Activitat Qualificable 3.2.2 – Configuració del servici SSH. Autenticació d'Usuaris

Índex

Objectius:

1. Entendre els fonaments de SSH.
2. Configurar l'accés SSH mitjançant autenticació per contrasenya.
3. Generar i configurar l'accés per clau pública/privada.
4. Configurar el servidor SSH per utilitzar només autenticació per claus.

1. Introducció

La eina instal.la per defecte per accedir de forma remota als contenidors de AWS s'anomena **OpenSSH** (Open Secure Shell). Es tracta d'un conjunt d'aplicacions que permeten administrar servidors de manera segura des de la teua màquina, xifrant tota la comunicació fent ús del **protocol SSH**.

2. Autenticació SSH

L'autenticació d'usuaris en SSH pot fer-se de dues formes principals:

1. **Autenticació per contrasenya**: Cada usuari introdueix la seua contrasenya per accedir al servidor.
2. **Autenticació per claus**: S'utilitza un parell de claus criptogràfiques (una pública i una privada). La clau pública s'emmagatzema al servidor, i la clau privada roman al client.

2.1 Connexió SSH amb autenticació per contrasenya

Per defecte, les màquines de AWS no permeten l'autenticació SSH per contrasenya. Tanmateix. Si vols activar-la (només per finalitats educatives), has de seguir aquests passos:

Pas 1: Modificar la configuració del servidor SSH

Al servidor, obre el fitxer de configuració de SSH (`sshd_config`):

```
sudo nano /etc/ssh/sshd_config
```

Pas 2: Habilitar l'autenticació per contrasenya

Busca la següent línia i assegura't que estiga activada:

```
PasswordAuthentication yes
```

Si la línia comença amb un #, lleva el comentari perquè tinga efecte.

Encara que **aquesta configuració és suficient en la majoria de casos**, en algunes distribucions de linux s'estableixen configuracions addicionals en el directori `/etc/ssh/sshd_config.d/` per la qual cosa, si estem en una instancia de AWS, editarem el següent arxiu:

```
sudo vi /etc/ssh/sshd_config.d/60-cloudimg-settings.conf
```

i permetrem l'autenticació per contrasenya, ja que les directives d'aquest arxiu prevalen sobre l'anterior i en aquest arxiu no està permesa l'autenticació per contrasenya

Pas 3: Reiniciar el servei SSH

Després de fer els canvis, reinicia el servei SSH:

```
sudo systemctl restart ssh
```

Pas 4: Crea un Usuari i estableix una contrasenya

Abans de connectar-nos, crearem un nou usuari en el servidor. Per a això, utilitza el següent comandament:

```
sudo adduser nom_usuari
```

Substitueix `nom_usuari` pel nom que vulgues donar al nou usuari. El sistema et demanarà que especifiques una contrasenya per a aquest usuari i altres dades opcionals.

Pas 5: Connexió per contrasenya

Ara, des de la teua màquina local, pots connectar-te al servidor SSH amb aquest nou usuari i la contrasenya que has creat:

```
ssh nom_usuari@ip_del_servidor
```

- `nom_usuari`: el nom del nou usuari que has creat.
- `ip_del_servidor`: l'adreça IP del servidor remot.

Introdueix la contrasenya del nou usuari quan el sistema la demane.

Activitat 1

Crea al servidor remot un nou usuari `xyyyy` on **x** és el teu nom e **yyyy** el teu cognom en el servidor.

- Activa l'autenticació per contrasenya
- Connecta't des de la màquina local al servidor utilitzant la contrasenya d'aquest nou usuari.
- Comprova que tens accés al servidor i que pots utilitzar-lo.

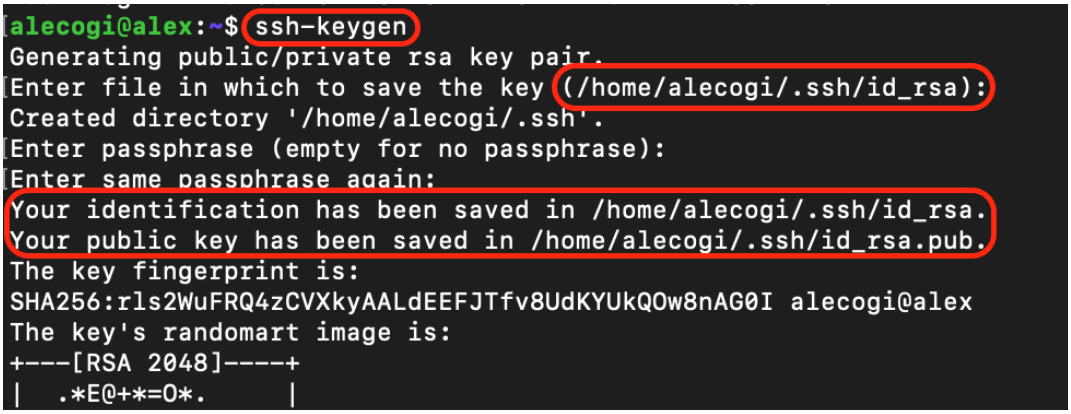
Pega captures de pantalla demostrant l'accés per usuari i contrasenya

