

#347729 - Configure User Groups, sudo Access, and Permissions

Scenario:

You are managing a system where user access and permissions need to be organized. This task requires creating a group for DevOps users, assigning them membership, and granting them limited sudo access for specific tasks.

Solution :

Configuration on ubuntu.example.com

Step 1: Create Group “devops”

- Execute **groupadd devops** command to create a group.

```
root@ubuntu:~# hostname
ubuntu.example.com
root@ubuntu:~#
root@ubuntu:~# groupadd devops
root@ubuntu:~#
root@ubuntu:~# cat /etc/group | grep devops
devops:x:1001:
```

Step 2: Create User john, jacob, olivia, tracy

- Execute **adduser john** command to create john user.

```
root@ubuntu:~# adduser john
Adding user `john' ...
Adding new group `john' (1002) ...
Adding new user `john' (1001) with group `john' ...
Creating home directory `/home/john' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for john
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@ubuntu:~#
```

- Execute **adduser jacob** command to create jacob user.

```
root@ubuntu:~#  
root@ubuntu:~# adduser jacob  
Adding user `jacob' ...  
Adding new group `jacob' (1003) ...  
Adding new user `jacob' (1002) with group `jacob' ...  
Creating home directory `/home/jacob' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for jacob  
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@ubuntu:~#
```

- Execute **adduser olivia** command to create olivia user.

```
root@ubuntu:~#  
root@ubuntu:~# adduser olivia  
Adding user `olivia' ...  
Adding new group `olivia' (1004) ...  
Adding new user `olivia' (1003) with group `olivia' ...  
Creating home directory `/home/olivia' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for olivia  
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@ubuntu:~# _
```

- Execute **adduser tracy** command to create tracy user.

```
root@ubuntu:~#  
root@ubuntu:~# adduser tracy  
Adding user `tracy' ...  
Adding new group `tracy' (1005) ...  
Adding new user `tracy' (1004) with group `tracy' ...  
Creating home directory `/home/tracy' ...  
Copying files from `/etc/skel' ...  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for tracy  
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@ubuntu:~#
```

Step 3: Add all the user create to “devops” group

- Execute **usermod -G devops <user_name>** command to add users to devops group.

```
root@ubuntu:~#  
root@ubuntu:~# usermod -G devops john  
root@ubuntu:~#  
root@ubuntu:~# usermod -G devops jacob  
root@ubuntu:~#  
root@ubuntu:~# usermod -G devops olivia  
root@ubuntu:~#  
root@ubuntu:~# usermod -G devops tracy  
root@ubuntu:~#  
root@ubuntu:~# cat /etc/group | grep devops  
devops:x:1001:john,jacob,olivia,tracy  
root@ubuntu:~#  
root@ubuntu:~#
```

Step 4: Change password of users to “DevOps”

- Execute `echo "<user_name>:Devops" | chpasswd` to change the password of user.

```
root@ubuntu:~#  
root@ubuntu:~# echo "john:DevOps" | chpasswd  
root@ubuntu:~#  
root@ubuntu:~# echo "jacob:DevOps" | chpasswd  
root@ubuntu:~#  
root@ubuntu:~# echo "olivia:DevOps" | chpasswd  
root@ubuntu:~#  
root@ubuntu:~# echo "tracy:DevOps" | chpasswd  
root@ubuntu:~#
```

Step 5: Give sudo access for specific command to devops group user and restrict it from jacob user

- To allow access of `adduser`, `groupadd`, `usermod` command for the users of devops group. Add **“%devops ALL=(ALL:ALL) NOPASSWD: /usr/sbin/adduser, /usr/sbin/addgroup, /usr/sbin/usermod”** this entry in `/etc/sudoers` file.
- To restrict access of `adduser`, `groupadd`, `usermod` command of jacob user. Add **“%jacob ALL=(ALL:ALL) NOPASSWD: !/usr/sbin/adduser, !/usr/sbin/addgroup, !/usr/sbin/usermod”** this entry in `/etc/ sudoers` file.

```
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
%devops ALL=(ALL:ALL) NOPASSWD: /usr/sbin/adduser, /usr/sbin/addgroup, /usr/sbin/usermod  
%jacob ALL=(ALL:ALL) NOPASSWD: !/usr/sbin/adduser, !/usr/sbin/addgroup, !/usr/sbin/usermod  
# Members of the admin group may gain root privileges  
%admin  ALL=(ALL) ALL  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
# See sudoers(5) for more information on "#include" directives:
```

