

Ansible – Lab1

Toka Farid Shawki

ITI- DevOps Track

Instructors: Mostafa Yehia & Ahmed Nabil

## INSTALLING ANSIBLE & PREPARING SSH

### 1. Install ansible.

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
E: The repository 'http://apt.kubernetes.io kubernetes-xenial InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: The repository 'https://ppa.launchpadcontent.net/deluge-team/ppa/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: The repository 'https://ppa.launchpadcontent.net/ubuntu-wine/ppa/ubuntu jammy Release' does not have a Release file.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
● toka-farid@localhost:~$ sudo apt install ansible
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-1).
0 upgraded, 0 newly installed, 0 to remove and 24 not upgraded.
● toka-farid@localhost:~$
```

### 2. Create a new user on the control machine and a new user on host 1. new user on the control machine:

```
● toka-farid@localhost:~$ sudo adduser control-host
[sudo] password for toka-farid:
Adding user 'control-host' ...
Adding new group 'control-host' (1002) ...
Adding new user 'control-host' (1002) with group 'control-host' ...
Creating home directory '/home/control-host' ...
Copying files from '/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for control-host
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
● toka-farid@localhost:~$
```

### new user on host 1:

```
● toka-farid@localhost:~$ sudo docker run --name host1 -itd ubuntu
e50958a3db98782ae30b12fb38d9de879b9aeb4e48894b837124048810768cf74
● toka-farid@localhost:~$ sudo docker exec -it host1 bash
root@e50958a3db98:/# apt update -y
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security amd64 Packages [270 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy InRelease [246 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [246 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [246 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy amd64 Packages [8450 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates amd64 Packages [8450 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-backports amd64 Packages [246 kB]
Fetched 17.5 MB in 10s (1750 kB/s)
Reading package lists... Done
root@e50958a3db98:/# service status
status: unrecognized service
root@e50958a3db98:/# service ssh status
* sshd is not running
root@e50958a3db98:/# service ssh start
* Starting OpenSSH Secure Shell server sshd
[ OK ]
root@e50958a3db98:/# service ssh status
* sshd is running
root@e50958a3db98:/# 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@e50958a3db98:/# su ansible
ansible@e50958a3db98:/# cd
ansible@e50958a3db98:~$ ls -la
. . . .bash_logout .bashrc .profile
ansible@e50958a3db98:~$
```

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

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
toka-farid@localhost:~$ 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:N+HmCQDBM5CSPVTHPy61C0Z0WU+LqEOWRhD/NhtQo8M.
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 22.04.2 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@e50958a3db98:~$
```

4. Generate SSH key pair on a control machine.

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
toka-farid@localhost:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/toka-farid/.ssh/id_rsa): /home/toka-farid/.ssh/devops
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/toka-farid/.ssh/devops
Your public key has been saved in /home/toka-farid/.ssh/devops.pub
The key fingerprint is:
SHA256:Qy41/xa+rDvILLPIGTaDPdY4AD0mSTUiuBLXeCWSAqw toka-farid@localhost
The key's randomart image is:
+----[RSA 3072]-----+
|O=oo.                |
|BB.o.                |
|Bo*   +              |
|E= .   + o           |
|. . . S . .          |
|+ o . . o .          |
|. @ . . . +          |
|+ 0o...o .           |
|+ .o.o+o             |
+----[SHA256]-----+
toka-farid@localhost:~$ cd .ssh
toka-farid@localhost:~/.ssh$ ls
devops      id_ed25519      known_hosts
devops.pub  id_ed25519.pub  known_hosts.old
toka-farid@localhost:~/.ssh$
```

## 5. Copy the public key to host 1.

```
ssh connect to host 172.17.0.2 port 22: connection refused
● toka-farid@localhost:~/.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 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.

● toka-farid@localhost:~/.ssh$
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

