Chapter 11.11: Lab Analyzing and Storing Logs

Marko Shaffer

Information Technology, Franklin University

ITEC 200: Linux Fundamentals

Professor Kagan Ulucay

7/6/2023

**Red Hat System Administration I CH. 11.11**

**Lab 08 CH 11.11 - Lab: Configuring and Securing SSH**

# ****Performance Checklist****

# ****In this lab, you will change the time zone on an existing server and configure a new log file for all events related to authentication failures.****

# ****Outcomes****

You should be able to:

* Update the time zone on an existing server.
* Configure a new log file to store all messages related to authentication failures.

# ****Log in to workstation as student using student as the password.****

|  |  |  |  |
| --- | --- | --- | --- |
|  | Franklin VM: | Standard User Account: | The Student's Root Account: |
| Username | kiosk | student | root |
| Password | redhat | student | redhat |

<https://franklin.instructure.com/courses/12488/modules/items/683350>

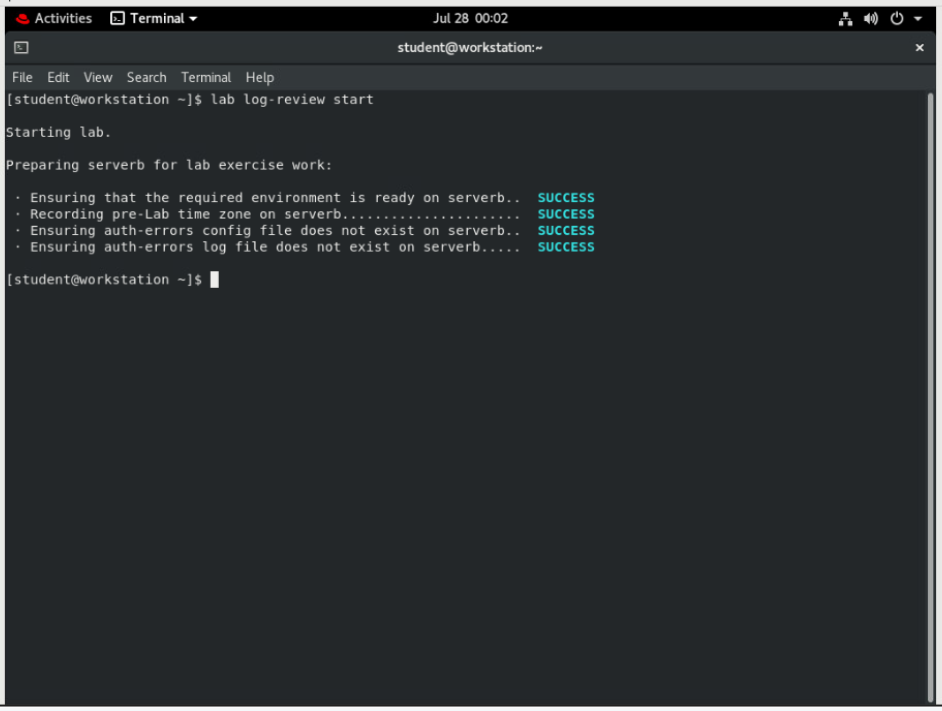
[kiosk@foundation0 ~]$ rht-vmctl start all

[kiosk@foundation0 ~]$ rht-vmview view workstation

# ****Start Lab****

On workstation, run **lab log-review start** to start the exercise. This script records the current time zone of the serverb system and ensures that the environment is setup correctly.

