245-[LX]-Lab - Managing Log Files

Managing Log Files

> **Note**
>
> All labs rely on previous courseware and lab information.

Objectives

In this lab, you will:

- Review the **lastlog** and secure log outputs of the Linux machine

Duration

This lab requires approximately **5-10 minutes** to complete.

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that you need to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that this lab describes.

Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch your lab.
   A **Start Lab** panel opens, and it displays the lab status.

   > **Tip**: If you need more time to complete the lab, choose the Start Lab button again to restart the timer for the environment.

2. Wait until you see the message *Lab status: ready*, then close the **Start Lab** panel by choosing the **X**.
3. At the top of these instructions, choose AWS.
   This opens the AWS Management Console in a new browser tab. The system will automatically log you in.

   > **Tip**: If a new browser tab does not open, a banner or icon is usually at the top of your browser with a message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon and then choose **Allow pop ups**.

4. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you will be able to see both browser tabs at the same time so that you can follow the lab steps more easily.

Task 1: Use SSH to connect to an Amazon Linux EC2 instance

In this task, you will connect to a Amazon Linux EC2 instance. You will use an SSH utility to perform all of these operations. The following instructions vary slightly depending on whether you are using Windows or Mac/Linux.

Windows Users: Using SSH to Connect

These instructions are specifically for Windows users. If you are using macOS or Linux, skip to the next section.

5. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
6. Select the **Download PPK** button and save the **labsuser.ppk** file.
   Typically your browser will save it to the Downloads directory.
7. Make a note of the **PublicIP** address.
8. Then exit the Details panel by selecting the **X**.
9. Download **PuTTY** to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer, download it here.
10. Open **putty.exe**
11. Configure your PuTTY session by following the directions in the following link: Connect to your Linux instance using PuTTY
12. Windows Users: Select here to skip ahead to the next task.

Task 2: Review secure log files

In this task, you use common Linux tools to review the **secure** log files and use the **lastlog** Linux application to review the previous logins.

21. To validate that you are in the **companyA** home folder, enter `pwd` and press Enter.

    If you are not in this folder, enter `cd companyA` and press Enter.

22. To use the secure log file as a test, enter `sudo less /tmp/log/secure` and press Enter. It should look like the following:

```
![Image shows the output of sudo less /tmp/log/secure lists the authentication failures.](images/tmp-log.jpg)

*Figure: The list of errors and failures include the following information: where the user was trying to access from (IP address), if they failed authentication, and which port.*
```

```
>**Note**
>
>Usually, the secure log file is located at **/var/log/secure**.  This lab presents a sample secure log file at **/tmp/log/secure**.
```

23. To exit the program, enter `q`
24. To view the last login times of all the users on the machine, enter `sudo lastlog` and press Enter. It should look like the following:

```
![Image shows output of sudo lastlog command and displays a list of every user and their most recent log in date/time. ](images/last-log.jpg)

*Figure: Examples of the users who last logged in were: root which shows as never logged in, bin never logged in, and daemon never logged in, etc. *
```

Lab Complete 🎓

🏁 Congratulations! You have completed the lab.

25. Select End Lab at the top of this page and then select Yes to confirm that you want to end the lab.

    A panel will appear, indicating that "DELETE has been initiated... You may close this message box now."
26. Select the **X** in the top right corner to close the panel.