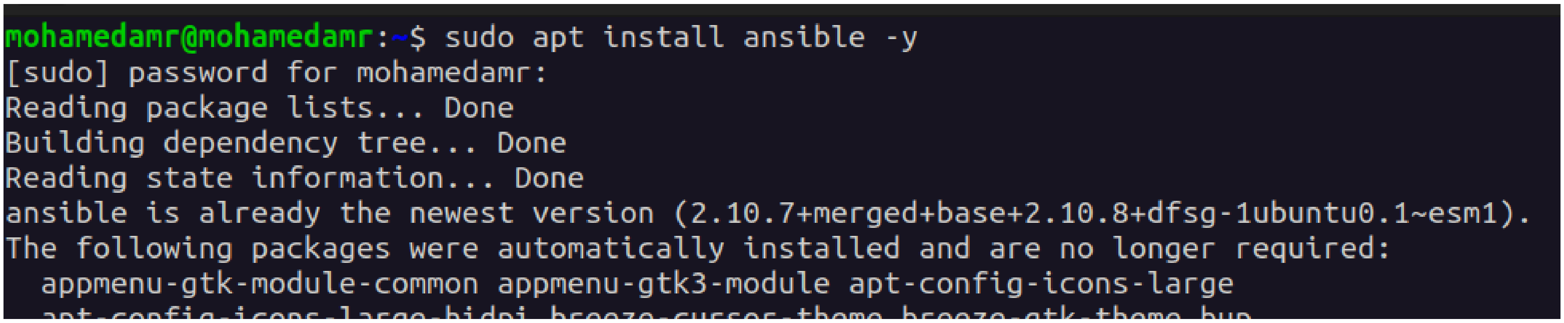
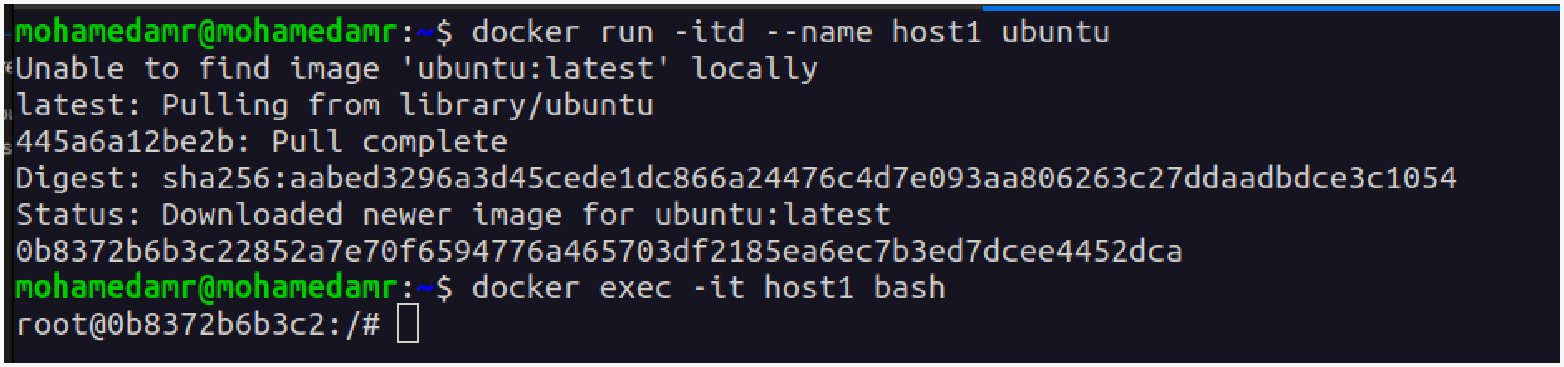
Install ansible



```
mohamedamr@mohamedamr:~$ sudo apt install ansible -y
[sudo] password for mohamedamr:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ansible is already the newest version (2.10.7+merged+base+2.10.8+dfsg-1ubuntu0.1~esm1).
The following packages were automatically installed and are no longer required:
  appmenu-gtk-module-common appmenu-gtk3-module apt-config-icons-large
  apt-config-icons-large-hidpi breeze-cursor-theme breeze-gtk-theme bup
```

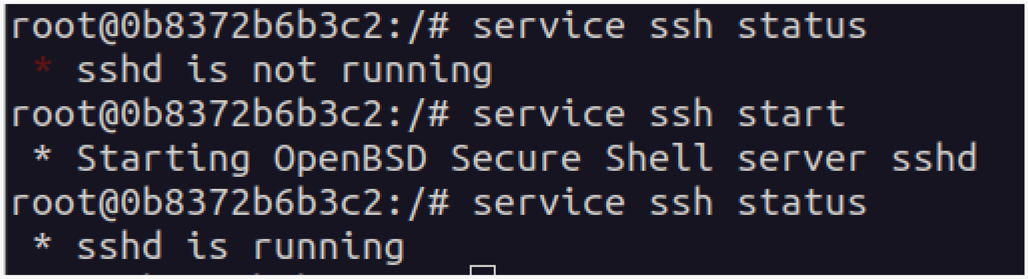
Create a new user on control machine and new user on host 1

