

**Name:** Zyad Mohamed Tawfik

**Track:** DevOps SV

**Course:** Ansible - Lab1

## Install ansible

```
ztawfik@ztawfik:~/Desktop$ ansible --version
ansible [core 2.15.4]
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/ztawfik/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3/dist-packages/ansible
  ansible collection location = /home/ztawfik/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/bin/ansible
  python version = 3.10.12 (main, Jun 11 2023, 05:26:28) [GCC 11.4.0] (/usr/bin/python3)
  jinja version = 3.0.3
  libyaml = True
ztawfik@ztawfik:~/Desktop$
```

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

```
ansible@da0a63fbd367: ~
root@da0a63fbd367:/# hostname
da0a63fbd367
root@da0a63fbd367:/# su - ansible
ansible@da0a63fbd367:~$ whoami
ansible
ansible@da0a63fbd367:~$
```

```
ansible@ztawfik: ~
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ su - ansible
Password:
ansible@ztawfik:~$
```

**Name:** Zyad Mohamed Tawfik

**Track:** DevOps SV

**Course:** Ansible - Lab1

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

```
ztawfik@ztawfik: ~/Desktop/ITI/Ansible
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ docker inspect host1 | grep IPAdd
    "SecondaryIPAddresses": null,
    "IPAddress": "172.17.0.2",
    "IPAddress": "172.17.0.2",
ztawfik@ztawfik:~/Desktop/ITI/Ansible$
```

```
ansible@da0a63fbd367: ~/.ssh
ansible@da0a63fbd367:~$ cd ~/.ssh/
ansible@da0a63fbd367:~/.ssh$ ll
total 12
drwx----- 2 ansible ansible 4096 Sep 15 09:29 ./
drwxr-x--- 4 ansible ansible 4096 Sep 15 09:29 ../
-rw----- 1 ansible ansible 741 Sep 15 09:29 authorized_keys
ansible@da0a63fbd367:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQCJz+v0ZwxU8/g7W2Cxyx4DJIV5EWSHSTZ0FZLzCMcZBY0Lfdtip1eGQ4kMvWxuxqPQzKd5yIrcbkSQk4n3YIa1n/EdHK5HmQXP4/OTETfAkCA5id48gFb680/nxCRXnr7PcIk1P1XeLLQ2fEAK90ldqZnRdDppRgrLVnaz+hi71v6+Mc+Kw3tbUkmOeJH0DVntnic67yzA02BlwM+UIH+r9hcChWtaR80/jwpUBLmtMs8KPrtvAd3e00Rq94c3dfpraaffq+Xlh5S73fQeh0pcP5J9mABjx6pbsKx9aIbC2f4ASMDcJlLoWz0Q+lBc3yNfxRNJ/jc5WNCRUJQ5TWCyOMFSeLCQf4WAJQ4bVzQpJzR6eUFktYnzO1GfL89900WFldv6dasDo02lmAPkH0+4XeK2xnBeT7bQ8f57mRU4VP51BSGL2ECW47mXMOxDKqQLwLxjoNhwyXNNb8la5JZvcKyEHC7LNPscUDyfhBnUd8SjmoSr9zfVvyBv6K8QexFdHu63KKM/ocR34lyCTsrJ7Rs6NOGk8nSY8Zp2zqHlFm1ac1/9+mB9wZ70qBfqEFyckj5S9uj40jIsEr/mFodyN3ucS+70Pov5EGnzKyWen8pnPUMyV3RXpr2qZWHA82jnnTfQ2usdIvK05+Tym0vQ7Vd6Yn7rUtGST0gn0UQ== ztawfik@ztawfik
ansible@da0a63fbd367:~/.ssh$
```

```
ansible@da0a63fbd367: ~
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ 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:/8tzDM9zgivLzc+RRlc1j9BTTxyZc/ymWzhiUtZYBe4.
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)

 * 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ansible@da0a63fbd367:~$
```

**Name:** Zyad Mohamed Tawfik

**Track:** DevOps SV

**Course:** Ansible - Lab1

Generate SSH key pair on control machine

Copy the public key to host 1

```
ztawfik@ztawfik: ~/Desktop/ITI/Ansible
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ztawfik/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ztawfik/.ssh/id_rsa
Your public key has been saved in /home/ztawfik/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:PnW9KthK57I9TB9YeM0yc0cLJ1CH3mFV6xP+WWKhCNA ztawfik@ztawfik
The key's randomart image is:
+---[RSA 4096]-----+
|  ..  .+.+. |
| .E . .o . |
|  . = o.+ |
| .o.Oo*.. |
| S o*o*+=. |
| . .=.o.Oo= |
| +=.+ o... |
| .o== .. |
| o+oo. |
+---[SHA256]-----+
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ls ~/.ssh/
id_rsa id_rsa.pub known_hosts known_hosts.old
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ssh-copy-id ansible@172.17.0.2
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/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.
```

