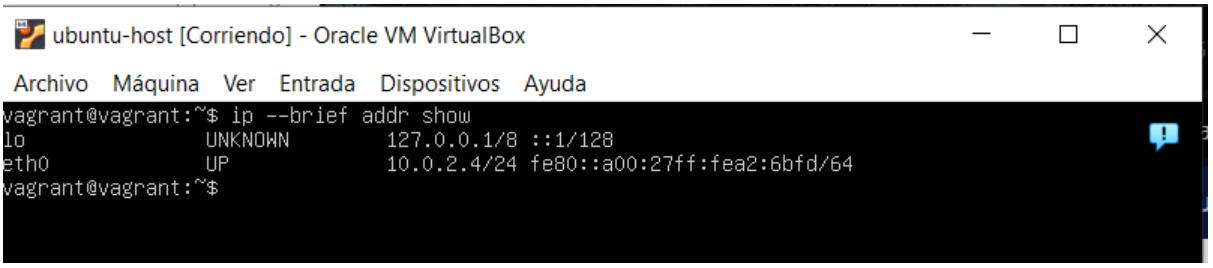
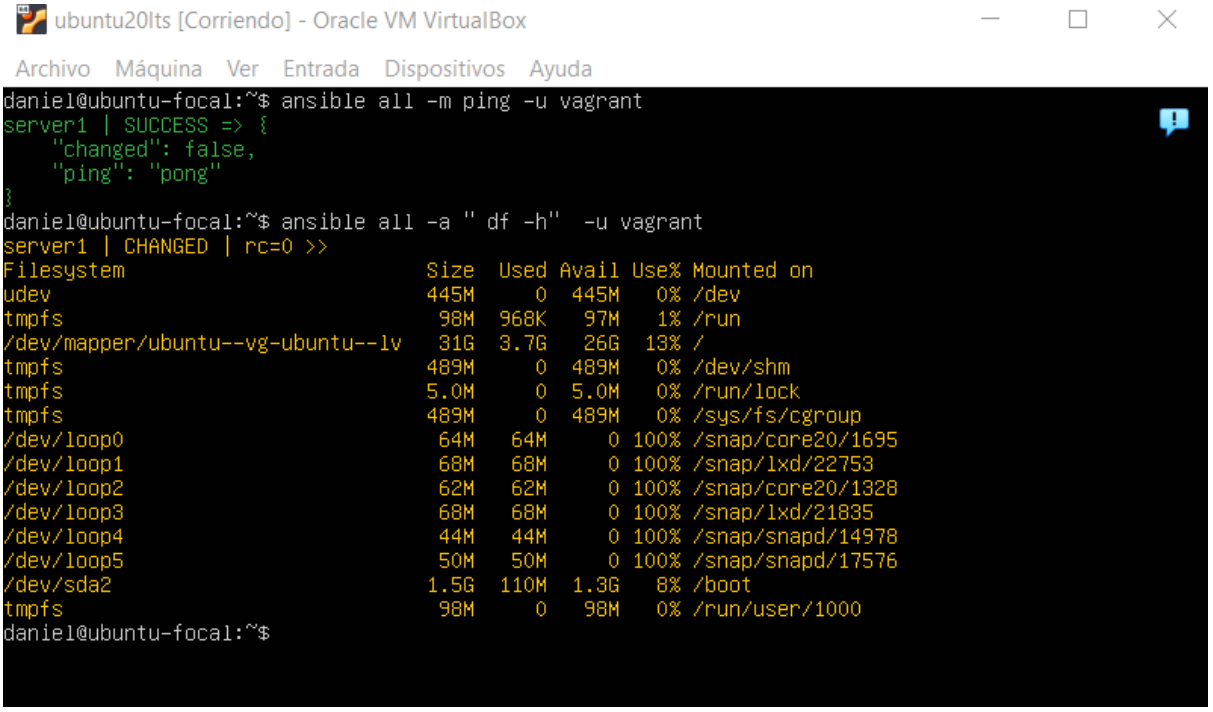
Ansible