Create a Docker Container for Host 1



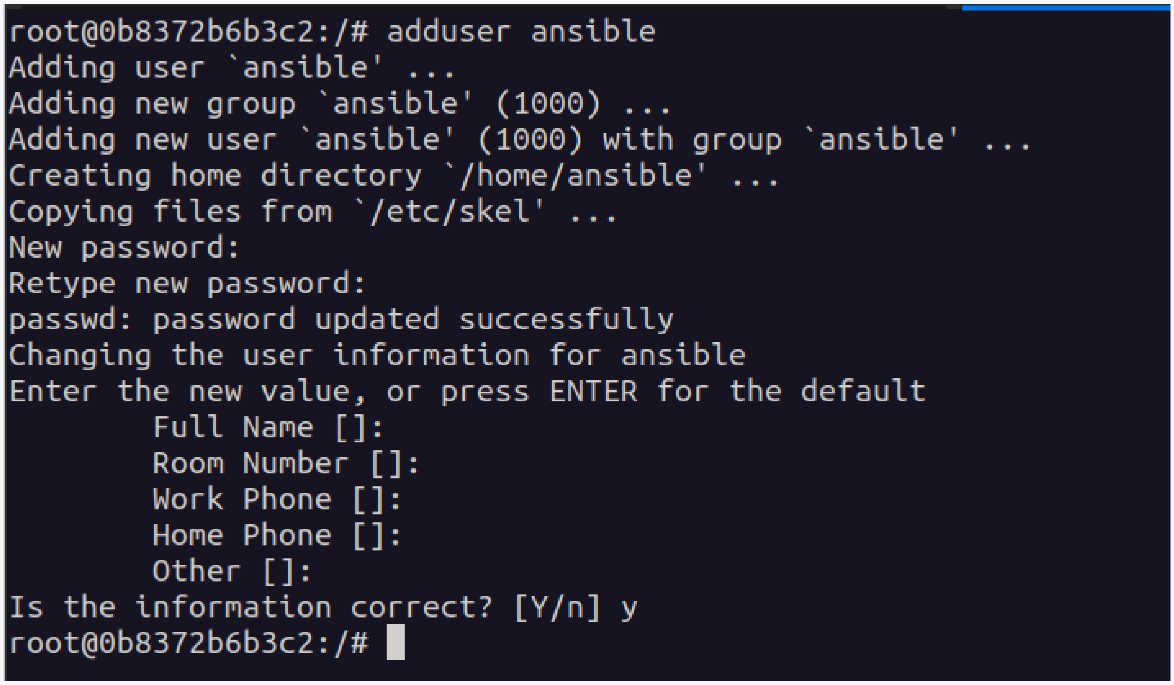
```
mohamedamr@mohamedamr:~$ docker run -itd --name host1 ubuntu
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
445a6a12be2b: Pull complete
Digest: sha256:aabed3296a3d45cede1dc866a24476c4d7e093aa806263c27ddaadbdce3c1054
Status: Downloaded newer image for ubuntu:latest
0b8372b6b3c22852a7e70f6594776a465703df2185ea6ec7b3ed7dcee4452dca
mohamedamr@mohamedamr:~$ docker exec -it host1 bash
root@0b8372b6b3c2:/#
```

Update and install SSH on the Container



```
root@0b8372b6b3c2:/# service ssh status
 * sshd is not running
root@0b8372b6b3c2:/# service ssh start
 * Starting OpenBSD Secure Shell server sshd
root@0b8372b6b3c2:/# service ssh status
 * sshd is running
```

