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.

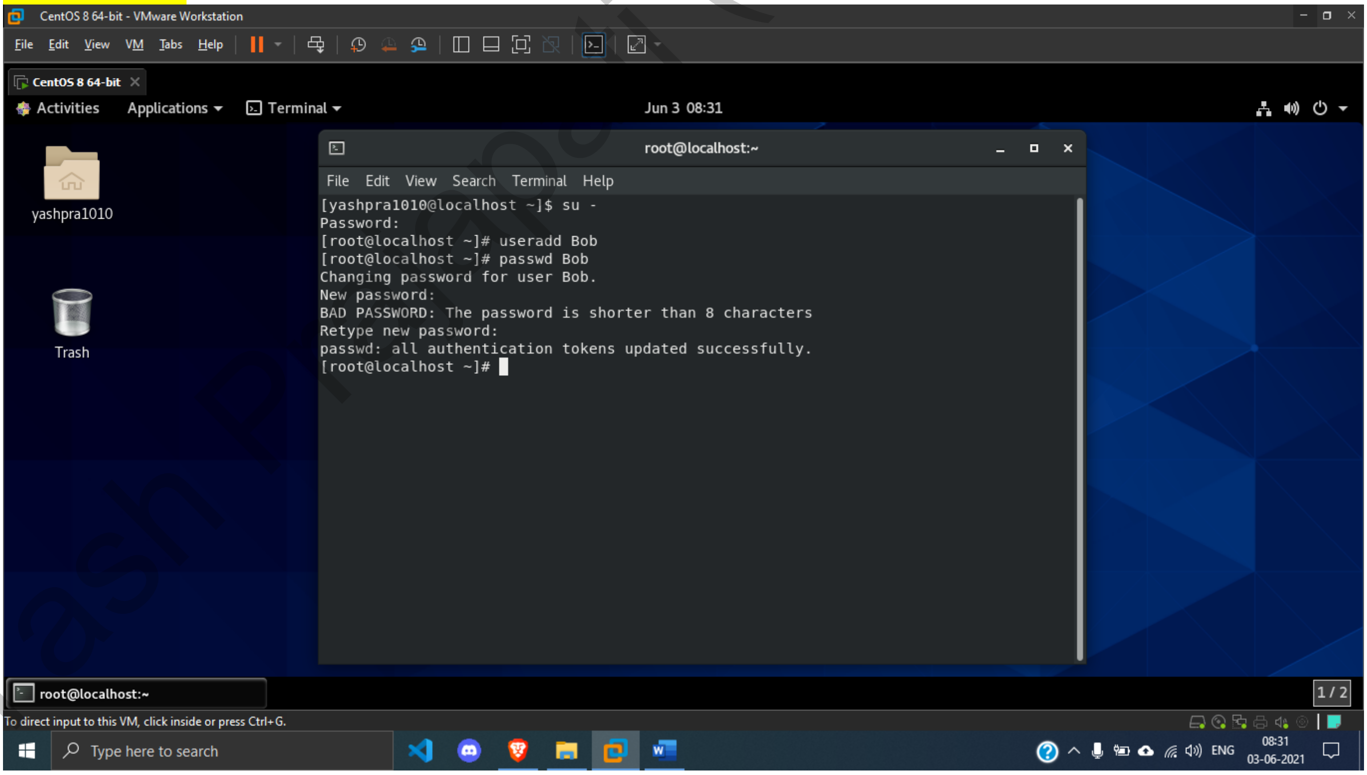
Exercise:

