AWS re:Start

LAB

Managing Log Files

WEEK 3

aws re/start

Overview

Log files are integral to Linux system administration, residing mainly in /var/log and offering insights into system operations, errors, and user activities. Understanding severity levels like INFO, WARNING, ERROR, and CRITICAL helps prioritize issue resolution. Tools like grep, less, and tail facilitate efficient log analysis, extracting specific information and monitoring real-time updates.

Log rotation is crucial for managing log files, preventing excessive disk usage. This process involves archiving older logs, maintaining recent ones for analysis, and ensuring optimal system performance and storage efficiency. Maintaining a log history aids in auditing, compliance, and troubleshooting efforts.

Note: This lab was made using Windows Subsystem for Linux.

Topics covered

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

Task 1

Use SSH to connect to an Amazon Linux EC2 instance

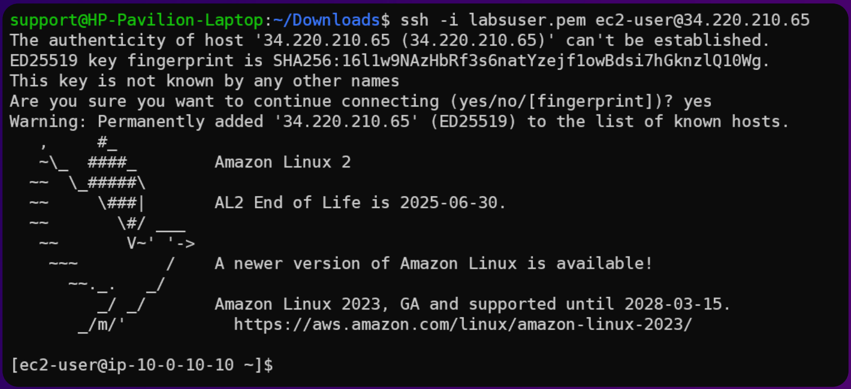
Initial Preparations

In the AWS Management Console, select the EC2 instance and make note of the **Public IPv4 address**.

Download the **private key file** labsuser.pem. Change to the Downloads directory and modify the permissions on the key to be read-only (r--------).

Connect to the instance using SSH

Establish a connection to the EC2 instance using the ssh command, the key and the instance’s public IPv4 address.



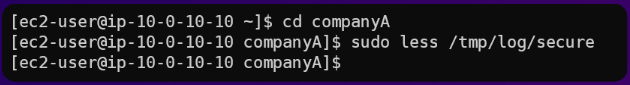
```
support@HP-Pavilion-Laptop:~/Downloads$ ssh -i labsuser.pem ec2-user@34.220.210.65
The authenticity of host '34.220.210.65 (34.220.210.65)' can't be established.
ED25519 key fingerprint is SHA256:16l1w9NAzHbRf3s6natYzejf1owBdsi7hGknzlQ10Wg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.220.210.65' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-10-10 ~]$
```

