Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

Session - 28 Agenda:

1. Managing Users & Groups with Ansible

Managing Users & Groups in Linux:

On Linux every process runs as a particular user and every file and folder is owned by a certain user. Further, access to these files and folders are restricted by users. This shows how important it is to learn how user management is done on Linux as a normal user or an admin. Information about local users can be found in etc/passwd:

```
$ tail -10 /etc/passwd
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
cockpit-ws:x:989:984:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:983:User for cockpit-ws instances:/nonexisting:/sbin/nologin
gnome-initial-setup:x:987:982::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:986:981::/var/lib/chrony:/sbin/nologin
dnsmasq:x:985:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:/usr/sbin/nologin
vikasnehra:x:1000:1000:Vikas Nehra:/home/vikasnehra:/bin/bash
```

The format is interpreted as follows:

username:password:uid:gid:gecos:home/dir:shell

Groups also have ID and every user belongs to a default group, User Private Group (UPG). Users can also have supplementary groups. These supplementary groups help users to have access to permissions for other files and processes. Information on groups is usually found at etc/group:

```
$ tail -10 /etc/group
cockpit-wsinstance:x:983:
gnome-initial-setup:x:982:
sshd:x:74:
chrony:x:981:
slocate:x:21:
dnsmasq:x:980:
tcpdump:x:72:
sgx:x:979:
systemd-oom:x:978:
vikasnehra:x:1000:
```

The format is interpreted as follows:

groupname:password:GID:<list of users>

Creating Users in Linux:

You can add users with the useradd command.

```
# useradd -m -d /home/john -c "JOHN" -s /bin/sh john
# tail -1 /etc/passwd
john:x:1001:1001:JOHN:/home/john:/bin/sh
# tail -1 /etc/group
john:x:1001:
```

Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

Modifying Users:

User account details can be modified using usermod command.

```
# usermod -s /bin/bash john
# tail -1 /etc/passwd
john:x:1001:1001:john:/home/john:/bin/bash
```

Setting User Password:

User password can be set/reset by using the passwd command.

```
# passwd john
Changing password for user john.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Same can be verified from the /etc/shadow file.

```
# tail -1 /etc/shadow
john:$6$9za4UabfKmf3h3Du$wUbqGJi/DJJvV3mZvTeBM/Gl3r9n232CQiRf9DFSJ5COhZlW91o
0hqaJbpBtgPX3sa8ONnHILZ/dFTtO43i9f.:19531:0:99999:7:::
```

User account aging can be viewed or controlled by using chage command.

```
# chage -l john
Last password change                    : Jun 23, 2023
Password expires                        : never
Password inactive                       : never
Account expires                         : never
Minimum number of days between password change      : 0
Maximum number of days between password change      : 99999
Number of days of warning before password expires   : 7
```

```
# chage john
Changing the aging information for john
Enter the new value, or press ENTER for the default
    Minimum Password Age [0]:
    Maximum Password Age [99999]:
    Last Password Change (YYYY-MM-DD) [2023-06-23]:
    Password Expiration Warning [7]:
    Password Inactive [-1]:
    Account Expiration Date (YYYY-MM-DD) [-1]:
```

Default user options can be viewed or managed by /etc/default/useradd file.

```
# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

OR

```
# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Deleting The User:

You can delete the user by using the userdel command.

```
# userdel -r john
# tail -1 /etc/passwd
vikasnehra:x:1000:1000:Vikas Nehra:/home/vikasnehra:/bin/bash
# grep john /etc/passwd
# grep john /etc/group
```

Managing Users & Groups with Ansible:

To manage users and groups with ansible we can either use ansible ad-hoc command or we can use ansible playbooks.

1. Using Ansible Ad-Hoc Command:

Let's consider an example to create a user having username as ravi with login shell as /bin/sh having user id 1050 on node1.

```
$ ansible node1 -m command -a 'sudo useradd -c "Ravi" -s /bin/sh -u 1050 ravi'
```

Verify the same.

```
$ ansible node1 -m command -a 'tail -1 /etc/passwd'
node1 | CHANGED | rc=0 >>
ravi:x:1050:1050:Ravi:/home/ravi:/bin/sh

$ ansible node1 -m command -a 'tail -1 /etc/group'
node1 | CHANGED | rc=0 >>
ravi:x:1050:
```

2. Using Ansible Playbooks:

Let's take a few examples of managing users & groups by using ansible playbook.

```
$ vim users.yml
---
- name: Managing Users & Groups
  hosts: node1
  become: yes
  vars:
    password: mySecret
  tasks:
    - name: Add a simple user called Greta Grace
      user:
        name: gretagrace
```

Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

```
    comment: Greta Grace

  - name: Add user amit with a password
    user:
      name: amit
      password: "{{ password | password_hash('sha512') }}"
      update_password: on_create

  - name: Add a group called nehraclasses
    group:
      name: nehraclasses
      state: present

  - name: Add a user Ashish and add them to a group nehraclasses
    user:
      name: ashish
      groups: nehraclasses
      append: yes

  - name: Add user Rahul and generate for them an SSH key
    user:
      name: rahul
      generate_ssh_key: yes
      ssh_key_bits: 2048
      ssh_key_file: .ssh/id_rsa

  - name: Add user noHome with no home and set account to expire on certain date
    user:
      name: noHome
      create_home: no
      expires: 1590155615

  - name: Add a user Suraj having login shell as sh and add them to a group nehraclasses
    user:
      name: suraj
      shell: /bin/sh
      groups: nehraclasses
      append: yes

  - name: Add the user 'Vijay Sharma' with a specific uid as 1077 having username as vijay,
having home directory as /home/vijaysharma
    user:
      name: vijay
      comment: Vijay Sharma
      uid: 1077
      createhome: yes          # Defaults to yes
      home: /home/vijaysharma    # Defaults to /home/<username>
...
```

Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

Check the playbook for syntax errors.

$ ansible-playbook users.yml --syntax-check

Execute the playbook.

$ ansible-playbook users.yml

Verify the tasks.

