Fichero de configuración para SSH

Os vamos a contar cómo crear y configurar un archivo de configuración OpenSSH para crear accesos directos a servidores a los que accedas con frecuencia en sistemas operativos Linux o Unix.

Puedes configurar tu cliente ssh OpenSSH utilizando varios archivos de la siguiente manera para ahorrar tiempo y escribir las opciones de línea de comandos del cliente ssh utilizadas con frecuencia, como puerto, usuario, nombre de host, archivo de identidad y mucho más para que sea más fácil acceder desde Linux/macOS o Unix.

Para ello crearemos un archivo en la carpeta .ssh llamado config

```
vi ~/.ssh/config
```

Si queremos que sea accesible para todos los usuarios del sistema lo editaremos en la carpeta /etc/ssh/ssh_config (no confundir con el sshd_config)

Tienes que introducir un parámetro por línea y pueden estar separados por espacios o signos =

Para introducir comentarios puedes usar la # esas líneas se ignoran

Ejemplos

```
Host tecno01
     HostName hosta26b29-02.tecnocratica.net
     User eduardo
     Port 22
```

Ahora podrás acceder tecleando simplemente ssh tecno01

En este caso vamos a usar un archivo .key diferente.

```
Host proxmox01
     HostName 192.168.1.100
```

```
    User root
    IdentityFile ~/.ssh/proxmox.key
```

Parámetros posibles

Host: Define para qué host o hosts se aplica la sección de configuración. La sección termina con una nueva sección de Host o al final del archivo.

HostName: especifica el nombre de host real para iniciar sesión. También se permiten direcciones IP numéricas.

User: Define el nombre de usuario para la conexión SSH.

IdentityFile: especifica un archivo desde el cual se lee la identidad de autenticación DSA, ECDSA o DSA del usuario. El valor predeterminado es ~/.ssh/identity para la versión 1 del protocolo y ~/.ssh/id_dsa, ~/.ssh/id_ecdsa y ~/.ssh/id_rsa para la versión 2 del protocolo. La opción IdentityFile en la configuración SSH o en la CLI se refiere al archivo de clave privada, que debe mantenerse confidencial.

Protocol: especifica las versiones de protocolo que ssh debe admitir en orden de preferencia. Los valores posibles son 1 y 2.

Puerto: especifica el número de puerto para conectarse en el host remoto.

Cipher: Cipher es un parámetro de la versión 1 del protocolo para indicar el tipo de cifrado para cifrar sesiones. Los tipos admitidos son Blowfish, des y 3des (predeterminado).

Ciphers: El parámetro Ciphers indica el tipo de cifrado para cifrar sesiones en la versión 2 del protocolo. Los cifrados disponibles y los valores predeterminados son:

```
aes128-ctr, aes192-ctr, aes256-ctr, arcfour256, arcfour128,
aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, aes192-cbc, aes256-cbc, arcfour
```

HostKeyAlgorithms: El parámetro HostKeyAlgorithms establece el orden de preferencia para los algoritmos de clave de host en la versión 2 del protocolo. El orden predeterminado es ssh-rsa,ssh-dss.

Conectarse a equipos con SSH antiguos

Una de las principales ventajas de este archivo de configuración es la posibilidad de conectarse de forma fácil a equipos con versiones de RSA o protocolos SSH obsoletos

Ejemplos

```
Host switch-viejo
        Hostname 192.168.3.14
        user admin
        HostKeyAlgorithms ssh-rsa
        KexAlgorithms diffie-hellman-group1-sha1
        port 22
```

```
Host otro-sw-viejo
        Hostname 192.168.37.254
        user admin
        HostKeyAlgorithms ssh-dss
        KexAlgorithms diffie-hellman-group1-sha1
        Ciphers +aes256-cbc
        port 22
```

```
Host otro-sw-viejo-mas
        Hostname 192.168.37.254
        user admin
□□KexAlgorithms +diffie-hellman-group1-sha1
□□Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc
□□PubKeyAcceptedKeyTypes +ssh-rsa
        port 8122
```

Revision #4
Created 31 March 2024 09:36:23 by etaboada
Updated 31 March 2024 10:05:28 by etaboada