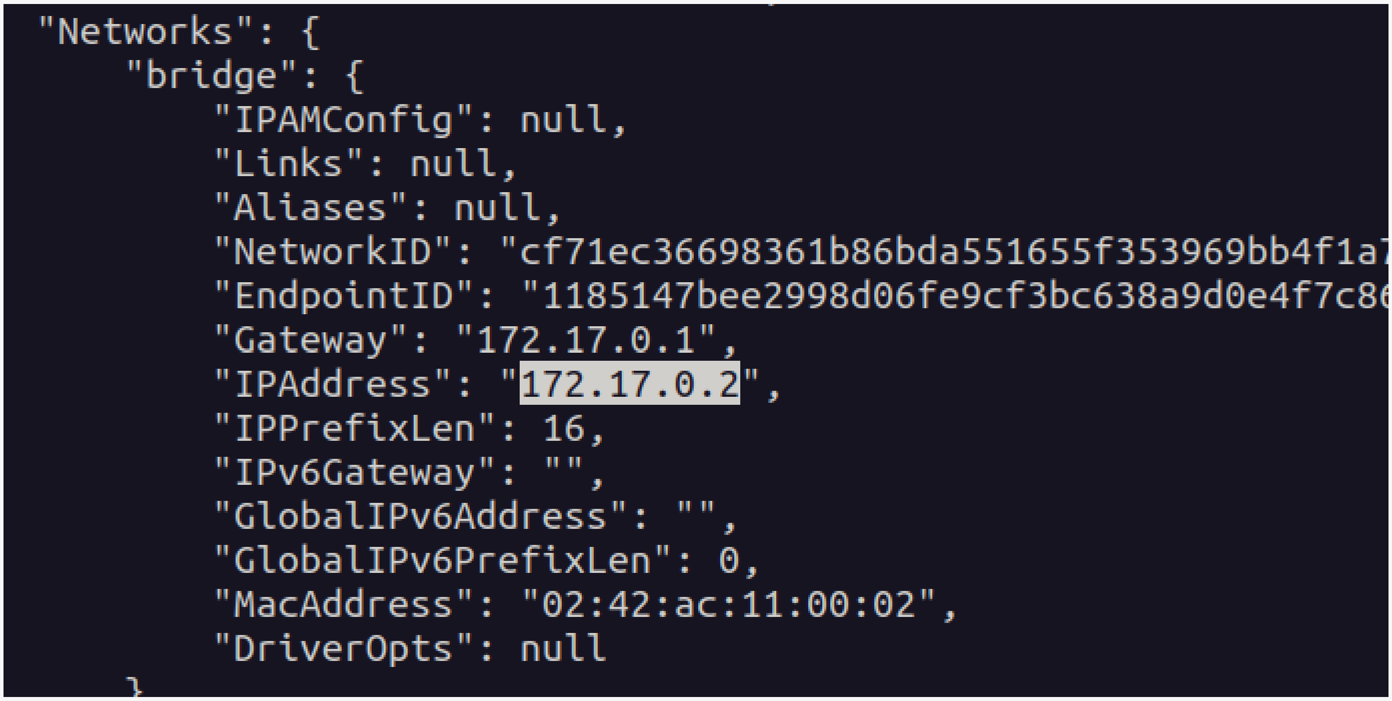
User “ansible” creation on the Container “host1”



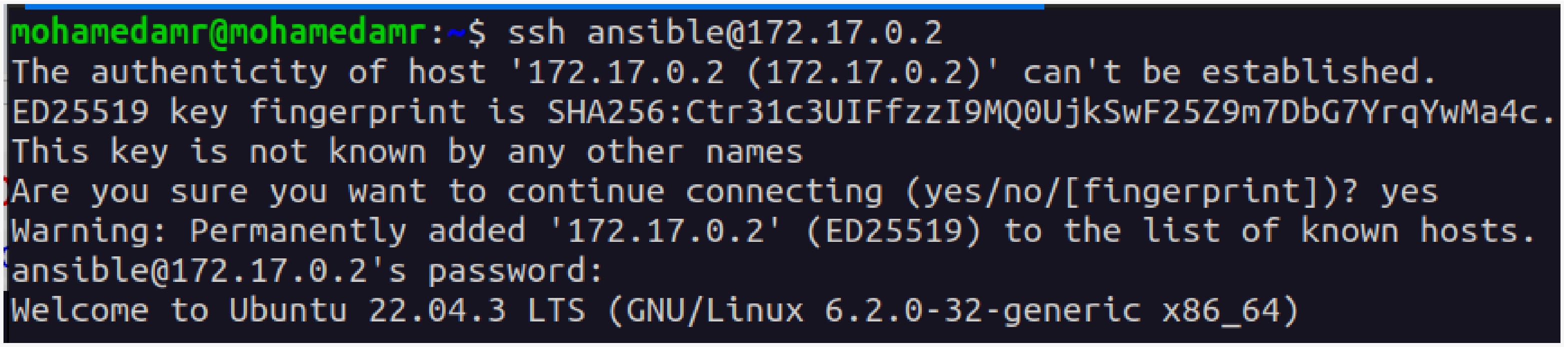
```
root@0b8372b6b3c2:/# adduser ansible
Adding user `ansible' ...
Adding new group `ansible' (1000) ...
Adding new user `ansible' (1000) with group `ansible' ...
Creating home directory `/home/ansible' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ansible
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@0b8372b6b3c2:/#
```

Make sure you can ssh into host 1 (using password)

