INSTALLING ANSIBLE & PREPARING SSH

- Install ansible
- Create a new user on control machine and new user on host 1
- Make sure you can ssh into host 1 (using password)
- Generate SSH key pair on control machine
- Copy the public key to host 1
- Make sure you can ssh into host 1 (using prv/pub)

EXPLORER

OPEN EDITORS 1 unsaved

Dockerfile

ANSIBLE

Dockerfile

Dockerfile ●

Dockerfile > ...

```
FROM ubuntu

RUN apt update -y && apt install ssh -y && apt install sudo -y

RUN adduser ansible

RUN echo "ansible:123" | chpasswd

RUN usermod -aG sudo ansible

ENTRYPOINT service ssh restart && bash

# 172.17.0.2
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL bash - .ssh

```
[Mon May 01] @samy: $pwd
/home/samy/Ansible
[Mon May 01] @samy: $ls
Dockerfile
```

```
[Mon May 01] @samy: $sudo docker build -t hosts .
[+] Building 70.0s (9/9) FINISHED
 => [internal] load .dockerignore                                                    0.1s
 => => transferring context: 2B                                                      0.0s
 => [internal] load build definition from Dockerfile                                 0.1s
 => => transferring dockerfile: 300B                                                 0.0s
 => [internal] load metadata for docker.io/library/ubuntu:latest                     0.0s
 => CACHED [1/5] FROM docker.io/library/ubuntu                                       0.0s
 => [2/5] RUN apt update -y && apt install ssh -y && apt install sudo -y            66.9s
 => [3/5] RUN adduser ansible                                                        0.4s
 => [4/5] RUN echo "ansible:123" | chpasswd                                          0.3s
 => [5/5] RUN usermod -aG sudo ansible                                               0.4s
 => exporting to image                                                               1.9s
 => => exporting layers                                                              1.9s
 => => writing image sha256:23e531237fd0c1280e67eb6f3908c51baa293885bb75c381b11ac329a16c90ae  0.0s
 => => naming to docker.io/library/hosts                                             0.0s
```

```
[Mon May 01] @samy: $sudo docker run --name server_1 -itd hosts
bad9e5c12825aa4dff89a24c1c0f3aa8eef1403126f64c4564e87f4e3bfe1cff
[Mon May 01] @samy: $sudo docker ps -a
CONTAINER ID   IMAGE                                  COMMAND                  CREATED          STATUS                      PORTS     NAMES
bad9e5c12825   hosts                                  "/bin/sh -c 'service…"   47 seconds ago   Up 46 seconds                         server
_1
a88eb01423e3   gcr.io/k8s-minikube/kicbase:v0.0.39    "/usr/local/bin/entr…"   3 weeks ago      Exited (137) 2 weeks ago              miniku
be
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL bash - .ssh

```
[Mon May 01] @samy: $sudo docker inspect server_1
[
    {
        "Id": "bad9e5c12825aa4dff89a24c1c0f3aa8eef1403126f64c4564e87f4e3bfe1cff",
        "Created": "2023-05-01T09:28:55.686433332Z",