2.2 Autenticació per clau publica/privada

Pas 1: Generació de claus SSH

Genera un parell de claus (pública i privada) al teu ordinador local executant el següent comandament:

```
ssh-keygen -t rsa -b 4096
```



- Això genera dues claus: una clau privada (guardada a `~/.ssh/id_rsa`) i una clau pública (guardada a `~/.ssh/id_rsa.pub`).
- Pots deixar els valors per defecte, o bé introduir una contrasenya addicional per protegir la teua clau privada.

Pas 2: Copiar la clau pública al servidor

Per poder utilitzar l'autenticació per claus, **la clau pública del client ha d'estar al servidor**, més concretament al fitxer `authorized_keys` situat en el **directory ~./ssh** del usuari remot amb el que vols connectar-te al servidor. Pots copiar la clau generada al pas anterior utilitzant el comandament `ssh-copy-id`

```
ssh-copy-id usuari@ip_del_servidor
```

> Per a poder utilitzar aquest comandament, abans has de tenir accés per usuari i contrasenya, cosa que no sempre estarà disponible.

Si no tens `ssh-copy-id`, pots fer-ho manualment:

- Conecta't al servidor amb l'usuari `ubuntu` present per defecte a les nostres màquines de AWS

- Si no existeix, crea la carpeta `.ssh` al directory **home** de l'usuari amb el que volem connectarnos al servidor

```
mkdir -p ~/.ssh
```

- Copia la clau pública a un fitxer anomenat `authorized_keys` dins del directory .ssh creat al pas anterior:

```
cat ~/.ssh/id_rsa.pub | ssh usuari@ip_del_servidor 'cat >>
~/.ssh/authorized_keys'
```

Pas 3: Habilitar l'autenticació per clau Publica/Privada

Al servidor, obre el fitxer de configuració de SSH (`sshd_config`):

```
sudo nano /etc/ssh/sshd_config
```

Busca la següent línia i assegura't que estiga activada:

```
PubkeyAuthentication yes
```

Si la línia comença amb un #, lleva el comentari perquè tinga efecte.

Després de fer els canvis, reinicia el servei SSH perquè les modificacions tinguen efecte:

```
sudo systemctl restart ssh
```

Pas 4: Connexió al servidor utilitzant la clau privada

Una vegada copiada la clau pública al servidor i activada l'autenticació per clau

pública/privada pots connectar-te des de la teua màquina local sense utilitzar una contrasenya:

```
ssh usuari@ip_del_servidor
```

Activitat 2

Du a terme les següents tasques:

- Genera un nou usuari a la màquina remota
- Genera un parell de claus SSH a la màquina local
- Copia la clau pública al servidor.
- Habilita l'accés per usuari/contrasenya
- Connecta't al servidor utilitzant la teua clau privada, sense contrasenya.

Pega captures de pantalla demostrant l'accés per usuari i contrasenya

2.3 Configuració del servidor per utilitzar només autenticació per clau pública/privada

Ara, tornarem a configurar el servidor SSH per rebutjar connexions que utilitzen contrasenya i només permetre l'accés mitjançant claus.

Pas 1: Modificar la configuració del servidor SSH

Al servidor, obre el fitxer de configuració de SSH:

```
sudo nano /etc/ssh/sshd_config
```

Canvia les següents opcions:

```
PasswordAuthentication no
PubkeyAuthentication yes
```

Això desactivarà l'autenticació per contrasenya i activarà només l'autenticació mitjançant claus públiques.

Pas 2: Reiniciar el servei SSH

Després de fer els canvis, reinicia el servei SSH perquè les modificacions tinguen efecte:

```
sudo systemctl restart ssh
```

Activitat 3

Du a terme les següents tasques:

- Modifica el fitxer de configuració de SSH per desactivar l'autenticació per contrasenya.
- Assegura't que només pots connectar-te al servidor utilitzant la clau privada.
- (opcional) Per augmentar la seguretat canvia el port per defecte en el que el teu servidor ssh escolta les connexions per el por 32002 i connectat fent us d'aquest port.

Pega captures de pantalla demostrant l'accés per usuari i contrasenya

3. Preguntes de Repàs

1. Quina diferència hi ha entre l'autenticació per contrasenya i per claus SSH?
2. Per què és més segur utilitzar claus SSH que contrasenyes?
3. Com podries afegir més seguretat a una connexió SSH?
4. Quins avantatges té canviar el port predeterminat de SSH?

4. Bibliografía / Webgrafía

- Ubuntu Server Docs. OpenSSH. https://ubuntu.com/server/docs/service-openssh. **Canonical**
- Documentación oficial openSSH server. https://www.openssh.com. **Internet System Consortium.**