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

COMMANDS

useradd Bob
passwd Bob
Set password – bob123

SOLUTION



```
[yashpra1010@localhost ~]$ su -
Password:
[root@localhost ~]# useradd Bob
[root@localhost ~]# passwd Bob
Changing password for user Bob.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

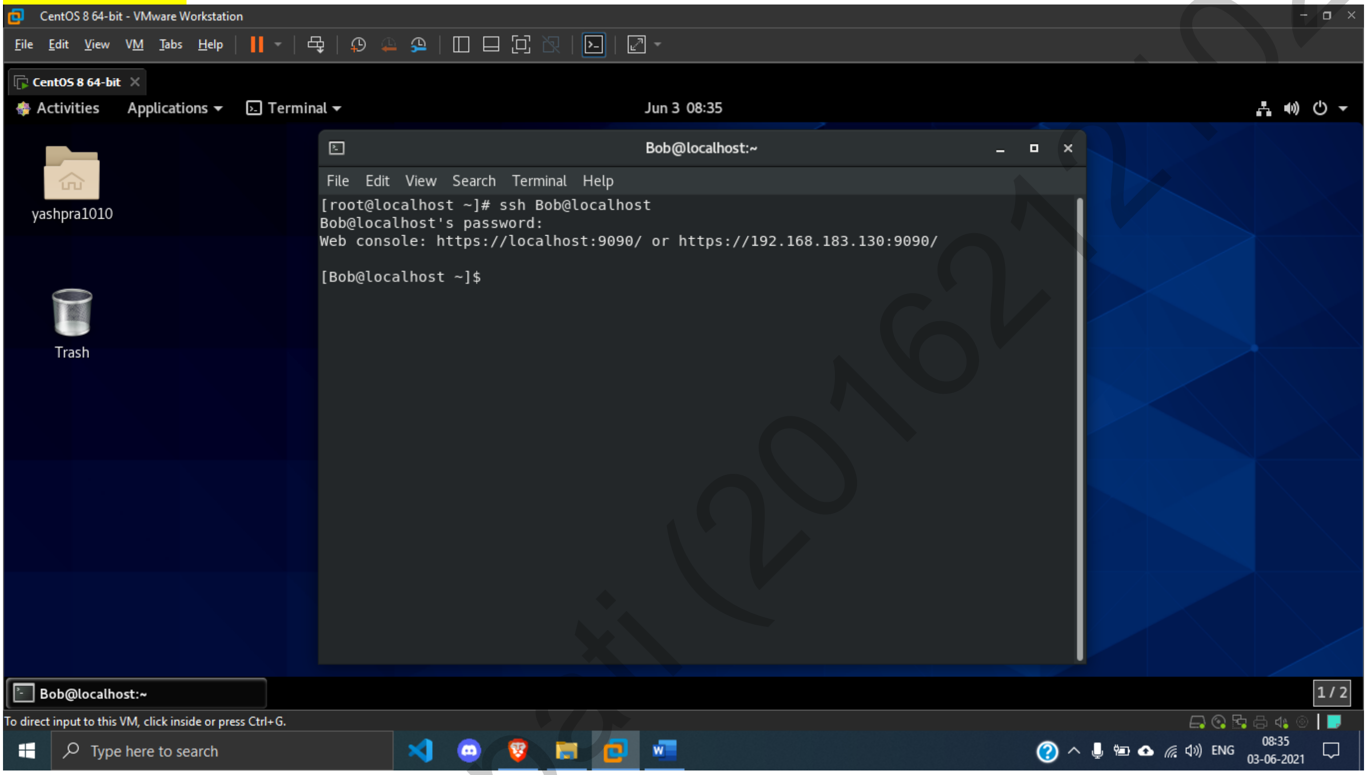
CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities Applications Terminal
Jun 3 08:31
root@localhost:~
File Edit View Search Terminal Help
yashpra1010
Trash
root@localhost:~
1 / 2
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
08:31
03-06-2021

2. Open an SSH session to localhost as Bob.

COMMANDS

ssh Bob@localhost

SOLUTION



CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities
Applications
Terminal
Jun 3 08:35
yashpra1010
Trash
Bob@localhost:~
File Edit View Search Terminal Help
Bob@localhost:~
1 / 2
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
08:35
03-06-2021

```
[root@localhost ~]# ssh Bob@localhost
Bob@localhost's password:
Web console: https://localhost:9090/ or https://192.168.183.130:9090/