        "Path": "/bin/sh",
        "Args": [
            "-c",
            "service ssh restart && bash"
        ],
        "State": {
            "Status": "running",
            "Running": true,
            "Paused": false,
            "Restarting": false,
            "OOMKilled": false,
            "Dead": false,
            "Pid": 12728,
            "ExitCode": 0,
            "Error": "",
            "StartedAt": "2023-05-01T09:28:56.137093772Z",
            "FinishedAt": "0001-01-01T00:00:00Z"
```

```
                "NetworkID": "60240c76465c387a9ae871e91659e77eed247a101d01b5df77a973058
                "EndpointID": "34b12345deae8b9af839df47dcf1531afd83df19f4c29d4ee63b757c
                "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
            }
```

```
[Mon May 01] @samy: $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:tTtPfnHHkuMJjptjSZnhbeYar8R8d2pvvpbbwbFvsWg.
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 5.14.0-162.23.1.el9_1.x86_64 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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ansible@bad9e5c12825:~$ exit
logout
Connection to 172.17.0.2 closed.
```

```
[Mon May 01] @samy: $ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/samy/.ssh/id_rsa): /home/samy/.ssh/key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/samy/.ssh/key
Your public key has been saved in /home/samy/.ssh/key.pub
The key fingerprint is:
SHA256:yDmOwElHq84CyJauh54lg5Oyk5LWwPQWo+CK6rC8PHc samy@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]----+
|    .            |
```

```
[Mon May 01] @samy: $pwd
/home/samy/Ansible
[Mon May 01] @samy: $cd .ssh/
bash: cd: .ssh/: No such file or directory
[Mon May 01] @samy: $cd ..
[Mon May 01] @samy: $pwd
/home/samy
[Mon May 01] @samy: $cd .ssh/
[Mon May 01] @samy: $ls
key  key.pub  known_hosts  known_hosts.old
[Mon May 01] @samy: $
```

```
[Mon May 01] @samy: $pwd
/home/samy/.ssh
[Mon May 01] @samy: $ssh-copy-id -i ./key.pub ansible@172.17.0.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "./key.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.

[Mon May 01] @samy: $
```

```
[Mon May 01] @samy: $ssh ansible@172.17.0.2
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.14.0-162.23.1.el9_1.x86_64 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: Mon May  1 09:35:42 2023 from 172.17.0.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ansible@bad9e5c12825:~$ cd .ssh/
ansible@bad9e5c12825:~/.ssh$ ls
authorized_keys
ansible@bad9e5c12825:~/.ssh$
```

```
[Mon May 01] @samy: $pwd
/home/samy/.ssh
[Mon May 01] @samy: $ssh ansible@172.17.0.2 -i .key/
Warning: Identity file .key/ not accessible: No such file or directory.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.14.0-162.23.1.el9_1.x86_64 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: Mon May  1 15:54:32 2023 from 172.17.0.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ansible@bad9e5c12825:~$
```