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

```
ansible@da0a63fbd367: ~
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ls ~/.ssh/
id_rsa id_rsa.pub known_hosts known_hosts.old
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ssh -i ~/.ssh/id_rsa 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: Fri Sep 15 09:21:15 2023 from 172.17.0.1
ansible@da0a63fbd367:~$
```

**Name:** Zyad Mohamed Tawfik

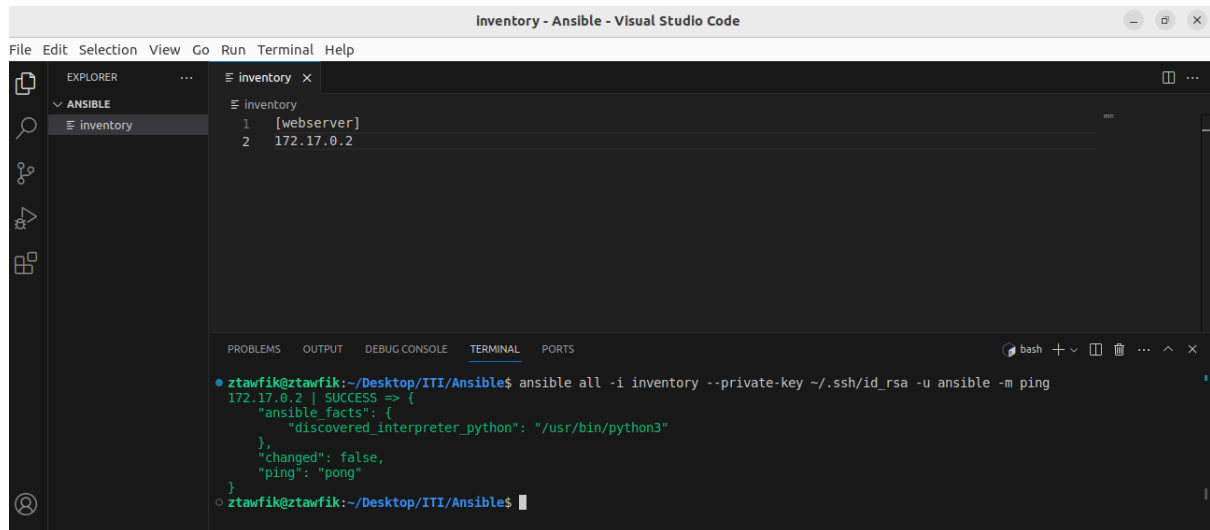
**Track:** DevOps SV

**Course:** Ansible - Lab1

Create the inventory file

Put the IP of host 1 in the inventory file

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



The screenshot shows the Visual Studio Code interface with the 'inventory' file open in the editor. The file contains two hosts: '1' with role 'webserver' and '2' with IP '172.17.0.2'. The terminal window shows the command `ansible all -i inventory --private-key ~/.ssh/id_rsa -u ansible -m ping` being executed. The output shows that the ping was successful for both hosts, with the first host returning 'pong'.

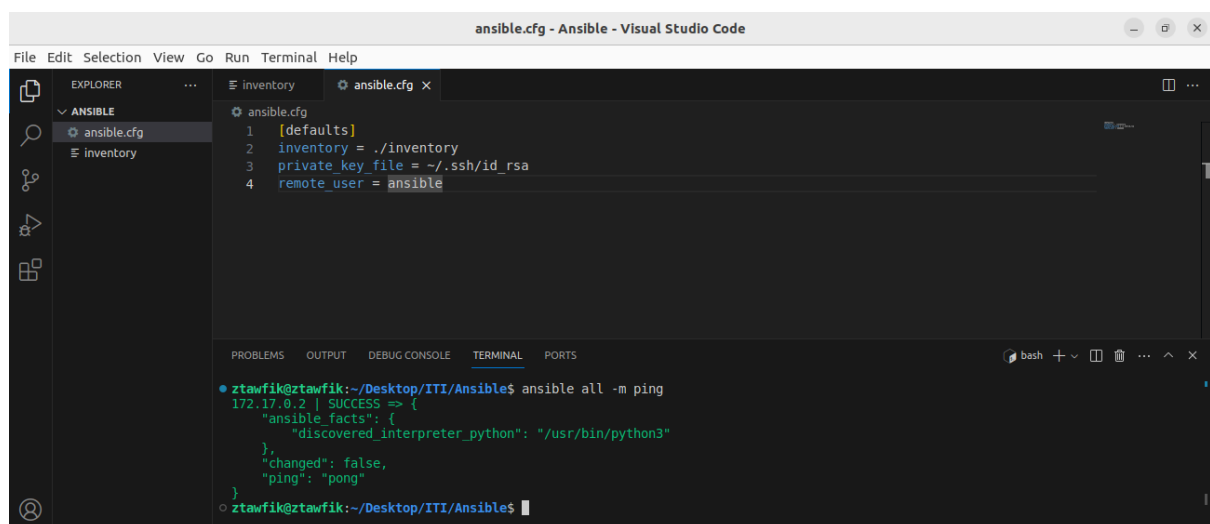
```
inventory
1 [webserver]
2 172.17.0.2

ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ansible all -i inventory --private-key ~/.ssh/id_rsa -u ansible -m ping
172.17.0.2 | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
ztawfik@ztawfik:~/Desktop/ITI/Ansible$
```

