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 PuTTY timeout to keep the PuTTY session open for a longer period of time.:
    - Select **Connection**
    - Set **Seconds between keepalives** to `30`
12. Configure your PuTTY session:
    - Select **Session**
    - **Host Name (or IP address):** Paste the **Public DNS or IPv4 address** of the instance you made a note of earlier.
      Alternatively, return to the EC2 Console and select **Instances**. Check the box next to the instance you want to connect to and in the *Description* tab copy the **IPv4 Public IP** value.
    - Back in PuTTY, in the **Connection** list, expand **SSH**
    - Select **Auth** *(don't expand it)*
    - Select **Browse**
    - Browse to and select the lab#.ppk file that you downloaded
    - Select **Open** to select it
    - Select **Open** again.
13. Select **Yes**, to trust and connect to the host.
14. When prompted **login as**, enter: `ec2-user`
    This will connect you to the EC2 instance.
15. Windows Users: Select here to skip ahead to the next task.

macOS and Linux Users

These instructions are specifically for Mac/Linux users. If you are a Windows user, skip ahead to the next task.

16. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
17. Select the **Download PEM** button and save the **labsuser.pem** file.
18. Make a note of the **PublicIP** address.
19. Then exit the Details panel by selecting the **X**.
20. Open a terminal window, and change directory `cd` to the directory where the *labsuser.pem* file was downloaded. For example, if the *labuser.pem* file was saved to your Downloads directory, run this command:

```
cd ~/Downloads
```

21. Change the permissions on the key to be read-only, by running this command:

```
chmod 400 labsuser.pem
```

22. Run the below command *(replace **<public-ip>** with the **PublicIP** address you copied earlier)*. Alternatively, return to the EC2 Console and select **Instances**. Check the box next to the instance you want to connect to and in the *Description* tab copy the **IPv4 Public IP** value.:

```
ssh -i labsuser.pem ec2-user@<public-ip>
```

23. Type `yes` when prompted to allow the first connection to this remote SSH server.
Because you are using a key pair for authentication, you will not be prompted for a password.

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.

24. 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.

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

```
[ec2-user@ip-10-0-10-50 ~]$ cd companyA
[ec2-user@ip-10-0-10-50 companyA]$ sudo less /tmp/log/secure
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218
Aug 23 03:47:13 centos7 sshd[3283]: input_userauth_request: invalid user guest [preauth]
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=193.201.224.218
Aug 23 03:47:15 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181 ssh2
Aug 23 03:47:16 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:17 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181 ssh2
Aug 23 03:47:18 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
```

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**.

26. To exit the program, enter `q`
27. 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:

```
[ec2-user@ip-10-0-10-50 companyA]$ sudo lastlog
Username         Port     From             Latest
root                                       **Never logged in**
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
ftp                                        **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
dbus                                       **Never logged in**
rpc                                        **Never logged in**
libstoragemgmt                             **Never logged in**
sshd                                       **Never logged in**
rngd                                       **Never logged in**
rpcuser                                    **Never logged in**
nfsnobody                                  **Never logged in**
ec2-instance-connect                           **Never logged in**
postfix                                    **Never logged in**
chrony                                     **Never logged in**
tcpdump                                    **Never logged in**
ec2-user         pts/0    205.251.233.182  Thu Aug 26 22:11:38 +0000 2021
```

*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. *

Additional challenge

What information can you extract for some of your business purposes?

Lab Complete

Congratulations! You have completed the lab.

28. 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."

29. Select the **X** in the top right corner to close the panel.

About the AWS component

Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more *instance sizes* so that you can scale your resources to the requirements of your target workload.

This lab uses a **t3.micro** instance, which should be selected by default. This instance type has 1 virtual CPU and 1 GiB of memory.

Additional resources

- Amazon EC2 Instance Types
- Amazon Machine Images (AMI)
- Status Checks for Your Instances
- Amazon EC2 Service Quotas
- Terminate Your Instance

For more information about AWS Training and Certification, see https://aws.amazon.com/training/.

Your feedback is welcome and appreciated.
If you would like to share any suggestions or corrections, please provide the details in our AWS Training and Certification Contact Form.