**[student@workstation ~]$ lab log-review start**

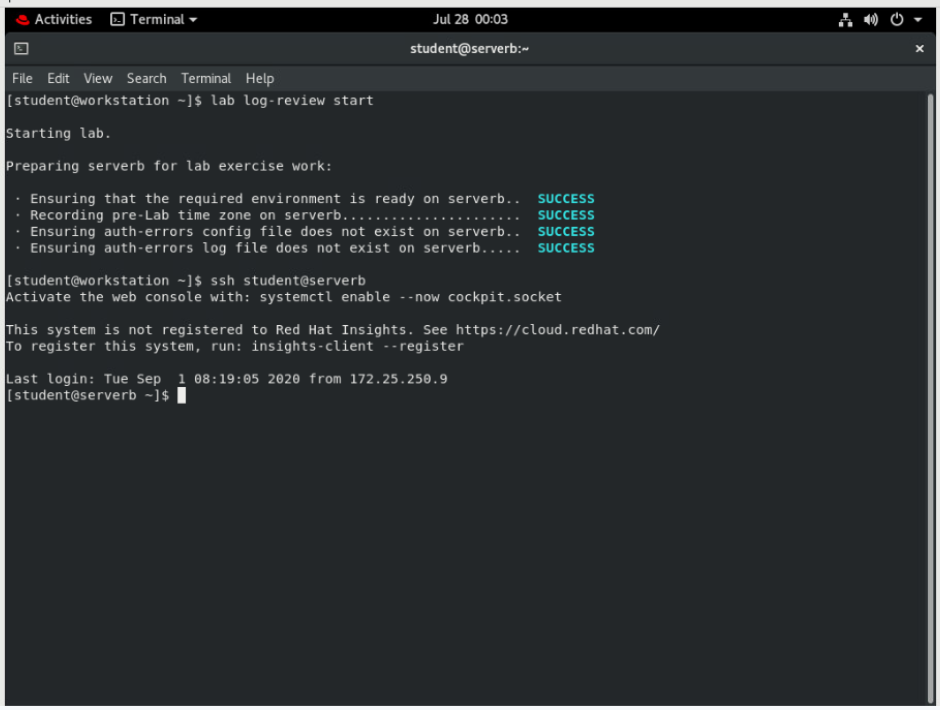


# From workstation, open an SSH session to serverb as student.

**[student@workstation ~]$ ssh student@serverb**

*...output omitted...*

**[student@serverb ~]$**



# Pretend that the serverb system has been relocated to Jamaica and you must update the time zone appropriately. Use sudo to elevate the student user privileges for the timedatectl command to update the time zone. Use student as the password if asked.

* 1. **Use the timedatectl command to view available time zones and determine the appropriate time zone for Jamaica.**

**[student@serverb ~]$ timedatectl list-timezones | grep Jamaica**

America/Jamaica

* 1. **Use the timedatectl command to set the time zone of the serverb system to America/Jamaica.**

**[student@serverb ~]$ sudo timedatectl set-timezone America/Jamaica**

**[sudo] password for student: student**

* 1. **Use the timedatectl command to verify that the time zone is successfully set to America/Jamaica.**

