Institute of Computer Technology

B. Tech Computer Science and Engineering

Subject: BOSS (2CSE204)

**PRACTICAL-9**

**AIM: - To learn about analyzing and storing logs in linux.**

**Commands:**

* **Timedatectl –** This command is used to manage time component in linux systems.
* **Journalctl –** This command is used to retrieve system logs from log files.

**Exercise:**

**1. Create user Bob and set password “bob123”.**

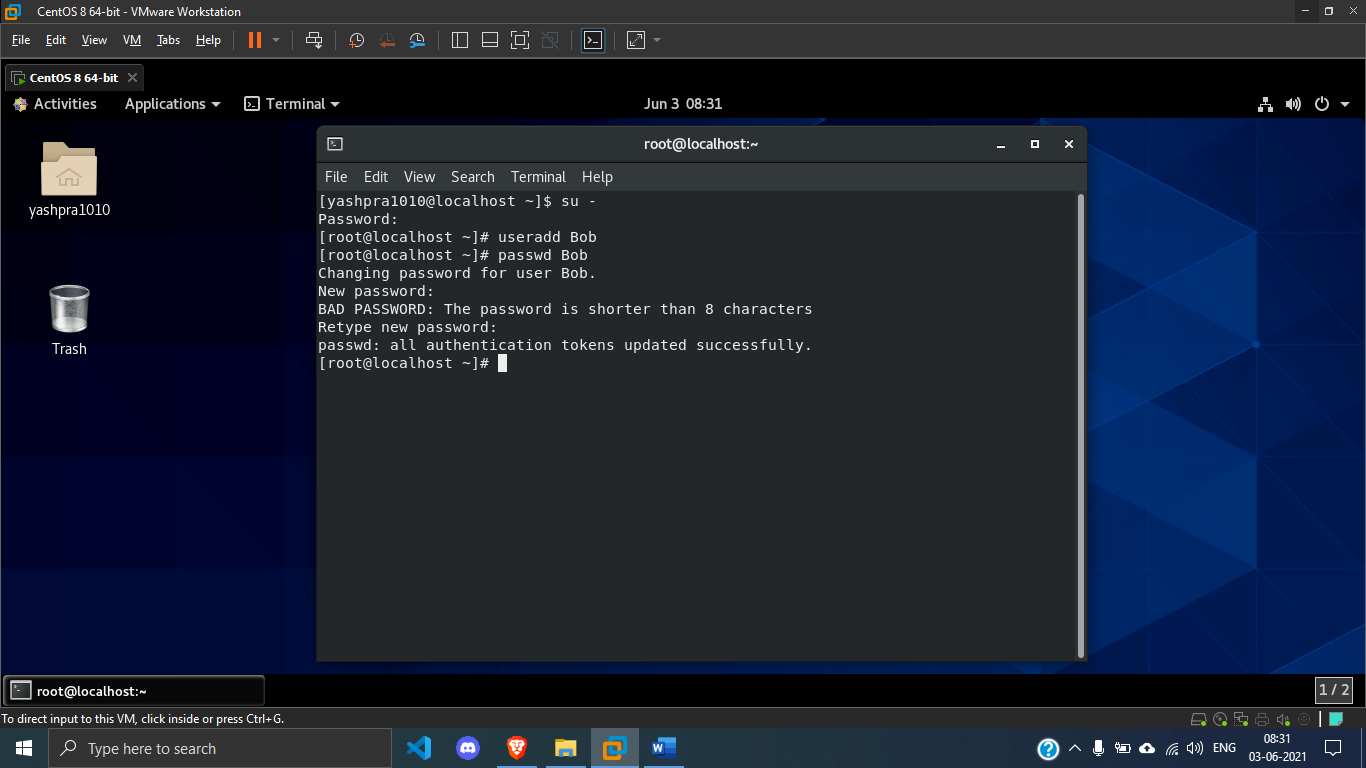
