Configuración Servidor SSH Centos 7

En esta práctica se va a configurar el *Secure Shell* SSH (en español, intérprete de órdenes segura) en un Servidor Centos 7. La organización de esta práctica se resume en los siguientes pasos:

1. Pasos Previos
2. Instalación del servicio SSH y configuración
3. Configuración segura
4. Configuración firewall para SSH en la VLAN de Gestión
5. Configuración segura con criptografía pública
6. Consulta de registros

1. Pasos Previos

Configure el nombre a la máquina con el nombre sshC.grupoXX.net

A partir de entonces acceda a realizar la gestión a través de la VLAN de gestión. Configure el acceso ssh sólo por la IP indicada en la VLAN de Gestión.

Reinicie la máquina.

Aclaración. Este manual está pensado para IP de VLAN de Gestión 10.0.100.210. Trabaje usted con la IP adecuada.

2. Instalación del servicio SSH y configuración

A la hora de acceder de forma remota a una máquina, no conviene acceder como root. Deberíamos crear un usuario con privilegios de root.

- Paso 1: Creación de un nuevo usuario:

  ```
  adduser  ussh
  passwd ussh
  ```

Introducir de passwd la misma estáis usando como root, por ejemplo.

- Paso 2: Privilegios de root (“super usuario”)

  ```
  gpasswd –a ussh wheel
  ```

Procedemos a instalar el servicio ssh.

```
yum –y install openssh-server
```

El fichero de configuración del servicio ssh, se encuentra en `/etc/ssh/sshd_conf`. Lo abrimos. Le quitamos el comentario (almohadilla) a la línea ListenAddress 0.0.0.0.

Cambiamos 0.0.0.0 por la IP VLAN de Gestión, en este caso 10.XX.100.210

Nos debe quedar: ListenAddress 10.0.100.210

Guardamos.

Reiniciamos el servicio, systemctl restart sshd

Abrimos terminal en la máquina de trabajo y ejecutamos ssh ussh@10.0.100.210

Con lo que ya estaremos conectados remotamente. Este servicio deberá ser instalado en cada una de las configuraciones de los servicios a realizar.

Para poder ejecutar comando de **root**, tendremos que usar el comando sudo. Si en algún momento queremos tener todos los privilegios de **root**, ejecutamos ***su root***

Comprobemos que el firewall permite el servicio ssh.

```
[ussh@sshc ~]$ sudo firewall-cmd --list-all
```

Responderá algo así:

public (default, active)

interfaces: enp0s3 enp0s8

sources:

services: ssh (observamos activo el servicio ssh)

ports:

masquerade: no

forward-ports:

icmp-blocks:

rich rules:

Configuración firewall

Esta configuración no es del todo óptima.

En primer lugar, disponemos de dos o tres VLAN, a saber, la VLAN de Producción (Zona Pública), la VLAN de Gestión (Zona home) y lo más probable la VLAN de Storage (Zona Internal).

Estas tres zonas deberán de estar configuradas adecuadamente. Cada zona, debe tener configurado: la interface, los servicios, los puertos, etc.

En la página web https://www.certdepot.net/rhel7-get-started-firewalld/ encontraremos un manual sobre el firewall.

En el punto 4 configuraremos adecuadamente el firewall.

Aprovechamos también, para instalar las herramientas net-tools.

```
sudo yum -y install net-tools
```

Ahora podemos comprobar, por ejemplo, los puertos que el servidor gestiona.

```
[ussh@sshc ~]$ netstat -pan |more
```

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 10.0.100.210:22         0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
-
tcp        0      0 10.0.100.210:22         10.0.100.100:49937      ESTABLISHED
-
raw6       0      0 :::58                   :::*                    7
-
raw6       0      0 :::58                   :::*                    7
-
```

Donde observamos que está escuchado por 10.0.100.210:22 y tiene establecida una conexión con 10.0.100.100:49937 (por el puerto 49937)

Si queremos comprobar que el servicio se encuentra en funcionamiento, podemos consultar cuáles son los procesos que el servidor tiene en marcha y hacer una búsqueda de la cadena SSH en la respuesta.

```
[ussh@sshc ~]$ ps -aef | grep ssh

root      2888  2886  0 17:17 ?        00:00:00 sshd: ussh [priv]
```

Para parar el servicio: systemctl stop sshd

Para iniciar el servicio: systemctl start sshd

Hasta ahora hemos realizado una configuración básica. Sólo hemos indicado la IP por donde sólo debe permitir la conexión remota (VLAN de Gestión).

Recordad: Si no se indica lo contrario, los usuarios del sistema tienen permiso de acceso al servicio ssh.

Actividad:

Añade un nuevo usuario, sin privilegios, y verifica que es posible la conexión desde terminal. No olvides configurarle contraseña.

