

Llaves SSH en entornos *nix (linux, MacOS X, Windows WSL)

Introducción a las llaves SSH

El uso de llaves SSH es primordial para operaciones con servidores, ya sean aisladas o automatizadas. Añaden una capa extra de seguridad frente al uso de contraseñas y una versatilidad a las operaciones que se hace necesario tener nuestro par de llaves SSH.

Podemos tener nuestro par de llaves único (acosenjado por cuestiones de seguridad, ya que su revocación es más fácil) o por dispositivo.

Llaves OpenSsh (OpenSsh Keys)

Como norma general los servidores unix usan OpenSSH Server y por tanto sus llaves requieren que esten en este formato. Si usamos un entorno tipo unix (Linux, MacOS X, Windows WSL, FreeBSD) ese formato no supondra ningun problema. Si usamos Windows sin WSL, entonces seguramente usemos algun programa como Putty que tiene su formato cerrado, y el procedimiento requiere convertir sus llaves publicas a formato OpenSSH.

“ Puedes consultar nuestro manual [Manual para conexión SSH con Putty](#)

Generar un par de llaves

Vamos generar un par de llaves OpenSSH, sin contraseña, para operaciones desatendidas y porque creemos que es suficiente el nivel de seguridad que no sofrece, sin necesidad de añadir la capa extra con la contraseña.

Tan sencillo como posicionarnos en nuestro home, y ejecutar el comando, admitiendo todos los pasos por defecto.

Eso creara un par de llaves con el nombre `id_rsa` (privada) y `id_rsa.pub` (publica)

```
yamna@nox:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/yamna/.ssh/id_rsa):
Created directory '/home/yamna/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/yamna/.ssh/id_rsa
Your public key has been saved in /home/yamna/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:20RVkgzXUBA9/V2tkoDejoim+L7zAtjvfxxvva4CmQaA yamna@nox
The key's randomart image is:
+---[RSA 3072]----+
|          ..oBXo..|
|  .      . .oo.+ +|
|  . .    . ... . o+|
|E   .    ... o . o|
|.. . . oSo. . .   |
|o . + + o+.      |
| o + + o..       |
|. + o   .o.      |
| o+*o....++      |
+-----[SHA256]-----+
```

ssh-keygen

Parte pública

Si queremos acceder a un servidor remoto (root o usuario) deberemos añadir la llave publica a el fichero de autorizaciones del sistema remoto o bien facilitarselo al administrador para que el haga su trabajo.

No existe ningun problema en enviar esta llave (la pública) a alguien, incluso en modo texto. A fin de cuentas es la llave pública que no sirve nada más que para que otros la ulticen para **autorizarnos** a nosotros.

Parte privada

Esta es la parte que si tenemos que atender a su seguridad. La perdida de un dispositivo, que tenga esa llave, unido a que el hacker pueda analizar nuestro historico, le dará la oportunidad de acceder de forma inmediata a todos los servicios en los que tu par de llaves esten autorizadas. Asi

pues, la más mínima sospecha de intrusión, sustracción, pérdida de dispositivo, con ese par de llaves, conlleva a la revocación inmediata de las llaves y aviso a los administradores implicados. (como si perdieras la contraseña)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como esta, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Revision #1

Created 31 May 2021 21:15:05 by Abkrim

Updated 21 April 2022 08:02:57 by Abkrim