ansible@e50958a3db98:/$ cd
ansible@e50958a3db98:~$ ls -a
. .bash_history .bashrc .profile
.. .bash_logout .cache
ansible@e50958a3db98:~$ ls -a
. .bash_history .bashrc .profile
.. .bash_logout .cache .ssh
ansible@e50958a3db98:~$ cd .ssh/
ansible@e50958a3db98:~/.ssh$ ls
authorized_keys
ansible@e50958a3db98:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDKEp55ajFfLTbkNwikYCG340B8Z7rsK/tL9L78j6dhnZggy/+DhbU891aw1A0PnCsI3NFVwKdusOpKpwJ28raFpsHZ9vR7+IU7+oo
477R0ZPHV6i0x1lY/y5px6KrNZU2rkjX3sPX8Tmkv2Y4vWI9df8coI0hYc7xqyNU0xGH1abeFmMNHBYBqWIB4/HtF0dyWwUoMfyu7WteWEonE+JeiBds2iNsP//aF0Px63DmXwuvHk
0Vjj/LY7YgHQwhREp02/LRCSHk3apvjks2073Jkbo3a8nMDqxjLDRGo0jh89x4RBdHmafbcDhqe3/xuMtoVZsNEYShIRxp81l0rHj1rrXf/QxDRVAF+pd3C3PHwgg3yraR+E22SV5op
ioi0mTffmG00RCwT6YwPjQVztIb/2m+0ZBgR0hZlq3RWilho5mzKdA69p2AJRk8vNucopRj7nYemqc4/dCqXatUIFAmxKhcE7EXJ8th/NotBd09/Rp2EiBXgV5qJ0brI/vx+0= tok
a-farid@localhost
ansible@e50958a3db98:~/.ssh$
```

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

```
● toka-farid@localhost:~/.ssh$ ssh -i devops ansible@172.17.0.2
Welcome to Ubuntu 22.04.2 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.

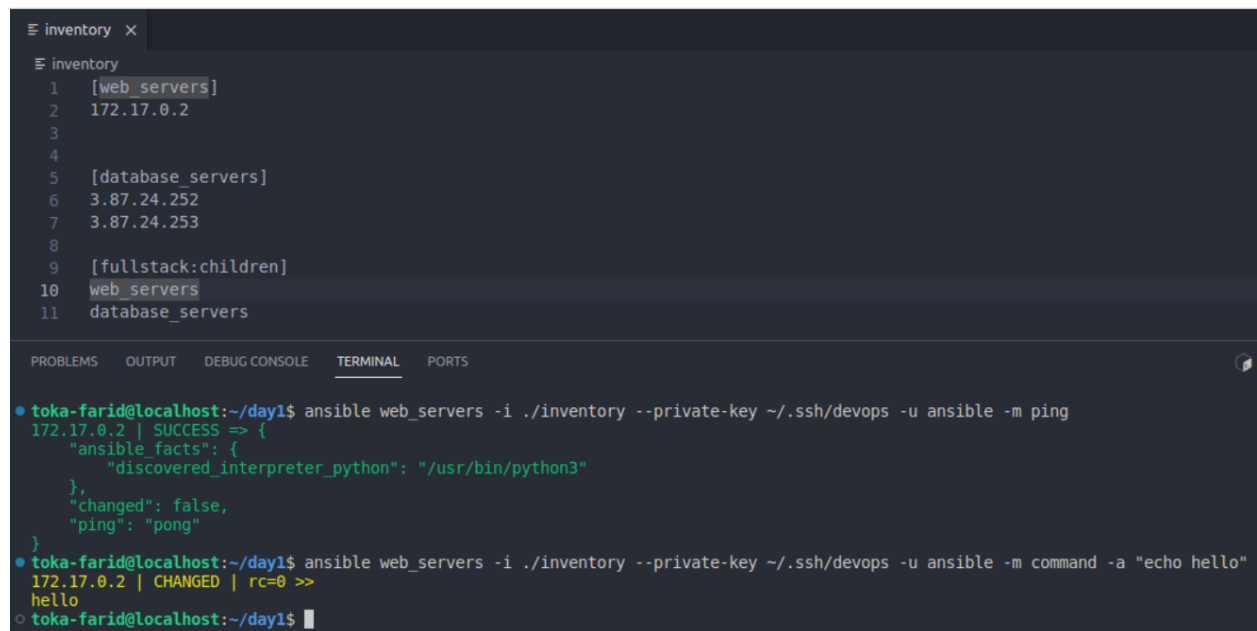
To restore this content, you can run the 'unminimize' command.
Last login: Thu Sep 14 12:22:42 2023 from 172.17.0.1
ansible@e50958a3db98:~$
```

## INVENTORY FILE

1. Create the inventory file.
2. Put the IP of host 1 in the inventory file.
3. Use the inventory file path in your ad-hoc command instead of using the IP hard-coded.

Example:

```
ansible all -i inventory --private-key ~/.ssh/devops -u ubuntu -m ping
```



```
inventory x
inventory
1 [web_servers]
2 172.17.0.2
3
4
5 [database_servers]
6 3.87.24.252
7 3.87.24.253
8
9 [fullstack:children]
10 web_servers
11 database_servers