[Bob@localhost ~]$
```

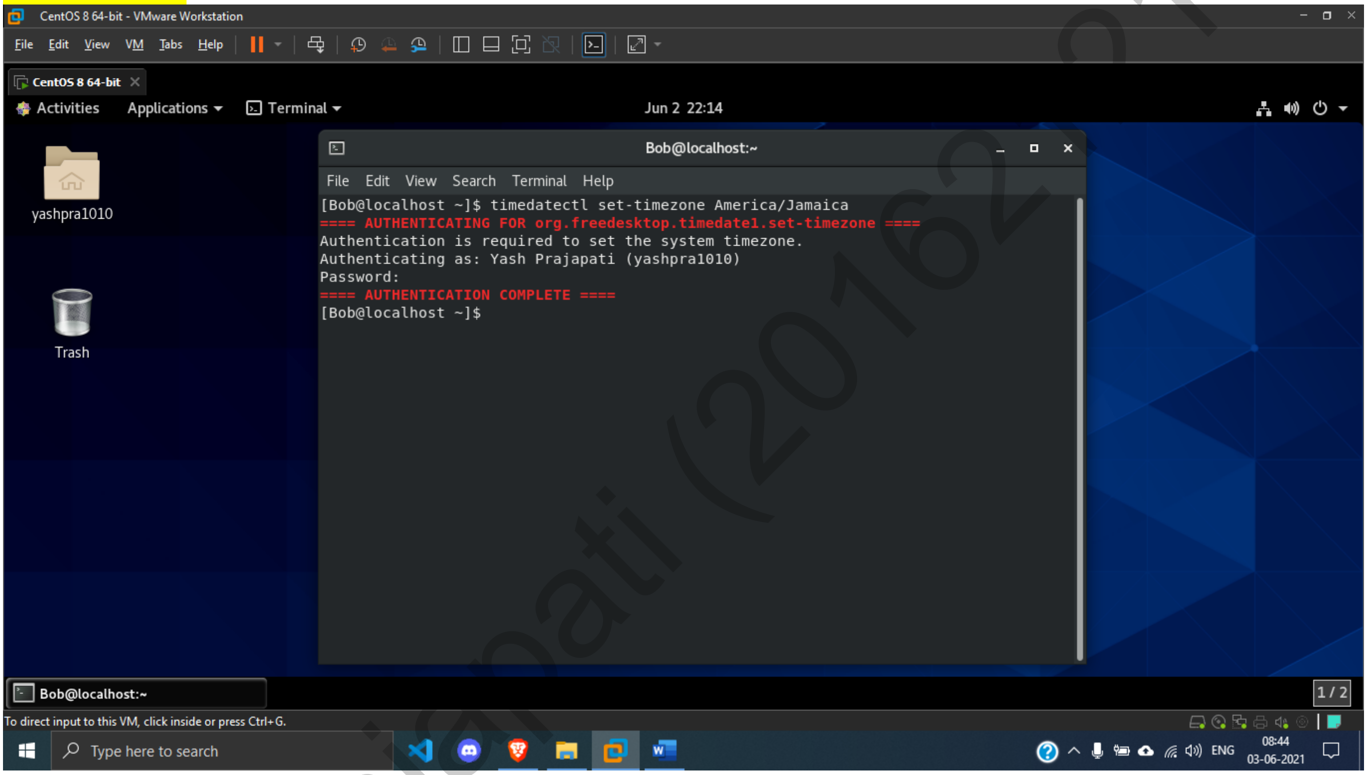
3. For the sake of this activity, pretend that the localhost system has been relocated to Jamaica and you must update the time zone appropriately.

COMMANDS

timedatectl list-timezones

timedatectl set-timezone America/Jamica

SOLUTION


CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities Applications Terminal
Jun 2 22:14
yashpra1010
Trash
Bob@localhost:~
File Edit View Search Terminal Help
Bob@localhost:~
1 / 2
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
08:44
03-06-2021