Task 2

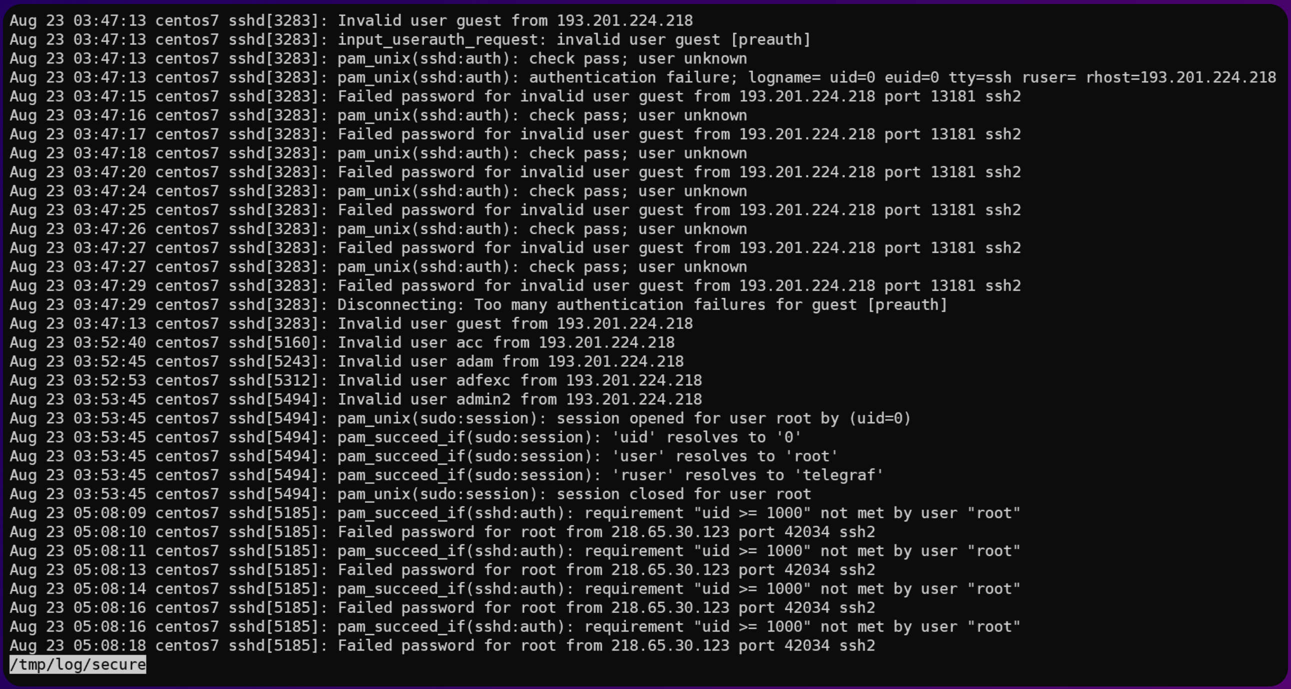
Review secure log files

Step 1: Review the secure log files

Usually, the secure log file is located at **/var/log/secure**. This lab presents a sample secure log file at **/tmp/log/secure**. To use the secure log file as a test, enter the command sudo less /tmp/log/secure.



```
[ec2-user@ip-10-0-10-10 ~]$ cd companyA
[ec2-user@ip-10-0-10-10 companyA]$ sudo less /tmp/log/secure
[ec2-user@ip-10-0-10-10 companyA]$
```



