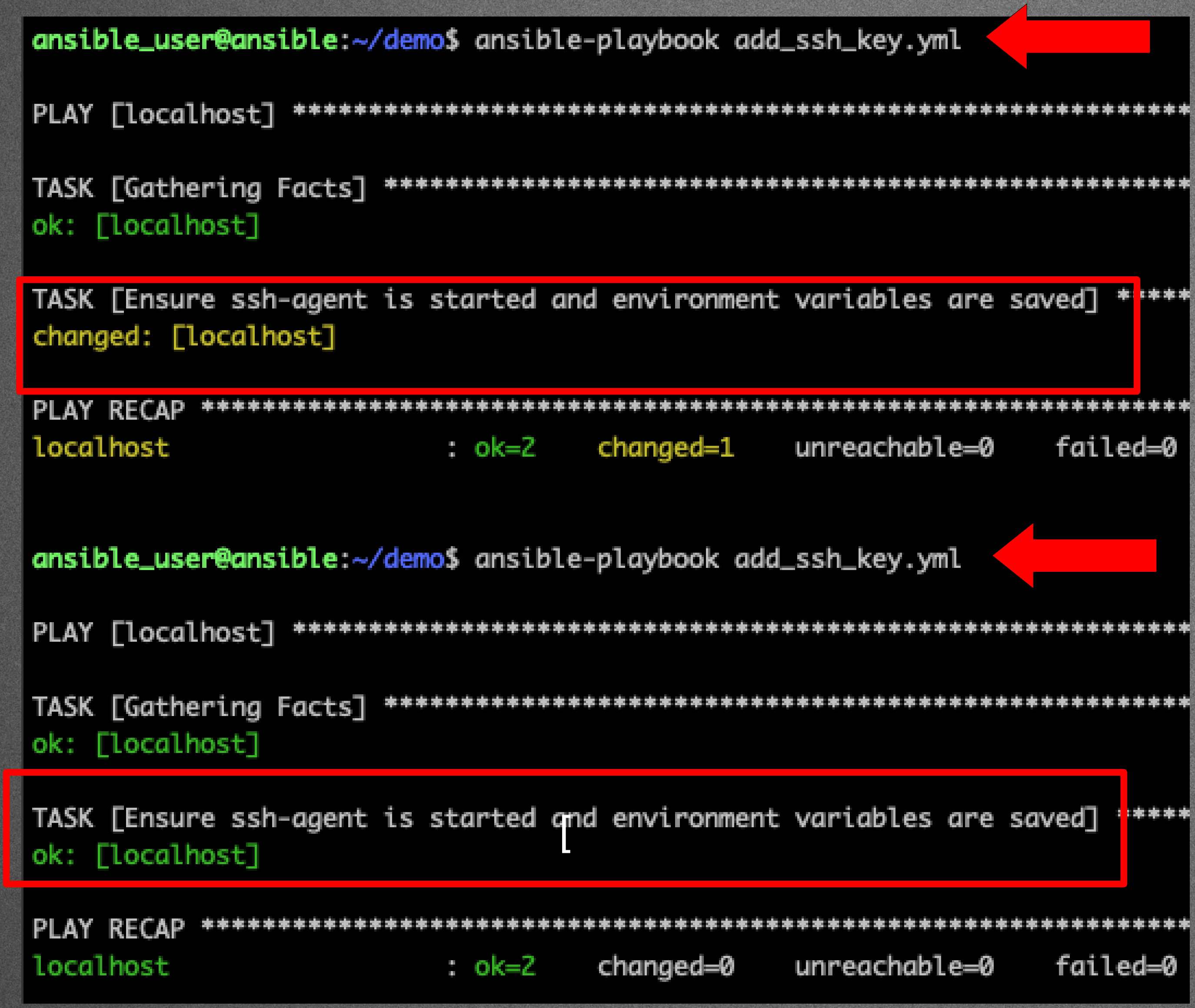
Now the `.bashrc` file is updated to start the SSH-Agent when the user logs in

Now the ssh-agent will startup when we login to the server



```
# BEGIN Ansible SSH agent configuration
# Ansible modified: SSH agent setup
if [ -z "$SSH_AUTH_SOCK" ]; then
    eval "$(ssh-agent -s)" > ~/.ssh-agent-variables
    ssh-add ~/.ssh/DemoSSHKey
fi
if [ -f ~/.ssh-agent-variables ]; then
    source ~/.ssh-agent-variables
fi
# END Ansible SSH agent configuration
```

Idempotent

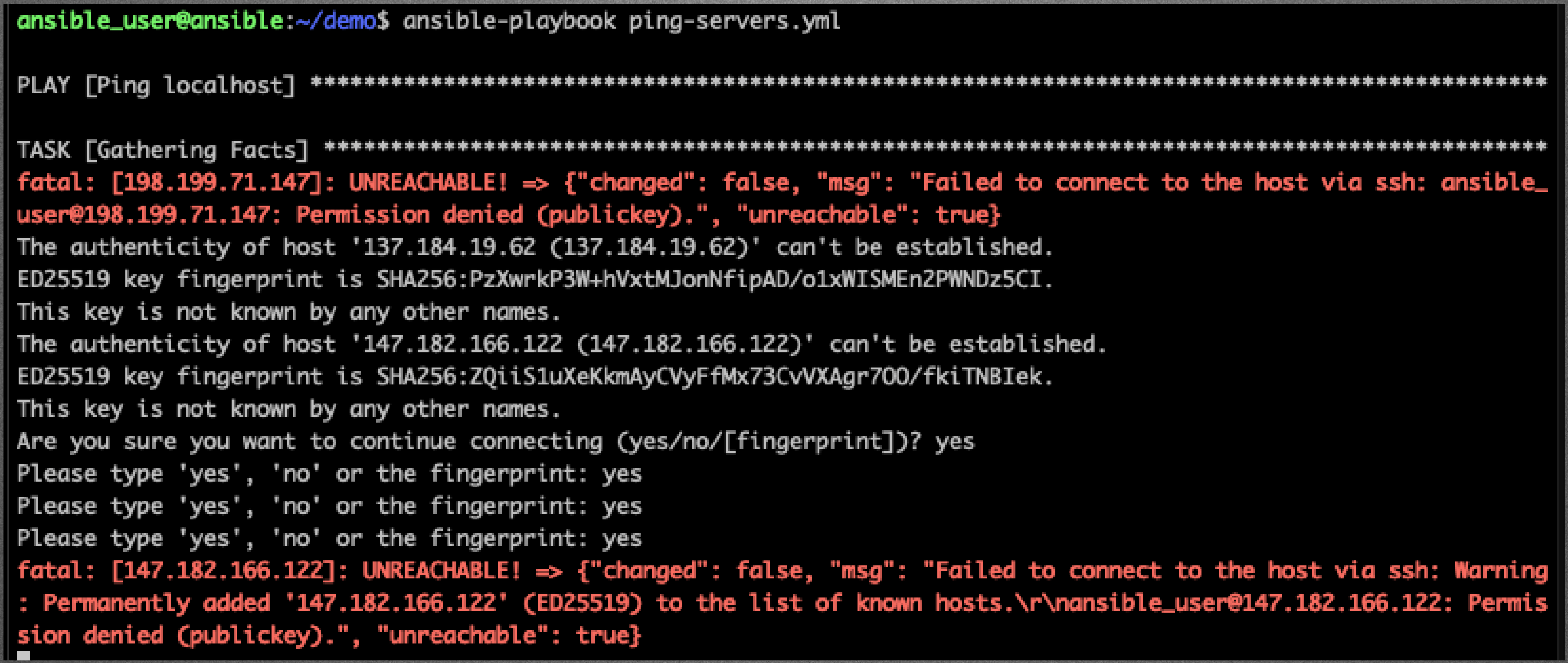


```
ansible_user@ansible:~/demo$ ansible-playbook add_ssh_key.yml

PLAY [localhost] *********************************************************

TASK [Gathering Facts] ***************************************************
ok: [localhost]

TASK [Ensure ssh-agent is started and environment variables are saved] *****
changed: [localhost]

PLAY RECAP ***************************************************************
localhost                  : ok=2    changed=1    unreachable=0    failed=0


ansible_user@ansible:~/demo$ ansible-playbook add_ssh_key.yml

PLAY [localhost] *********************************************************

TASK [Gathering Facts] ***************************************************
ok: [localhost]

TASK [Ensure ssh-agent is started and environment variables are saved] *****
ok: [localhost]

PLAY RECAP ***************************************************************
localhost                  : ok=2    changed=0    unreachable=0    failed=0
```

- Idempotency ensures repeatability: Running the same operation multiple times produces the same outcome without unintended side effects.
- Prevents duplication and redundancy: Ensures that changes are only applied if necessary, making configuration management predictable and reliable.