```
[Bob@localhost ~]$ timedatectl set-timezone America/Jamaica
==== AUTHENTICATING FOR org.freedesktop.timedate1.set-timezone ====
Authentication is required to set the system timezone.
Authenticating as: Yash Prajapati (yashpra1010)
Password:
==== AUTHENTICATION COMPLETE ====
[Bob@localhost ~]$
```

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

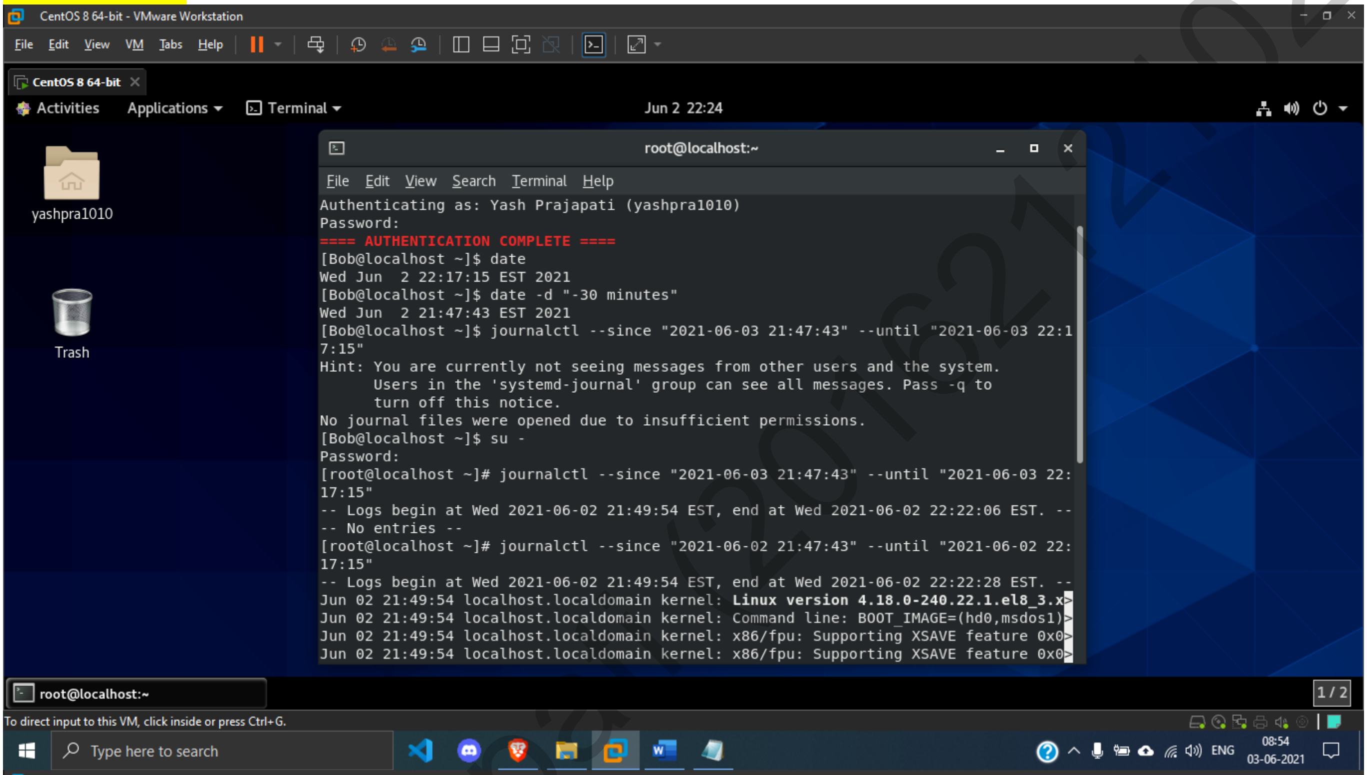
COMMANDS

date

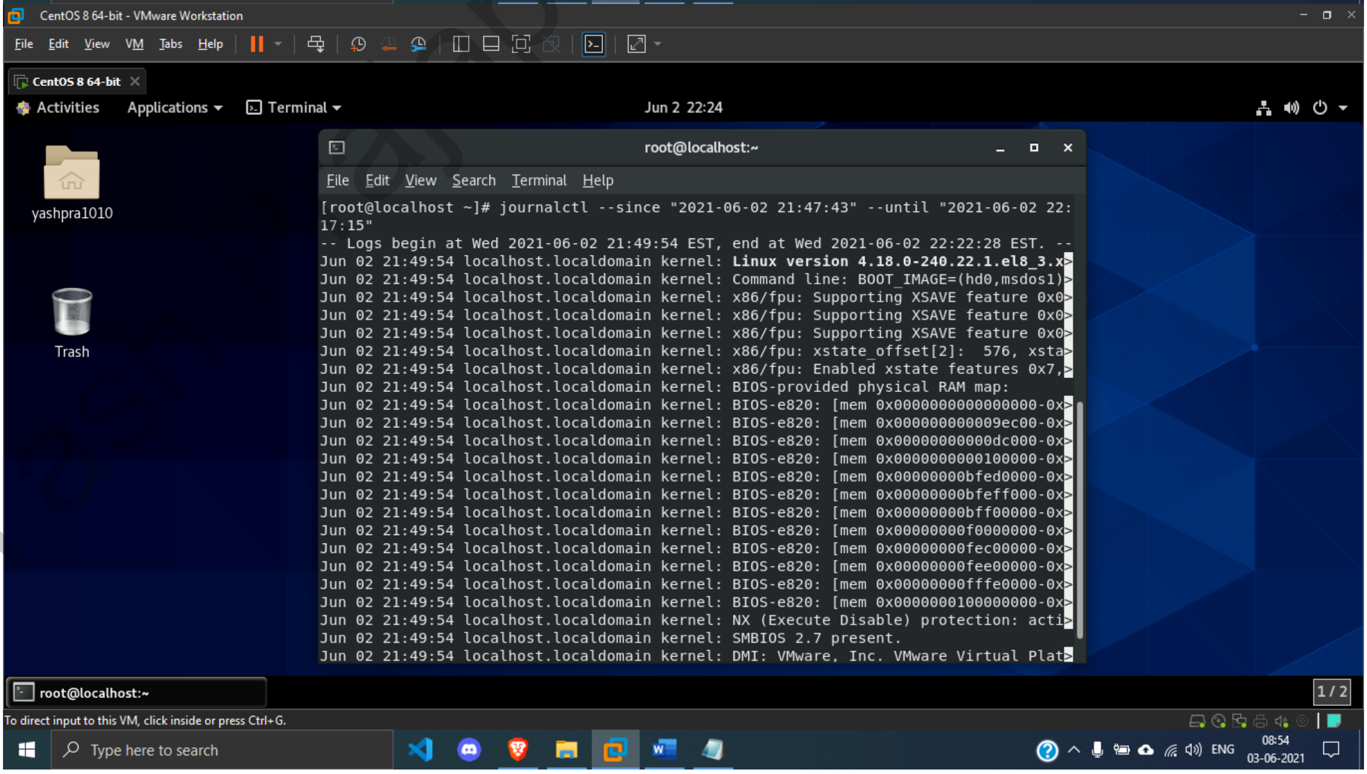
date -d “-30 minutes”

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

SOLUTION


CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities
Applications
Terminal
Jun 2 22:24
yashpra1010
Trash
root@localhost:~
File Edit View Search Terminal Help
root@localhost:~
1 / 2
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
08:54
03-06-2021

