

Troubleshooting the SSH Connection

Finding solutions



February 2, 2024

Git-gotech

Houston Texas

|  |  |
| --- | --- |
| **SSH Connectivity issues and solutions** | |
| **Issue** | **Soultion** |
| Connection not possible | nc <public ip> 22 for verification |
| Connection not possible | Add a public IP address |
| Connection not possible | If the security list that permits SSH connections is removed, you can't access the instance. Ensure a security list that opens port 22 is present |
| Connection not possible | Check the instance accessibility status metric to determine whether the instance is responding to an Address Resolution Protocol (ARP) request. If the ARP ping fails, the metric shows that the instance is unresponsive. If there isn't an ongoing infrastructure issue, then the instance probably has a software issue or a network misconfiguration that you must resolve yourself. |
| Connection not possible | The steps for confirming that SSH is running [systemctrl status] |
| Connection not possible | You can capture the instance's serial console data history in the Console or by using the console-history resource in the CLI. This information can help determine the cause of connectivity problems. |
| Connection not possible | Update PuTTY tool |
| Hostname Resolution | Most resolution errors occur when the reference to the SSH host can’t be mapped to a network address. While this is almost exclusively DNS related, the root cause isn’t always a DNS issue |
| Connection Timeout | ssh sysadmin@10.1.10.205 |
| Connection Refused | • Verify that the host IP address is correct for the Droplet. • Verify that your network supports connectivity over the SSH port being used. Some public networks may block port 22 or custom SSH ports. You can do this by, for example, testing other hosts using the same port with a known working SSH server. This can help you determine if the issue isn’t specific to your Droplet. • Verify the Droplet firewall rules. Check that they’re not set to a default policy of DROP and the port is not added to allow connections. • Verify that the service is currently running and bound to the expected port. |
| Checking the SSH Service Port |  |
| Check the service is working | ss -plnt |
| Remote Hostname Identification Error | Verify the correct information |
| Connection Timeout Error | Validate the server information |
| Connection Failure | Check the IP address is correct |
| Firewall issues | Firewall Configuration Checking |
| SSH Status | Status of SSH Checking |
| SSH Port Issues | SSH Port Checking |



Online reading: [[LayerStack Tutorials - LayerStack - How to troubleshoot SSH connectivity issues](https://www.layerstack.com/resources/tutorials/How-to-troubleshoot-SSH-connectivity-issues)]

How to troubleshoot SSH connectivity issues

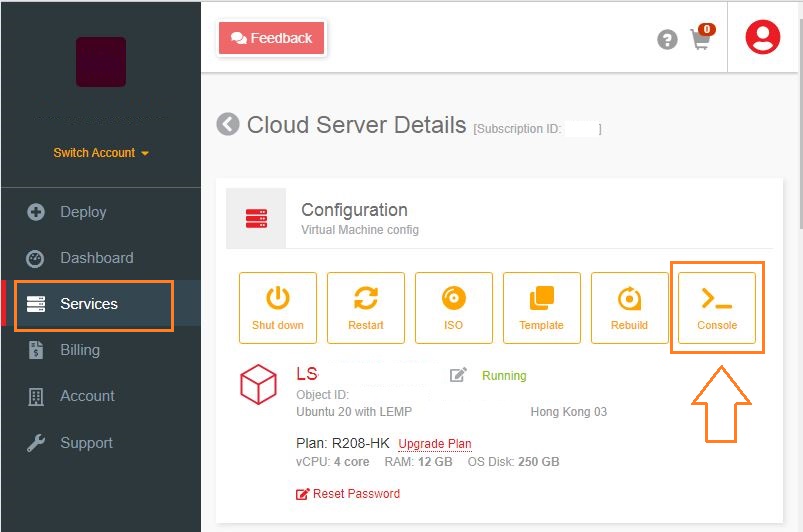
2021-02-01 By Mark 29747 Views [linux](https://www.layerstack.com/resources/tutorials/tags/linux)[ssh](https://www.layerstack.com/resources/tutorials/tags/%20ssh)[troubleshooting](https://www.layerstack.com/resources/tutorials/tags/%20troubleshooting)[layerpanel](https://www.layerstack.com/resources/tutorials/tags/%20layerpanel)

13 reviews

The SSH (Secure Shell or Secure Socket Shell) is a service that provides a secure way for users and system administrators to access a server over an insecure network. In some cases, the server cannot be accessed via SSH or the SSH service becomes refused the connection which needs to be further investigated.

Before proceeding with SSH troubleshooting, you need to make sure that:

* There are no SSH access restriction rules set on the firewall level in the [LayerPanel](https://cp.layerpanel.com/) & server-side.
* Your server is working correctly through the Console in the [LayerPanel](https://cp.layerpanel.com/) as follows.



