



Ansible

Session 6 – 7th Jan 2023 Summary

- Launch two instances, one for controller node and other for target node, use putty to login to these instances
- On the target node, a **user account** is created

```
root@ip-172-31-4-153:~  
# Using username "ec2-user".  
# Authenticating with public key "test_key_aws_mumbia_daccount"  
Register this system with Red Hat Insights: insights-client --register  
Create an account or view all your systems at https://red.ht/insights-dashboard  
[ec2-user@ip-172-31-4-153 ~]$ sudo su - root  
[root@ip-172-31-4-153 ~]#  
[root@ip-172-31-4-153 ~]#  
[root@ip-172-31-4-153 ~]# whoami  
root  
[root@ip-172-31-4-153 ~]# useradd vimal  
[root@ip-172-31-4-153 ~]# passwd vimal  
Changing password for user vimal.  
New password:  
BAD PASSWORD: The password is shorter than 8 characters  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@ip-172-31-4-153 ~]#
```

- From the controller node the ansible will login to target node as to the **non-root user** and not to the **root user**
- Create an inventory on the controller node

```
root@ip-172-31-15-13:~  
[root@ip-172-31-15-13 ~]# vim /etc/ansible/hosts
```

```
root@ip-172-31-15-13:~  
# This is the default ansible 'hosts' file.  
#  
35.154.138.108 ansible_user=vimal ansible_password=redhat  
# It should live in /etc/ansible/hosts  
..
```

- The ansible login to the target node as a **general user (non-root user)** can run basic commands “date”, “id” etc

```
[root@ip-172-31-15-13 ~]# ansible all -m command -a date
35.154.138.108 | CHANGED | rc=0 >>
Sat Jan  7 08:56:17 AM UTC 2023
[root@ip-172-31-15-13 ~]# ansible all -m command -a id
35.154.138.108 | CHANGED | rc=0 >>
uid=1001(vimal) gid=1001(vimal) groups=1001(vimal) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- The ansible login to the target node as a **general user (non-root user)** cannot run the system level commands.

```
[root@ip-172-31-15-13 ~]# ansible all -m command -a "yum install httpd -y"
35.154.138.108 | FAILED | rc=1 >>
Not root, Subscription Management repositories not updated

This system is not registered with an entitlement server. You can use subscription-manager to register.
Error: This command has to be run with superuser privileges (under the root user on most systems).non-zero return code
[root@ip-172-31-15-13 ~]# ansible all -m package -a "name=httpd state=present"
35.154.138.108 | FAILED! => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "msg": "This command has to be run under the root user.",
  "results": []
}
```

- For this on the target node, the general user should be given **sudo power** to run system level commands.

```
[root@ip-172-31-4-153 ~]# vi /etc/sudoers
[root@ip-172-31-4-153 ~]#
```

```
vimal ALL=(ALL) ALL
```

- The command to see the help

```
[root@ip-172-31-15-13 ~]# ansible -h

Privilege Escalation Options:
  control how and which user you become as on target hosts

  --become-method BECOME_METHOD
                        privilege escalation method to use (default=sudo), use
                        `ansible-doc -t become -l` to list valid choices.

  --become-user BECOME_USER
                        run operations as this user (default=root)

  -b, --become
                        run operations with become (does not imply password
                        prompting)
```

- The general user internally run the command with **sudo power**, becoming “root” at that point in time

```
root@ip-172-31-15-13:~  
[root@ip-172-31-15-13 ~]# ansible all -m package -a "name=httpd state=present"  
--become-method=sudo --become-user=root --become --ask-become-pass  
BECOME password:  
|
```

```
35.154.138.108 | CHANGED => {  
  "ansible_facts": {  
    "discovered_interpreter_python": "/usr/bin/python3"  
  },  
  "changed": true,  
  "msg": "",  
  "rc": 0,  
  "results": [  
    "Installed: httpd-filesystem-2.4.53-7.el9.noarch",  
    "Installed: mod_lua-2.4.53-7.el9.x86_64",  
    "Installed: httpd-2.4.53-7.el9.x86_64",  
    "Installed: apr-util-bdb-1.6.1-20.el9.x86_64",  
    "Installed: apr-util-openssl-1.6.1-20.el9.x86_64",  
    "Installed: redhat-logos-httpd-90.4-1.el9.noarch",  
    "Installed: apr-1.7.0-11.el9.x86_64",  
    "Installed: mod_http2-1.15.19-2.el9.x86_64",  
    "Installed: apr-util-1.6.1-20.el9.x86_64",  
    "Installed: httpd-core-2.4.53-7.el9.x86_64",  
    "Installed: httpd-tools-2.4.53-7.el9.x86_64",  
    "Installed: mailcap-2.1.49-5.el9.noarch"  
  ]  
}
```

- The command to see the internal configuration file of ansible

```
[root@ip-172-31-15-13 ~]# ansible --version  
ansible [core 2.13.3]  
  config file = /etc/ansible/ansible.cfg  
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']  
  ansible python module location = /usr/lib/python3.9/site-packages/ansible  
  ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections  
  executable location = /usr/bin/ansible  
  python version = 3.9.14 (main, Sep 21 2022, 00:00:00) [GCC 11.3.1 20220421 (Red Hat 11.3.1-2)]  
  jinja version = 3.1.2  
  libyaml = True
```

- The options can be put in a file and make it default