—----------

Install ansible on redhat:

sudo yum update
sudo yum install epel-release
sudo yum install ansible

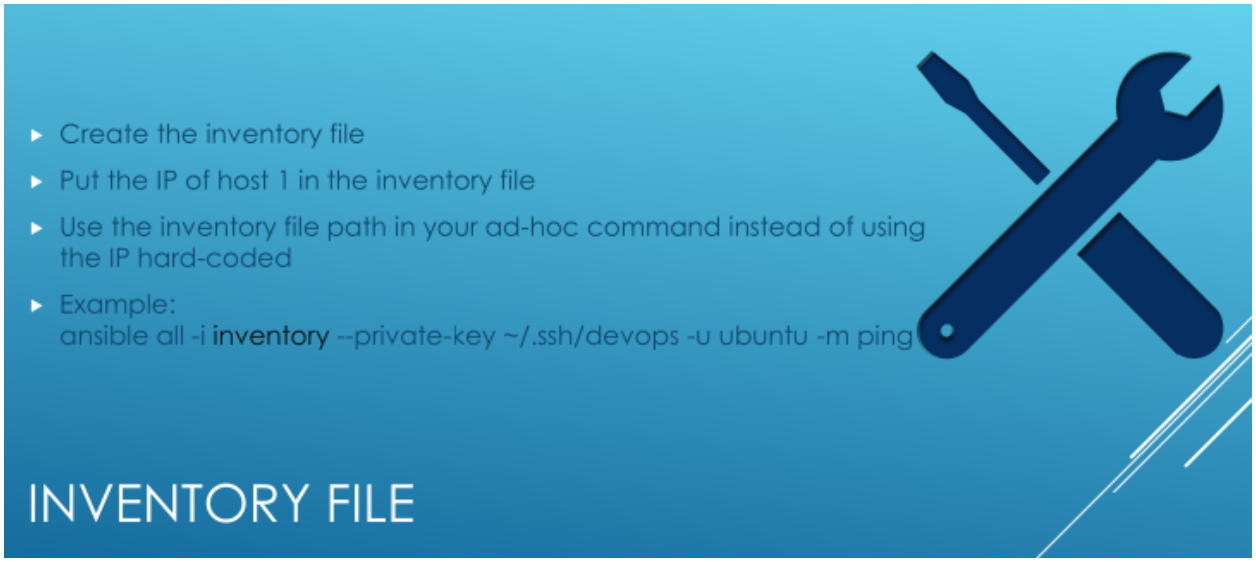
ansible --version

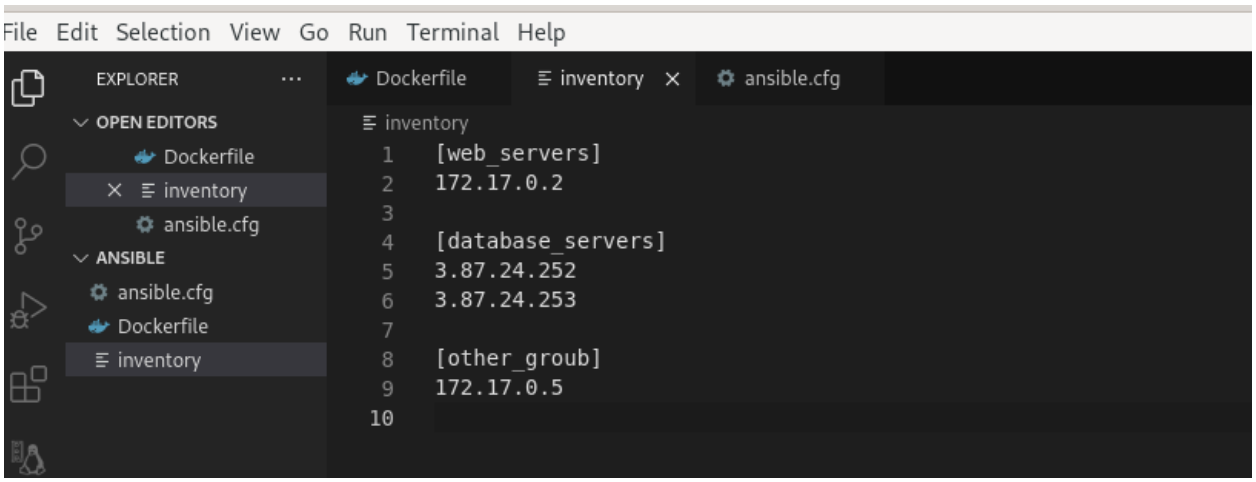
```
Complete!
[Mon May 01] @samy: $ansible --version
ansible [core 2.13.3]
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/samy/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3.9/site-packages/ansible
  ansible collection location = /home/samy/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/bin/ansible
  python version = 3.9.14 (main, Jan  9 2023, 00:00:00) [GCC 11.3.1 20220421 (Red Hat 11.3.1-2)]
  jinja version = 3.1.2
  libyaml = True
[Mon May 01] @samy: $
```

—----------

ansible all -i 172.17.0.2, --private-key ~/.ssh/key -u ansible -m ping

```
[Mon May 01] @samy: $ansible all -i 172.17.0.2, --private-key ~/.ssh/key -u ansible -m ping
172.17.0.2 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
[Mon May 01] @samy: $
```