**[student@serverb ~]$ timedatectl**

Local time: Tue 2019-02-19 11:12:46 EST

Universal time: Tue 2019-02-19 16:12:46 UTC

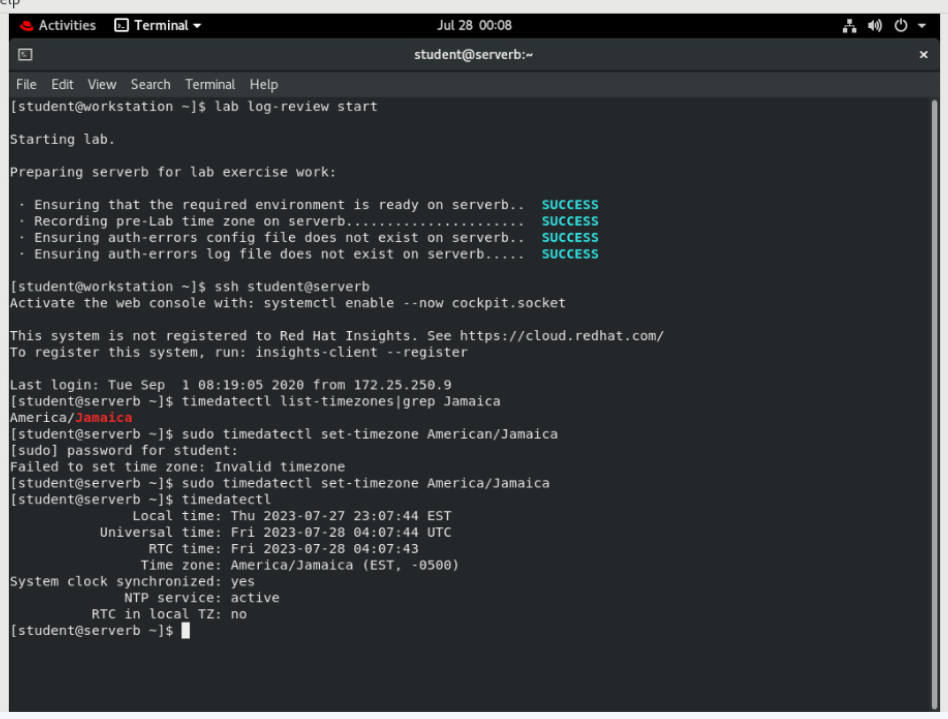
RTC time: Tue 2019-02-19 16:12:45

**Time zone: America/Jamaica (EST, -0500)**

System clock synchronized: yes

NTP service: active

RTC in local TZ: no



# Display the log events recorded in the previous 30 minutes on serverb.

* 1. **Use the date command to determine the time frame to view the journal entries.**

**[student@serverb ~]$ date**

Fri Feb 22 07:31:05 EST 2019

**[student@serverb ~]$ date -d "-30 minutes"**

Fri Feb 22 07:01:31 EST 2019

* 1. **Use the journalctl command --since and --until options to display log events recorded in the previous 30 minutes on serverb. To quit journalctl, press q.**

**[student@serverb ~]$ journalctl --since *07:01:00* --until *07:31:00***

*...output omitted...*

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Reached target Timers.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Reached target Paths.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Starting D-Bus User Message Bus Socket.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Listening on D-Bus User Message Bus Socket.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Reached target Sockets.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Reached target Basic System.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Reached target Default.

Feb 22 07:24:28 serverb.lab.example.com systemd[1138]: Startup finished in 123ms.

Feb 22 07:24:28 serverb.lab.example.com systemd[1]: Started User Manager for UID 1000.

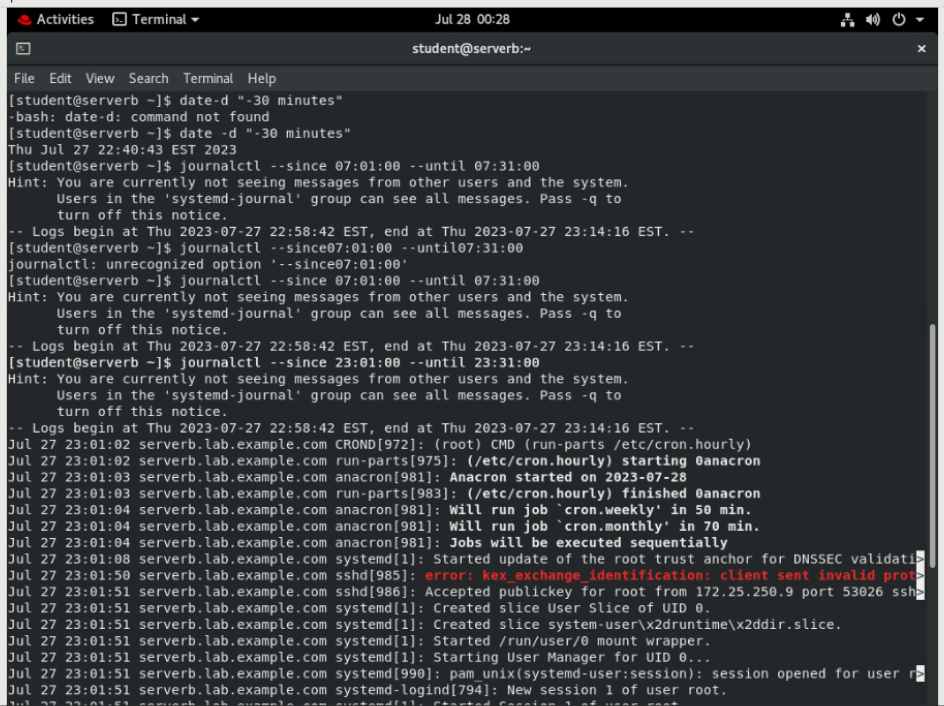
Feb 22 07:24:28 serverb.lab.example.com sshd[1134]: pam\_unix(sshd:session): session opened for user student by (uid=0)