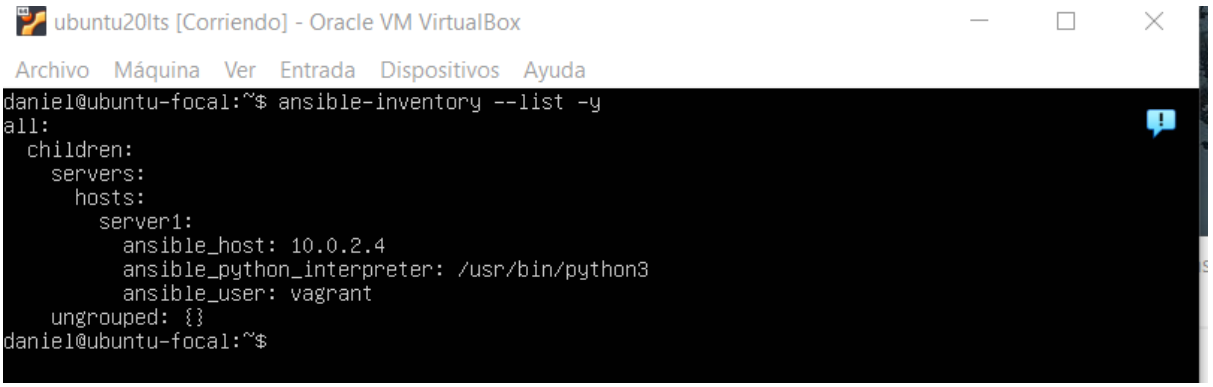
host ip address



Connection from control node to host



ansible inventory file



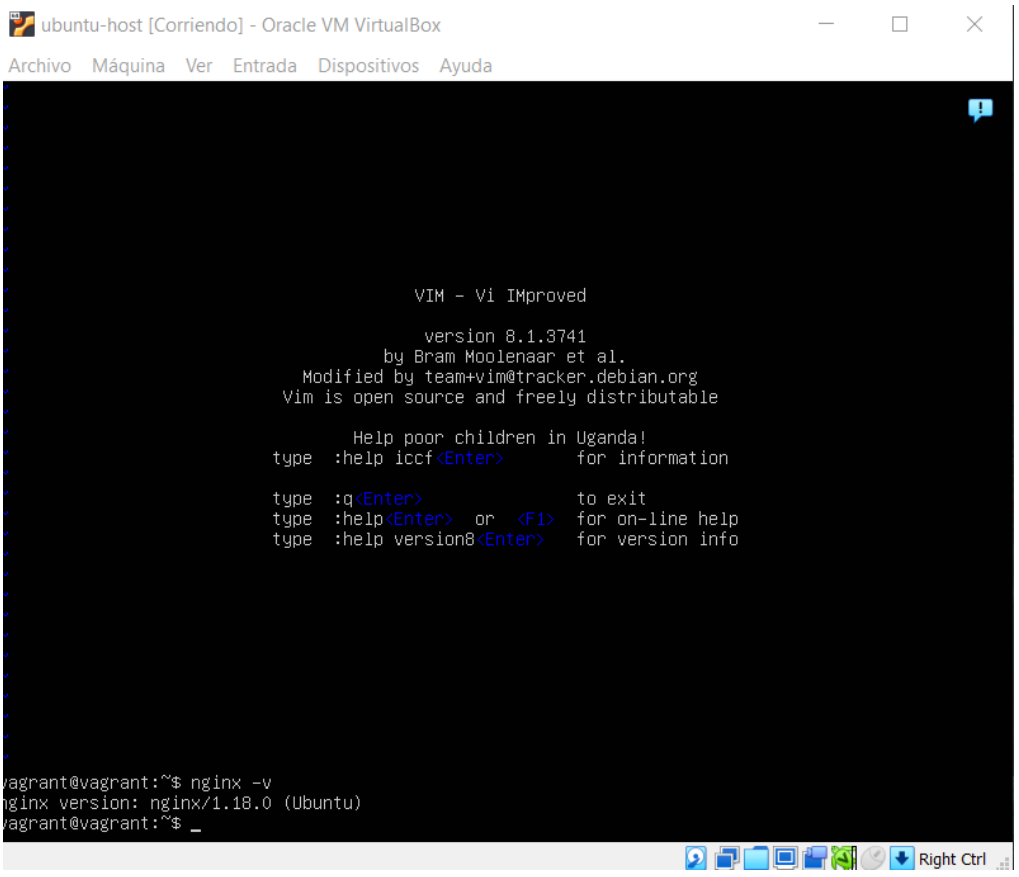
ansible playbook

```
daniel@ubuntu-focal:/etc/ansible$ cat playbook.yml
---
- hosts: servers
  become: true
  tasks:
    - name: Install packages
      apt: name={{item}} update_cache=yes state=latest
      loop: [ 'nginx', 'vim' ]
      tags: ['setup']

daniel@ubuntu-focal:/etc/ansible$ _
```

