

**MANUAL DE CONFIGURACIÓN DEL SERVIDOR SSH**

Administración de Servicios en Red

Equipo 5:

Campos Gómez Fernanda Ivette

Hernández López César Erick

Ruiz Pérez Alejandro

**ÍNDICE**

[**Introducción**](#_irw4bdpnceqg) **3**

[**Configurando el servidor SSH**](#_z01mbrj1yldr) **3**

[Creación de Usuarios y Grupo.](#_3zj7j9bw6g7t) 3

[Creación de Usuarios.](#_sxru877mvsmb) 3

[Archivo de Configuración](#_muaoneg4bh0w) 4

[**Bibliografía**](#_qydde6avjq8h) **5**

# Introducción

El presente documento, tiene como objetivo brindar una guía de apoyo para poder configurar correctamente un servidor SSH, dicha configuración servirá para que nuestro servidor pueda ofrecer canales seguros.

# Configurando el servidor SSH

Una vez que hayamos instalado openSSH-server, necesitaremos crear los usuarios que usaran dicho servidor y abrir el archivo de configuración para indicar lo que debe y no debe de hacer nuestro servidor.

Primero, detendremos el servidor usando el siguiente comando:

$ sudo systemctl stop ssh

## Creación de Usuarios y Grupo.

Primero, crearemos los usuarios y un grupo para hacer las pruebas de nuestro servidor.

## Creación de Usuarios.

El comando que nos ayudará con la creación de usuarios, es el de “useradd”, dicho comando tiene la siguiente sintaxis:

---------------------------------------------------------------------------------------------------

-g: Grupo principal que queremos tenga el usuario (debe existir previamente)

-d: Carpeta home del usuario. Suele ser /home/nombre-usuario

-m: Crear carpeta home si es que no existe.

-s: Intérprete de comandos (shell) del usuario. Suele ser /bin/bash

---------------------------------------------------------------------------------------------------

“passwd”: este comando nos permitirá asignar contraseñas a nuestros usuarios

---------------------------------------------------------------------------------------------------

Una vez que entendamos el funcionamiento de los comandos, tecleamos lo siguiente en la terminal:

$ sudo useradd -d /etc/ssh/sshredes/cuatro/fer -m -s /bin/bash fer

$ sudo passwd fer

$ sudo useradd -d /etc/ssh/sshredes/cuatro/ceci -m -s /bin/bash ceci

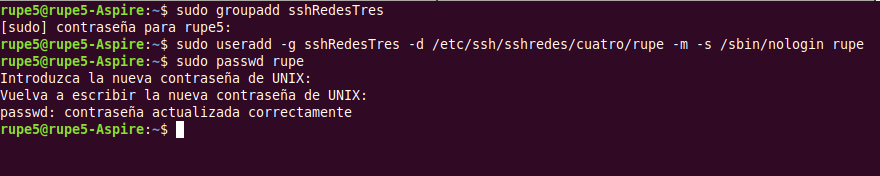
$ sudo passwd ceci

Hacemos un grupo llamado sshRedesTres para el usuario rupe

$ sudo groupadd sshRedesTres

$ sudo useradd -g sshRedesTres -d /etc/ssh/sshredes/cuatro/rupe -m -s /sbin/nologin rupe

$ sudo passwd rupe



## Archivo de Configuración

Ahora abriremos el archivo de configuración. Dicho archivo se encuentra en **/etc/ssh/sshd\_config**

$ sudo sublr /etc/ssh/sshd\_config

Nos daremos cuenta que gran parte del archivo está comentado, lo que no está comentado lo dejaremos tal cual se encuentra, y sólo descomentaremos y agregaremos (según sea el caso) las siguientes líneas:

#Asignamos el puerto en donde escuchará nuestro servidor

Port 22

#ListenAddress 0.0.0.0

#ListenAddress ::

#Descomentamos estas líneas, las cuales contienen las llaves que se crearon cuando

#se instaló el openssh.

HostKey /etc/ssh/ssh\_host\_rsa\_key

HostKey /etc/ssh/ssh\_host\_ecdsa\_key

HostKey /etc/ssh/ssh\_host\_ed25519\_key

#\*\*\*\*\*\*\* Autenticación:\*\*\*\*\*\*\*\*\*\*\*

LoginGraceTime 10m #Desconectar después de x minutos

PermitRootLogin no #Denegamos el login por root

MaxAuthTries 6 #Número máximo de intentos de login

MaxSessions 5 #Máximas sesiones activas

#\*\*\*\*\*\*\*\*Accesos Autorizados\*\*\*\*\*\*\*\*

#Descomentar estas lineas si queremos controlar los accesos de usuarios.

#(Si los usuarios no estan en el sistema,se rechazan automaticamente)

#AllowGroups sshRedesTres #Permitimos el grupo sshRedesTres

#AllowUsers alejandro #Permitimos el acceso a alejandro

#DenyUsers fer@10.100.74.10 #Denegamos el acceso por IP al usuario fer

#DenyUsers \*@10.100.74.10 #Denegamos el acceso por IP

#\*\*\*\*\*\*\*\*\*Acceso por Llaves\*\*\*\*\*\*\*\*\*\*\*

PubkeyAuthentication yes #habilitamos el acceso por llave pública

#Autorizamos el acceso y el servidor buscará la llave en el home del cliente

AuthorizedKeysFile %h/.ssh/authorized\_keys %h/.ssh/authorized\_keys2

#\*\*\*\*\*\*\*\*\*\*\*\*Habilitamos la visión por ventanas X11\*\*\*\*\*\*\*\*\*\*\*\*\*

X11Forwarding yes

Guardamos el archivo y para este punto, nuestro servidor debería estar listo para funcionar.

Así que lo volvemos a poner en marcha para que cargue todos los cambios que hemos realizado. Para ello tecleamos el siguiente comando:

$ sudo systemctl start ssh

Con esto daremos por finalizado el proceso de configuración del servidor

# Bibliografía

[1] <http://www.castaglia.org/proftpd/doc/devel-guide/toc.html>

[2] <https://linuxize.com/post/how-to-create-a-sudo-user-on-ubuntu/>