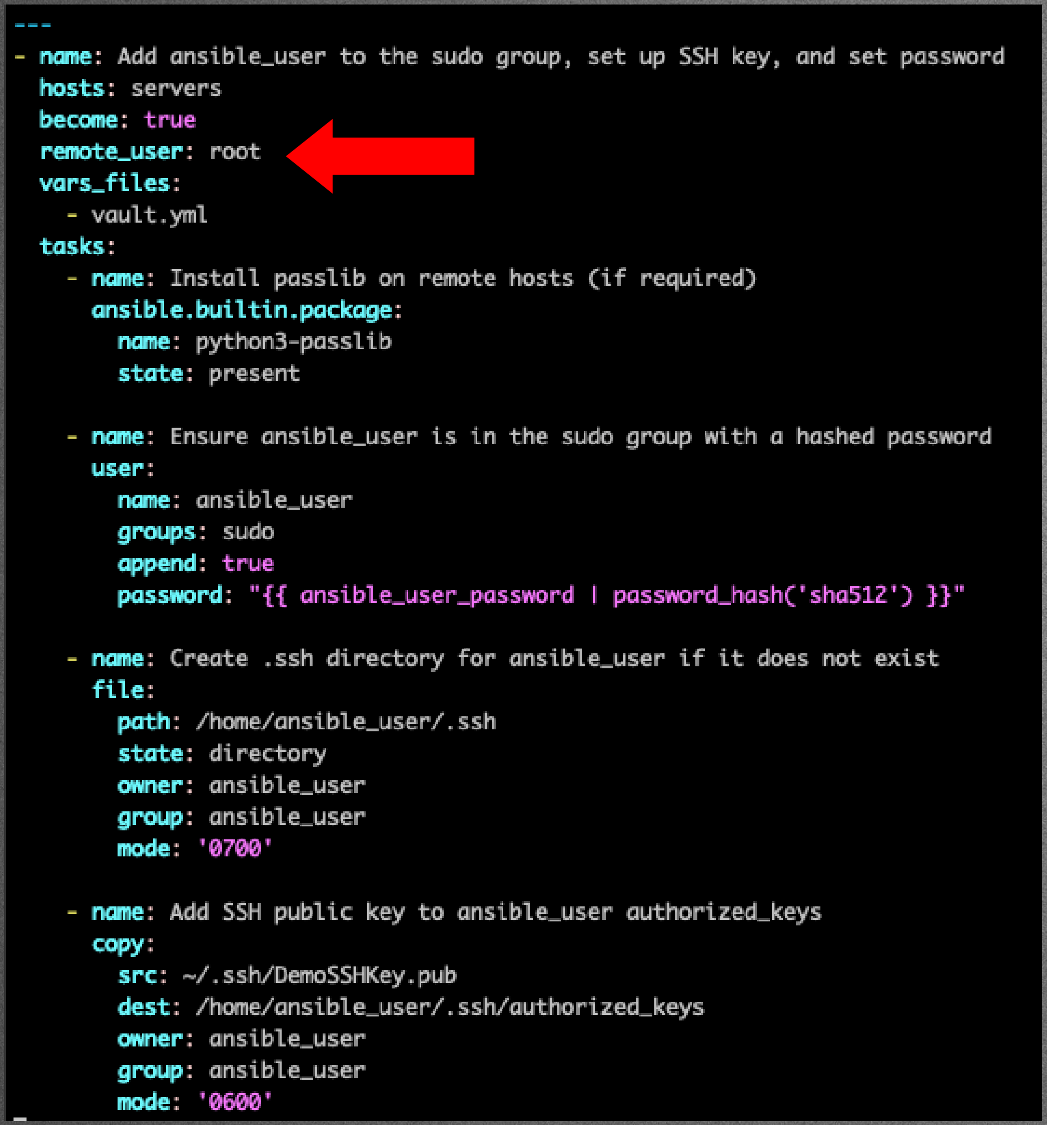
Now we are ready

- Oh, right. First time SSHing, getting the fingerprint message.
- Also, we are trying to connect as ansible_user

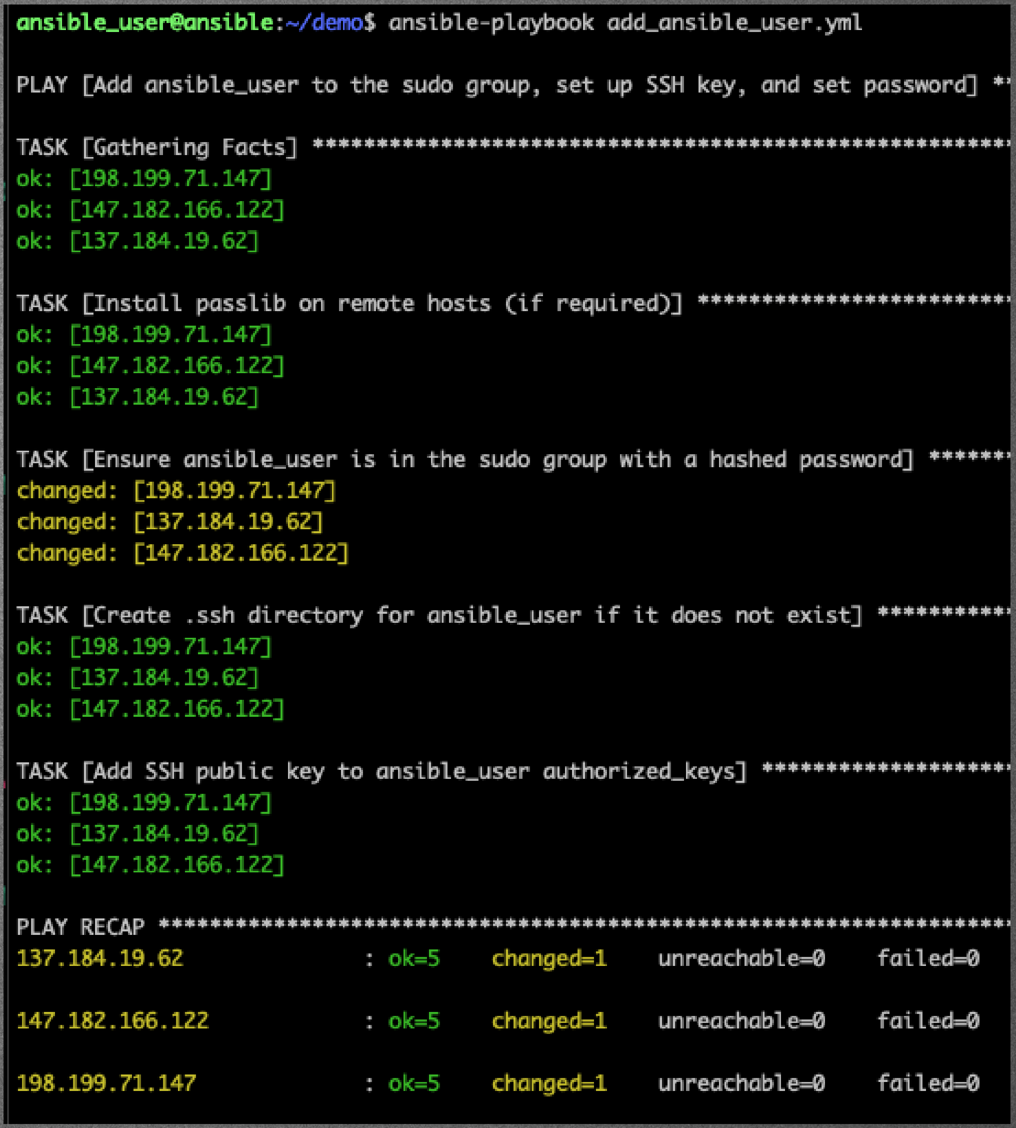


```
ansible_user@ansible:~/demo$ ansible-playbook ping-servers.yml

PLAY [Ping localhost] *********************************************************************************************

TASK [Gathering Facts] ********************************************************************************************
fatal: [198.199.71.147]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ansible_
user@198.199.71.147: Permission denied (publickey).", "unreachable": true}
The authenticity of host '137.184.19.62 (137.184.19.62)' can't be established.
ED25519 key fingerprint is SHA256:PzXwrkP3W+hVxtMJonNfipAD/o1xWISMEn2PWNDz5CI.
This key is not known by any other names.
The authenticity of host '147.182.166.122 (147.182.166.122)' can't be established.
ED25519 key fingerprint is SHA256:ZQiiS1uXeKkmAyCVyFfMx73CvVXAgr7OO/fkiTNBIek.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Please type 'yes', 'no' or the fingerprint: yes
Please type 'yes', 'no' or the fingerprint: yes
Please type 'yes', 'no' or the fingerprint: yes
fatal: [147.182.166.122]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: Warning
: Permanently added '147.182.166.122' (ED25519) to the list of known hosts.\r\nansible_user@147.182.166.122: Permis
sion denied (publickey).", "unreachable": true}
```