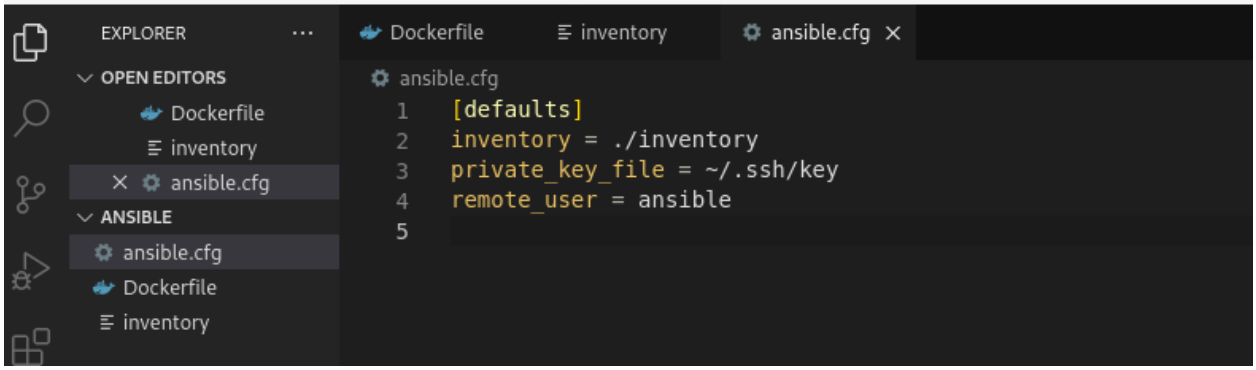
ansible web_servers -i inventory --private-key ~/.ssh/key -u ansible -m ping

```
[Mon May 01] @samy: $pwd
/home/samy/.ssh
[Mon May 01] @samy: $cd ../Ansible/
[Mon May 01] @samy: $ansible web_servers -i inventory --private-key ~/.ssh/key -u ansible -m ping
172.17.0.2 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
[Mon May 01] @samy: $
```

—----------

- Create the configuration file
- Insert some values in the configuration file
- Run the minimized ad-hoc command
- Example: ansible all -m ping

CONFIGURATION FILE



$ansible web_servers -m ping

```
[Mon May 01] @samy: $ansible web_servers -m ping
172.17.0.2 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
[Mon May 01] @samy: $
```

—----------

- Insert the correct values in the configuration file
- Example: ansible all -m command -a "whoami"
- What is the output of the command ?

AD-HOC COMMAND ESCALATION USING ROOT USER

```
[Mon May 01] @samy: $ansible web_servers -m command -a "whoami"
172.17.0.2 | CHANGED | rc=0 >>
ansible
[Mon May 01] @samy: $ansible web_servers -m command -a "whoami" --become
172.17.0.2 | FAILED | rc=-1 >>
Missing sudo password
[Mon May 01] @samy: $ansible web_servers -m command -a "whoami" --become --ask-become-pass
BECOME password:
172.17.0.2 | CHANGED | rc=0 >>
root
[Mon May 01] @samy: $
```

EXPLORER

OPEN EDITORS
- Dockerfile
- inventory
- ansible.cfg

ANSIBLE
- ansible.cfg
- Dockerfile
- inventory

Dockerfile | inventory | ansible.cfg

ansible.cfg

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

[privilege_escalation]
become = true
become_ask_pass = true
```

```
[Mon May 01] @samy: $ansible web_servers -m command -a "whoami"
BECOME password:
172.17.0.2 | CHANGED | rc=0 >>
root
[Mon May 01] @samy: $
```

EXPLORER

OPEN EDITORS
- Dockerfile
- inventory
- ansible.cfg
- day1-playbook....

ANSIBLE
- ansible.cfg
- day1-playbook.yml
- Dockerfile
- inventory

Dockerfile | inventory | ansible.cfg | day1-playbook.yml

day1-playbook.yml > YAML > {} 0 > name

```yaml
- name: play1
  hosts: web_servers
  tasks:
  - name: task1
    ping:
```

```
[Mon May 01] @samy: $ansible-playbook ~/Ansible/day1-playbook.yml
BECOME password:

PLAY [play1] ***********************************************************************************************************

TASK [Gathering Facts] *************************************************************************************************
ok: [172.17.0.2]

TASK [task1] ***********************************************************************************************************
ok: [172.17.0.2]