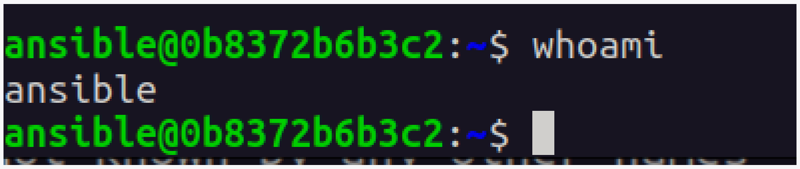
Getting the ip of host1



```
 "Networks": {
     "bridge": {
         "IPAMConfig": null,
         "Links": null,
         "Aliases": null,
         "NetworkID": "cf71ec36698361b86bda551655f353969bb4f1a7
         "EndpointID": "1185147bee2998d06fe9cf3bc638a9d0e4f7c8
         "Gateway": "172.17.0.1",
         "IPAddress": "172.17.0.2",
         "IPPrefixLen": 16,
         "IPv6Gateway": "",
         "GlobalIPv6Address": "",
         "GlobalIPv6PrefixLen": 0,
         "MacAddress": "02:42:ac:11:00:02",
         "DriverOpts": null
     }
```

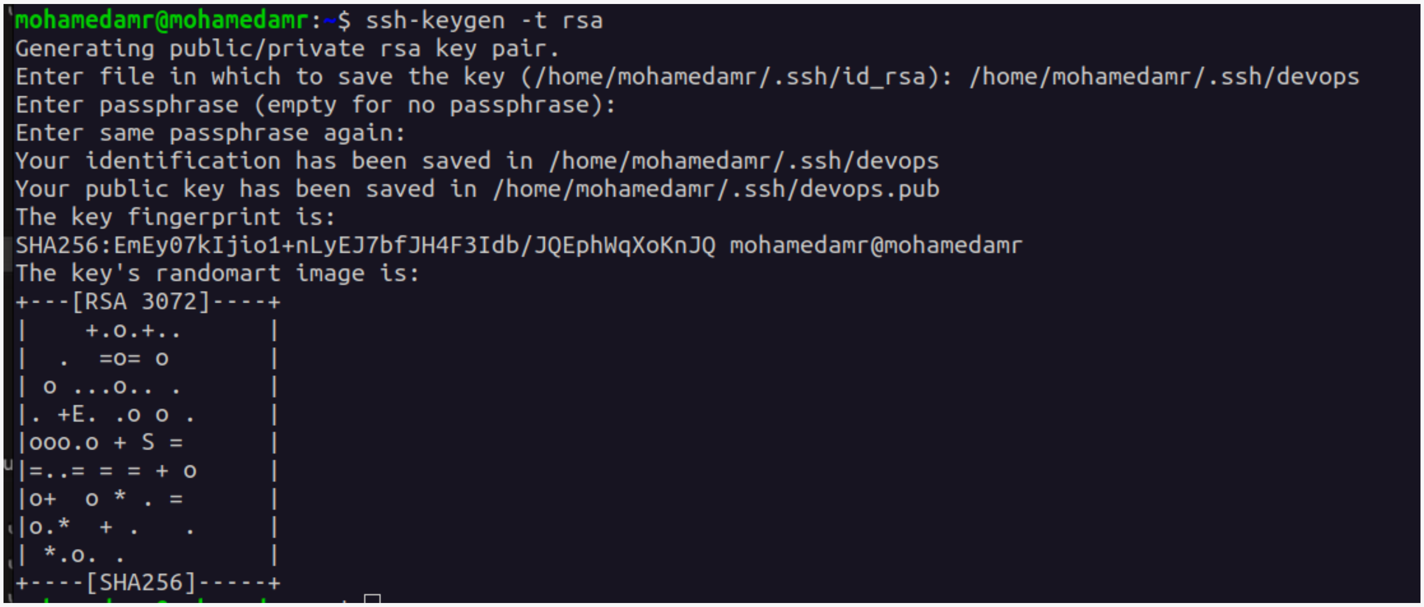


```
mohamedamr@mohamedamr:~$ ssh ansible@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:Ctr31c3UIFfzzI9MQ0UjkSwF25Z9m7DbG7YrqYwMa4c.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
ansible@172.17.0.2's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-32-generic x86_64)
```