Add ansible_user to servers

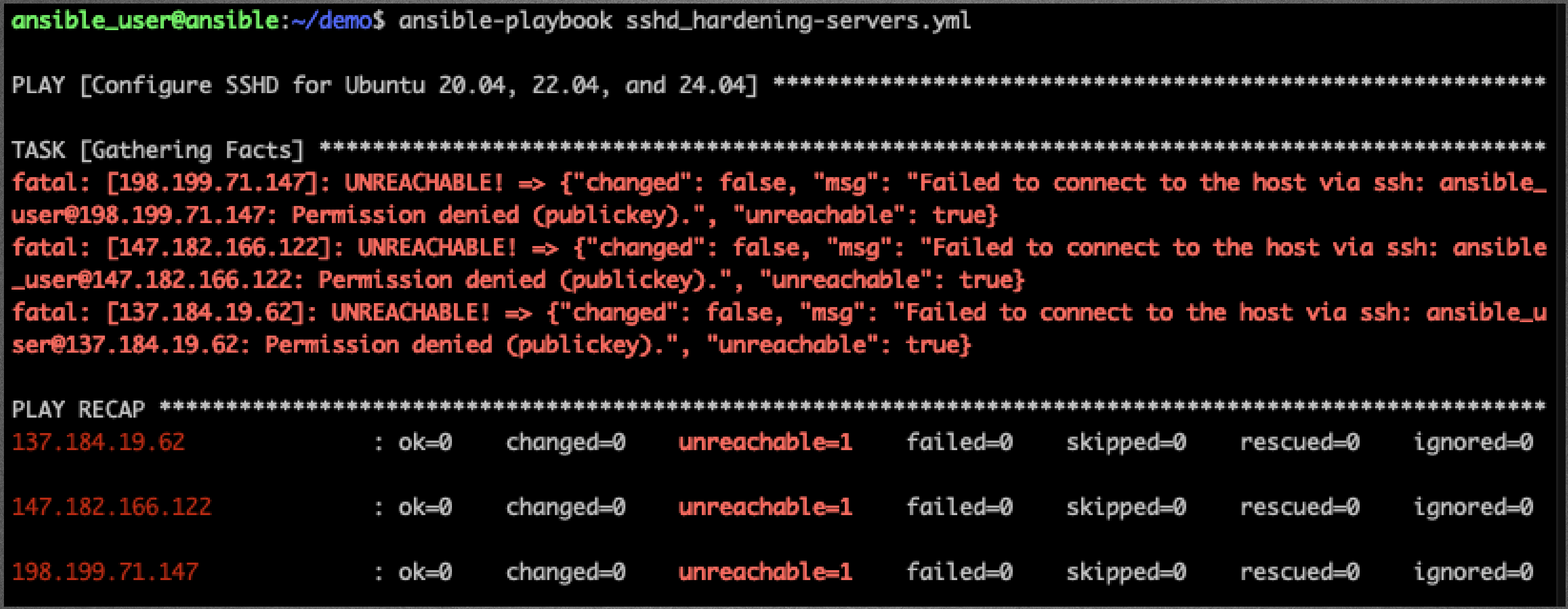


```yaml
---
- name: Add ansible_user to the sudo group, set up SSH key, and set password
  hosts: servers
  become: true
  remote_user: root
  vars_files:
    - vault.yml
  tasks:
    - name: Install passlib on remote hosts (if required)
      ansible.builtin.package:
        name: python3-passlib
        state: present

    - name: Ensure ansible_user is in the sudo group with a hashed password
      user:
        name: ansible_user
        groups: sudo
        append: true
        password: "{{ ansible_user_password | password_hash('sha512') }}"

    - name: Create .ssh directory for ansible_user if it does not exist
      file:
        path: /home/ansible_user/.ssh
        state: directory
        owner: ansible_user
        group: ansible_user
        mode: '0700'

    - name: Add SSH public key to ansible_user authorized_keys
      copy:
        src: ~/.ssh/DemoSSHKey.pub
        dest: /home/ansible_user/.ssh/authorized_keys
        owner: ansible_user
        group: ansible_user
        mode: '0600'
```



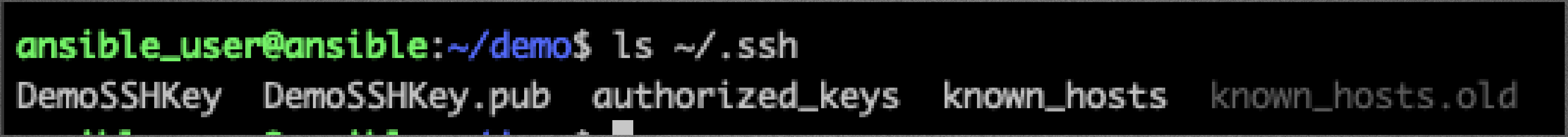
```
ansible_user@ansible:~/demo$ ansible-playbook add_ansible_user.yml

PLAY [Add ansible_user to the sudo group, set up SSH key, and set password] **

TASK [Gathering Facts] ******************************************************
ok: [198.199.71.147]
ok: [147.182.166.122]
ok: [137.184.19.62]

TASK [Install passlib on remote hosts (if required)] ************************
ok: [198.199.71.147]
ok: [147.182.166.122]
ok: [137.184.19.62]

TASK [Ensure ansible_user is in the sudo group with a hashed password] ******
changed: [198.199.71.147]
changed: [137.184.19.62]
changed: [147.182.166.122]

TASK [Create .ssh directory for ansible_user if it does not exist] **********
ok: [198.199.71.147]
ok: [137.184.19.62]
ok: [147.182.166.122]

TASK [Add SSH public key to ansible_user authorized_keys] *******************
ok: [198.199.71.147]
ok: [137.184.19.62]
ok: [147.182.166.122]

PLAY RECAP ******************************************************************
137.184.19.62              : ok=5    changed=1    unreachable=0    failed=0

147.182.166.122            : ok=5    changed=1    unreachable=0    failed=0

198.199.71.147             : ok=5    changed=1    unreachable=0    failed=0
```

Wait, what?