```
[ussh@sshc ~]$ sudo adduser usuario1
```

3. Configuración segura

El servidor SSH instalado permite soportar tanto la versión 1 como la versión 2 del protocolo SSH. Recomendamos que se desactive el soporte de la versión 1 por razones de seguridad, ya que esta versión tiene graves problemas de vulnerabilidad.

En otros casos puede ser interesante poder cambiar el puerto habitual del protocolo SSH que es el 22, por cualquier otro.

Ya hemos visto que podemos indicar las direcciones IP por la que escucha, si queremos añadir otras, se añaden líneas ListenAddress (no es nuestro caso).

Es importante por motivos de seguridad NO PERMITIR que se puede acceder con el usuario root (root@IP_VLAN_GESTION).

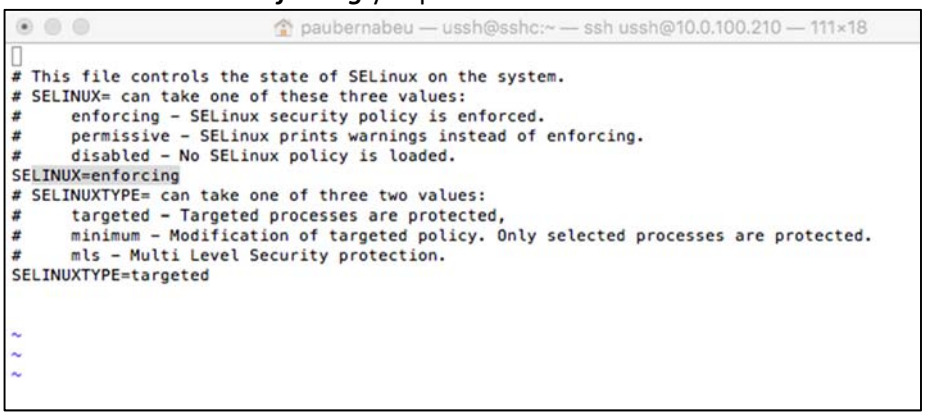
Como hemos visto, todos los usuarios del sistema, por defecto, tiene acceso mediante SSH. Deberíamos indicar cuáles son los usuarios a los que permitir el acceso vía SSH.

Consideraciones respecto a SELinux y firewall

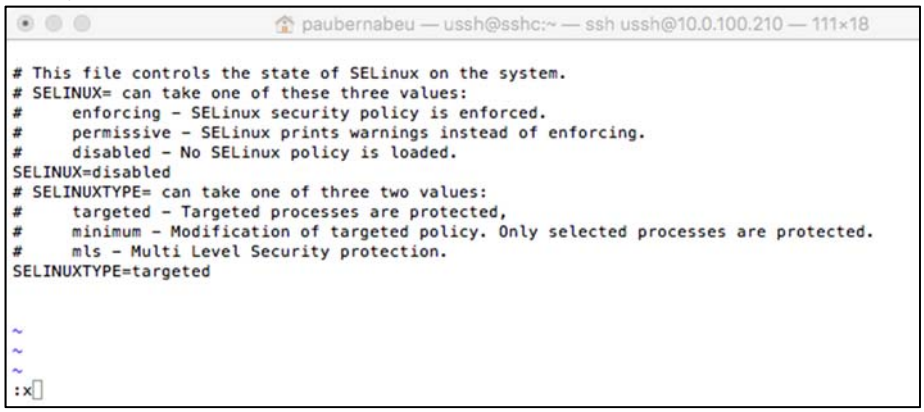
Previamente debemos deshabilitar SELinux(al cambiar de puerto). O bien configurar dicho servicio simultáneamente con SELinux. En el laboratorio optamos por desactivarlo.

[ussh@sshc ~]$ sudo vi /etc/selinux/config

Tendremos SELinux en modo ***enforcing*** y lo pasamos a ***disabled*.**



Tras el cambio, SELINUX=disabled



En cuanto el firewall debe tener activo el puerto 2222 para tcp.
sudo firewall-cmd --permanent --zone=public --add-port=2222/tcp
sudo firewall-cmd –reload

Reiniciamos la máquina para que los cambios en SELinux tengan efecto.

Abrimos el fichero de configuración del servicio ssh (mostramos una parte y en negrita los cambios realizados)

[ussh@sshc ~]$ sudo vi /etc/ssh/sshd_config

$OpenBSD: sshd_config,v 1.93 2014/01/10 05:59:19 djm Exp $

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with OpenSSH
# is to specify options with their default value where possible, but leave them commented.
Uncommented options override the default value.

# If you want to change the port on a SELinux system, you have to tell SELinux
# about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 2222
#AddressFamily any
ListenAddress 10.0.100.210
#ListenAddress ::

# The default requires explicit activation of protocol 1
Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
```

```
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
AllowUsers ussh
```

Reiniciamos el servicio:

```
[ussh@sshc ~]$ sudo systemctl restart sshd
```

Comprueba la configuración para los usuarios: root, ussh y usuario1

```
ssh –p 2222 root@IP_VLAN_GESTION
ssh –p 2222 ussh@IP_VLAN_GESTION (sólo este debe poder conectarse)
ssh –p 2222 usuario1@IP_VLAN_GESTION
```