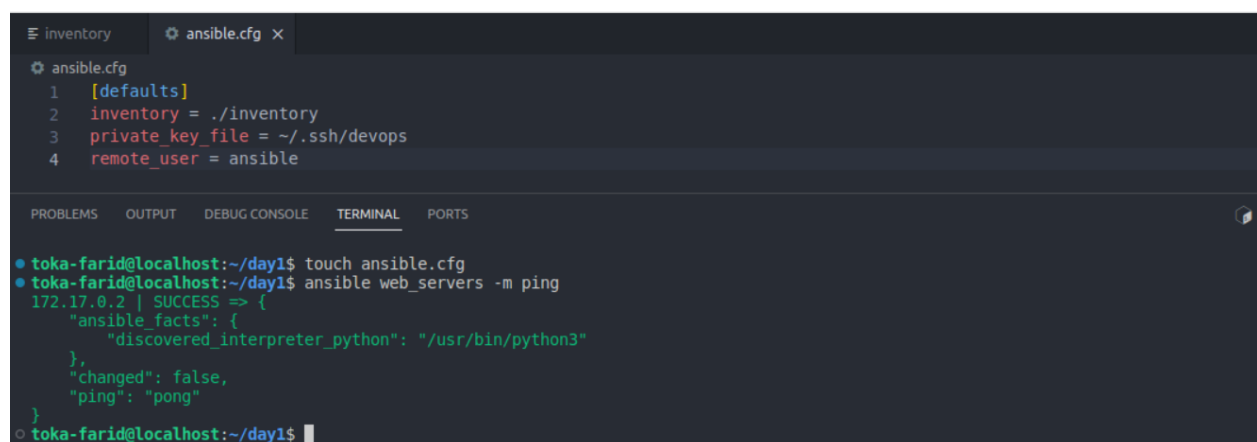
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

• toka-farid@localhost:~/day1$ 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"
}
• toka-farid@localhost:~/day1$ ansible web_servers -i ./inventory --private-key ~/.ssh/devops -u ansible -m command -a "echo hello"
172.17.0.2 | CHANGED | rc=0 >>
hello
• toka-farid@localhost:~/day1$
```

## CONFIGURATION FILE

1. Create the configuration file.
2. Insert some values in the configuration file.
3. Run the minimized ad-hoc command

Example: `ansible all -m ping`



```
inventory x ansible.cfg x
ansible.cfg
1 [defaults]
2 inventory = ./inventory
3 private_key_file = ~/.ssh/devops
4 remote_user = ansible

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

• toka-farid@localhost:~/day1$ touch ansible.cfg
• toka-farid@localhost:~/day1$ ansible web_servers -m ping
172.17.0.2 | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
• toka-farid@localhost:~/day1$
```

## AD-HOC COMMAND ESCALATION USING ROOT USER

1. Insert the correct values in the configuration file.

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

What is the output of the command ?

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

root@e50958a3db98:/# apt install sudo -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sudo
0 upgraded, 1 newly installed, 0 to remove and 8 not upgraded.
Need to get 821 kB of archives.
After this operation, 2568 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 sudo amd64 1.9.9-1ubuntu2.4 [821 kB]
Fetched 821 kB in 4s (207 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package sudo.
(Reading database ... 10378 files and directories currently installed.)
Preparing to unpack .../sudo_1.9.9-1ubuntu2.4_amd64.deb ...
Unpacking sudo (1.9.9-1ubuntu2.4) ...
Setting up sudo (1.9.9-1ubuntu2.4) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@e50958a3db98:/# usermod -aG sudo ansible
root@e50958a3db98:/# su ansible
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ansible@e50958a3db98:/$ sudo apt update
[sudo] password for ansible:
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [993 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [966 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1255 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1235 kB]
Fetched 4787 kB in 4s (1088 kB/s)
Reading package lists... Done
```

```
Inventory  ansible.cfg x
ansible.cfg
1  [defaults]
2  inventory = ./inventory
3  private_key_file = ~/.ssh/devops
4  remote_user = ansible
5
6  [privilege_escalation]
7  become = true

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS
● toka-farid@localhost:~/day1$ ansible web_servers -m command -a "whoami"
172.17.0.2 | CHANGED | rc=0 >>
ansible
● toka-farid@localhost:~/day1$ ansible web_servers -m command -a "whoami" --ask-become-pass
BECOME password:
172.17.0.2 | CHANGED | rc=0 >>
root
○ toka-farid@localhost:~/day1$
```