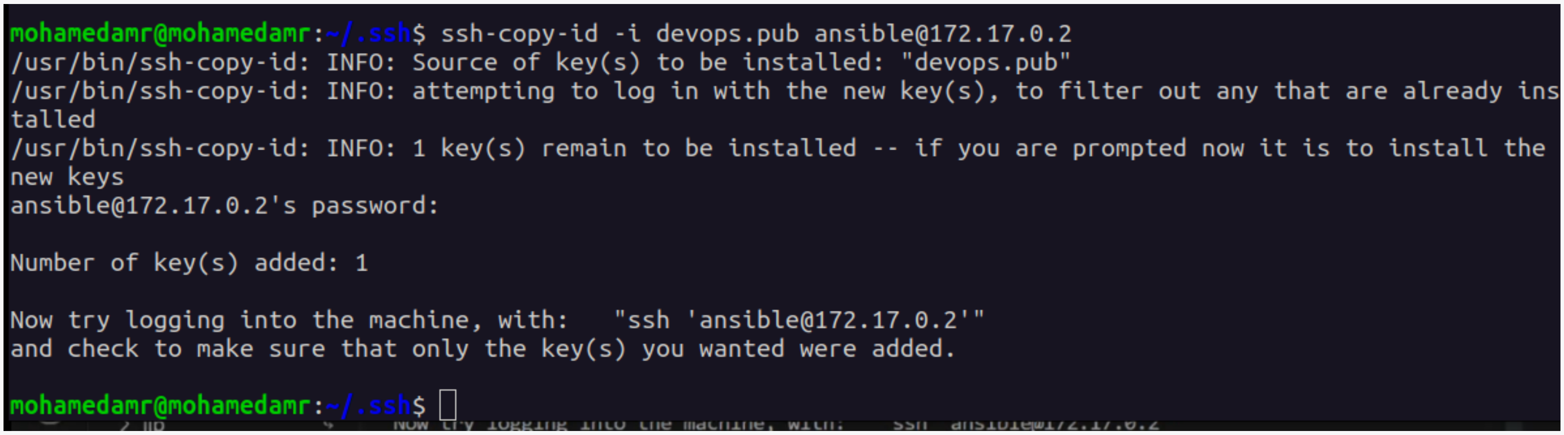
```
ansible@0b8372b6b3c2:~$ whoami
ansible
ansible@0b8372b6b3c2:~$
```

Generate SSH key pair on control machine



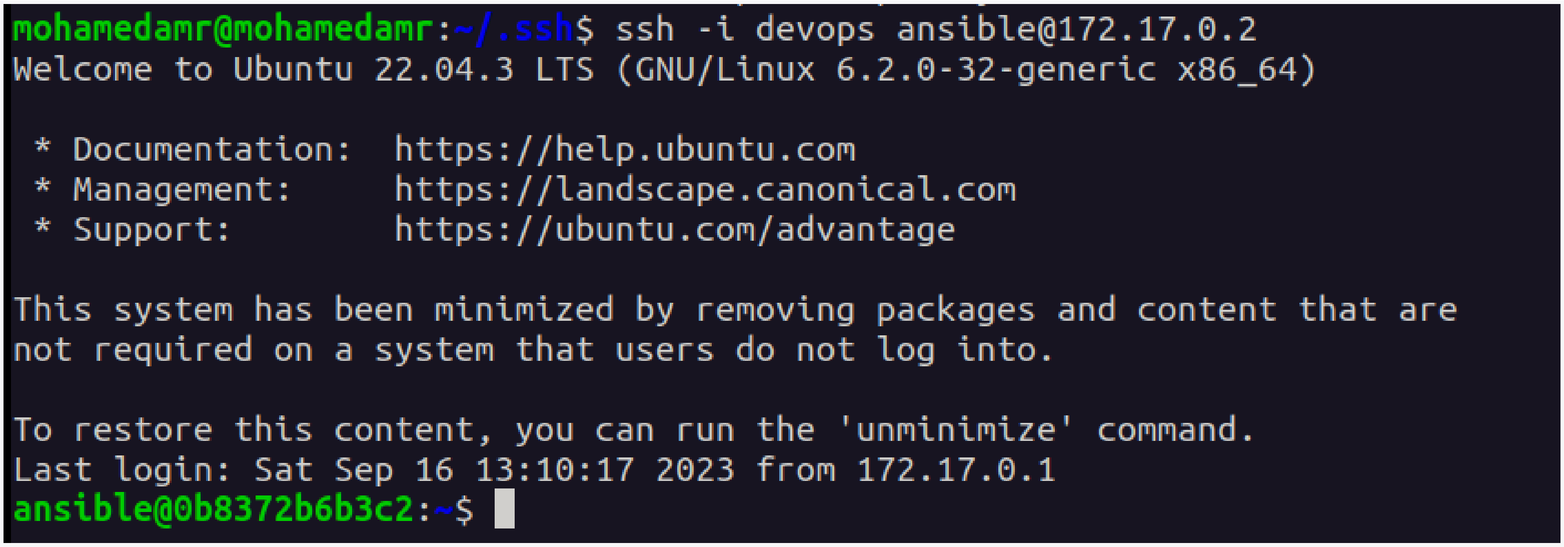
```
mohamedamr@mohamedamr:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mohamedamr/.ssh/id_rsa): /home/mohamedamr/.ssh/devops
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mohamedamr/.ssh/devops
Your public key has been saved in /home/mohamedamr/.ssh/devops.pub
The key fingerprint is:
SHA256:EmEy07kIjio1+nLyEJ7bfJH4F3Idb/JQEphWqXoKnJQ mohamedamr@mohamedamr
The key's randomart image is:
+---[RSA 3072]----+
|    +.o.+..      |
|  .  =o= o       |
| o ...o.. .      |
|. +E. .o o .     |
|ooo.o + S =      |
|=..= = = + o     |
|o+  o * . =      |
|o.*  + .   .     |
| *.o. .          |
+----[SHA256]-----+
```