Step 6: Check whether user can run specified commands using sudo and restrict access from jacob user

- Login to john user shell and check whether john can create a user by sudo access.

```
root@ubuntu:~# su - john
john@ubuntu:~$
john@ubuntu:~$ sudo adduser jerry
Adding user `jerry' ...
Adding new group `jerry' (1007) ...
Adding new user `jerry' (1006) with group `jerry' ...
Creating home directory `/home/jerry' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jerry
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
john@ubuntu:~$ _
```

- Login to olivia user shell and check whether olivia can create a group by sudo access.

```
root@ubuntu:~# su - olivia
olivia@ubuntu:~$
olivia@ubuntu:~$ sudo addgroup sysadm
Adding group `sysadm' (GID 1008) ...
Done.
olivia@ubuntu:~$ _
```

- Login to tracy user shell and check whether tracy can do usermod by sudo access.

```
root@ubuntu:~# su - tracy
tracy@ubuntu:~$
tracy@ubuntu:~$ #sudo usermod -G sysadm tracy
tracy@ubuntu:~$
tracy@ubuntu:~$ cat /etc/group | grep sysadm
sysadm:x:1008:tracy
tracy@ubuntu:~$
```

- Login to jacob user shell and check whether jacob can't execute adduser, addgroup, usermod by sudo access.

```
root@ubuntu:~# su - jacob
jacob@ubuntu:~$
jacob@ubuntu:~$ sudo adduser jack
Sorry, user jacob is not allowed to execute '/usr/sbin/adduser jack' as root on ubuntu.example.com.
jacob@ubuntu:~$
jacob@ubuntu:~$ sudo addgroup dev
Sorry, user jacob is not allowed to execute '/usr/sbin/addgroup dev' as root on ubuntu.example.com.
jacob@ubuntu:~$
jacob@ubuntu:~$ sudo usermod -G sysadm jacob
Sorry, user jacob is not allowed to execute '/usr/sbin/usermod -G sysadm jacob' as root on ubuntu.example.com.
jacob@ubuntu:~$
jacob@ubuntu:~$
```

Congratulations we have successfully configured user group, sudo access and permission on ubuntu.example.com machine.

Now, Let's Configure on opensuse.example.com machine

Configuration on opensuse.example.com

Repeat the same process which we have performed on ubuntu.example.com machine

Step 1: Create Group “devops”

- Execute **groupadd devops** command to create a group.

```
opensuse:~ # hostname
opensuse.example.com
opensuse:~ #
opensuse:~ # groupadd devops
opensuse:~ #
opensuse:~ # cat /etc/group | grep devops
devops:x:1000:
opensuse:~ #
```

Step 2: Create User john, jacob, olivia, tracy

- Execute **useradd <user_name>** command to create john user.
- In ubuntu.example.com to create user command is “adduser <user_name>” but in opensuse.example.com command is “**useradd <user_name>**”

```
opensuse:~ #
opensuse:~ # useradd john
Creating mailbox file: File exists
opensuse:~ # useradd olivia
Creating mailbox file: File exists
opensuse:~ # useradd jacob
Creating mailbox file: File exists
opensuse:~ # useradd tracy
Creating mailbox file: File exists
opensuse:~ #
```

Step 3: Add all the user create to “devops” group

- Execute **usermod -G devops <user_name>** command to add users to devops group.

```
opensuse:~ #  
opensuse:~ # usermod -G devops john  
opensuse:~ #  
opensuse:~ # usermod -G devops jacob  
opensuse:~ #  
opensuse:~ # usermod -G devops olivia  
opensuse:~ #  
opensuse:~ # usermod -G devops tracy  
opensuse:~ #  
opensuse:~ # cat /etc/group | grep devops  
devops:x:1000:john,jacob,olivia,tracy  
opensuse:~ # _
```