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

[Mon May 01] @samy: $
```

EXPLORER

OPEN EDITORS
- Dockerfile
- inventory
- ansible.cfg
- day1-playbook....

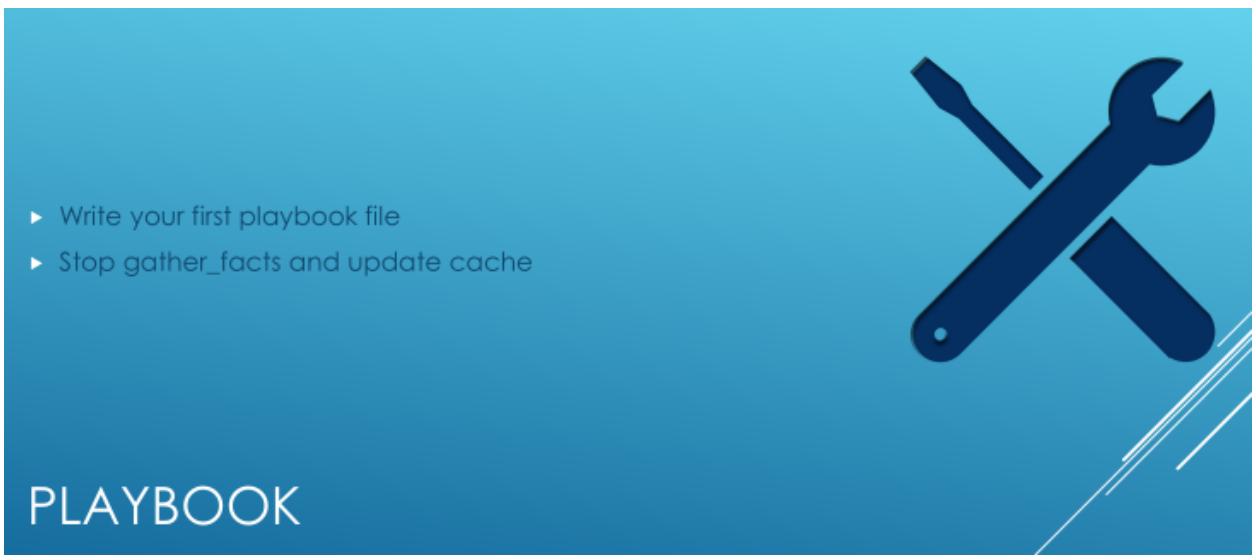
ANSIBLE
- ansible.cfg
- day1-playbook.yml
- Dockerfile
- inventory

Dockerfile | inventory | ansible.cfg | day1-playbook.yml

day1-playbook.yml > YAML > {} 0 > [ ] tasks > {} 1 > {} debug

```yaml
# - name: play1
#   hosts: web_servers
#   tasks:
#   - name: task1
#     ping:

- name: play2
  hosts: web_servers
  tasks:
  - name: task2
    command: cd mydir
    register: output_value
    ignore_errors: true
  - name: failed command debugining
    debug:
      msg: "{{ output_value }}"
```

```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL                                                    bash

[Mon May 01] @samy: $ansible-playbook ~/Ansible/day1-playbook.yml
BECOME password:

PLAY [play2] ***********************************************************************************************************

TASK [Gathering Facts] *************************************************************************************************
ok: [172.17.0.2]

TASK [Task2] ***********************************************************************************************************
fatal: [172.17.0.2]: FAILED! => {"changed": false, "cmd": "cd mydir", "msg": "[Errno 2] No such file or directory: b'cd'", "rc": 2, "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}
...ignoring

TASK [failed command debugining] ***************************************************************************************
ok: [172.17.0.2] => {
    "msg": {
        "changed": false,
        "cmd": "cd mydir",
        "failed": true,
        "msg": "[Errno 2] No such file or directory: b'cd'",
        "rc": 2,
        "stderr": "",
        "stderr_lines": [],
        "stdout": "",
        "stdout_lines": []
    }
}

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



EXPLORER

OPEN EDITORS
- Dockerfile
- inventory
- ansible.cfg
- day1-playbook....