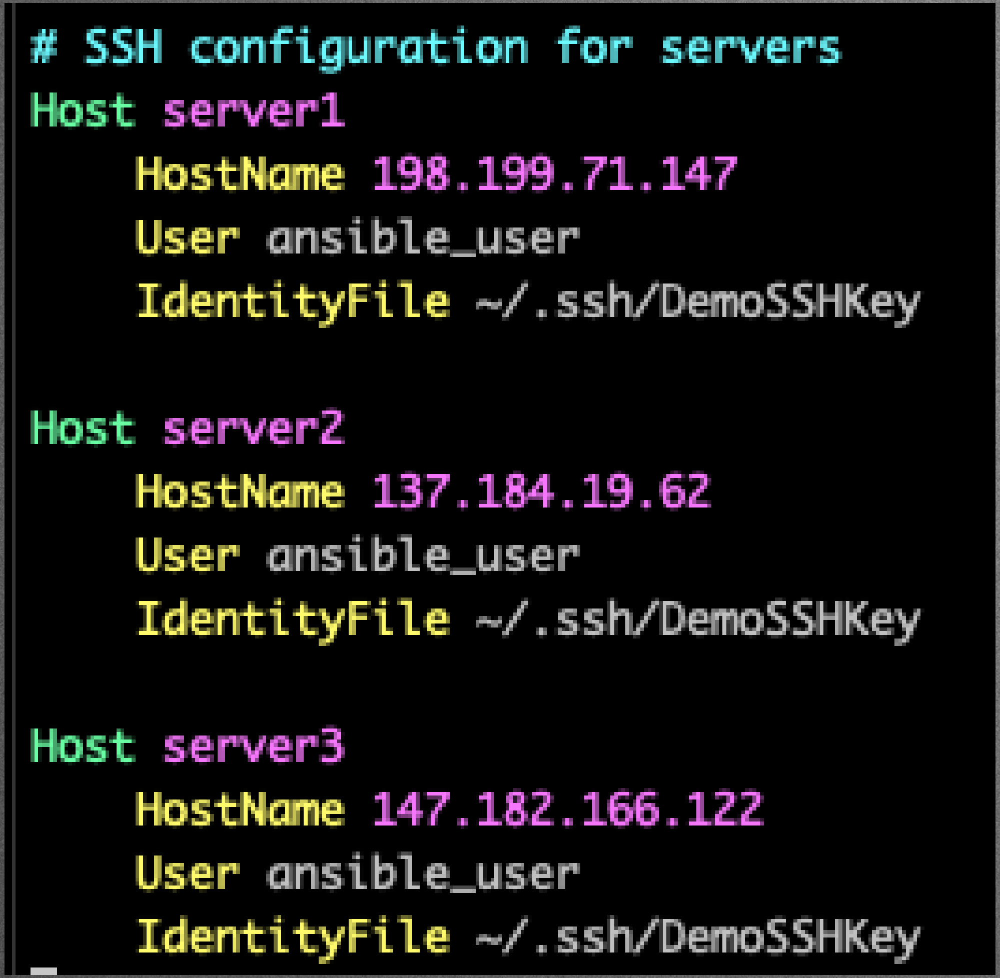


```
ansible_user@ansible:~/demo$ ansible-playbook sshd_hardening-servers.yml

PLAY [Configure SSHD for Ubuntu 20.04, 22.04, and 24.04] **********************************************************

TASK [Gathering Facts] ********************************************************************************************
fatal: [198.199.71.147]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ansible_
user@198.199.71.147: Permission denied (publickey).", "unreachable": true}
fatal: [147.182.166.122]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ansible
_user@147.182.166.122: Permission denied (publickey).", "unreachable": true}
fatal: [137.184.19.62]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect to the host via ssh: ansible_u
ser@137.184.19.62: Permission denied (publickey).", "unreachable": true}

PLAY RECAP ********************************************************************************************************
137.184.19.62              : ok=0    changed=0    unreachable=1    failed=0    skipped=0    rescued=0    ignored=0

147.182.166.122            : ok=0    changed=0    unreachable=1    failed=0    skipped=0    rescued=0    ignored=0

198.199.71.147             : ok=0    changed=0    unreachable=1    failed=0    skipped=0    rescued=0    ignored=0
```

Ahhh, I need an ssh client config

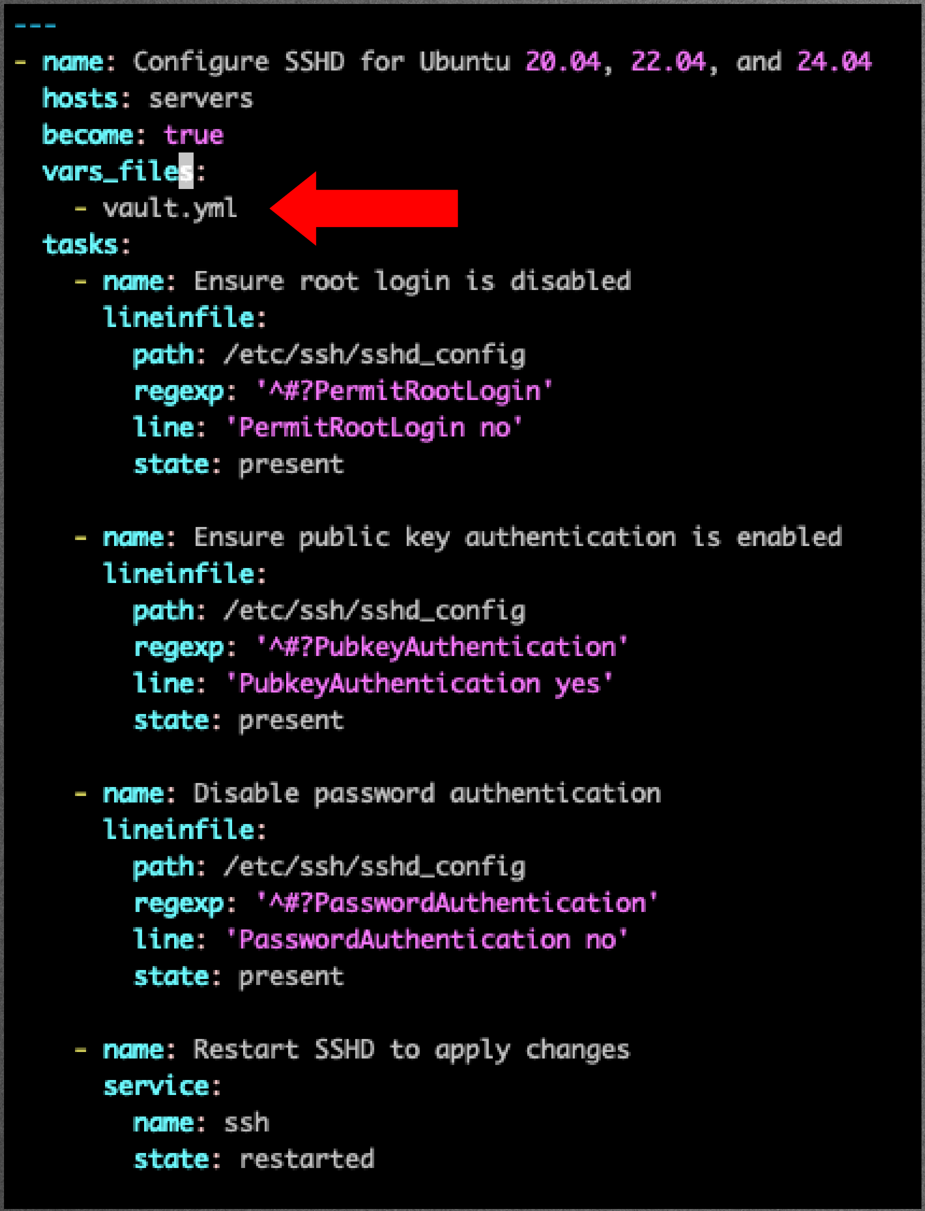


```
ansible_user@ansible:~/demo$ ls ~/.ssh
DemoSSHKey  DemoSSHKey.pub  authorized_keys  known_hosts  known_hosts.old
```

