

Unable to negotiate with X.X.X.X.X port YY: no matching host key type found. Their offer: ssh-rsa,ssh-dss

Introducción

Es un extraño error que veces puede acontecer cuando conectamos a determinados sistemas que han sido actualizados o no, que difieren de la norma general, o entran en conflicto con nuestro cliente SSH por ausencia o defecto de configuración.

“ Edición y lectura necesaria hasta el final 21/07/2022

```
ssh root@remotehost -p2244
Unable to negotiate with 99.99.99.99 port 2244: no matching host key type found. Their offer:
ssh-rsa,ssh-dss
```

Con debug

```
OpenSSH_8.9p1 Ubuntu-3, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /home/abkrim/.ssh/config
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 *
debug3: expanded UserKnownHostsFile '~/ssh/known_hosts' -> '/home/abkrim/.ssh/known_hosts'
debug3: expanded UserKnownHostsFile '~/ssh/known_hosts2' -> '/home/abkrim/.ssh/known_hosts2'
debug2: resolving "remotehost" port 2244
debug3: resolve_host: lookup remotehost:2244
debug3: ssh_connect_direct: entering
debug1: Connecting to remotehost [99.99.99.99] port 2244.
```

```
debug3: set_sock_tos: set socket 3 IP_TOS 0x10
debug1: Connection established.
debug1: identity file /home/abkrim/.ssh/id_rsa type 0
debug1: identity file /home/abkrim/.ssh/id_rsa-cert type -1
debug1: identity file /home/abkrim/.ssh/id_ecdsa type -1
debug1: identity file /home/abkrim/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/abkrim/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/abkrim/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/abkrim/.ssh/id_ed25519 type -1
debug1: identity file /home/abkrim/.ssh/id_ed25519-cert type -1
debug1: identity file /home/abkrim/.ssh/id_ed25519_sk type -1
debug1: identity file /home/abkrim/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /home/abkrim/.ssh/id_xmss type -1
debug1: identity file /home/abkrim/.ssh/id_xmss-cert type -1
debug1: identity file /home/abkrim/.ssh/id_dsa type -1
debug1: identity file /home/abkrim/.ssh/id_dsa-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
debug1: Remote protocol version 2.0, remote software version OpenSSH_5.3
debug1: compat_banner: match: OpenSSH_5.3 pat OpenSSH_5* compat 0x0c000002
debug2: fd 3 setting O_NONBLOCK
debug1: Authenticating to remotehost:2244 as 'root'
debug3: put_host_port: [remotehost]:2244
debug3: record_hostkey: found key type RSA in file /home/abkrim/.ssh/known_hosts:57
debug3: load_hostkeys_file: loaded 1 keys from [remotehost]:2244
debug1: load_hostkeys: fopen /home/abkrim/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug3: order_hostkeyalgs: prefer hostkeyalgs: rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-
cert-v01@openssh.com,rsa-sha2-512,rsa-sha2-256
debug3: send packet: type 20
debug1: SSH2_MSG_KEXINIT sent
debug3: receive packet: type 20
debug1: SSH2_MSG_KEXINIT received
debug2: local client KEXINIT proposal
debug2: KEX algorithms: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,sntrup761x25519-sha512@openssh.com,diffie-
hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-
sha512,diffie-hellman-group14-sha256,ext-info-c
debug2: host key algorithms: rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-
```

v01@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com

debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

debug2: compression ctos: none,zlib@openssh.com,zlib

debug2: compression stoc: none,zlib@openssh.com,zlib

debug2: languages ctos:

debug2: languages stoc:

debug2: first_kex_follows 0

debug2: reserved 0

debug2: peer server KEXINIT proposal

debug2: KEX algorithms: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

debug2: host key algorithms: ssh-rsa,ssh-dss

debug2: ciphers ctos: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se

debug2: ciphers stoc: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se

debug2: MACs ctos: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

debug2: MACs stoc: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96

debug2: compression ctos: none,zlib@openssh.com

debug2: compression stoc: none,zlib@openssh.com

debug2: languages ctos:

debug2: languages stoc:

debug2: first_kex_follows 0

debug2: reserved 0

```
debug1: kex: algorithm: diffie-hellman-group-exchange-sha256
debug1: kex: host key algorithm: (no match)
Unable to negotiate with 99.99.99.99 port 24: no matching host key type found. Their offer:
ssh-rsa,ssh-dss
```

Solución

en nuestra fichero `~/.ssh/config` (si no existe podemos crearlo) añadimos.

```
HostKeyAlgorithms ssh-rsa
PubkeyAcceptedKeyTypes ssh-rsa
```

Problemas

Tras el uso de este tip, al día siguiente aparecio una serie de problemas en el que me fallaban las conexiones a todas mis maquinas via ssh, no pudiendo logearme.

```
No Kerberos credentials available (default cache: FILE:/tmp/krb5cc_1000)
```

Tras una búsqueda en internet ninguna de las opciones me parecia correcta y algo me indicaba que la salida por la tangente de la edición del config de mi cliente **ssh** era la raíz del problema, desactive las valores indicados.

Y todo volvio a funcionar de nuevo.

Asi que dejo el tip, porque es posible que ayude a alguien, en ambos sentidos, y proque espero tener un hueco (que dificil) para ponerme con este problema y verlo en amplitud.

Agradecimientos

Iba con prisa y no pude pararme mucho, hasta que un dia el problema ya empezo a ser pesado.

Gracias [How To Configure Custom Connection Options for your SSH Client](#) donde se explica superbien como configurar el fichero `~/.ssh/config` por hosts, y cadauno con sus cosas.

“ En mi caso tenia un fichero para conectarme rápidamente a los mas de 200 servidores que manejo, pero ahora los que me dan problema puedo llamarlos con `ssh` directamente.

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 #3

Created 20 July 2022 08:48:53 by Abkrim

Updated 26 February 2023 06:41:13 by Abkrim