***COMMANDS***

useradd Bob

passwd Bob

Set password – bob123

***SOLUTION***

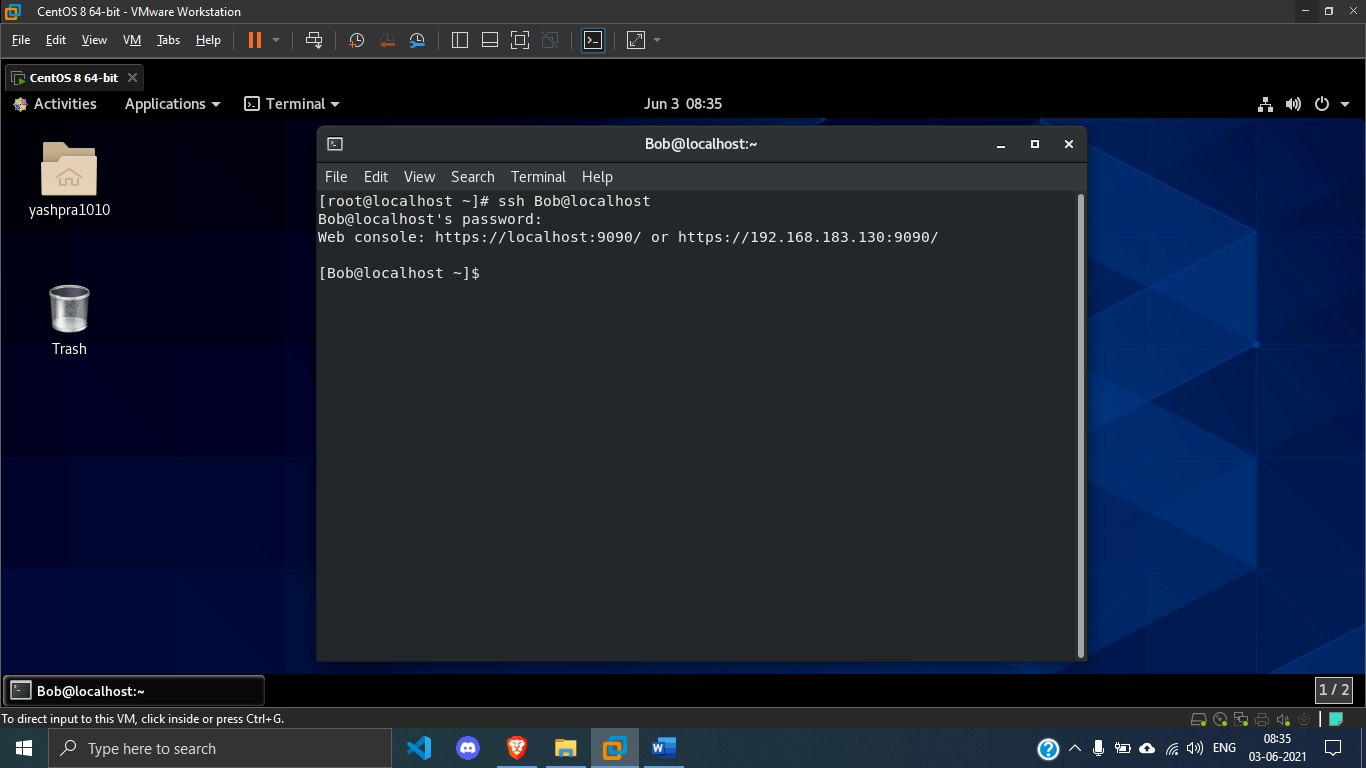


**2. Open an SSH session to localhost as Bob.**

***COMMANDS***

ssh Bob@localhost

***SOLUTION***



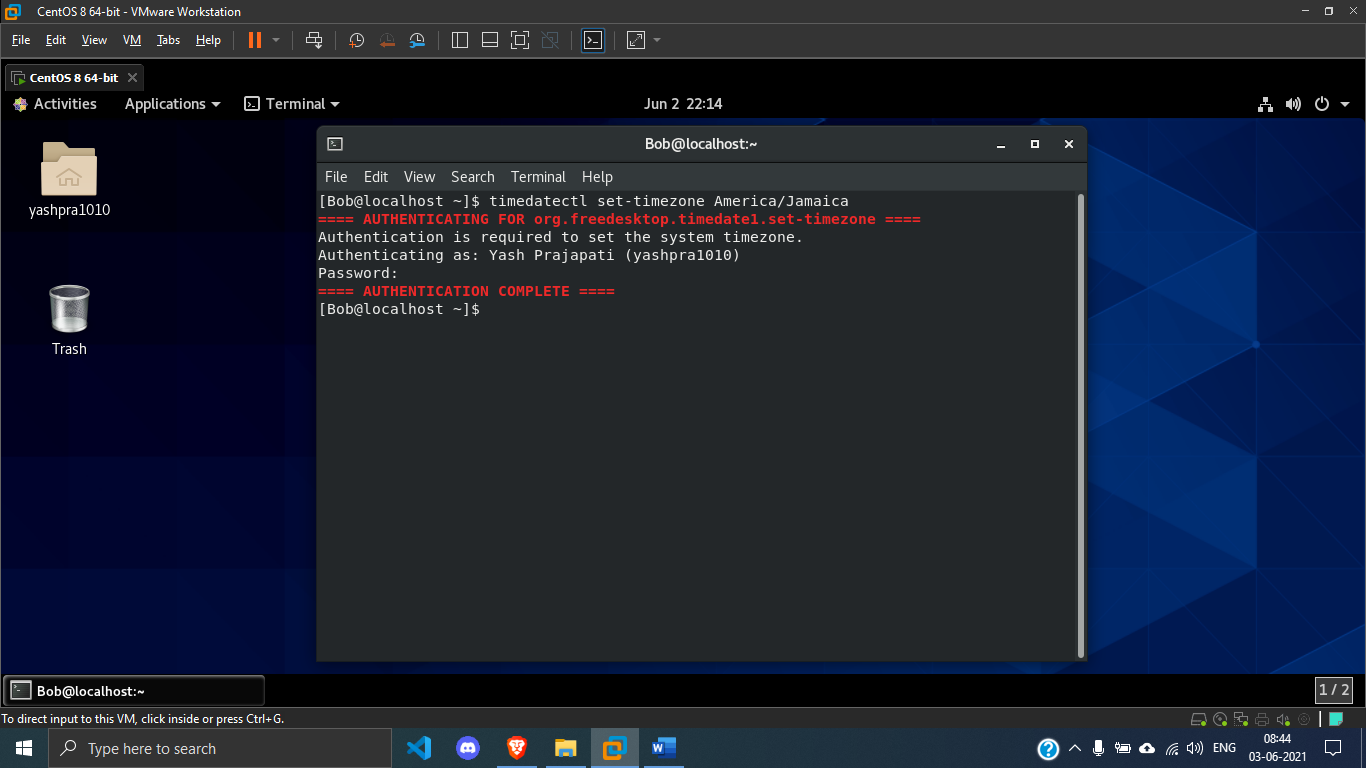
**3. For the sake of this activity, pretend that the localhost system has been relocated to Jamaica and you must update the time zone appropriately.**