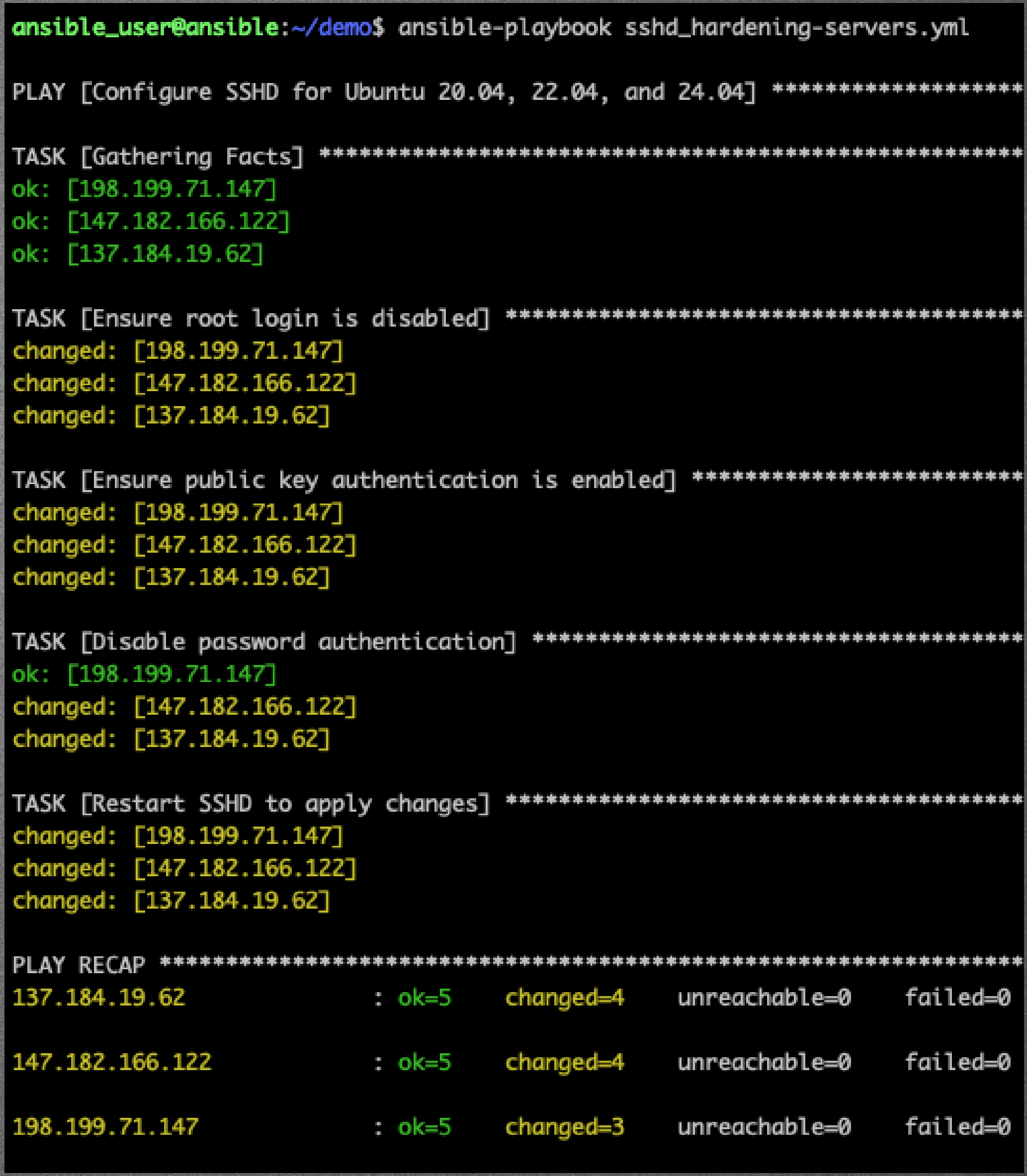


```
# SSH configuration for servers
Host server1
    HostName 198.199.71.147
    User ansible_user
    IdentityFile ~/.ssh/DemoSSHKey

Host server2
    HostName 137.184.19.62
    User ansible_user
    IdentityFile ~/.ssh/DemoSSHKey

Host server3
    HostName 147.182.166.122
    User ansible_user
    IdentityFile ~/.ssh/DemoSSHKey
```

SSHD Hardening

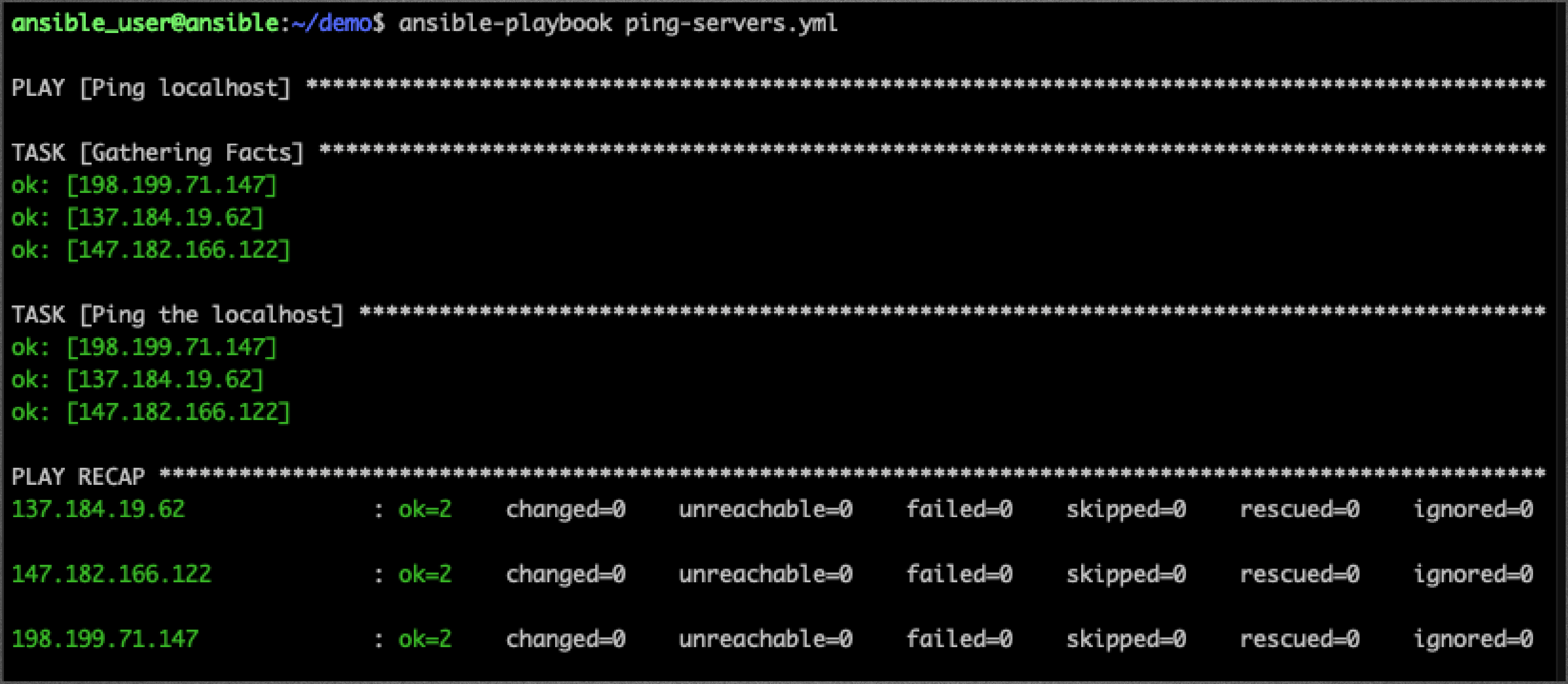


```
---
- name: Configure SSHD for Ubuntu 20.04, 22.04, and 24.04
  hosts: servers
  become: true
  vars_files:
    - vault.yml
  tasks:
    - name: Ensure root login is disabled
      lineinfile:
        path: /etc/ssh/sshd_config
        regexp: '^#?PermitRootLogin'
        line: 'PermitRootLogin no'
        state: present

    - name: Ensure public key authentication is enabled
      lineinfile:
        path: /etc/ssh/sshd_config
        regexp: '^#?PubkeyAuthentication'
        line: 'PubkeyAuthentication yes'
        state: present

    - name: Disable password authentication
      lineinfile:
        path: /etc/ssh/sshd_config
        regexp: '^#?PasswordAuthentication'
        line: 'PasswordAuthentication no'
        state: present

    - name: Restart SSHD to apply changes
      service:
        name: ssh
        state: restarted
```



