'Failed to establish SSH session '

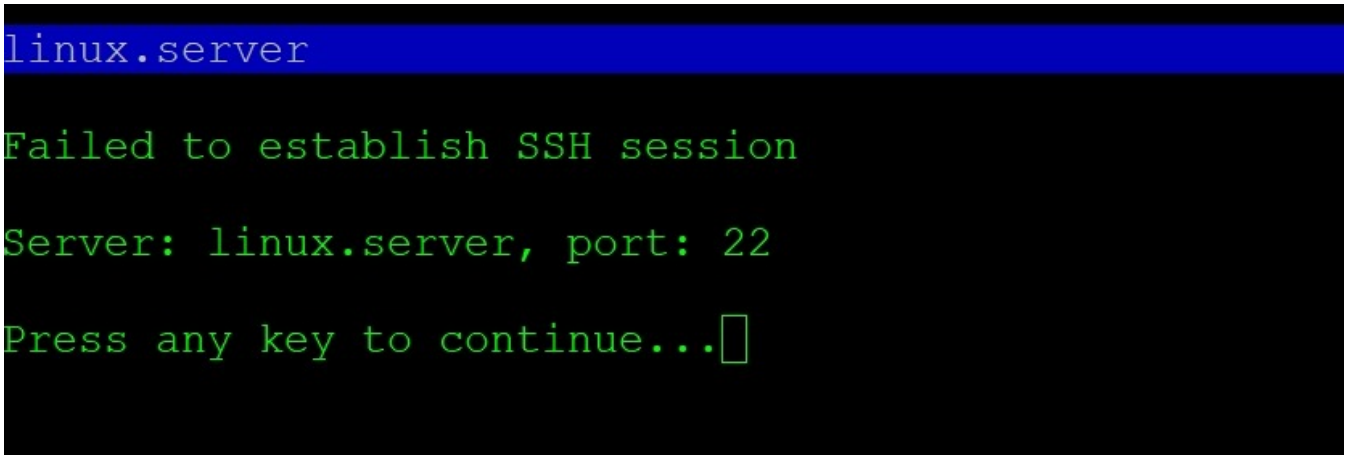
222 Manu Chacko October 17, 2025 Common Errors & Troubleshooting 14631

Troubleshooting "Failed to Establish SSH Session" errors with ezeelogin

---

Overview: This article addresses troubleshooting steps for resolving "Failed to establish SSH session" errors encountered when using Ezeelogin's shell interface. Covering firewall configurations, SELinux checks, SSH timeout adjustments, log inspections, and log size management, it provides comprehensive solutions to ensure seamless SSH connectivity.

'Failed to establish SSH session' error ; unable ssh via Ezeelogin shell



Follow the below steps:

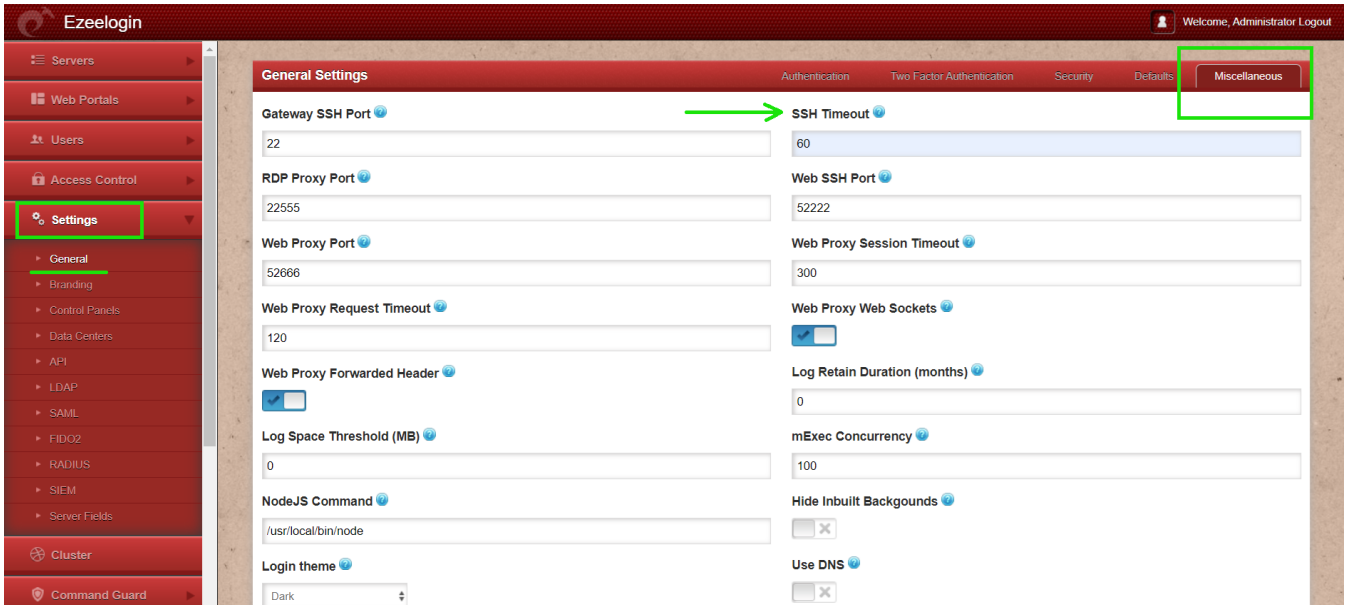
Step 1. Make sure that the iptables / firewall is not blocking ssh traffic (check ssh port is open on both gateway & target server) and make sure SSHD is not blocked in /etc/hosts.allow or /etc/hosts.deny

```
telnet <server_ip> 22
```

Step 2. Make sure that SELinux is disabled on jumpbox / gateway server and the target server. You can find it by typing '**sestatus**'

```
root@gateway:~# sestatus
SELinux status: disabled
```

Step 3. Increase ssh timeout value to 60 seconds.Do refer to this **user manual**.



Step 4. Check ezsh log for errors. You can get it from '**/home/{username}/ezsh.log** '

Step 5. *Also, check for the SSHD error log of the remote server to which you are trying to login.*

If it is Centos it will be **/var/log/secure**

If it is Ubuntu it will be **/var/log/auth.log**

- On the remote server run the below command.

```
root@remote_server:~# systemctl restart systemd-logind.service
```

Step 7. Try to re-add the server and try to access it again.

Step 8. Check the size of the **/var/log/btmp**. You can check that by running the following command on the remote server

```
root@remote_server:~# ls -lah /var/log/btmp
```

If you are unable to ssh via the ezsh interface and you get the error on /home/{username}/ezsh.log

```
Authentication by SSH key DB failed :

Channel failed (shell): Timed out waiting on socket
```

You can find the following logs on /var/log/secure and /var/log/messages on the remote server.

```
  sshd[236622]: Accepted publickey for root from 46.232.178.114 port 40506 ssh2: RSA SHA256:cpVnOWHn+WeiGl4JuYAlMtx39Vx5Dz82CuN7I12yITI

 sshd[236622]: pam_unix(sshd:session): session opened for user root by (uid=0)

systemd-logind: New session c100 of user root.

systemd: Started Session c100 of user root.

systemd-logind: Removed session c100.
```

If the size of **/var/log/btmp** is high then truncate the logs in **/var/log/btmp**. You can truncate the logs by running the following command on the remote server.

```
root@remote_server:~# > /var/log/btmp
```

Related Articles:

[Authentication by ssh key failed]

[Error: Server login failed. Error waiting for connection. FAILED: Could not connect]

[Interrupt SSH session to remote server]

[Failure establishing SSH session: Unable to exchange encryption keys]