```
$ ansible node1 -m command -a 'tail -9 /etc/passwd'
node1 | CHANGED | rc=0 >>
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:/usr/sbin/nologin
vikasnehra:x:1000:1000:Vikas Nehra:/home/vikasnehra:/bin/bash
gretagrace:x:1001:1001:Greta Grace:/home/gretagrace:/bin/bash
amit:x:1002:1002::/home/amit:/bin/bash
ashish:x:1003:1004::/home/ashish:/bin/bash
rahul:x:1004:1005::/home/rahul:/bin/bash
noHome:x:1005:1006::/home/noHome:/bin/bash
suraj:x:1006:1007::/home/suraj:/bin/sh
vijay:x:1077:1077:Vijay Sharma:/home/vijaysharma:/bin/bash

$ ansible node1 -m command -a 'tail -9 /etc/group'
node1 | CHANGED | rc=0 >>
vikasnehra:x:1000:
gretagrace:x:1001:
amit:x:1002:
nehraclasses:x:1003:ashish,suraj
ashish:x:1004:
rahul:x:1005:
noHome:x:1006:
suraj:x:1007:
vijay:x:1077:

$ ssh node1
Activate the web console with: systemctl enable --now cockpit.socket
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: Fri Jun 23 19:59:13 2023 from 192.168.229.128

[vikasnehra@node1 ~]$ su - amit
Password: mySecret

[vikasnehra@node1 ~]$ id -a ashish
uid=1003(ashish) gid=1004(ashish) groups=1004(ashish),1003(nehraclasses)

$ sudo su -
[root@node1 ~]# cd /home/rahul/

[root@node1 rahul]# ls -al
total 12
drwx------. 4 rahul rahul  90 Jun 23 19:58 .
drwxr-xr-x. 9 root  root  113 Jun 23 19:58 ..
```

Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

```
-rw-r--r--. 1 rahul rahul  18 Nov  5  2021 .bash_logout
-rw-r--r--. 1 rahul rahul 141 Nov  5  2021 .bash_profile
-rw-r--r--. 1 rahul rahul 492 Nov  5  2021 .bashrc
drwxr-xr-x. 4 rahul rahul  39 Feb 26 21:05 .mozilla
drwx------. 2 rahul rahul  38 Jun 23 19:58 .ssh

[root@node1 rahul]# cd .ssh/

[root@node1 .ssh]# ls -al
total 8
drwx------. 2 rahul rahul   38 Jun 23 19:58 .
drwx------. 4 rahul rahul   90 Jun 23 19:58 ..
-rw-------. 1 rahul rahul 1864 Jun 23 19:58 id_rsa
-rw-r--r--. 1 rahul rahul  427 Jun 23 19:58 id_rsa.pub

[root@node1 ~]# chage -l noHome
Last password change                                    : Jun 23, 2023
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : May 22, 2020
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7

[root@node1 ~]# grep suraj /etc/passwd
suraj:x:1006:1007::/home/suraj:/bin/sh

[root@node1 ~]# id -a vijay
uid=1077(vijay) gid=1077(vijay) groups=1077(vijay)

[root@node1 ~]# grep vijay /etc/passwd
vijay:x:1077:1077:Vijay Sharma:/home/vijaysharma:/bin/bash

[root@node1 ~]# ls -ld /home/vijaysharma/
drwx------. 3 vijay vijay 78 Jun 23 19:58 /home/vijaysharma/

[root@node1 home]# ls -ld /home/noHome
```

Managing Users & Groups with Ansible

By: Er. Vikas Nehra (M. Tech, B. Tech), Experience: 15 + Years

Deleting The Users & Groups:

Let's create an ansible playbook for the same.

[vikasnehra@node1 ~]$ vim del_users.yml

```
---
- name: Deleting Users & Groups
  hosts: node1
  become: yes
  tasks:
    - name: Deleting The User Vijay Sharma
      user:
        name: vijay
        state: absent

    - name: Deleting The Group nehraclasses
      group:
        name: nehraclasses
        state: absent
...
```

Check the playbook for syntax errors.

$ ansible-playbook del_users.yml --syntax-check

Execute the playbook.

$ ansible-playbook del_users.yml

Verify the tasks.

$ ansible node1 -m command -a 'tail -9 /etc/passwd'

$ ansible node1 -m command -a 'grep vijay /etc/passwd'

$ ansible node1 -m command -a 'tail -9 /etc/group'

$ ansible node1 -m command -a 'grep nehraclasses /etc/group'

Thank You