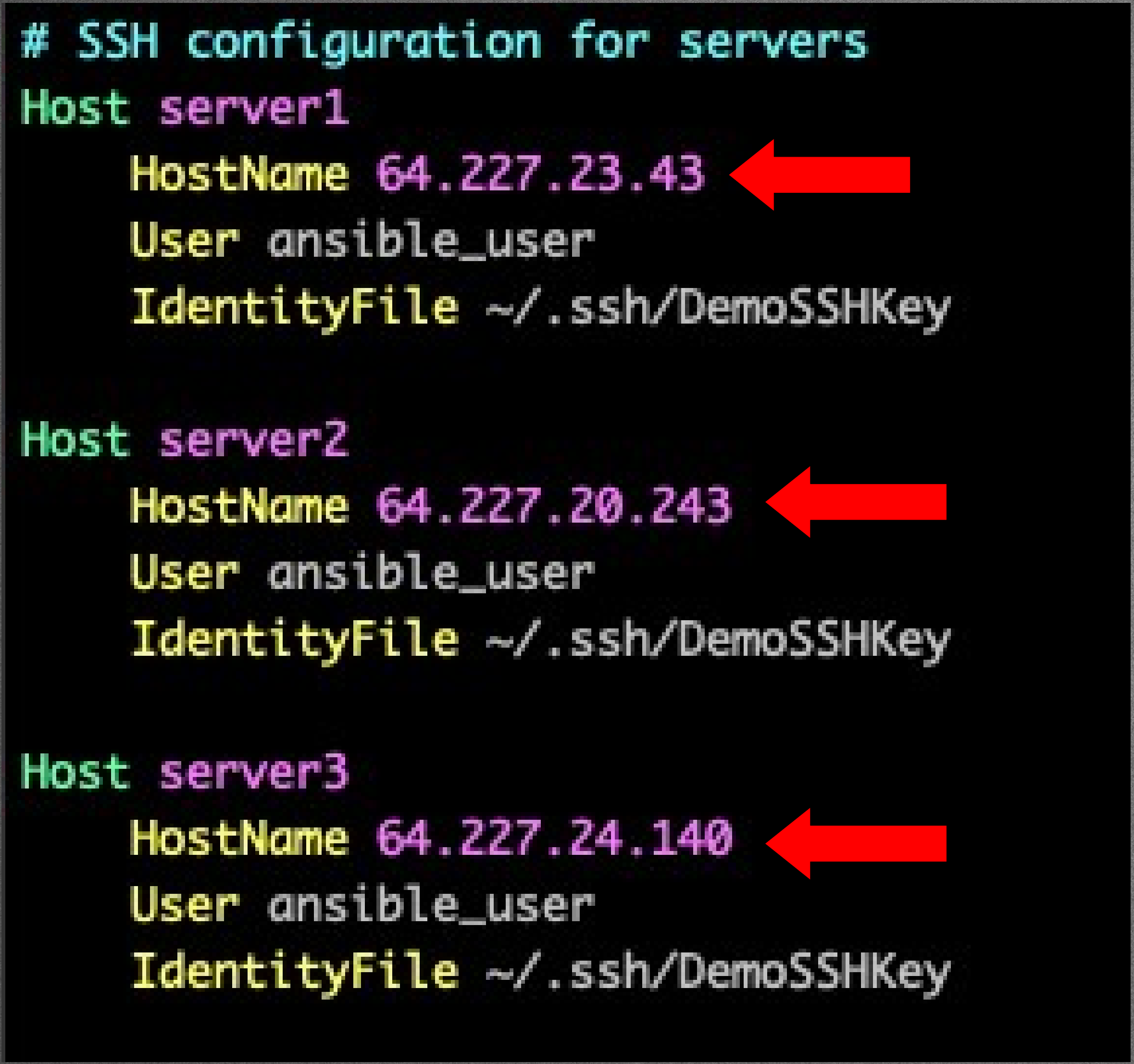
```
ansible_user@ansible:~/demo$ ansible-playbook sshd_hardening-servers.yml

PLAY [Configure SSHD for Ubuntu 20.04, 22.04, and 24.04] *******************

TASK [Gathering Facts] *********************************************************
ok: [198.199.71.147]
ok: [147.182.166.122]
ok: [137.184.19.62]

TASK [Ensure root login is disabled] *******************************************
changed: [198.199.71.147]
changed: [147.182.166.122]
changed: [137.184.19.62]

TASK [Ensure public key authentication is enabled] *************************
changed: [198.199.71.147]
changed: [147.182.166.122]
changed: [137.184.19.62]

TASK [Disable password authentication] *****************************************
ok: [198.199.71.147]
changed: [147.182.166.122]
changed: [137.184.19.62]

TASK [Restart SSHD to apply changes] *******************************************
changed: [198.199.71.147]
changed: [147.182.166.122]
changed: [137.184.19.62]

PLAY RECAP *********************************************************************
137.184.19.62              : ok=5    changed=4    unreachable=0    failed=0

147.182.166.122            : ok=5    changed=4    unreachable=0    failed=0

198.199.71.147             : ok=5    changed=3    unreachable=0    failed=0
```

Now we can ping servers



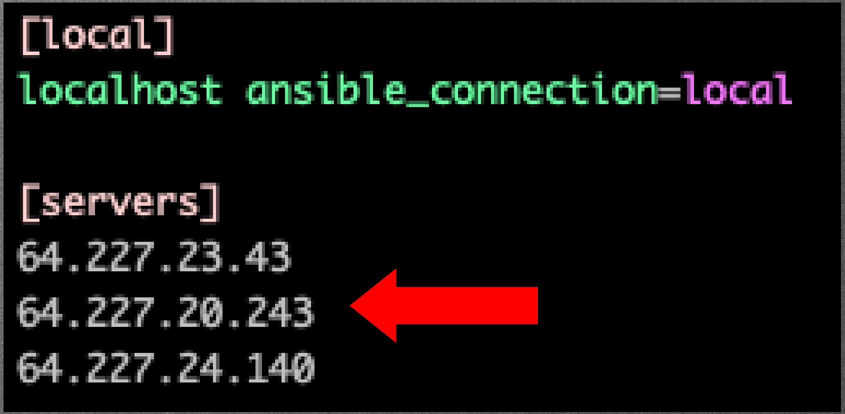
```
ansible_user@ansible:~/demo$ ansible-playbook ping-servers.yml

PLAY [Ping localhost] *********************************************************************************************

TASK [Gathering Facts] ********************************************************************************************
ok: [198.199.71.147]
ok: [137.184.19.62]
ok: [147.182.166.122]

TASK [Ping the localhost] *****************************************************************************************
ok: [198.199.71.147]
ok: [137.184.19.62]
ok: [147.182.166.122]

PLAY RECAP ********************************************************************************************************
137.184.19.62              : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

147.182.166.122            : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

198.199.71.147             : ok=2    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Let’s redo that with new servers



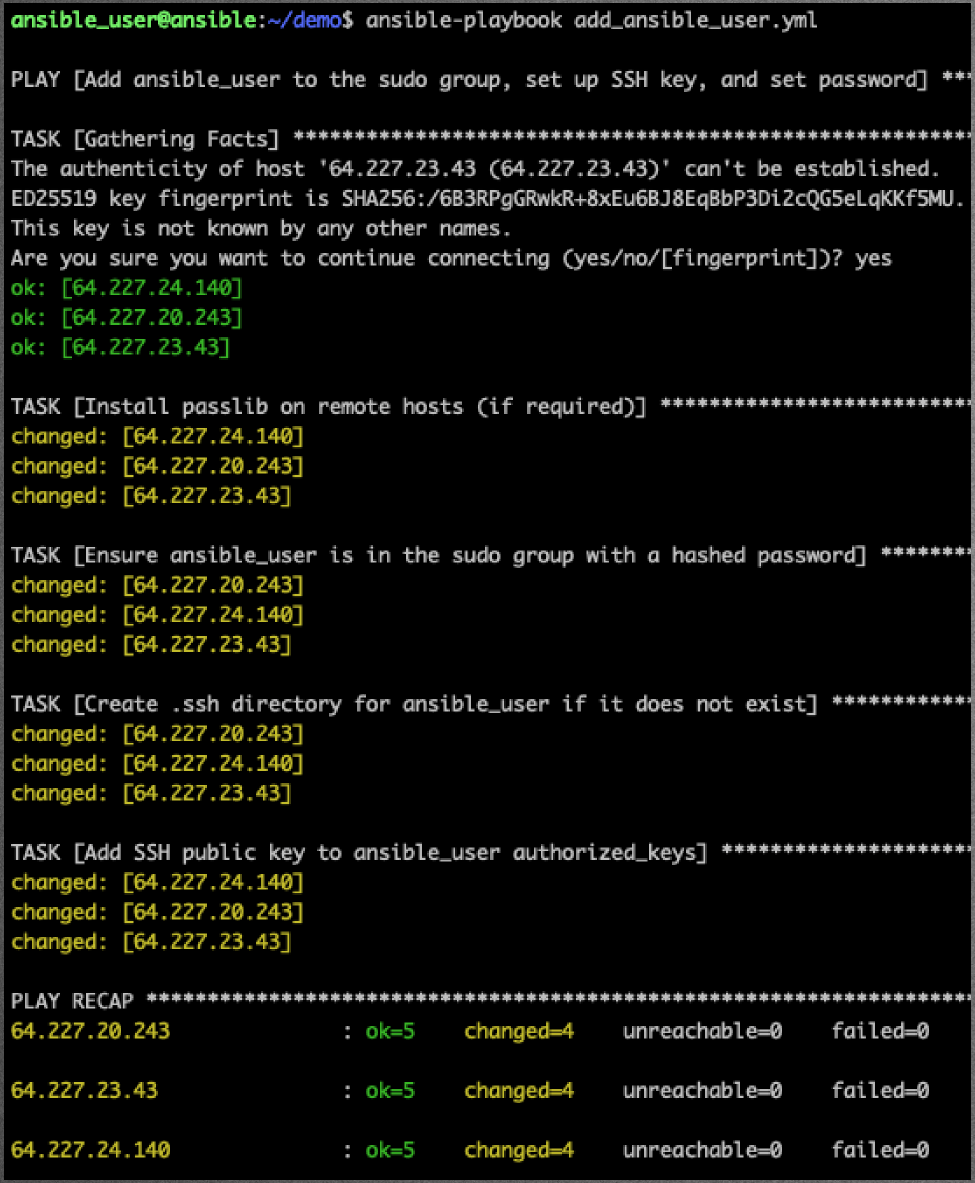
```
# SSH configuration for servers
Host server1
    HostName 64.227.23.43
    User ansible_user
    IdentityFile ~/.ssh/DemoSSHKey