```
[root@ip-172-31-15-13 ~]# vim /etc/ansible/ansible.cfg
```

```
# for example, for 2.9: https://github.com/ansible/ansible/blob/stable-2.9/examples/ansible.cfg

[privilege_escalation]
become = true
become_method = sudo
become_user = root
become_ask_pass = true
```

- The command to generate the ansible configuration file

```
[root@ip-172-31-15-13 ~]# ansible-config init
```

- The command to copy the generated configuration file into the main configuration file

```
[root@ip-172-31-15-13 ~]# ansible-config init --disabled > /etc/ansible/ansible.cfg
```

- To login from one system to another using “ssh”, there are two ways of authentication one is **password based authentication** and other is **key based authentication** (password less based authentication)
- On the ansible controller node, we create one user account

```
[root@ip-172-31-15-13 ~]# whoami
root
[root@ip-172-31-15-13 ~]# useradd devops
[root@ip-172-31-15-13 ~]# passwd devops
Changing password for user devops.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-15-13 ~]# su - devops
[devops@ip-172-31-15-13 ~]$ pwd
/home/devops
[devops@ip-172-31-15-13 ~]$
```


- For key based authentication, we need to generate a key on the controller node

```
[devops@ip-172-31-15-13 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/devops/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/devops/.ssh/id_rsa
Your public key has been saved in /home/devops/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Zth/qjOENxSM4UvYUvHYN5RwvFFRa1pya4/YF/RpCuw devops@ip-172-31-15-13.ap-sou
th-1.compute.internal
The key's randomart image is:
+---[RSA 3072]-----+
|      +=.ooooo. |
|      =.oo+   . |
|      o = o.oo. =. |
|      o +..o. *..o|
|      ooS  o. o+. |
|      .o+.. .+oo. |
|      o ..Eo.o o |
|      o o   . |
|      .+. |
+-----[SHA256]-----+
```

- Copy the key from controller node to target node, for authorization

```
[devops@ip-172-31-15-13 ~]$ ssh-copy-id vimal@35.154.138.108
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/devops/.ssh
/id_rsa.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 prompt
ed now it is to install the new keys
vimal@35.154.138.108's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'vimal@35.154.138.108'"
and check to make sure that only the key(s) you wanted were added.
```

- Now we try to login to the general user, it will not ask for password, this is called password less based authentication

```
[devops@ip-172-31-15-13 ~]$ ssh vimal@35.154.138.108
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Sat Jan  7 09:49:10 2023 from 52.66.243.228
```

- The default location of the key can be changed, by specifying the location of the key in the inventory file

```
root@ip-172-31-15-13:~  
# This is the default ansible 'hosts' file.  
#  
35.154.138.108 ansible_user=vimal ansible_path=/my.key
```

- As a general user we can create playbook but we cannot change the default configuration file, so we can create a personal configuration file with extension “.cfg”

```
devops@ip-172-31-15-13:~/code  
[devops@ip-172-31-15-13 code]$  
[devops@ip-172-31-15-13 code]$  
[devops@ip-172-31-15-13 code]$ whoami  
devops  
[devops@ip-172-31-15-13 code]$ pwd  
/home/devops/code  
[devops@ip-172-31-15-13 code]$ ls  
web.yml  
[devops@ip-172-31-15-13 code]$ touch ansible.cfg  
[devops@ip-172-31-15-13 code]$ ls  
ansible.cfg web.yml  
[devops@ip-172-31-15-13 code]$
```

- Similarly, we can create personal inventory file

```
[devops@ip-172-31-15-13 code]$ ls  
ansible.cfg web.yml  
[devops@ip-172-31-15-13 code]$ ansible all --list-hosts  
[WARNING]: Unable to parse /home/devops/code/inventory as an inventory source  
[WARNING]: No inventory was parsed, only implicit localhost is available  
[WARNING]: provided hosts list is empty, only localhost is available. Note that  
the implicit localhost does not match 'all'  
hosts (0):  
[devops@ip-172-31-15-13 code]$ pwd  
/home/devops/code  
[devops@ip-172-31-15-13 code]$ touch inventory  
[devops@ip-172-31-15-13 code]$ pwd  
/home/devops/code  
[devops@ip-172-31-15-13 code]$ ls  
ansible.cfg inventory web.yml  
[devops@ip-172-31-15-13 code]$ cat inventory  
[devops@ip-172-31-15-13 code]$ ansible all --list-hosts  
[WARNING]: provided hosts list is empty, only localhost is available. Note that  
the implicit localhost does not match 'all'  
hosts (0):
```

Important Links –

Hash13 link for Sessions and extra sessions recordings –

<https://learning.hash13.com/>

How to build Inventory:-

https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.html

Ansible Documentation- Copy Module -

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/copy_module.html

Ansible Documentation- Package Module -

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/package_module.html

Ansible Documentation- Service Module –

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/service_module.html

Ansible Documentation – Debug Module –

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/debug_module.html

Ansible Inventory Documentation –

https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.html