

Instalación y Configuración de SSH

A continuación, se detalla el procedimiento técnico ejecutado para cumplir con cada uno de los requerimientos del desafío.

Requerimiento 1: Configuración Segura de OpenSSH Server

1.1. Respaldo de la Configuración Original

Se inicia el proceso creando una copia de seguridad del archivo de configuración de SSH para garantizar una posible reversión en caso de errores. `sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup`

```
[alexuyugen@localhost ~]$ ls -l /etc/ssh/sshd_config.backup
-rw-----. 1 root root 3667 jul 22 19:51 /etc/ssh/sshd_config.backup
[alexuyugen@localhost ~]$
```

1.2. Modificación del Archivo `sshd_config`

Se edita el archivo de configuración para aplicar las políticas de seguridad. Se deja `PasswordAuthentication yes` de forma temporal para facilitar la copia de la clave SSH desde Windows en el siguiente requerimiento. `sudo nano /etc/ssh/sshd_config`

Las directivas modificadas y añadidas fueron:

- Port 2222
- PermitRootLogin no
- PubkeyAuthentication yes
- PasswordAuthentication yes (Configuración temporal)
- AllowUsers alexuyugen

```
[alexuyugen@localhost ~]$ sudo cat /etc/ssh/sshd_config | grep -E 'Port|PermitRootLogin|PubkeyAuthentication|PasswordAuthentication|AllowUsers'
[sudo] password for alexuyugen:
Port 2222
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
# PasswordAuthentication. Depending on your PAM configuration,
# the setting of "PermitRootLogin without-password".
# PAM authentication, then enable this but set PasswordAuthentication
#GatewayPorts no
AllowUsers alexuyugen
[alexuyugen@localhost ~]$
```

(Esta captura es el estado final de como quedó configurado sshd_config)

1.3. Actualización de Políticas de SELinux y Firewall

Se ajustan las reglas de SELinux y firewall para permitir el tráfico a través del nuevo puerto 2222.

```
sudo semanage port -a -t ssh_port_t -p tcp 2222 sudo
```

```
firewall-cmd --permanent --add-port=2222/tcp sudo
```

```
firewall-cmd --permanent --remove-service=ssh sudo
```

```
firewall-cmd --reload
```

```
[alexuyugen@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 2222/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[alexuyugen@localhost ~]$
```

1.4. Reinicio y Verificación del Servicio SSH

Se reinicia el servicio `sshd` para aplicar los cambios y se verifica que esté activo. sudo

```
systemctl restart sshd sudo systemctl status sshd
```

```
[alexuyugen@localhost ~]$ sudo systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-07-23 13:02:34 -04; 9min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 990 (sshd)
      Tasks: 1 (limit: 10723)
    Memory: 5.2M
       CPU: 411ms
   CGroup: /system.slice/sshd.service
           └─990 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

jul 23 13:02:31 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
jul 23 13:02:34 localhost.localdomain sshd[990]: Server listening on 0.0.0.0 port 2222.
jul 23 13:02:34 localhost.localdomain sshd[990]: Server listening on :: port 2222.
jul 23 13:02:34 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
jul 23 13:10:37 localhost.localdomain sshd[2918]: Accepted publickey for alexuyugen from 192.168.196.1 port 62145 ssh2: ED25519 SHA256:ypWqiw5Cee2QFQq5r7N5S
jul 23 13:10:37 localhost.localdomain sshd[2918]: pam_unix(sshd:session): session opened for user alexuyugen(uid=1000) by alexuyugen(uid=0)
lines 1-18/18 (END)
```

Requerimiento 2: Implementación de Autenticación con Claves SSH

2.1. Generación de Claves SSH en la Máquina Local (Windows)

Se generan un par de claves (pública y privada) en el equipo cliente con Windows utilizando PowerShell. `ssh-keygen -t ed25519`

```
PS C:\Users\Alex Henriquez> ls -l 'C:\Users\Alex Henriquez\.ssh\'

Directorio: C:\Users\Alex Henriquez\.ssh

Mode                LastWriteTime         Length Name
----                -
-a----            22-07-2025      20:25           432 id_ed25519
-a----            22-07-2025      20:25           113 id_ed25519.pub
-a----            15-05-2025         9:58          3401 id_rsa
-a----            15-05-2025         9:58           753 id_rsa.pub
-a----            21-07-2025      21:52         14841 known_hosts
-a----            21-07-2025      21:52         14093 known_hosts.old

PS C:\Users\Alex Henriquez> |
```