Step 4: Change password of users to “DevOps”

- Execute **echo “<user_name>:Devops” | chpasswd** to change the password of the user.

```
opensuse:~ #  
opensuse:~ # echo "john:DevOps" | chpasswd  
BAD PASSWORD: it is based on a dictionary word  
BAD PASSWORD: is too simple  
opensuse:~ #  
opensuse:~ # echo "olivia:DevOps" | chpasswd  
BAD PASSWORD: it is based on a dictionary word  
BAD PASSWORD: is too simple  
opensuse:~ #  
opensuse:~ # echo "jacob:DevOps" | chpasswd  
BAD PASSWORD: it is based on a dictionary word  
BAD PASSWORD: is too simple  
opensuse:~ #  
opensuse:~ # echo "tracy:DevOps" | chpasswd  
BAD PASSWORD: it is based on a dictionary word  
BAD PASSWORD: is too simple  
opensuse:~ #  
opensuse:~ #
```


Step 5: Give sudo access for specific command to devops group user and restrict it from jacob user

- To allow access of adduser, groupadd, usermod command for the users of devops group. Add
**“%devops ALL=(ALL:ALL) NOPASSWD:
/usr/sbin/adduser, /usr/sbin/addgroup,
/usr/sbin/usermod”** this entry in /etc/sudoers file.
- To restrict access of adduser, groupadd, usermod command of jacob user. Add
**“%jacob ALL=(ALL:ALL) NOPASSWD:
!/usr/sbin/adduser, !/usr/sbin/addgroup,
!/usr/sbin/usermod”** this entry in /etc/ sudoers file.

```
## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL:ALL) ALL

## Same thing without a password
%wheel ALL=(ALL:ALL) NOPASSWD: ALL
%devops ALL=(ALL:ALL) NOPASSWD: /usr/sbin/groupadd, /usr/sbin/useradd, /usr/sbin/usermod
jacob ALL=(ALL:ALL) NOPASSWD: !/usr/sbin/groupadd, !/usr/sbin/useradd, !/usr/sbin/usermod_
## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
-- INSERT --
```

87,90

Bot

Step 6: Check whether user can run specified commands using sudo and restrict access from jacob user

- Login to john user shell and check whether john can create a user by sudo access.

```
opensuse:~ # su - john
john@opensuse:~>
john@opensuse:~> sudo useradd kim
john@opensuse:~>
```

- Login to olivia user shell and check whether olivia can create a group by sudo access.

```
opensuse:~ # su - olivia
olivia@opensuse:~>
olivia@opensuse:~> sudo groupadd ops
olivia@opensuse:~>
olivia@opensuse:~> exit
logout
opensuse:~ # _
```

- Login to tracy user shell and check whether tracy can do usermod by sudo access.

```
opensuse:~ # su - tracy
tracy@opensuse:~>
tracy@opensuse:~> sudo usermod -G ops kim
tracy@opensuse:~>
tracy@opensuse:~> cat /etc/group | grep ops
devops:x:1000:john,olivia,tracy
ops:x:1002:kim
tracy@opensuse:~> exit
logout
opensuse:~ #
```

- Login to jacob user shell and check whether jacob can't execute adduser, addgroup, usermod by sudo access.

```
opensuse:~ # su - jacob
jacob@opensuse:~>
jacob@opensuse:~> sudo useradd pat
Sorry, user jacob is not allowed to execute '/usr/sbin/useradd pat' as root on opensuse.example.com.
jacob@opensuse:~>
jacob@opensuse:~> sudo groupadd database
Sorry, user jacob is not allowed to execute '/usr/sbin/groupadd database' as root on opensuse.example.com.
jacob@opensuse:~>
jacob@opensuse:~> sudo usermod -G database pat
Sorry, user jacob is not allowed to execute '/usr/sbin/usermod -G database pat' as root on opensuse.example.com.
jacob@opensuse:~> exit
logout
opensuse:~ # _
```

Congratulations we have successfully configured user group, sudo access and permission on opensuse.example.com machine.