***COMMANDS***

timedatectl list-timezones

timedatectl set-timezone America/Jamica

***SOLUTION***



**4. Display all the log events recorded in the previous 30 minutes from the current time on localhost.**

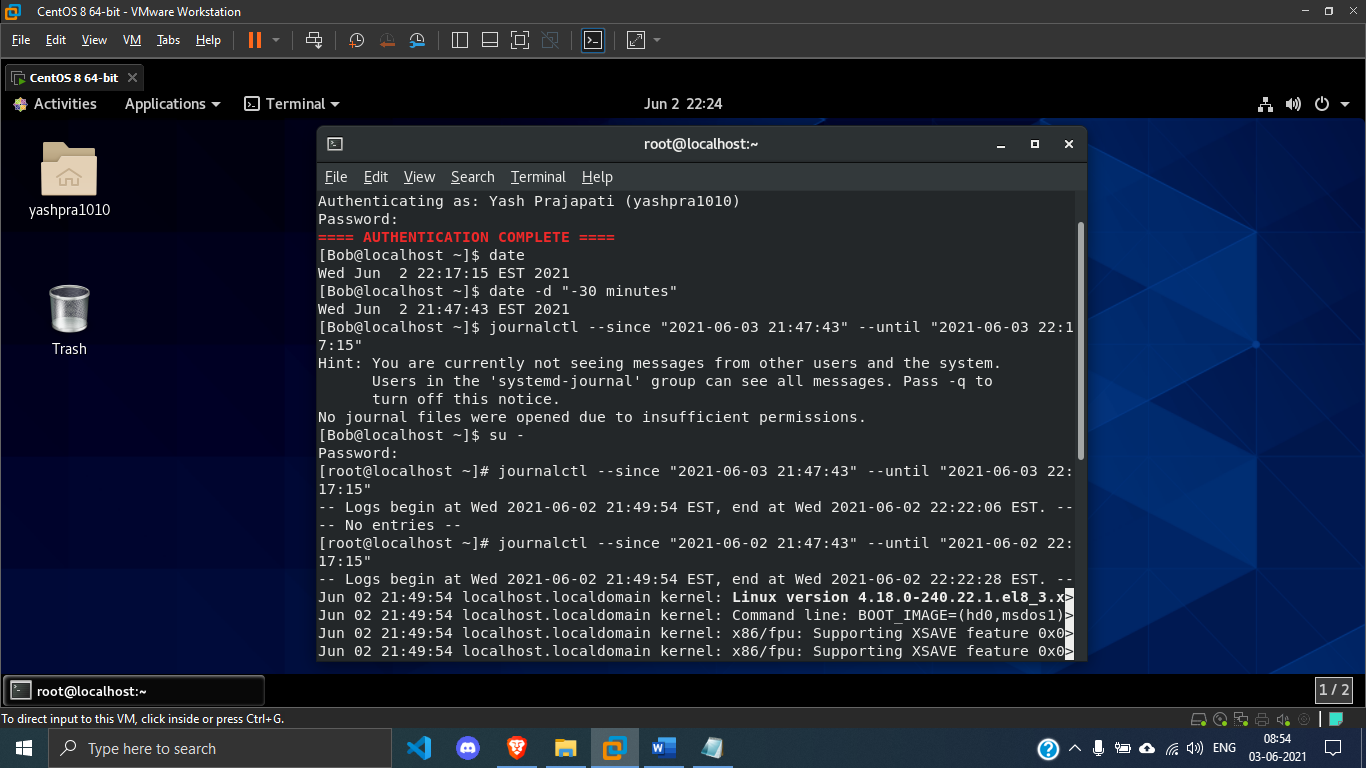
***COMMANDS***

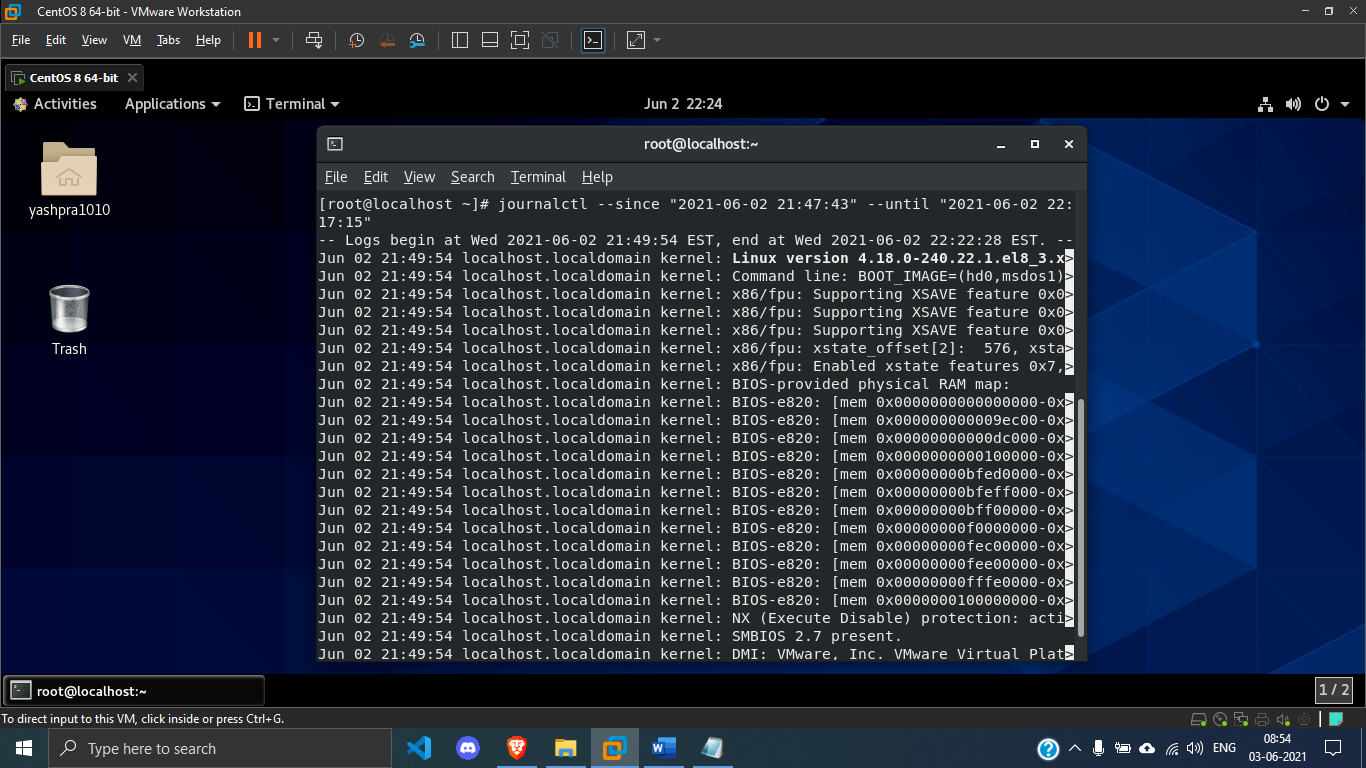
date

date -d “-30 minutes”

journalctl --since "2021-06-02 21:47:43" --until "2021-06-02 22:17:15"

***SOLUTION***





**5. Create the /etc/rsyslog.d/auth-errors.conf file with the necessary lines to help the rsyslog service write messages related to authentication and security issues to the new /var/log/auth-errors file. Use the authpriv facility and the alert priority in the configuration file.**

***COMMANDS***

cat /etc/rsyslog.conf

vi /etc/rsyslog.d/auth-errors.conf

enter in vi = authpriv.alert /var/log/auth-errors

logger -p authprive.alert "Logging test for our facility authpriv.alert"

***SOLUTION***