Host server2
    HostName 64.227.20.243
    User ansible_user
    IdentityFile ~/.ssh/DemoSSHKey

Host server3
    HostName 64.227.24.140
    User ansible_user
    IdentityFile ~/.ssh/DemoSSHKey
```

- Update 2 files:
  - `~/.ssh/config`
  - `inventory.ini`

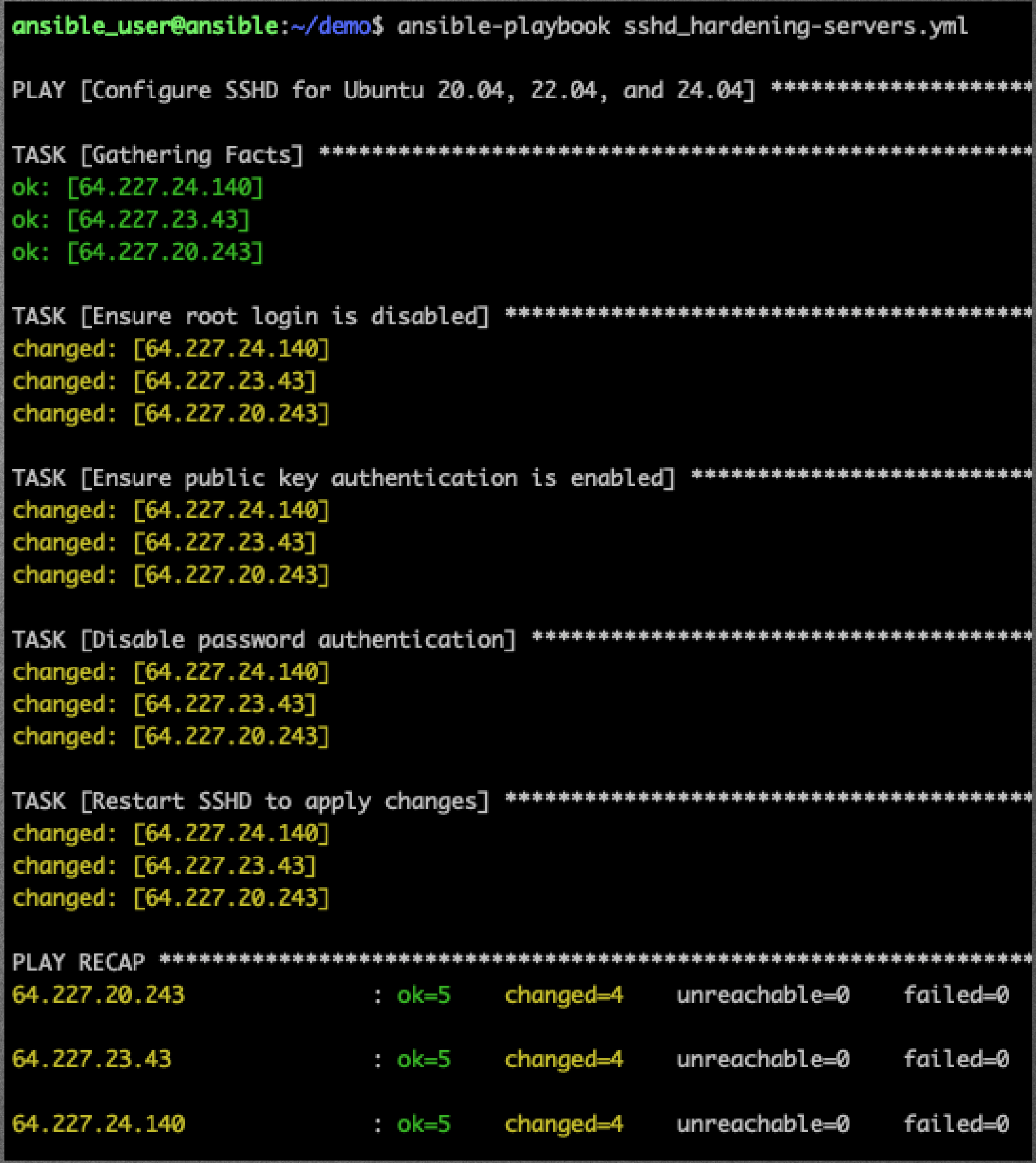


```
[local]
localhost ansible_connection=local

[servers]
64.227.23.43
64.227.20.243
64.227.24.140
```

ansible_user & sshd_hardening



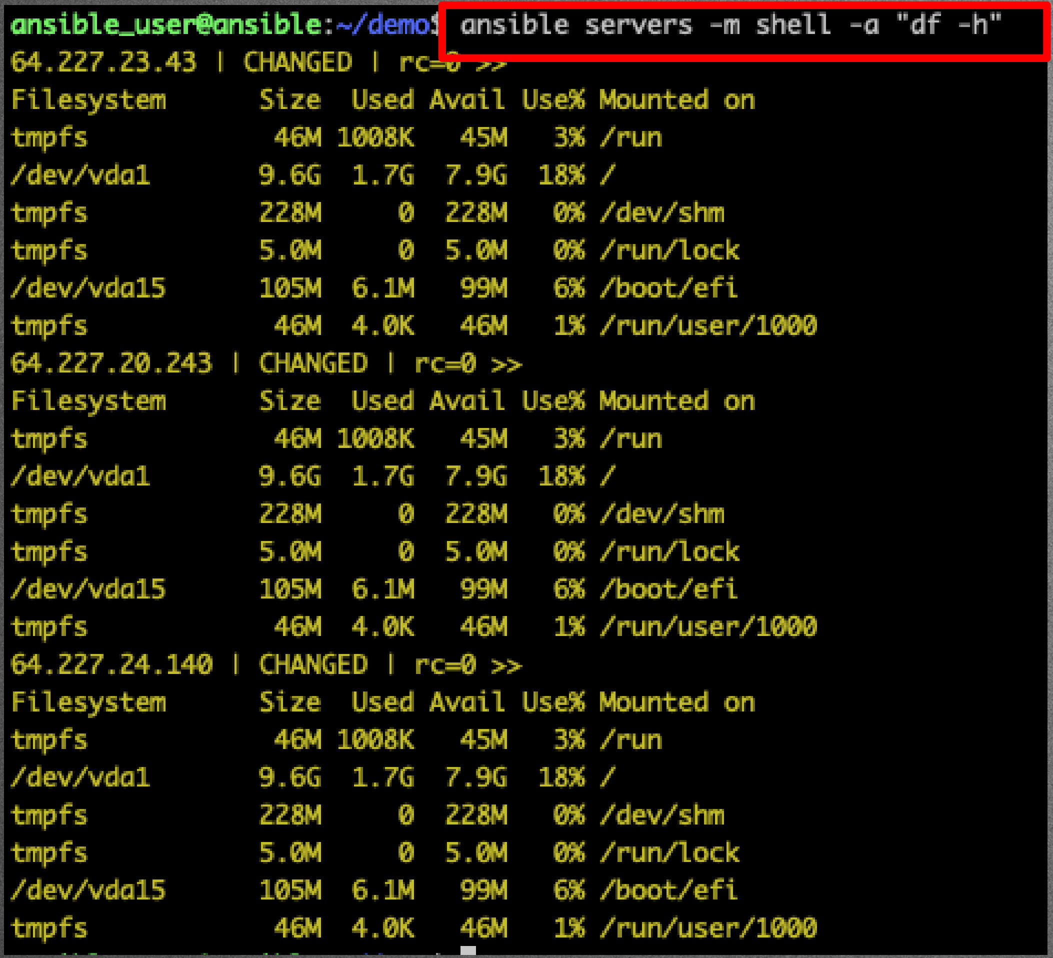
```
ansible_user@ansible:~/demo$ ansible-playbook add_ansible_user.yml