```
Authenticating as: Yash Prajapati (yashpra1010)
Password:
==== AUTHENTICATION COMPLETE ====
[Bob@localhost ~]$ date
Wed Jun  2 22:17:15 EST 2021
[Bob@localhost ~]$ date -d "-30 minutes"
Wed Jun  2 21:47:43 EST 2021
[Bob@localhost ~]$ journalctl --since "2021-06-03 21:47:43" --until "2021-06-03 22:1
7:15"
Hint: You are currently not seeing messages from other users and the system.
      Users in the 'systemd-journal' group can see all messages. Pass -q to
      turn off this notice.
No journal files were opened due to insufficient permissions.
[Bob@localhost ~]$ su -
Password:
[root@localhost ~]# journalctl --since "2021-06-03 21:47:43" --until "2021-06-03 22:
17:15"
-- Logs begin at Wed 2021-06-02 21:49:54 EST, end at Wed 2021-06-02 22:22:06 EST. --
-- No entries --
[root@localhost ~]# journalctl --since "2021-06-02 21:47:43" --until "2021-06-02 22:
17:15"
-- Logs begin at Wed 2021-06-02 21:49:54 EST, end at Wed 2021-06-02 22:22:28 EST. --
Jun 02 21:49:54 localhost.localdomain kernel: Linux version 4.18.0-240.22.1.el8_3.x>
Jun 02 21:49:54 localhost.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x0>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x0>
```


CentOS 8 64-bit - VMware Workstation
File Edit View VM Tabs Help
CentOS 8 64-bit
Activities
Applications
Terminal
Jun 2 22:24
yashpra1010
Trash
root@localhost:~
File Edit View Search Terminal Help
root@localhost:~
1 / 2
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
ENG
08:54
03-06-2021