Copy the public key to host 1



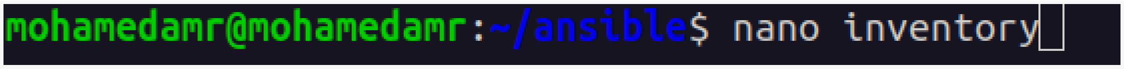
```
mohamedamr@mohamedamr:~/.ssh$ ssh-copy-id -i devops.pub ansible@172.17.0.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "devops.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already ins
talled
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the
new keys
ansible@172.17.0.2's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'ansible@172.17.0.2'"
and check to make sure that only the key(s) you wanted were added.

mohamedamr@mohamedamr:~/.ssh$ 
```

Make sure you can ssh into host 1 (using prv/pub)



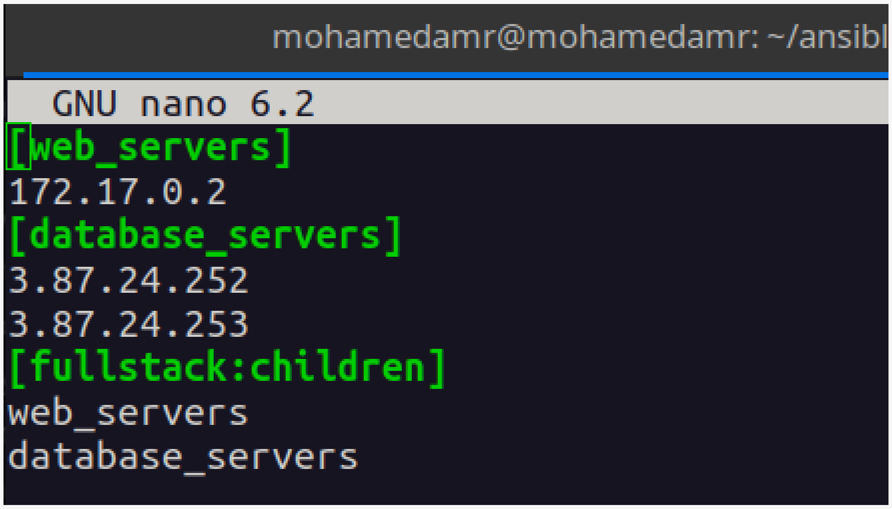
```
mohamedamr@mohamedamr:~/.ssh$ ssh -i devops ansible@172.17.0.2
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-32-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 16 13:10:17 2023 from 172.17.0.1
ansible@0b8372b6b3c2:~$ 
```

-Create the inventory file



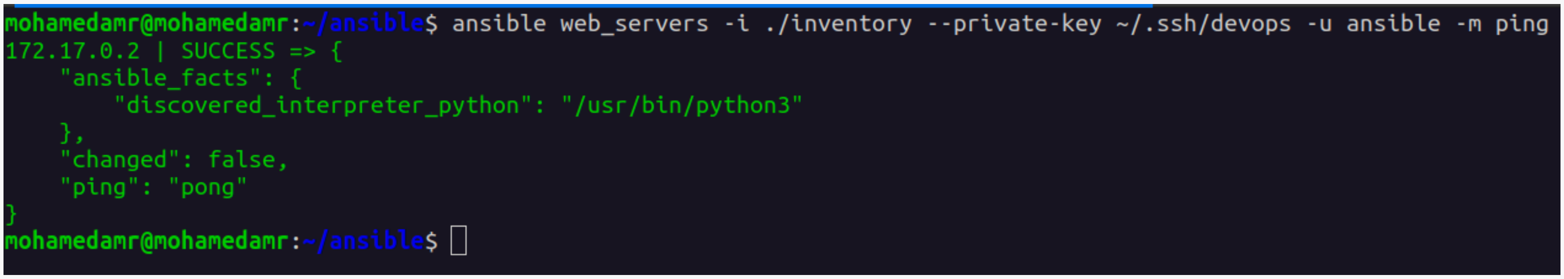
```
mohamedamr@mohamedamr:~/ansible$ nano inventory
```