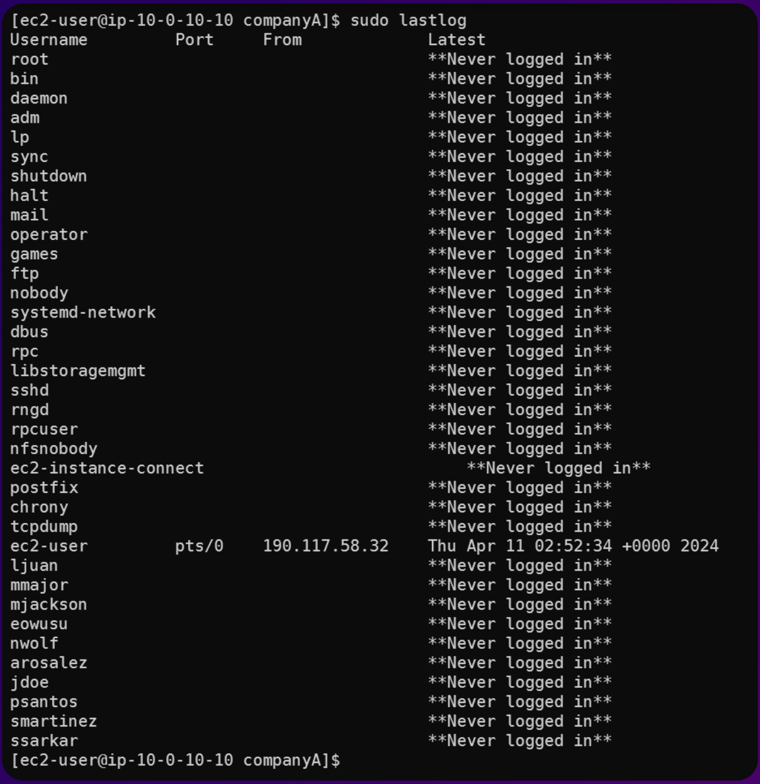
```
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218
Aug 23 03:47:13 centos7 sshd[3283]: input_userauth_request: invalid user guest [preauth]
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): 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
Aug 23 03:47:20 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181 ssh2
Aug 23 03:47:24 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:25 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181 ssh2
Aug 23 03:47:26 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:27 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181 ssh2
Aug 23 03:47:27 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
Aug 23 03:47:29 centos7 sshd[3283]: Failed password for invalid user guest from 193.201.224.218 port 13181 ssh2
Aug 23 03:47:29 centos7 sshd[3283]: Disconnecting: Too many authentication failures for guest [preauth]
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218
Aug 23 03:52:40 centos7 sshd[5160]: Invalid user acc from 193.201.224.218
Aug 23 03:52:45 centos7 sshd[5243]: Invalid user adam from 193.201.224.218
Aug 23 03:52:53 centos7 sshd[5312]: Invalid user adfexc from 193.201.224.218
Aug 23 03:53:45 centos7 sshd[5494]: Invalid user admin2 from 193.201.224.218
Aug 23 03:53:45 centos7 sshd[5494]: pam_unix(sudo:session): session opened for user root by (uid=0)
Aug 23 03:53:45 centos7 sshd[5494]: pam_succeed_if(sudo:session): 'uid' resolves to '0'
Aug 23 03:53:45 centos7 sshd[5494]: pam_succeed_if(sudo:session): 'user' resolves to 'root'
Aug 23 03:53:45 centos7 sshd[5494]: pam_succeed_if(sudo:session): 'ruser' resolves to 'telegraf'
Aug 23 03:53:45 centos7 sshd[5494]: pam_unix(sudo:session): session closed for user root
Aug 23 05:08:09 centos7 sshd[5185]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Aug 23 05:08:10 centos7 sshd[5185]: Failed password for root from 218.65.30.123 port 42034 ssh2
Aug 23 05:08:11 centos7 sshd[5185]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Aug 23 05:08:13 centos7 sshd[5185]: Failed password for root from 218.65.30.123 port 42034 ssh2
Aug 23 05:08:14 centos7 sshd[5185]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Aug 23 05:08:16 centos7 sshd[5185]: Failed password for root from 218.65.30.123 port 42034 ssh2
Aug 23 05:08:16 centos7 sshd[5185]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"
Aug 23 05:08:18 centos7 sshd[5185]: Failed password for root from 218.65.30.123 port 42034 ssh2
/tmp/log/secure
```

Task 2

Review secure log files

Step 2: Review previous logins

To view the last login times of all the users on the machine, enter the sudo lastlog command.



```
[ec2-user@ip-10-0-10-10 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    190.117.58.32    Thu Apr 11 02:52:34 +0000 2024
ljuan                                      **Never logged in**
mmajor                                     **Never logged in**
mjackson                                   **Never logged in**
eowusu                                     **Never logged in**
nwolf                                      **Never logged in**
arosalez                                   **Never logged in**
jdoe                                       **Never logged in**
psantos                                    **Never logged in**
smartinez                                  **Never logged in**
ssarkar                                    **Never logged in**
[ec2-user@ip-10-0-10-10 companyA]$
```

Conclusions

Managing log files

Effective management of log files is essential for maintaining system health and security by providing valuable insights into system operations, errors, and user activities.

The /var/log/secure file

The /var/log/secure file is a critical log file that contains security-related events, including login attempts, access to protected resources, and changes in security settings, making it a valuable resource for system administrators.

The lastlog command

The lastlog command is a useful tool for tracking user login activities, enhancing security measures, and facilitating auditing processes by providing information about the last login times of users.

Log rotation

Log rotation is a necessary practice for efficient log management, preventing disk space issues, and ensuring the availability of historical logs for analysis, troubleshooting, and compliance purposes.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru

aws re/start