Breves apuntes sobre SSH

SSH (**Secure Shell**) é un protocolo de rede que se emprega para a comunicación segura entre 2 dispositivos distintos a través dunha rede. Proporciona un canal seguro a través do que se poden transmitir datos cifrados, para protexer a confidencialidade e a integridade da información. Emprégase habitualmente para acceder de xeito remoto, así como para administrar servidores ou transferir ficheiros.

Aínda que existen diferentes implementacións tanto de clientes como de servidores **SSH**, a máis empregada é **OpenSSH**

Instalación do servidor OpenSSH:

```
apt update

apt install openssh-server
```

Os arquivos de configuración e as claves criptográficas do servidor openssh-server están localizadas en /etc/ssh. Algúns destes arquivos son:

- **ssh_config**: recolle as directivas de configuración do cliente openssh
- **sshd_config**: recolle as directivas de configuración do servidor openssh-server (por exemplo permite configurar o porto, se o usuario root pode iniciar sesión ou non por ssh, etc).
    - **Port** (establecer porto)
    - **PasswordAuthentication** (acceso por contrasinal)
    - **PermitRootLogging** (inicio de sesión para o usuario root)
    - Arquivos de claves host (privada e pública) do servidor para diferentes algoritmos (DSA, ECDSA, ED25519, RSA)

A primeira vez que desde un cliente ssh se establece unha conexión ao servidor aparece unha mensaxe indicando que non se coñece a identidade do mesmo. O que pasa é que o servidor envía a súa clave pública e o que equipo cliente non a coñece. Unha vez aceptada a clave pública nesa primeira conexión, o usuario debe autenticarse. O equipo cliente gardará as claves host públicas dos

servidores aos que se vai conectando en **.ssh/know_hosts** dentro do directorio *home* do usuario que lanzou a conexión.

O feito de gardar as claves públicas permite que en conexións posteriores:

- se a clave enviada polo equipo remoto non coincide coa clave pública gardada en *know_hosts* non aparecerá mensaxe de advertencia e o usuario debe autenticarse para poder iniciar sesión no equipo remoto.
- Se a clave enviada polo equipo remoto NON coincide coa clave pública gardada aparecerá un erro e abórtase a conexión, por motivos de seguridade (enténdese que o servidor está sendo suplantado)

Se queremos borrar as claves host no servidor faremos:

```
rm /etc/ssh/ssh_host
```

Podes xeralas de novo con:

```
ssh-keygen -A
```

Cando se xeran as claves do servidor de novo, haberá unha discrepancia entre as clave pública que envía o servidor e a que está gardada (identificando ao servidor) nos clientes, gardada no arquivo *known_hosts*.

Cando se tenta realizar a conexión desde o cliente, a propia mensaxe de erro dá as instrucións para eliminar as claves host almacenadas no cliente. Unha vez feito isto, nunha nova conexión irase ao inicio, como se o cliente se conectase por primeira vez.

Sempre que se inicia conexión por ssh pídese que o usuario introduza un contrasinal. Mediante a autenticación por claves, usando criptografía de clave simétricas, permítese que os usuarios se autentiquen no sistema empregando unha identidade dixital (formada por unha parella de claves pública-privada).

O procedemento a seguir é crear unha identidade dixital e copiar a clave pública no arquivo de claves autorizadas no host remoto (neste caso o servidor).

Para isto é necesario que o usuario cree a súa identidade dixital, xerando unha parella de claves privada-pública.

```
ssh-keygen
```

Isto xera claves RSA que se gardan en /home/usuario/.ssh, pódese empregar *passphase* para protexer a clave privada.

Se se quere xerar outra clave distinta á que se xera por defecto, podemos empregar os modificadores de ***ssh-keygen***:

- --t <tipo_clave>: permite especificar o tipo de clave (RSA,DSA,etc).
- --b <tamaño_clave>: permite especificar o tamaño da clave.
- --C "< comentario >": permite incluír un comentario para distinguila de outras.
- --f : permite especificar a ruta e nome dos ficheiros das claves.

Para poder empregar esta identidada dixital hai que autorizar o seu uso no equipo remoto. Para facer isto debemos copiar a clave pública no arquivo de arquivo de claves autorizads (authorized_keys) na conta que se teña no equipo remoto ao que se queira acceder.

```
ssh-copy-id -i (identity_file) -p (porto)
(usuario_a_Acceder)@(IP_servidor_a_Acceder)
```

Exemplos:
```
ssh-copy-id -i /home/ana/.ssh/chave_ana.pub -p 22
root@192.168.1.100
ssh-copy-id -p 10022 root@192.168.1.100
```

Configuracións favoritas

Pode darse o caso que se tenga que acceder a múltiples equipos por ssh usando diferentes usuarios, portos, etc. Para facilitar este proceso é posible crear diferentes configuracións favoritas para cada conexión. Estas configuracións créanse no arquivo ~/.ssh/config (se non existe hai que crealo).

#Configuración
```
Host (alias para conexión)
Hostname (dirección do host ao que desexas conectarte)
User (usuario que se quere utilizar na conexión)
IdentityFile (ruta da clave privada)
Port (porto a utilizar)
```

Un exemplo podería ser

```
Host meuservidor
HostName 192.168.1.100
User xan
IdentityFile ~/.ssh/chave_xan
```

Unha vez, podemos acceder a meuservidor con:

```
ssh meuservidor
```