How to fix: Connection refused by port 22 Debian/Ubuntu

11 months agoby Karim Buzdar

SSH provides a secure way to access and manage Linux servers. Sometimes while connecting to SSH servers, users often encounter "Connection refused" error by port 22. It happens because of several reasons like SSH service is not running, the port is blocked by the firewall, or the server is using a different port. It can also occur because of the IP conflict issue. In this article, we will discuss some of the solutions that you should try in order to fix the error.

Note: The commands discussed here have been tested on Ubuntu 20.04 LTS. The same commands are also valid for the Debian system.

Fix Connection refused error

This is the "Connection refused" error you might encounter while connecting to a remote system over SSH.

```
kbuzdar@mint:~$ ssh kbuzdar@192.168.72.157
ssh: connect to host 192.168.72.157 port 22: Connection refused
kbuzdar@mint:~$
```

Follow the below solutions step by step in order to solve the "Connection refused" error.

Make sure OpenSSH is installed

One of the reasons you may receive a "Connection refused" error is because the OpenSSH server is not installed on the target server.

First, you will need to make sure that the OpenSSH server is installed on the system which you are trying to access via SSH. In order to check whether OpenSSH is installed or not, issue the following command in the Target server's Terminal:

```
$ sudo apt list --installed | grep openssh-server
```
This command basically filters the term "openssh-server" from the list of installed packages. If you receive the following similar output, it indicates the OpenSSH server is installed. On the other hand, if you receive no output, it means OpenSSH is missing on the target server.

```
kbuzdar@ubuntu:~$ apt list --installed | grep openssh-server

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

openssh-server/focal-updates,now 1:8.2p1-4ubuntu0.1 amd64 [installed]
kbuzdar@ubuntu:~$
```

In case it is not installed on the target server, you can install it using the following command as sudo:

```
$ sudo apt install openssh-server
```
Then type sudo password, and when asked for confirmation, press 'y'. Once installed, confirm it using the same command

```
$ sudo apt list --installed | grep openssh-server
```
Check SSH service

OpenSSH service runs in the background and listens to incoming connections. The stopped OpenSSH service can be one of the reasons you are receiving a "Connection refused" error.

Therefore, it is necessary to check whether the OpenSSH service is running or not using the following command in Terminal:

```
$ sudo service ssh status
```
If you see the following output, it means the service is active and running in the background.

```
kbuzdar@ubuntu:~$ sudo service ssh status
[sudo] password for kbuzdar:
 ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2020-10-07 03:45:38 PDT; 3h 44min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
```

On the other hand, if you receive **inactive (dead),** that means the service is not running**.** You can run the OpenSSH service using the following command as sudo in Terminal:

```
$ sudo service ssh start
```
In order to restart the service, use the following command:

```
$ sudo service ssh restart
```
Check SSH server listening port

Another reason for receiving a "Connection refused" error is because you are trying to connect to the wrong port. For instance, if the server is configured to listen on port 2244, and you are trying to connect to its default port 22, then, in this case, you will receive a "Connection refused" error.

Before trying to connect, you need to check the SSH server listening port. If it is the default port (22), then you can connect it using the following command:

```
$ ssh [username]@[remoteserver IP or hostname]
```
If it is some port other than the default port, you will need to connect to the SSH server using this port:

```
$ ssh -p [port number] [username]@[ip address]
```
In order to check which on which port the OpenSSH server is listening to; use the following command in Terminal:

```
$ sudo netstat -ltnp | grep sshd
```
You will receive the output similar to the following:

```
kbuzdar@ubuntu:~$ sudo netstat -ltnp | grep 'sshd'
tcp        0      0 0.0.0.0:2244           0.0.0.0:*              LISTEN      17165/sshd: /usr/sb
tcp6       0      0 :::2244                :::*                   LISTEN      17165/sshd: /usr/sb
```

In the third column, you can see the server listening port is 2244. If this is the case, you will need to connect to the SSH server using this port.

```
$ ssh -p [2244] [username]@[ip address]
```
Allow SSH in firewall

Firewall blocking the SSH port can be another major reason for the "Connection refused" error. If a firewall is running on the SSH server, you will need to allow the SSH port in it using the following command. Replace the *port* by the port number the SSH server is listening to:

```
$ sudo ufw allow port /tcp
```
For instance, if the SSH server is listening to port 2244, then you can allow it in the firewall as:

```
$ sudo ufw allow 2244/tcp
```

```
kbuzdar@ubuntu:~$ sudo ufw allow 2244
Rule added
Rule added (v6)
kbuzdar@ubuntu:~$
```

Reload the firewall using the following command:

```
$ sudo ufw reload
```

In order to confirm if the rules have been added, check the status of the firewall using the following command in Terminal:

```
$ sudo ufw status
```

The following output shows that the port 2244 is allowed in the firewall.

```
kbuzdar@ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
2244/tcp                   ALLOW       Anywhere
2244/tcp (v6)              ALLOW       Anywhere (v6)
```

Resolve Duplicate IP address conflict

The "Connection refused" error can also occur because of duplicate IP address conflict. So, make sure the system does not have a duplicate IP address.

Install the arping utility on your system using the following command:

```
$ sudo apt install arping
```

Then ping the SSH server's IP address.

```
$ ping <ip-address>
```

In the output, if you see the reply from more than one MAC address, then it shows that there is a duplicate IP running on the system. If this is the case, change the IP address of the SSH server and try connecting again with the new IP address.

This is how to fix the "Connection refused" error by port 22 in Linux systems. In this article, we have described a few ways that will surely help you in solving the "Connection refused" error.

ABOUT THE AUTHOR

Karim Buzdar

Karim Buzdar holds a degree in telecommunication engineering and holds several sysadmin certifications. As an IT engineer and technical author, he writes for various web sites. He blogs at LinuxWays.