15°

Lab - AWS re/Start

Adm de Log Files

SWIPE

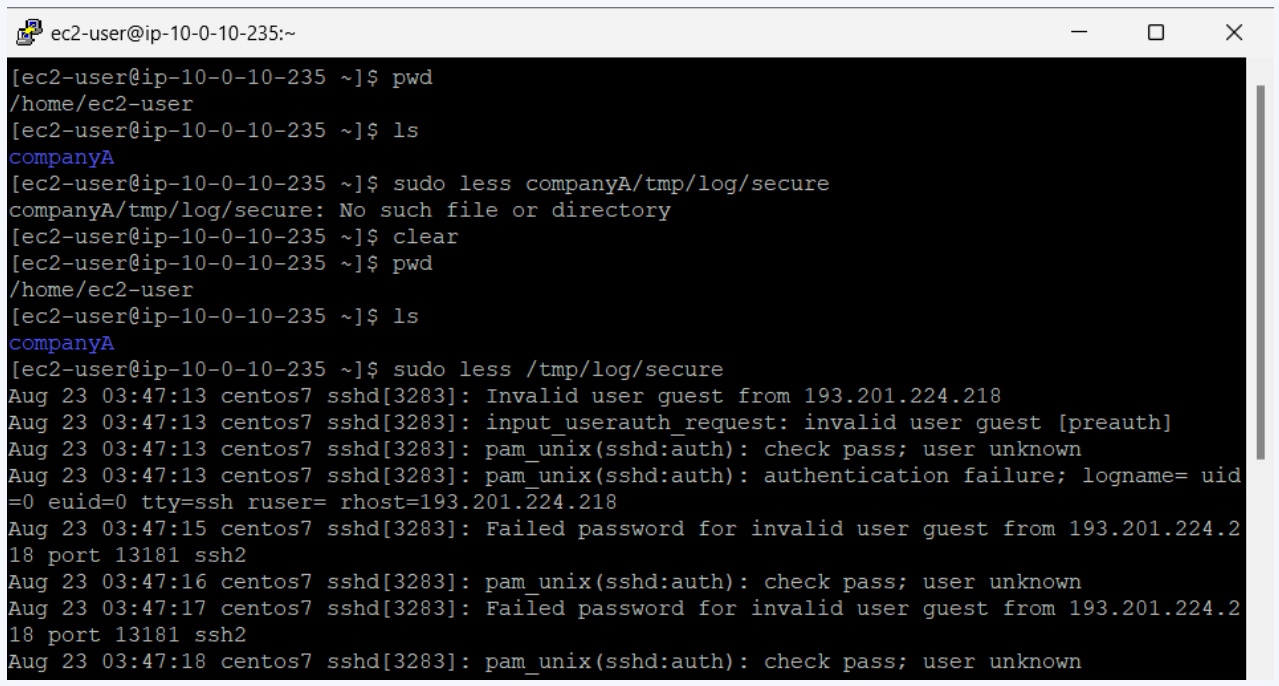
Tarea 01

Revisando Archivos de registro seguros

Log Files == Archivos de registro. A continuación, se tratarán los siguientes temas:

- Revisar lastlog y los resultados de registro seguros de la máquina de Linux

Nota: Para usar el archivo de registro seguro como prueba utilizamos el comando:
sudo less /temp/log/secure
OJO, también se puede encontrar en el directorio *var/log/secure*. Para salir del *log file* usamos la tecla **q**



Tarea 01

Otro comando útil es **sudo lastlog**, que nos permite ver la hora del último inicio de sesión de todos los usuarios de la máquina virtual

```
[ec2-user@ip-10-0-10-235 ~]$ 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**
chrony                                     **Never logged in**
rpcuser                                    **Never logged in**
nfsnobody                                  **Never logged in**
ec2-instance-connect                           **Never logged in**
postfix                                    **Never logged in**
tcpdump                                    **Never logged in**
ec2-user         pts/0    38.250.129.138   Sun Dec 31 18:16:49 +0000 2023
```

SWIPE