```
[root@localhost ~]# journalctl --since "2021-06-02 21:47:43" --until "2021-06-02 22:
17:15"
-- Logs begin at Wed 2021-06-02 21:49:54 EST, end at Wed 2021-06-02 22:22:28 EST. --
Jun 02 21:49:54 localhost.localdomain kernel: Linux version 4.18.0-240.22.1.el8_3.x>
Jun 02 21:49:54 localhost.localdomain kernel: Command line: BOOT_IMAGE=(hd0,msdos1)>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x0>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x0>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: Supporting XSAVE feature 0x0>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: xstate_offset[2]:  576, xsta>
Jun 02 21:49:54 localhost.localdomain kernel: x86/fpu: Enabled xstate features 0x7,>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-provided physical RAM map:
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x000000000009ec00-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000000dc000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000bfed0000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000bfeff000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000bff00000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000f0000000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x00000000fffe0000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: BIOS-e820: [mem 0x0000000100000000-0x>
Jun 02 21:49:54 localhost.localdomain kernel: NX (Execute Disable) protection: acti>
Jun 02 21:49:54 localhost.localdomain kernel: SMBIOS 2.7 present.
Jun 02 21:49:54 localhost.localdomain kernel: DMI: VMware, Inc. VMware Virtual Plat>
```

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

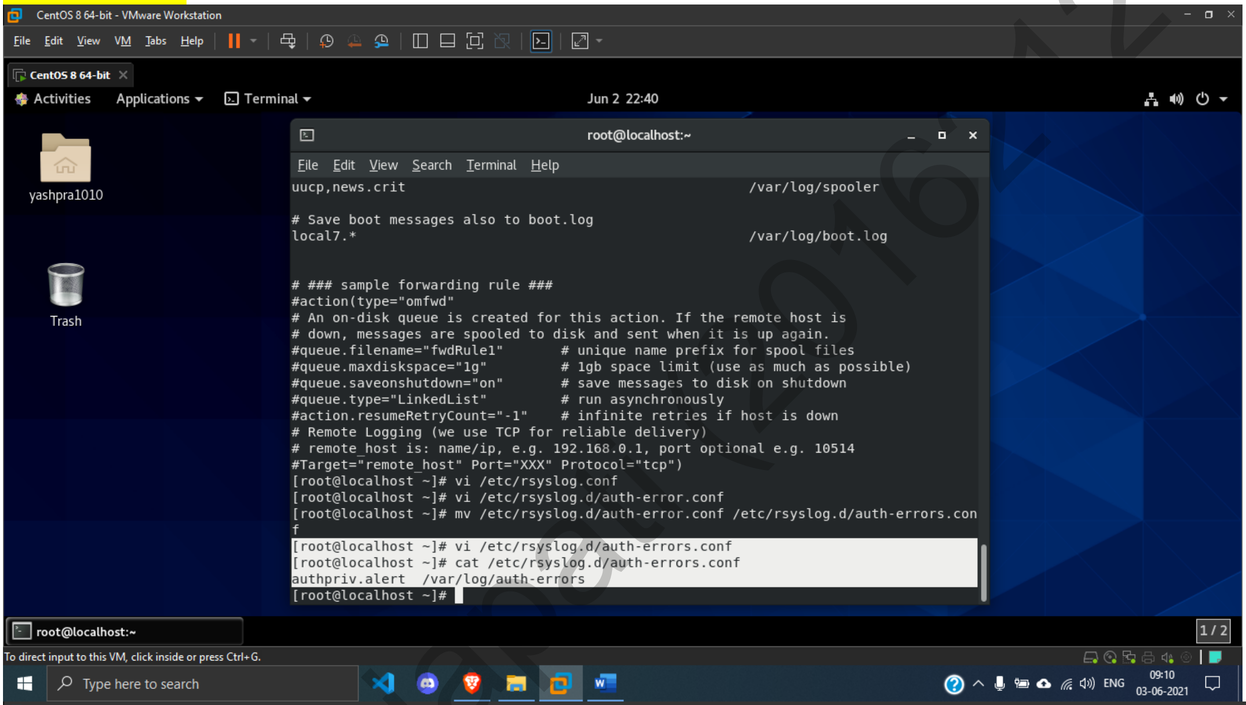
cat /etc/rsyslog.conf

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"

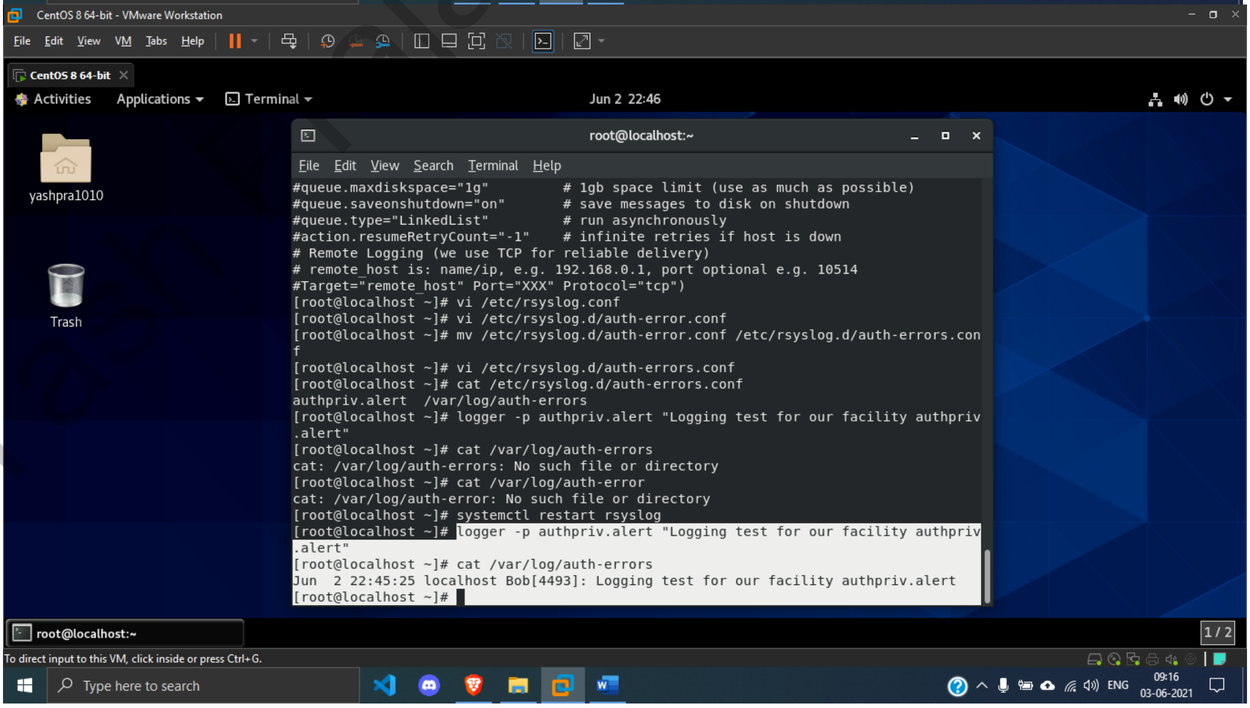
SOLUTION