4. Configuración firewall para SSH en la VLAN de Gestión

La configuración a realizar es:

- Crear la zona **public** para la VLAN de Gestión y la zona Home para la zona VLAN de gestión.
- Asignaremos a la zona **public** la interfaz (enp0s3 o la que sea la adecuada en cada caso). Y a la zona **home** (enp0s8 o la adecuada).
- Activaremos sólo el servicio **FTP** en la VLAN de producción y el servicio **SSH** en la VLAN de Gestión.
- Añadiremos el puerto **2222/tcp** en la zona HOME
- Todo los servicios adicionales aparezcan, puertos, etc deberán ser borrados.

Tras los 5 pasos nos queda:

```
[root@sshc ussh]# sudo firewall-cmd --zone=home --list-all
home (default, active)
  interfaces: enp0s8
  sources:
  services: ssh
  ports: 2222/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:

[root@sshc ussh]# sudo firewall-cmd --zone=public --list-all
public
  interfaces:
  sources:
  services: ftp
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Recuerde debe ejecutar sudo firewall-cmd –reload para activar los cambios realizados.

Verifique el correcto funcionamiento desde un terminal.

5. Configuración segura con criptografía pública

A fin de aumentar la seguridad de la conexión se pueden crear claves de identificación de usuario. Primero hemos de crear un *id_rsa* y *una id_rsa.pub,* que son las claves privadas y pública respectivamente. La clave pública se ha de copiar en el servidor en el directorio .ssh del mismo usuario, en el archivo *authorized_keys*.

Es recomendable eliminar el acceso con contraseña porque los usuarios pueden usar contraseñas fáciles que pueden ser rotas con ataques de fuerza bruta.

Pasos:

- ✓ En el equipo cliente

```
[ussh@sshc ~]$ ssh-keygen -t dsa -C "Clave Centos.Red Hat 7"
Generating public/private dsa key pair.
Enter file in which to save the key (/home/ussh/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ussh/.ssh/id_dsa.
Your public key has been saved in /home/ussh/.ssh/id_dsa.pub.
The key fingerprint is:
9a:e6:dd:94:56:0a:ea:d0:f6:71:fa:48:9e:c8:7d:2a Clave Centos.Red Hat 7
The key's randomart image is:
+--[ DSA 1024]----+
|                 |
|                 |
|                 |
|                 |
|        S   .    |
|     . + . +     |
|    . B o *      |
|     BEB X.      |
|      =.X+o      |
+-----------------+
```

Conviene introducir una “passphrase”

- ✓ Copiar la clave pública en el servidor:

  Opción 1: En la máquina local

  [root@client ~]$ ssh-copy-id ussh@VLAN_Gestion

Tras proporcionar la contraseña, la clave pública será añadida al fichero *.ssh/autorized_keys.* Con lo que la clave privada ya puede ser usada para loguear en el servidor.

Opción 2: Instalación manual de la clave

Asumimos que ya tenemos generadas las claves (pública y privada).

Hemos de copiar la clave pública al servidor en el directorio del usuario sobre el que vamos a acceder ussh.

Haremos una transferencia segura a través de la orden sftp. Para ello en la máquina cliente:

```
[root@client ~]$ cd .ssh/ (directorio ha guardado las claves generadas)

[root@client .ssh ~]$ sftp –P 2222 ussh@VLAN_GESTION
Connected to …

sftp>mkdir .ssh
sftp>put id_dsa.put .ssh/authorized_keys
…..
….
sftp> quit
```

Una vez copiada la clave pública del cliente en la ubicación correcta, activaremos en el servidor que sólo permitiremos acceder con certificados.

```
[ussh@sshc ~]$ sudo vi /etc/ssh/sshd_config
[sudo] password for ussh:

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

Y además le indicamos que active la autentificación con clave pública.

```
AllowUsers ussh

#RSAAuthentication yes
PubkeyAuthentication yes
```

Reiniciamos el servicio ssh:

```
[ussh@sshc ~]$ sudo systemctl restart sshd
```

Desde el cliente hemos de comprobar el funcionamiento. En la orden se indica la identificación del usuario y la dirección del servidor y en este caso el puerto al ser distinto de 22. A continuación pide la contraseña empleada en la creación de la claves (passphrase). Esta

contraseña permite usar la clave privada del usuario para descifrar los datos enviados por el servidor.

```
[root@client ~]$ ssh –p 222 ussh@IP_VLAN_GESTION_SERVER
```

6. Consulta de registros

Con el fin de tener el máximo control de los servidores conviene saber dónde se encuentran los ficheros de registros o logs. Cualquier tipo de problema que tenga el servidor SSH se almacena en estos ficheros.

Los ficheros se encuentran en el directorio /var/log, como es habitual, y son los ficheros /var/log/messages* y /var/log/secure.