2.2. Obtención de la Clave Pública en Windows

Tras la generación, la clave pública fue mostrada en la consola. Se procedió a seleccionar y copiar esta cadena de texto directamente desde la terminal para su posterior instalación en el servidor.

```
PS C:\Users\Alex Henriquez> ls -l 'C:\Users\Alex Henriquez\.ssh\'

Directorio: C:\Users\Alex Henriquez\.ssh

Mode                LastWriteTime         Length Name
----                -
-a----            22-07-2025      20:25           432 id_ed25519
-a----            22-07-2025      20:25           113 id_ed25519.pub
-a----            15-05-2025         9:58          3401 id_rsa
-a----            15-05-2025         9:58           753 id_rsa.pub
-a----            21-07-2025      21:52         14841 known_hosts
-a----            21-07-2025      21:52         14093 known_hosts.old

PS C:\Users\Alex Henriquez> type 'C:\Users\Alex Henriquez\.ssh\id_ed25519.pub'
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINv7b8dWHEA+MlbfsKWA2GomwPqc+PgXndNsVYIM5ca alex henriquez@DESKTOP-N81SVSI
PS C:\Users\Alex Henriquez>
```

2.3. Instalación Manual de la Clave Pública en el Servidor

Se accede al servidor mediante contraseña y se instala la clave pública copiada en el archivo `authorized_keys` del usuario `alexxyugen`.

Conexión inicial desde Windows ssh -p 2222

alexxyugen@IP_DEL_SERVIDOR # Comandos ejecutados

en el servidor Rocky Linux mkdir -p ~/.ssh chmod 700

~/.ssh nano ~/.ssh/authorized_keys

```
alexxyugen@localhost ~]$ ls -ld ~/.ssh ~/.ssh/authorized_keys
drwx-----, 2 alexxyugen alexxyugen 29 jul 22 21:34 /home/alexxyugen/.ssh
-rw-----, 1 alexxyugen alexxyugen 112 jul 22 21:34 /home/alexxyugen/.ssh/authorized_keys
alexxyugen@localhost ~]$ cat ~/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINv7b8dWHEA+M1bfsKWA2GomwPqc+PgXndNsYVyIM5ca alex henriquez@DESKTOP-N81SVSI
alexxyugen@localhost ~]$
```

2.4. Ajuste de Permisos de Seguridad en el Servidor

Se aplican los permisos restrictivos necesarios para que el servicio SSH acepte la clave.

chmod 600 ~/.ssh/authorized_keys

2.5. Verificación del Acceso sin Contraseña

Se realiza una nueva conexión desde Windows, la cual resulta exitosa sin solicitar contraseña, validando la correcta instalación de la clave. ssh -p 2222

alexxyugen@IP_DEL_SERVIDOR

```
PS C:\Users\Alex Henriquez>
PS C:\Users\Alex Henriquez> ssh -p 2222 alexxyugen@192.168.196.137
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Wed Jul 23 18:56:00 2025 from 192.168.196.1
alexxyugen@localhost ~|$ |
```

Paso Final de Seguridad: Deshabilitar Autenticación por Contraseña

3.1. Deshabilitación de `PasswordAuthentication`

Para forzar el uso exclusivo de claves SSH, se edita nuevamente el archivo de configuración. `sudo nano /etc/ssh/sshd_config`

Se modifica la directiva a: `PasswordAuthentication no`

3.2. Reinicio del Servicio SSH

Se aplica el cambio final reiniciando el servicio. `sudo systemctl restart sshd`

```
[alaxyugen@localhost ~]$ systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-07-23 19:08:31 -04; 5s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 3164 (sshd)
    Tasks: 1 (limit: 10723)
   Memory: 1.5M
      CPU: 11ms
   CGroup: /system.slice/sshd.service
           └─3164 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

jul 23 19:08:31 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
jul 23 19:08:31 localhost.localdomain sshd[3164]: Server listening on 0.0.0.0 port 2222.
jul 23 19:08:31 localhost.localdomain sshd[3164]: Server listening on :: port 2222.
jul 23 19:08:31 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
[alaxyugen@localhost ~]$ |
```

Requerimiento 3: Monitoreo y Auditoría de Accesos SSH

4.1. Verificación de Registro de Intentos Fallidos

Se provoca un intento de conexión fallido (con una clave no autorizada) y se verifica que el evento quede registrado en `/var/log/secure`.

`sudo grep "permission denied" /var/log/secure`

```
[alaxyugen@localhost ~]$ sudo grep "permission denied" /var/log/secure
Jul 23 19:10:19 localhost sudo[3175]: alexyugen : TTY=pts/1 ; PWD=/home/alexyugen ; USER=root ; COMMAND=/bin/grep 'permission denied' /var/log/secure
[alaxyugen@localhost ~]$ sudo grep "permission denied" /var/log/secure
Jul 23 19:10:19 localhost sudo[3175]: alexyugen : TTY=pts/1 ; PWD=/home/alexyugen ; USER=root ; COMMAND=/bin/grep 'permission denied' /var/log/secure
Jul 23 19:10:25 localhost sudo[3178]: alexyugen : TTY=pts/1 ; PWD=/home/alexyugen ; USER=root ; COMMAND=/bin/grep 'permission denied' /var/log/secure
[alaxyugen@localhost ~]$ |
```

4.2. Creación y Mejora del Script de Auditoría

Se crea un script en Bash para automatizar la recolección de intentos fallidos. El script se mejora para detectar tanto fallos de contraseña como denegaciones de clave pública.

