



## 245-[LX]-Lab - Administración de archivos de registro

### Datos Generales:

**Nombre:** Tomás Alfredo Villaseca Constantinescu

**País:** Chile

**Fecha:** 09/09/2023

**Contacto:** [tomas.villaseca.c@gmail.com](mailto:tomas.villaseca.c@gmail.com)

Un archivo de registro o log es un archivo de texto que contiene una secuencia de eventos que ocurren en un sistema informático. Los archivos de registro pueden ser generados por una variedad de fuentes, incluyendo servidores, aplicaciones, dispositivos de red y sistemas operativos.

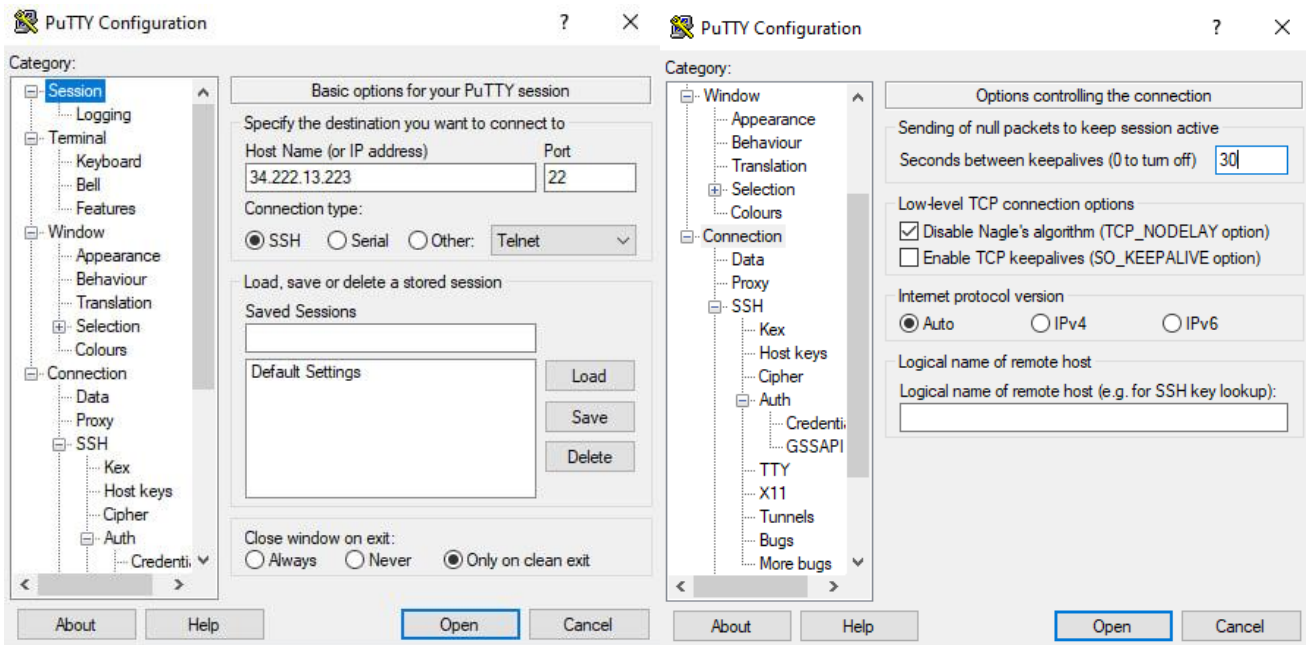
En este laboratorio, hará lo siguiente:

- Revisar el output de **lastlog** y secure log de la máquina de Linux

/var/log/secure = almacena información de autenticación para distribuciones de Linux derivadas de Red Hat (este laboratorio presenta una muestra de archivo secure log en /tmp/log/secure).

# Tarea 1: conectarse a una instancia EC2 de Amazon Linux mediante SSH

1. Abrir Putty.exe: Se ingresa dirección IPv4 de la instancia EC2 en la sección Session.
2. En la sección Connection → SSH → Auth → Credentials se ingresa el archivo PPK descargado anteriormente.
3. En la sección Connection se establece **Seconds between keepalive en 30 (el valor predeterminado es 0).**



4. Se hace click en "Open" para validar y conectarse al Host.

```
ec2-user@ip-10-0-10-186:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _ | _ | _ )  
  _ | ( _ /   Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-10-186 ~]$
```

## Tarea 2: Revisar archivos Secure Log

less = paginador que permite visualizar archivos de texto de gran tamaño

- Muestra el archivo de texto una pantalla a la vez

ec2-user@ip-10-0-10-41:~/companyA

```
[ec2-user@ip-10-0-10-41 companyA]$ pwd
/home/ec2-user/companyA
[ec2-user@ip-10-0-10-41 companyA]$ ls
CEO Documents Employees FolderListing.csv HR Management Roster.csv Sales SharedFolders Shipping
[ec2-user@ip-10-0-10-41 companyA]$ clear
[ec2-user@ip-10-0-10-41 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
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
```

lastlog = entrega información sobre inicios de sesión recientes desde el archivo /var/log/lastlog

ec2-user@ip-10-0-10-41:~/companyA

```
[ec2-user@ip-10-0-10-41 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
dbus         *Never logged in**
rpc          *Never logged in**
libstoragemgmt
sshd         *Never logged in**
rngd         *Never logged in**
chrony       *Never logged in**
rpcuser      *Never logged in**
nfsnobody    *Never logged in**
ec2-instance-connect
postfix      *Never logged in**
tcpdump      *Never logged in**
```

## Desafío adicional

¿Qué información se puede extraer para algunos de los propósitos de su empresa?

Los archivos de registro o logs pueden proporcionar información valiosa sobre el rendimiento, la seguridad y el uso de su empresa. Al analizar los archivos de registro, puede identificar problemas potenciales, mejorar la eficiencia y garantizar que su empresa cumpla con los requisitos normativos.

Algunas de las formas en que puede utilizar los archivos de registro para los propósitos de su empresa incluyen:

- **Rendimiento:** Los archivos de registro pueden ayudarlo a identificar problemas de rendimiento, como cuellos de botella en la red o errores de software. Al analizar los archivos de registro, puede identificar los problemas que están causando el rendimiento lento y tomar medidas para corregirlos.
- **Seguridad:** Los archivos de registro pueden ayudarlo a detectar ataques y amenazas de seguridad. Al analizar los archivos de registro, puede identificar las vulnerabilidades que están siendo explotadas y tomar medidas para remediarlas.
- **Uso:** Los archivos de registro pueden ayudarlo a comprender cómo se utilizan sus recursos. Al analizar los archivos de registro, puede identificar las áreas donde se puede mejorar la eficiencia y tomar medidas para reducir los costos.

A horizontal banner with a dark blue background. It features a network of glowing blue nodes connected by thin lines, creating a digital or molecular structure. The text "Laboratorio Completado" is centered in a white, sans-serif font.

Laboratorio Completado