```
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log


# ### sample forwarding rule ###
#action(type="omfwd"
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#queue.filename="fwdRule1"       # unique name prefix for spool files
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# Remote Logging (we use TCP for reliable delivery)
# remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
[root@localhost ~]# vi /etc/rsyslog.conf
[root@localhost ~]# vi /etc/rsyslog.d/auth-error.conf
[root@localhost ~]# mv /etc/rsyslog.d/auth-error.conf /etc/rsyslog.d/auth-errors.con
f
[root@localhost ~]# vi /etc/rsyslog.d/auth-errors.conf
[root@localhost ~]# cat /etc/rsyslog.d/auth-errors.conf
authpriv.alert  /var/log/auth-errors
[root@localhost ~]#
```



```
#queue.maxdiskspace="1g"         # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"       # save messages to disk on shutdown
#queue.type="LinkedList"         # run asynchronously
#action.resumeRetryCount="-1"    # infinite retries if host is down
# Remote Logging (we use TCP for reliable delivery)
# remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
[root@localhost ~]# vi /etc/rsyslog.conf
[root@localhost ~]# vi /etc/rsyslog.d/auth-error.conf
[root@localhost ~]# mv /etc/rsyslog.d/auth-error.conf /etc/rsyslog.d/auth-errors.con
f
[root@localhost ~]# vi /etc/rsyslog.d/auth-errors.conf
[root@localhost ~]# cat /etc/rsyslog.d/auth-errors.conf
authpriv.alert  /var/log/auth-errors
[root@localhost ~]# logger -p authpriv.alert "Logging test for our facility authpriv
.alert"
[root@localhost ~]# cat /var/log/auth-errors
cat: /var/log/auth-errors: No such file or directory
[root@localhost ~]# cat /var/log/auth-error
cat: /var/log/auth-error: No such file or directory
[root@localhost ~]# systemctl restart rsyslog
[root@localhost ~]# logger -p authpriv.alert "Logging test for our facility authpriv
.alert"
[root@localhost ~]# cat /var/log/auth-errors
Jun  2 22:45:25 localhost Bob[4493]: Logging test for our facility authpriv.alert
[root@localhost ~]#
```