Failure establishing SSH session: Unable to exchange encryption keys

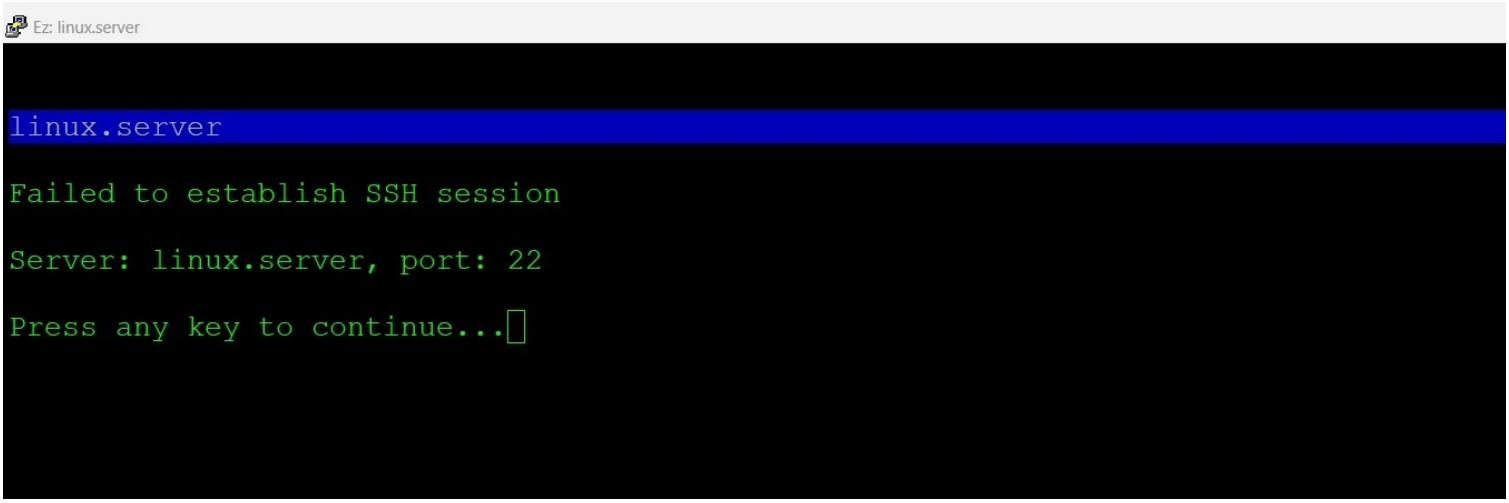
566 Nesvin KN October 27, 2025 Common Errors & Troubleshooting 9077

How to fix the error "Failure establishing SSH session" in ezsh (ezeelogin shell)?

Overview: This article describes resolving the **"Failure establishing SSH session"** error in **ezsh** by updating encryption algorithms.

How to fix the error "Failed to establish SSH session"?

This error occurs when a user tries to login to the remote servers that are added in gateway server. Refer below screenshot of the error.



Step 1: Check the ezsh log of the user from the gateway server.

Login to the gateway server as the root user and check the ezsh log of the user.

```
root@gateway :~# cat /home/{username}/ezsh.log

Failure establishing SSH session: Unable to exchange encryption keys
```

How to fix the error "Failure establishing SSH session: Unable to exchange encryption keys"?

Step 1: Login to the remote server from the gateway server with level 3 verbose to find out the KEX and Host Key algorithms used. Refer below example of SSH and algorithms.

```
root@gateway :~# ssh root@remote_server -vvv

debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
```

Step 2: Below are the **supported Key Exchange (KEX) and Host Key algorithms**.
If the currently running Ezeelogin version is below 7.29.11, upgrade to the latest version to ensure **support for the newest KEX and Host Key algorithms**.

> **Supported 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

Supported HostKeyAlgorithms:

ecdsa-sha2-nistp256
ssh-ed25519
ssh-rsa
ssh-dss
rsa-sha2-512
rsa-sha2-256

Refer detailed article to know more about KEX and HostKeyAlgorithms.

Step 3: Find the KEX and host key algorithm used.

Step 3.a: SSH from gateway server to remote server in verbose mode to get the detailed messages.

```
root@linux_server ~]# ssh username@linux_server_IP -vvv
```

Step 3.b: 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.**

```
debug1: kex: algorithm: curve25519-sha256
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
```

Step 4: Change the KEX and host key algorithm on the remote server.

Step 4.a: Edit the sshd_config file on the remote server and add the required KEX and host key algorithm.

```
root@linux_server ~]# vim /etc/ssh/sshd_config

KexAlgorithms diffie-hellman-group16-sha512
HostKeyAlgorithms rsa-sha2-512
```

Step 4.b: Restart the SSHD service to apply the changes made in **sshd_config**.

```
root@linux_server ~]# systemctl restart sshd
```

Step 5: After applying the configuration changes, try logging in to the remote server from the Ezeelogin shell (ezsh) and verify whether the error is resolved.

Related Articles:

Encryption technologies used in Ezeelogin.

KEX and Host Key Algorithms in SSH

List of supported PubkeyAcceptedKeyTypes in Ezeelogin

Online URL: https://www.ezeelogin.com/kb/article/failure-establishing-ssh-session-unable-to-exchange-encryption-keys-566.html