Error de acceso SSH con llaves ssh (Permission denied (publickey)) habiendo verificado que las llaves son correctas

Introducción

Desde OpenSSH 7.0 se deshabilito por defecto el intercambio de claves SSH-DSS. Esto puede producir un comportamiento de error, muy silencioso que es fácil de detectar y corregir.

Si tenemos una llave creada con el tipo dss y esta está autorizada en un sistema, o por error, no vimos que nos pasaban una llave con esa característica, para añadirla a un sistema, esta no funcionará en el sistema actualizado, y nos dará en primera instancia un error de **Denegación por llave incorrecta**.

Análisis

En el acceso general con esa llave sólo recibiremos un mensaje corto

```
root@server:~# ssh  user_remoto@servidor.remoto.tld -p 51514
user_remoto@servidor.remoto.tld: Permission denied (publickey).
```

Como siempre, debemos acostumbrarnos a analizar nuestros problemas con el aumento del sistemas de logs o de mensajes (debug)

Dejaremos el listado sólo en lo justo para ver el problema

```
root@server:~#  ssh  user_remoto@servidor.remoto.tld -p 51514 -vv
OpenSSH_8.2p1 Ubuntu-4ubuntu0.3, OpenSSL 1.1.1f  31 Mar 2020
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
...
debug1: Trying private key: /root/.ssh/id_rsa
debug1: Trying private key: /root/.ssh/id_ecdsa
debug1: Trying private key: /root/.ssh/id_ecdsa_sk
debug1: Trying private key: /root/.ssh/id_ed25519
debug1: Trying private key: /root/.ssh/id_ed25519_sk
debug1: Trying private key: /root/.ssh/id_xmss
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
```

Importante que nos indique que ha buscado la llave y no le ha valido.

Revisando la llave vemos que tiene el tipo ssh-dss el cual no está aceptado por el servidor remoto.

```
También es importante ver el log del **servidor sshd** si es posible, y dependiendo del nivel de log que tenga podremos ver que nos indica que el tipo dss no está aceptado
```

Revisamos el valor de la llave y vemos en el incio, que tenemos una llave tipo DSS.

```
root@server:~# cat .ssh/id_dsa.pub
ssh-dss AAAAB3N….
```

Opciones

Reconstrucción de la llave con formato rsa (Recomendado)

El tipo RSA es el más aconsejado. Si el sistema no te crea la llave por defecto con DSA o no se la crea al usuario que te está facilitando la llave, deberá forzar el comando de generación de sus llaves para que use el formato RSA.

```
root@server:~#  ssh-keygen -t rsa
```

Deberemos actualizar la llave en nuestro fichero de authorized_keys, y ya debería funcionar

Activación del algoritmo DSS en el servidor (No aconsejable)

Puede existir algún escenario, por prisas, situación específica, etc, que no nos permita de forma inmediata, el recrear la llave del servidor que quiere acceder, por lo que debemos reactivar el tipo de llave que tenemos.

Es imperativo, entender que esto es un atajo, muy común en los artículos de internet, que puede llevar a dejar nuestro sistema más inseguro, si luego no lo devolvemos a la normalidad.

Ese error, ocurre en el 90% de los casos, porque el administrador, va corriendo, y luego no vuelve atrás a corregir la situación.

Para ello debemos editar el fichero `/etc/ssh/sshd_config` añadiendo la línea siguiente:

```
PubkeyAcceptedKeyTypes=+ssh-dss
```

Centos 8

Requiere un paso adicional, relacionado con su System-wide Cryptographic Policies.

Primero deberíamos conocer el nivel actual (suele ser por defecto) para luego devolverlo a su estado original

```
$ update-crypto-policies --show
DEFAULT
```

```
Debemos, devolver en cuanto podamos, (nueva llave) nuestro sistema a la posición de seguridad inicial
```

Otros enlaces

- OpenSSH 7.o Release notes
- Chapter 5. Using system-wide cryptographic policie
- SSH keeps skipping my pubkey and asking for a password

- SSH connection issue on Fedora 30 with OpenSSH 8.0 (Using ssh-dss), still asking for password with public key setup

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 está, 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 2021-08-19 10:34:31 UTC by Abkrim
Updated 2021-08-19 10:48:21 UTC by Abkrim