Feb 22 07:26:56 serverb.lab.example.com systemd[1138]: Starting Mark boot as successful...

Feb 22 07:26:56 serverb.lab.example.com systemd[1138]: Started Mark boot as successful.

**lines 1-36/36 (END) q**

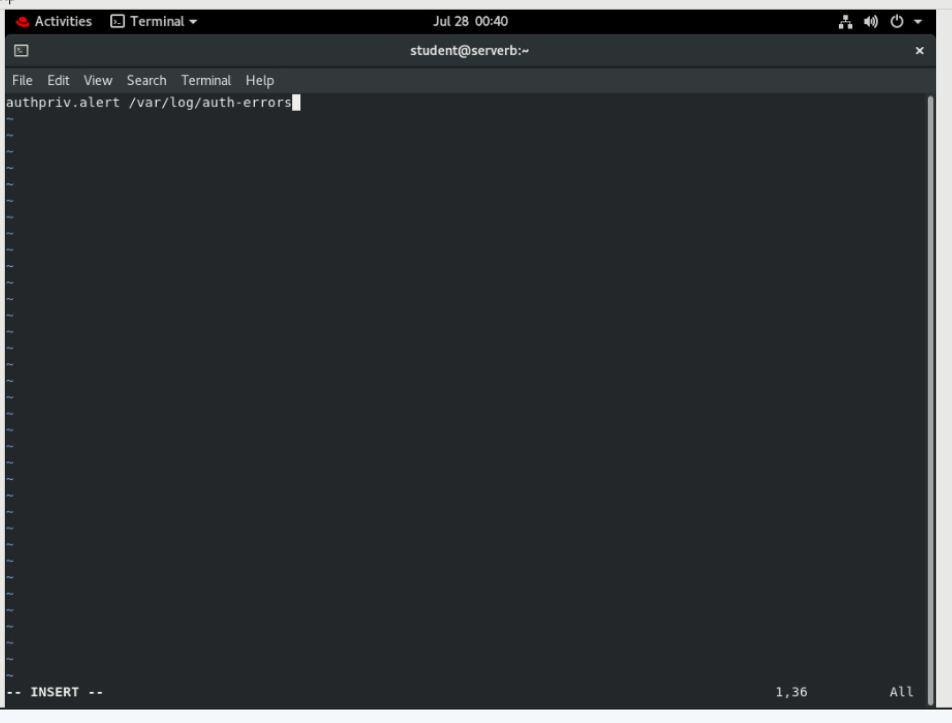
**[student@serverb ~]$**



# Create the /etc/rsyslog.d/auth-errors.conf file, configured to have 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.

* 1. Create the /etc/rsyslog.d/auth-errors.conf file to specify the new /var/log/auth-errors file as the destination for messages related to authentication and security issues. You may use the **sudo vim /etc/rsyslog.d/auth-errors.conf** command to create the configuration file.

authpriv.alert /var/log/auth-errors



* 1. Restart the rsyslog service so that the changes in the configuration file take effect.