-Put the IP of host 1 in the inventory file



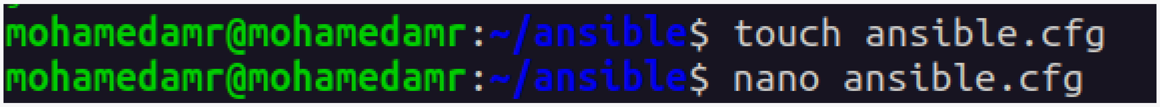
```
[web_servers]
172.17.0.2
[database_servers]
3.87.24.252
3.87.24.253
[fullstack:children]
web_servers
database_servers
```

Use the inventory file path in your ad-hoc command instead of using the IP hard-coded



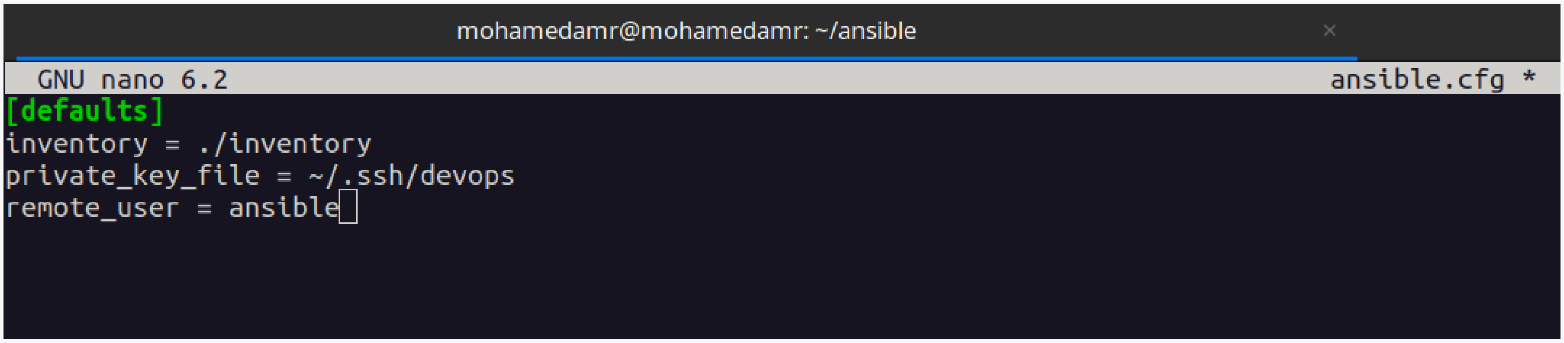
```
mohamedamr@mohamedamr:~/ansible$ ansible web_servers -i ./inventory --private-key ~/.ssh/devops -u ansible -m ping
172.17.0.2 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
mohamedamr@mohamedamr:~/ansible$
```

-Create the configuration file



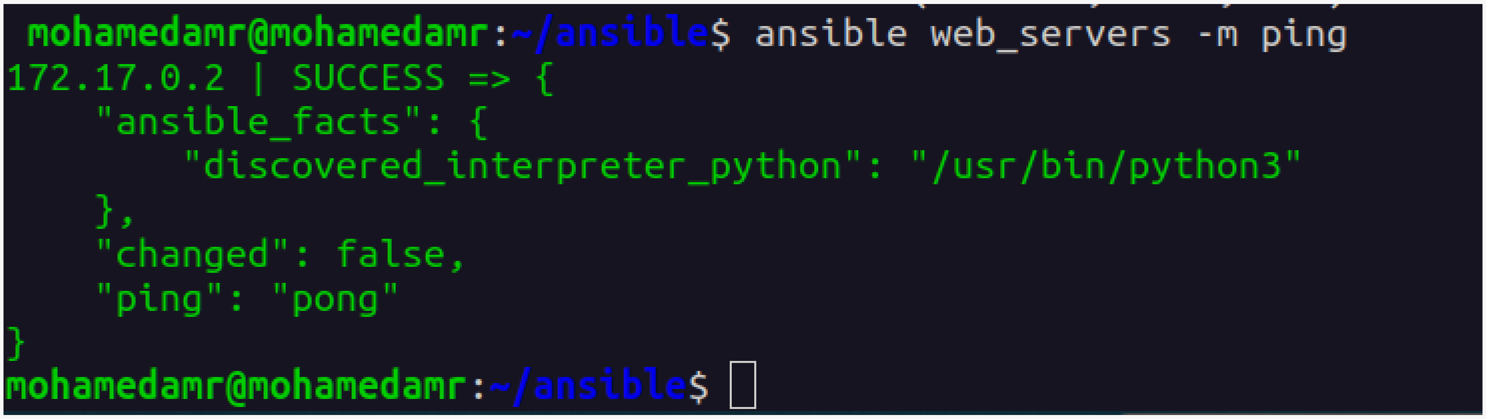
```
mohamedamr@mohamedamr:~/ansible$ touch ansible.cfg
mohamedamr@mohamedamr:~/ansible$ nano ansible.cfg
```

