



15°

Lab - AWS re/Start Adm de Log Files



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 /tmp/log/secure

OJO, también se puede encontrar en el directorio *var/log/secure*. Para salir del *log file* usamos la tecla **q**

```
ec2-user@ip-10-0-10-235:~  
[ec2-user@ip-10-0-10-235 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-10-0-10-235 ~]$ ls  
companyA  
[ec2-user@ip-10-0-10-235 ~]$ sudo less companyA/tmp/log/secure  
companyA/tmp/log/secure: No such file or directory  
[ec2-user@ip-10-0-10-235 ~]$ clear  
[ec2-user@ip-10-0-10-235 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-10-0-10-235 ~]$ ls  
companyA  
[ec2-user@ip-10-0-10-235 ~]$ 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 193.201.224.2  
18 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 193.201.224.2  
18 port 13181 ssh2  
Aug 23 03:47:18 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknown
```



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
```