

Chapter 11: Analyzing and Storing Logs (Task)

In this task, you **MUST** use the online lab environment at the Redhat classroom. Then start do the following instructions.

Your answer should be delivered in a pdf file contains the screenshots of your steps on the online lab environment.

Before You Begin

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

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
```

1. From **workstation**, open an SSH session to **serverb** as **student**.
2. 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.
3. Display the log events recorded in the previous 30 minutes on **serverb**.
4. 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.