PLAY [Add ansible_user to the sudo group, set up SSH key, and set password] ***

TASK [Gathering Facts] ******************************************************
The authenticity of host '64.227.23.43 (64.227.23.43)' can't be established.
ED25519 key fingerprint is SHA256:/6B3RPgGRwkR+8xEu6BJ8EqBbP3Di2cQG5eLqKKf5MU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
ok: [64.227.24.140]
ok: [64.227.20.243]
ok: [64.227.23.43]

TASK [Install passlib on remote hosts (if required)] ************************
changed: [64.227.24.140]
changed: [64.227.20.243]
changed: [64.227.23.43]

TASK [Ensure ansible_user is in the sudo group with a hashed password] *******
changed: [64.227.20.243]
changed: [64.227.24.140]
changed: [64.227.23.43]

TASK [Create .ssh directory for ansible_user if it does not exist] ***********
changed: [64.227.20.243]
changed: [64.227.24.140]
changed: [64.227.23.43]

TASK [Add SSH public key to ansible_user authorized_keys] ********************
changed: [64.227.24.140]
changed: [64.227.20.243]
changed: [64.227.23.43]

PLAY RECAP ******************************************************************
64.227.20.243              : ok=5    changed=4    unreachable=0    failed=0

64.227.23.43               : ok=5    changed=4    unreachable=0    failed=0

64.227.24.140              : ok=5    changed=4    unreachable=0    failed=0
```



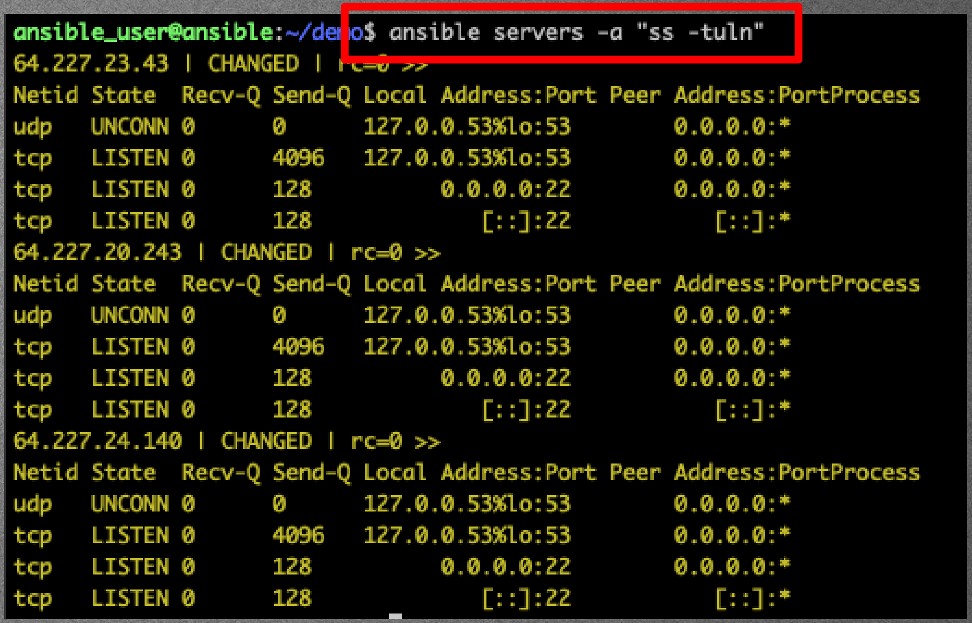
```
ansible_user@ansible:~/demo$ ansible-playbook sshd_hardening-servers.yml

PLAY [Configure SSHD for Ubuntu 20.04, 22.04, and 24.04] *******************

TASK [Gathering Facts] ******************************************************
ok: [64.227.24.140]
ok: [64.227.23.43]
ok: [64.227.20.243]

TASK [Ensure root login is disabled] ****************************************
changed: [64.227.24.140]
changed: [64.227.23.43]
changed: [64.227.20.243]

TASK [Ensure public key authentication is enabled] **************************
changed: [64.227.24.140]
changed: [64.227.23.43]
changed: [64.227.20.243]

TASK [Disable password authentication] **************************************
changed: [64.227.24.140]
changed: [64.227.23.43]
changed: [64.227.20.243]

TASK [Restart SSHD to apply changes] ****************************************
changed: [64.227.24.140]
changed: [64.227.23.43]
changed: [64.227.20.243]

PLAY RECAP ******************************************************************
64.227.20.243              : ok=5    changed=4    unreachable=0    failed=0

64.227.23.43               : ok=5    changed=4    unreachable=0    failed=0

64.227.24.140              : ok=5    changed=4    unreachable=0    failed=0
```

Ad-hoc commands

```
ansible servers -m shell -a “df -h”
ansible servers -a “ss -tuln”
```



```
ansible_user@ansible:~/demo$ ansible servers -m shell -a "df -h"
64.227.23.43 | CHANGED | rc=0 >>
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            46M 1008K   45M   3% /run
/dev/vda1       9.6G  1.7G  7.9G  18% /
tmpfs           228M     0  228M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/vda15      105M  6.1M   99M   6% /boot/efi
tmpfs            46M  4.0K   46M   1% /run/user/1000
64.227.20.243 | CHANGED | rc=0 >>
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            46M 1008K   45M   3% /run
/dev/vda1       9.6G  1.7G  7.9G  18% /
tmpfs           228M     0  228M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/vda15      105M  6.1M   99M   6% /boot/efi
tmpfs            46M  4.0K   46M   1% /run/user/1000
64.227.24.140 | CHANGED | rc=0 >>
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            46M 1008K   45M   3% /run
/dev/vda1       9.6G  1.7G  7.9G  18% /
tmpfs           228M     0  228M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/vda15      105M  6.1M   99M   6% /boot/efi
tmpfs            46M  4.0K   46M   1% /run/user/1000
```



```
ansible_user@ansible:~/demo$ ansible servers -a "ss -tuln"
64.227.23.43 | CHANGED | rc=0 >>
Netid State  Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0      127.0.0.53%lo:53        0.0.0.0:*
tcp   LISTEN 0      4096   127.0.0.53%lo:53        0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128             [::]:22           [::]:*
64.227.20.243 | CHANGED | rc=0 >>
Netid State  Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0      127.0.0.53%lo:53        0.0.0.0:*
tcp   LISTEN 0      4096   127.0.0.53%lo:53        0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128             [::]:22           [::]:*
64.227.24.140 | CHANGED | rc=0 >>
Netid State  Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
udp   UNCONN 0      0      127.0.0.53%lo:53        0.0.0.0:*
tcp   LISTEN 0      4096   127.0.0.53%lo:53        0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:22        0.0.0.0:*
tcp   LISTEN 0      128             [::]:22           [::]:*
```

Summary

- DevOps is awesome!
- Many demos and tutorials skip over how to set up a secure environment for Ansible
  - SSH & GPG Keys
  - SSH-Agent
  - GPG-Agent
  - `pass` – The Unix Password Manager
  - Ansible Vault

Questions?

CONTACT:
jkirch (at) tcc dot edu