`sudo nano /usr/local/bin/auditar_ssh.sh`

Contenido final del script:

```
#!/bin/bash
LOG_ORIGEN="/var/log/secure"
AUDIT_FILE="/var/log/ssh_auditoria_fallidos.log" echo "--- Reporte de Auditoría de
SSH - $(date) ---" >> $AUDIT_FILE grep -E "Failed password|permission denied"
$LOG_ORIGEN >> $AUDIT_FILE echo "Auditoría completada. Resultados guardados
en $AUDIT_FILE"
```



```
GNU nano 5.6.1 /usr/local/bin/auditar_ssh.sh
#!/bin/bash

# Define el archivo de log de origen y el de destino para la auditoría
LOG_ORIGEN="/var/log/secure"
AUDIT_FILE="/var/log/ssh_auditoria_fallidos.log"

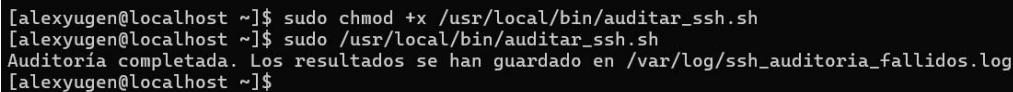
# Escribe un encabezado con la fecha actual en el archivo de auditoría
echo "--- Reporte de Auditoria de SSH - $(date) ---" >> $AUDIT_FILE

# Busca las líneas con "Failed password" y las agrega al archivo de auditoría
grep -E "Failed password|permission denied" $LOG_ORIGEN >> $AUDIT_FILE

echo "Auditoría completada. Los resultados se han guardado en $AUDIT_FILE"
```

4.3. Asignación de Permisos y Ejecución del Script

Se le otorgan permisos de ejecución al script y se procede a correrlo. sudo
chmod +x /usr/local/bin/auditar_ssh.sh sudo /usr/local/bin/auditar_ssh.sh



```
[alexuyugen@localhost ~]$ sudo chmod +x /usr/local/bin/auditar_ssh.sh
[alexuyugen@localhost ~]$ sudo /usr/local/bin/auditar_ssh.sh
Auditoría completada. Los resultados se han guardado en /var/log/ssh_auditoria_fallidos.log
[alexuyugen@localhost ~]$
```

Verificación del Archivo de Auditoría

Finalmente, se revisa el contenido del archivo de log generado por el script para confirmar su correcto funcionamiento. cat /var/log/ssh_auditoria_fallidos.log

```
[alexuyugen@localhost ~]$ sudo /usr/local/bin/auditar_ssh.sh
Auditoría completada. Los resultados se han guardado en /var/log/ssh_auditoria_fallidos.log
[alexuyugen@localhost ~]$ cat /var/log/ssh_auditoria_fallidos.log
--- Reporte de Intentos Fallidos de SSH - mié 23 jul 2025 13:24:22 -04 ---
Jul 23 13:22:22 localhost sudo[3072]: alexuyugen : 2 incorrect password attempts ; TTY=pts/1 ; PWD=/home/alexuyugen ; USER=root ; COMMAND=/bin/grep 'Failed p
ssword' /var/log/secure
--- Reporte de Auditoria de SSH - mié 23 jul 2025 18:57:45 -04 ---
Jul 23 13:22:22 localhost sudo[3072]: alexuyugen : 2 incorrect password attempts ; TTY=pts/1 ; PWD=/home/alexuyugen ; USER=root ; COMMAND=/bin/grep 'Failed p
ssword' /var/log/secure
--- Reporte de Auditoria de SSH - mié 23 jul 2025 19:13:31 -04 ---
Jul 23 13:22:22 localhost sudo[3072]: alexuyugen : 2 incorrect password attempts ; TTY=pts/1 ; PWD=/home/alexuyugen ; USER=root ; COMMAND=/bin/grep 'Failed p
ssword' /var/log/secure
Jul 23 19:10:19 localhost sudo[3175]: alexuyugen : TTY=pts/1 ; PWD=/home/alexuyugen ; USER=root ; COMMAND=/bin/grep 'permission denied' /var/log/secure
Jul 23 19:10:25 localhost sudo[3178]: alexuyugen : TTY=pts/1 ; PWD=/home/alexuyugen ; USER=root ; COMMAND=/bin/grep 'permission denied' /var/log/secure
Jul 23 19:10:43 localhost sudo[3181]: alexuyugen : TTY=pts/1 ; PWD=/home/alexuyugen ; USER=root ; COMMAND=/bin/grep 'permission denied' /var/log/secure
[alexuyugen@localhost ~]$
```