# Lab 02C

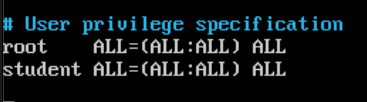
Perform the following activities on both of your virtual machines.  Record your commands and answer any questions in the lab activities.

Part 1) Ubuntu Server 18.04.1 Server­­

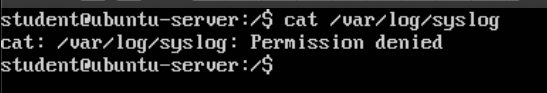
1. Create an ordinary user named **student**.  Working with root privileges, use **visudo**to modify the **/etc/sudoers**file. Add a line that grants the user named **student**full root privileges.

A picture containing bottle, text

Description automatically generated



1. Working as **student**view the **/var/log/syslog**or **/var/log/messages** file without and then with sudo. What is the result?



**\*When running as sudo the command is successfully executed\***

3. Working with root privileges, use **visudo**to modify the **/etc/sudoers** file. Add lines that:

a. Add a user alias named **ADMIN**that includes **max**and **jed**.

A picture containing object, clock

Description automatically generated

b. Add a command alias named **MEDIA**that includes **mount**and **umount**.

A picture containing object, clock

Description automatically generated

c. Allow **ADMIN**users and **mary**to run the **MEDIA**commands.

A picture containing object, indoor, sitting

Description automatically generated

4. Working as **max** or **jed**, test sudo using following steps:

a. Look for the **/boot** filesystem using **df -h**

b. Attempt to **umount  /boot** without using **sudo**.

c. Use **sudo**to **umount  /boot**.

d. Verify the **/boot**filesystem is no longer available using the **df -h**command.

A close up of text on a black background

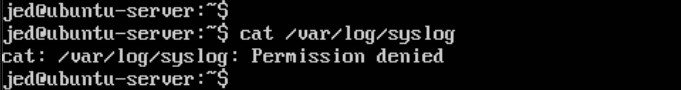
Description automatically generated

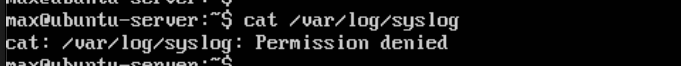
e. Make the **/boot** filesystem available again using the command **sudo mount /boot**.

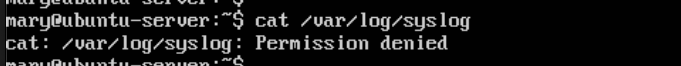
A close up of text on a black background

Description automatically generated

f. Ensure that users **jed**, **max**, or **mary**cannot run other commands using sudo. For example, attempt to view the **/var/log/syslog**or **/var/log/messages** file







g. Working with root privileges, view the **tail** of the **/var/log/syslog**or **/var/log/messages** file. What did you find in the file?

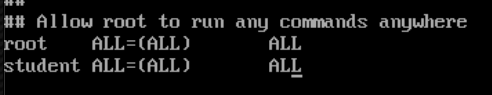
**\*Displays logging for different services such as: networking and time synchronization. User manager was started for UID 0. Reached target: Sockets, Basic System, and Default (I don’t understand what this all means, yet).**

Part 2) Fedora Server 28-1.1

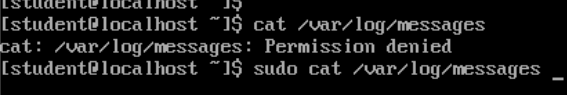
1. Create an ordinary user named **student**.  Working with root privileges, use **visudo**to modify the **/etc/sudoers**file. Add a line that grants the user named **student** full root privileges.

A screenshot of a cell phone

Description automatically generated



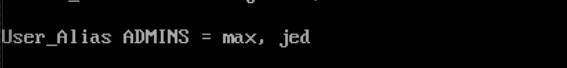
1. Working as **student** view the **/var/log/syslog** or **/var/log/messages** file without and then with sudo. What is the result?



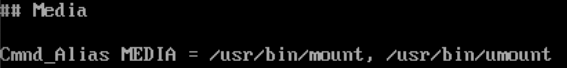
\*Running sudo allows access to /var/log/messages

3. Working with root privileges, use **visudo**to modify the **/etc/sudoers** file. Add lines that:

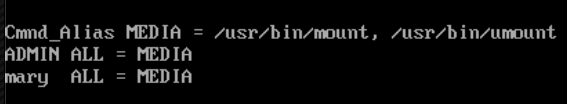
a. Add a user alias named **ADMIN**that includes **max**and **jed**.



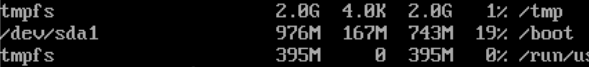
b. Add a command alias named **MEDIA**that includes **mount**and **umount**.



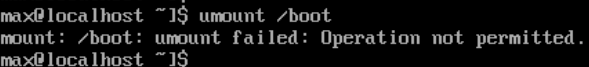
c. Allow **ADMIN**users and **mary** to run the **MEDIA**commands.



1. Working as **max** or **jed**, test sudo using following steps:
2. Look for the **/boot** filesystem using **df -h**



1. Attempt to **umount /boot** without using **sudo**.



c. Use **sudo**to **umount /boot**.

d. Verify the **/boot**filesystem is no longer available using the **df -h**command.

A black and silver text on a screen

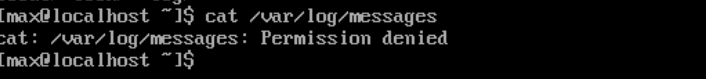
Description automatically generated

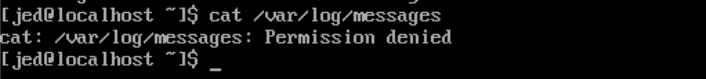
e. Make the **/boot** filesystem available again using the command **sudo mount /boot**.

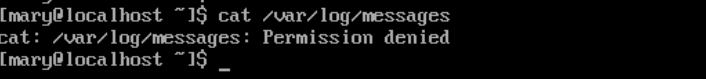
A black and silver text on a screen

Description automatically generated

f. Ensure that users **jed**, **max**, or **mary** cannot run other commands using sudo. For example, attempt to view the **/var/log/syslog** or **/var/log/messages** file.







g. Working with root privileges, view the **tail** of the **/var/log/syslog** or **/var/log/messages** file. What did you find in the file?

\*There is a log of with the USER\_LOGIN PID, hostname with a value of localhost.localdomain, and other daemons.

`