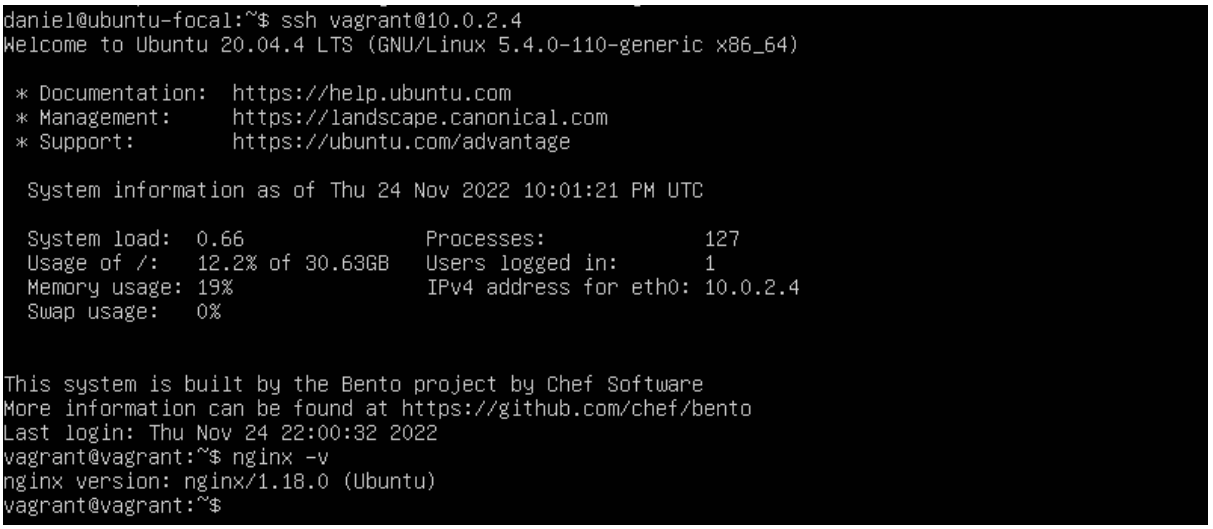
playbook execution

```
daniel@ubuntu-focal:/etc/ansible$ ansible-playbook -i hosts playbook.yml

PLAY [servers] ***************************************************************************************************

TASK [Gathering Facts] *******************************************************************************************
ok: [server1]

TASK [Install packages] ******************************************************************************************
changed: [server1] => (item=nginx)
changed: [server1] => (item=vim)

PLAY RECAP *******************************************************************************************************
server1                    : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=
0    ignored=0

daniel@ubuntu-focal:/etc/ansible$ _
```

packages installed on host



ssh connection from control node to host



PKI

Es una tecnología para autenticar usuarios y dispositivos en el mundo digital. Básicamente se tiene una o más aportes firman que una clave criptográfica pertenece a un usuario o dispositivo. Esta llave luego puede servir para identificar al usuario en redes digitales.

Depende de firmas digitales que utilizan criptografía de clave pública. Aqui, la clave secreta de cada entidad(usuario o dispositivo) solo la conoce esa entidad y la usa para firmar, esta es la llave privada.

SSH

Secure Shell es un protocolo de que facilita la comunicación segura entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. SSH encripta la sesión de conexión, por lo que es imposible que alguien pueda obtener contraseñas no encriptadas. Da un mecanismo para autenticar un usuario remoto, llevar entradas desde el cliente al host y devolverlas al cliente.