ANSIBLE
- ansible.cfg
- day1-playbook.yml
- Dockerfile
- inventory

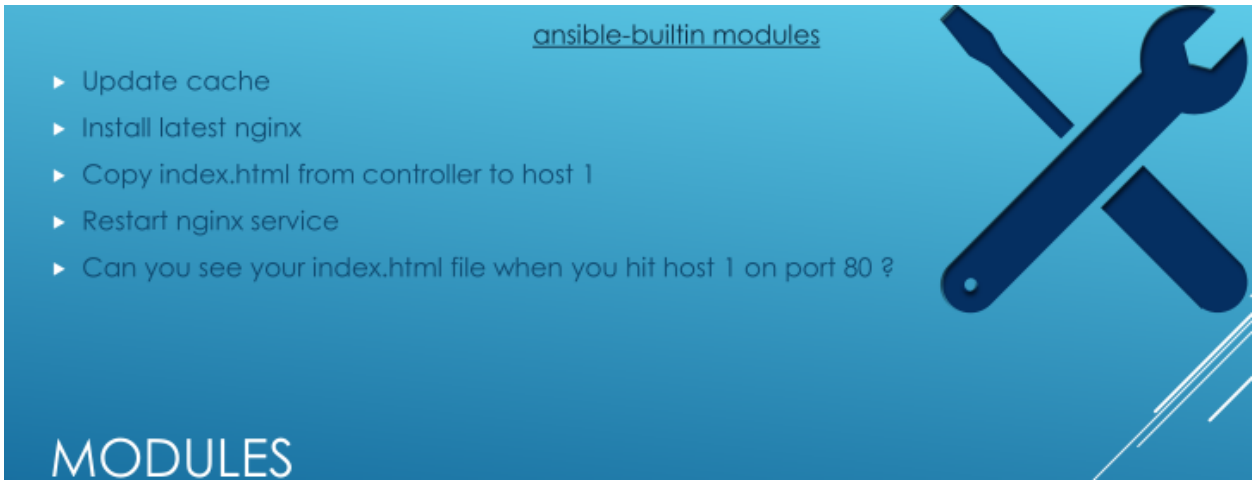
Dockerfile | inventory | ansible.cfg | day1-playbook.yml

day1-playbook.yml > YAML > {} 0 > [ ] tasks > {} 0 > {} apt > update_cache

```yaml
#       debug:
#         msg: "{{ output_value }}"

- name: play3
  hosts: web_servers
  gather_facts: false
  tasks:
  - apt:
      update_cache: true
```

PROBLEMS | OUTPUT | DEBUG CONSOLE | TERMINAL

```
[Mon May 01] @samy: $ansible-playbook ./Ansible/day1-playbook.yml
BECOME password:

PLAY [play3] ***********************************************************************************************

TASK [apt] *************************************************************************************************
ok: [172.17.0.2]

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

[Mon May 01] @samy: $
```



EXPLORER

OPEN EDITORS
- Dockerfile
- inventory
- ansible.cfg
- day1-playbook....
- index.html

ANSIBLE
- ansible.cfg
- day1-playbook.yml
- Dockerfile
- index.html
- inventory

OUTLINE

Dockerfile | inventory | ansible.cfg | day1-playbook.yml | index.html

day1-playbook.yml > Google Cloud Code > [ ] tasks > name

```yaml
- name: play3
  hosts: web_servers
  gather_facts: false
  tasks:
  - name: task1 (Update cache)
    apt:
      update_cache: true

  - name: task2 (Install latest nginx)
    apt:
      name: nginx
      state: latest

  - name: task3 (Copy index.html from controller to host 1)
    ansible.builtin.copy:
      src: ~/Ansible/index.html
      dest: /var/www/html/index.html

  - name: task4 (Restart nginx service)
    ansible.builtin.sysvinit:
      name: nginx
      state: restarted
      enabled: yes
```

PROBLEMS | OUTPUT | DEBUG CONSOLE | TERMINAL

```
[Tue May 02] @samy: $ansible playbook ~/Ansible/day1 playbook.yml
BECOME password:

PLAY [play3] ***********************************************************************************************************

TASK [task1 (Update cache)] ********************************************************************************************
ok: [172.17.0.2]

TASK [task2 (Install latest nginx)] ************************************************************************************
ok: [172.17.0.2]

TASK [task3 (Copy index.html from controller to host 1)] ***************************************************************
ok: [172.17.0.2]

TASK [task4 (Restart nginx service)] ***********************************************************************************
changed: [172.17.0.2]

PLAY RECAP *************************************************************************************************************
172.17.0.2                 : ok=4    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

[Tue May 02] @samy: $curl 172.17.0.2
===== Hello Ansbile =====
[Tue May 02] @samy: $
```