-Insert some values in the configuration file



```
mohamedamr@mohamedamr: ~/ansible
  GNU nano 6.2                                                          ansible.cfg *
[defaults]
inventory = ./inventory
private_key_file = ~/.ssh/devops
remote_user = ansible
```

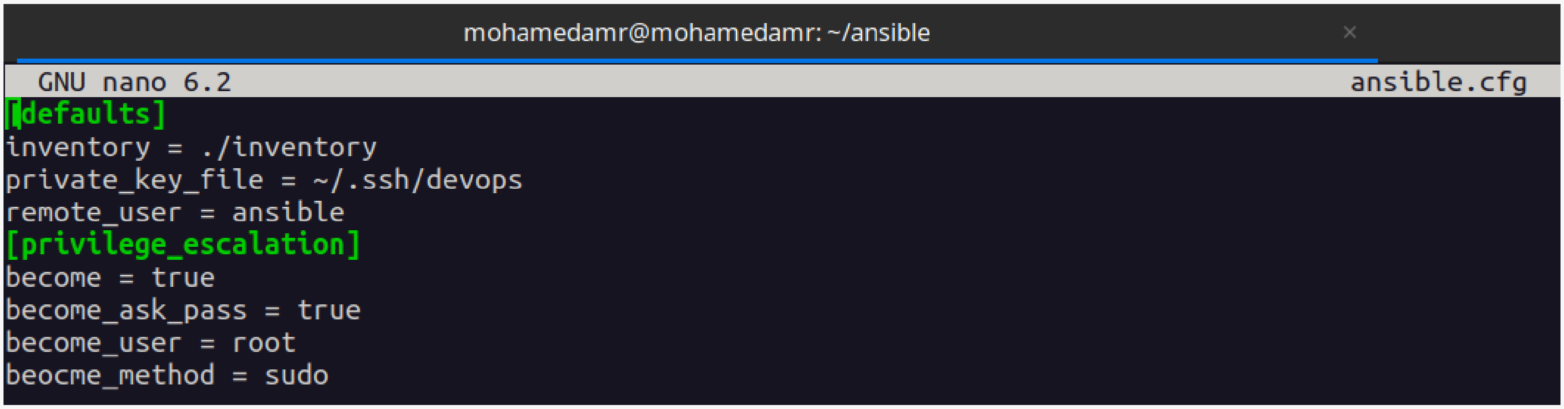
Run the minimized ad-hoc command



```
mohamedamr@mohamedamr:~/ansible$ ansible web_servers -m ping
172.17.0.2 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
mohamedamr@mohamedamr:~/ansible$
```

[AD-HOC COMMAND ESCALATION USING ROOT USER]

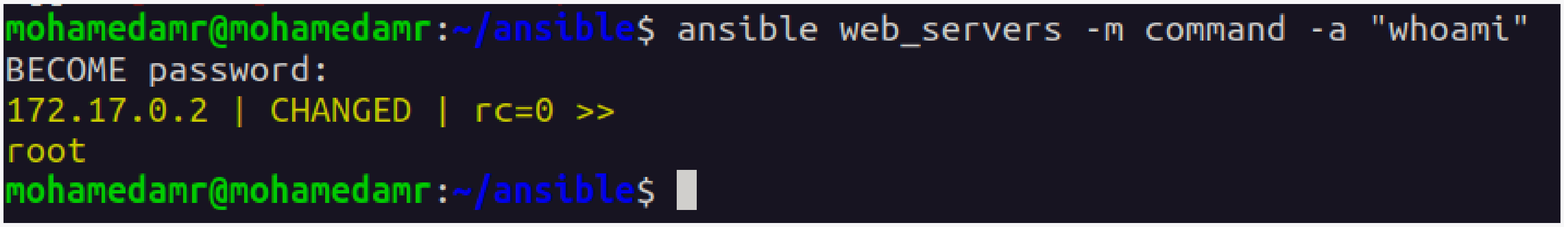
Insert the correct values in the configuration file



```
[defaults]
inventory = ./inventory
private_key_file = ~/.ssh/devops
remote_user = ansible
[privilege_escalation]
become = true
become_ask_pass = true
become_user = root
beocme_method = sudo
```

Example: ansible all -m command -a "whoami"

What is the output of the command ?



```
mohamedamr@mohamedamr:~/ansible$ ansible web_servers -m command -a "whoami"
BECOME password:
172.17.0.2 | CHANGED | rc=0 >>
root
mohamedamr@mohamedamr:~/ansible$
```