**[student@serverb ~]$ sudo systemctl restart rsyslog**

* 1. Use the **logger** command to write a new log message to the /var/log/auth-errors file. Apply the -p authpriv.alert option to generate a log message relevant to authentication and security issues.

**[student@serverb ~]$ logger -p authpriv.alert "Logging test authpriv.alert"**

* 1. Use the **tail** command to confirm that the /var/log/auth-errors file contains the log entry with the Logging test authpriv.alert message.

**[student@serverb ~]$ sudo tail /var/log/auth-errors**

Feb 19 11:56:07 serverb student[6038]: **Logging test authpriv.alert**

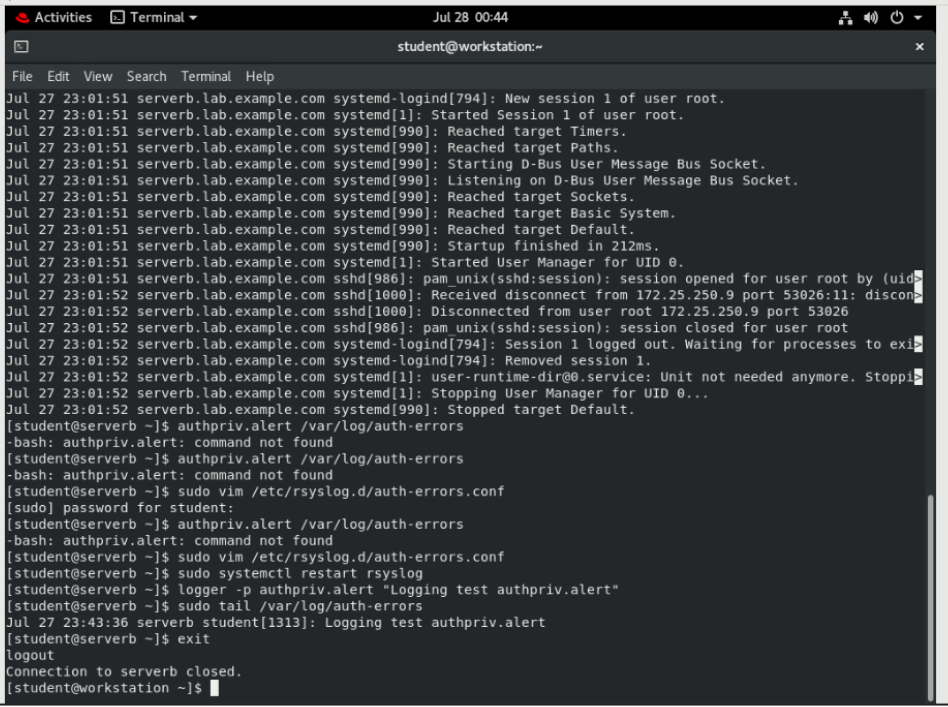
* 1. Log out of serverb.

**[student@serverb ~]$ exit**

logout

Connection to serverb closed.

