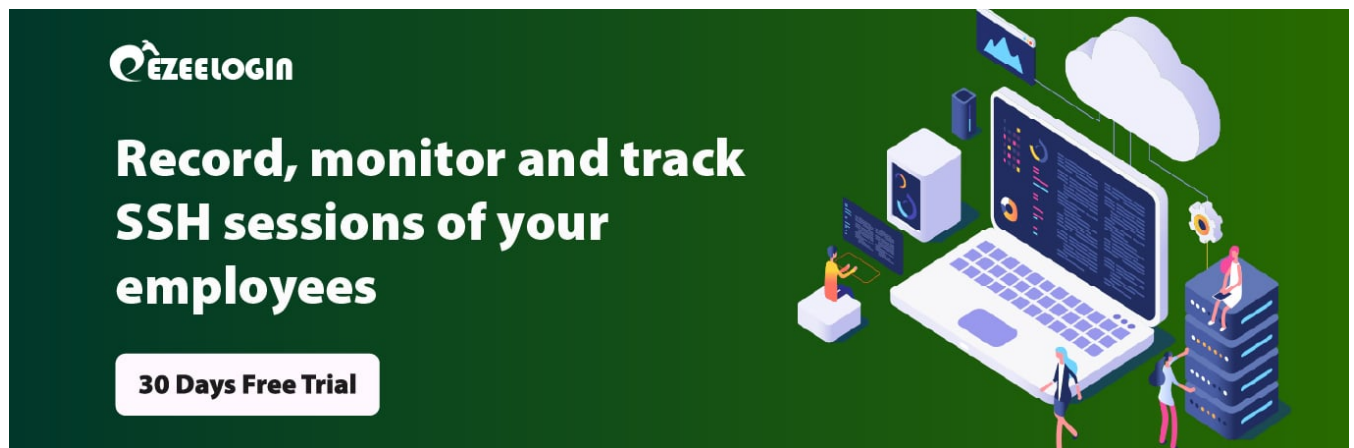


KEX and Host Key Algorithms in SSH

565 Nesvin KN May 24, 2023 [General](#) 28097



What are KEX and Host Key Algorithms?

KEX is the short form of **Key Exchange**: The algorithm is chosen to compute the secret encryption key. Examples would be `diffie-hellman-group-exchange-sha1` and modern `ecdh-sha2-nistp512`.

Public_key or Server Host key: The asymmetric encryption algorithm used in the server's private-public host key pair. Examples would be `ssh-rsa` and elliptic curve `ecdsa-sha2-nistp521`.

How to find the KEX (Key Exchange) and Host Key Algorithms in SSH?

1. SSH from one linux machine to another in verbose mode to get the detailed process.

2. **KEX** and host key algorithms used to SSH can be found in debug 1 level logs. Refer below example of **KEX** and host key algorithms.

```
debug2: languages stoc:
debug2: first_kex_follows 0
debug2: reserved 0
debug2: peer server KEXINIT proposal
debug2: KEX algorithms: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
debug2: host key algorithms: ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
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
debug2: compression stoc: none,zlib@openssh.com
debug2: languages ctos:
debug2: languages stoc:
debug2: first_kex_follows 0
debug2: reserved 0
debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug3: send packet: type 30
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug3: receive packet: type 31
debug1: Server host key: ecdsa-sha2-nistp256 SHA256:GXJh1wF70JTtuXN31hAdTuf4+PgF7RMUTVvMicierbcM
debug3: hostkeys_foreach: reading file "/root/.ssh/known_hosts"
debug3: record hostkey: found key type ECDSA in file /root/.ssh/known_hosts:1
debug3: load hostkeys: loaded 1 keys from 192.168.1.7
```

How to change the KEX and host key algorithm on the server

machine?

1. Edit `sshd_config` file and append the below lines with **KexAlgorithms** and **HostKeyAlgorithms**.

2. Restart `sshd` service to affect the changes made in `sshd_config`.

3. **SSH** from the client machine to the server machine to view the changed **KEX** and **host key algorithms**.

```
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-group16-sha512
debug2: host key algorithms: ssh-rsa,rsa-sha2-512,rsa-sha2-256
debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm
@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm
@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc
debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@op
enssh.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@op
enssh.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
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-group16-sha512
debug1: kex: host key algorithm: rsa-sha2-512
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug2: bits set: 2030/4096
debug3: send packet: type 30
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug3: receive packet: type 31
debug1: Server host key: ssh-rsa SHA256:7cr32AGB+4aTWbg3L+5gS+WUK17GAI5WF65sMCnWg/I
debug3: hostkeys_foreach: reading file "/root/.ssh/known_hosts"
debug3: record hostkey: found key type ECDSA in file /root/.ssh/known_hosts:1
```

How to view the list of KEX and Keys in the Linux server?

- How to list **keys** in the Linux server?



- How to list **KEX** in the Linux server?



Related Articles

[DSA key based authentication is not working](#)

[signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms](#)

[signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms](#)

Online URL: <https://www.ezeelogin.com/kb/article/kex-and-host-key-algorithms-in-ssh-565.html>