Create the configuration file

Insert some values in the configuration file

Run the minimised ad-hoc command



The screenshot shows the Visual Studio Code interface with the 'ansible.cfg' file open in the editor. The file contains the following configuration: `[defaults]`, `inventory = ./inventory`, `private_key_file = ~/.ssh/id_rsa`, and `remote_user = ansible`. The terminal window shows the command `ansible all -m ping` being executed. The output shows that the ping was successful for both hosts, with the first host returning 'pong'.

```
ansible.cfg
[defaults]
inventory = ./inventory
private_key_file = ~/.ssh/id_rsa
remote_user = ansible

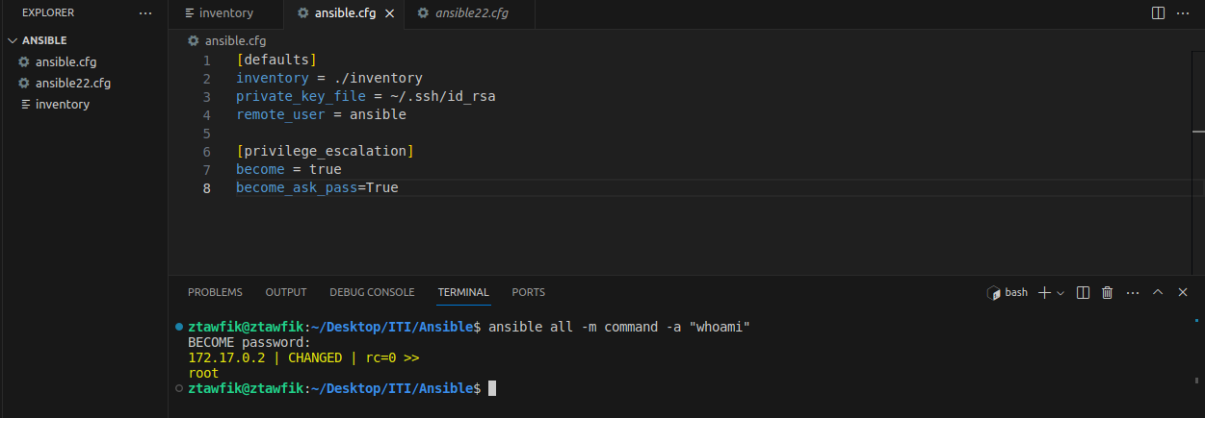
ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ansible all -m ping
172.17.0.2 | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
ztawfik@ztawfik:~/Desktop/ITI/Ansible$
```

**Name:** Zyad Mohamed Tawfik

**Track:** DevOps SV

**Course:** Ansible - Lab1

Insert the correct values in the configuration file for AD-HOC command escalation using root user



The screenshot shows an IDE with a file explorer on the left and a terminal at the bottom. The file explorer shows a project named 'ANSIBLE' with files 'ansible.cfg', 'ansible22.cfg', and 'inventory'. The main editor displays the 'ansible.cfg' file with the following content:

```
1 [defaults]
2 inventory = ./inventory
3 private_key_file = ~/.ssh/id_rsa
4 remote_user = ansible
5
6 [privilege_escalation]
7 become = true
8 become_ask_pass=True
```

The terminal at the bottom shows the command `ansible all -m command -a "whoami"` being executed. The output indicates a successful privilege escalation to the root user:

```
• ztawfik@ztawfik:~/Desktop/ITI/Ansible$ ansible all -m command -a "whoami"
BECOME password:
172.17.0.2 | CHANGED | rc=0 >>
root
○ ztawfik@ztawfik:~/Desktop/ITI/Ansible$
```