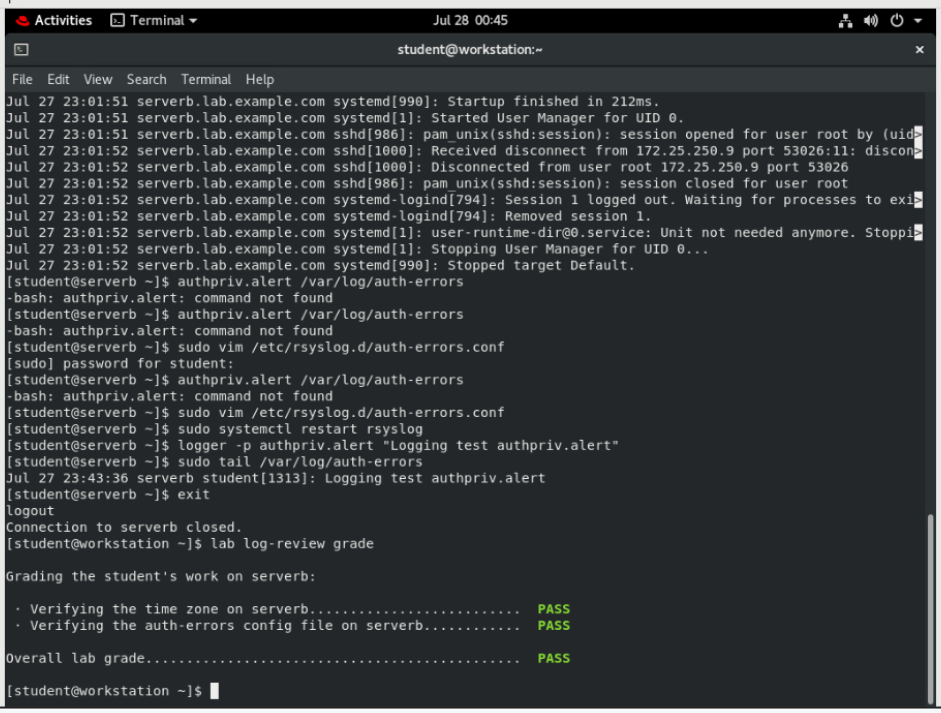
**[student@workstation ~]$**



# Evaluation

On workstation, run the **lab log-review grade** command to confirm success of this exercise.

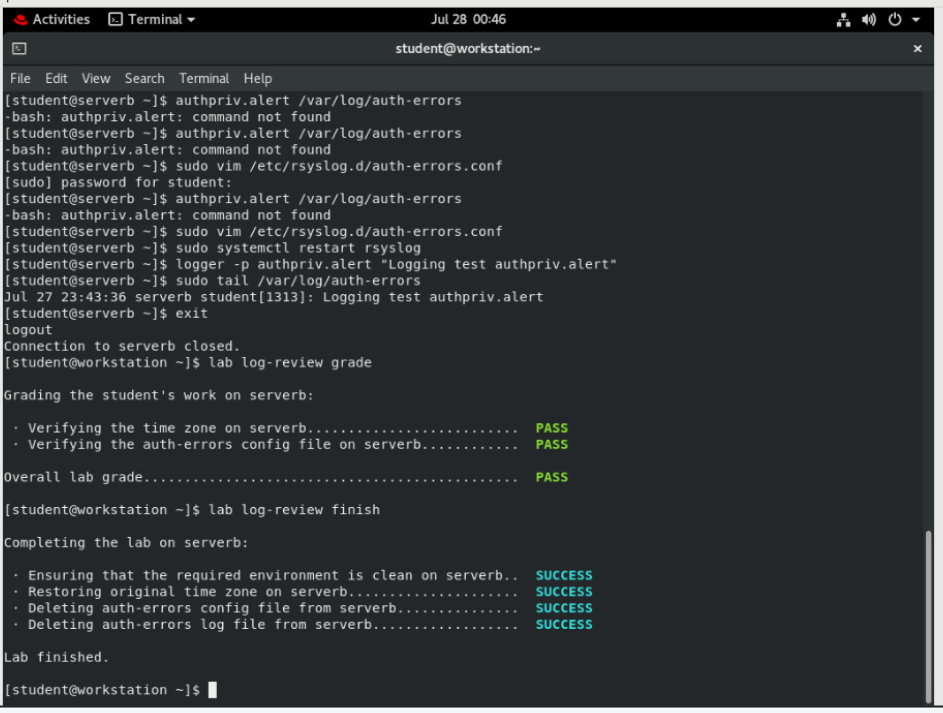
**[student@workstation ~]$ lab log-review grade**



# Finish

On workstation, run **lab log-review finish** to complete this lab. This script ensures that the original time zone is restored along with all the original time settings on serverb.

**[student@workstation ~]$ lab log-review finish**



This concludes the guided exercise.