Troubleshooting SSH Connectivity Issues

1. **Remote Hostname Identification Error**

You may get errors like the below ones when trying to access through SSH:

Remote Host Identification Has Changed

OR

ssh: Could not resolve hostname: Name or service not known

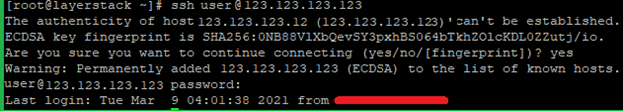
OR

Unable to open a connection to Host does not exist

A hostname error may occur when a host fails to connect to SSH using a specific network address.

To resolve such errors, you may follow the steps below:

* 1. Check if the hostname is correct.
  2. Check if the hostname has ping.
  3. If the hostname is not resolving properly, you can use the public IP address for SSH as below, where the user is the SSH username that you use and 123.123.123.123 is the server IP.
  4. # ssh user@123.123.123.123



1. **Connection Timeout Error**

This error shows up when a user tries to connect to a server, but the server refuses to establish the connection within a specified timeout period.

The common error messages in such cases are as below:

Error output

ssh: connect to host 123.123.123.123 port 22: connection timed out

OR

PuTTY error output

Network error: Connection time out

To correct this error, follow the below steps.

* 1. Make sure that the server IP address is correctly typed in.
  2. Confirm that your network allows SSH port connectivity.
  3. Verify that the firewall rules on your VPS are not at fault.

1. **Connection Failure**

Connection failure and timeout are both different. A connection failure occurs when your SSH request reaches the SSH port but the server refuses to accept it.

In this case, you may see the below errors:

Error output

ssh: connect to host 123.123.123.123 port 22: connection refused

OR

PuTTY error output

Network error: Connection refused

The resolution steps for connection failure are like those of connection timeout. To correct this error, use the following steps.

* 1. Make sure that the IP address of the server is correct.
  2. Confirm that your network allows SSH connection.
  3. Verify that the server firewall rules allow SSH access.

Basic solutions to troubleshoot SSH connectivity

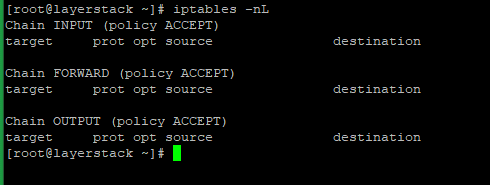
1. **Firewall Configuration Checking**

One of the common causes of SSH connectivity is firewall blocking and firewall applications differ between various OS being used in the server.

With **CentOS7**, it is firewalld, whereas, with **Ubuntu**, it is ufw. If these are not present in the server, probably it is using iptables.

The firewall rules in your server can be listed using the below command with sudo or as the root user.

# iptables -nL



If there are any REJECT or DROP rules, you should ensure that the INPUT chain allows the default SSH port 22.

The below command will show the list of services supported by firewalld.

# firewall-cmd --list-services

sshtbs3

If you are using a custom port for SSH, you can check with the --list-ports option.

In **Ubuntu** servers, with ufw installed, the below command can be used to check the firewall rules.

# ufw status

1. **Status of SSH Checking**

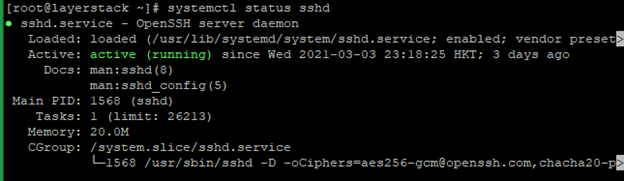
If you face any issues when connecting to a server using SSH, the first thing is to make sure that the SSH server is up and running. You can use the below commands to check the status of the SSH service in the server.

For older OS systems such as Ubuntu 14.04, Debian 8, or CentOS 6, use the service command.

# service ssh status

For new versions, use the systemctl command.

# systemctl status sshd

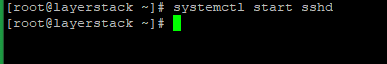


In case if the SSH service isn’t executing or active, the below commands can be used to start the service depending on the OS system.

# systemctl start sshd

OR

# service ssh start

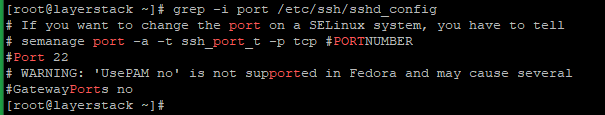


1. **SSH Port Checking**

The default SSH port in all OS systems is 22. You can also use a custom SSH port, which can be set in the configuration file of the SSH service located at the path ***/etc/ssh/sshd\_config*.**

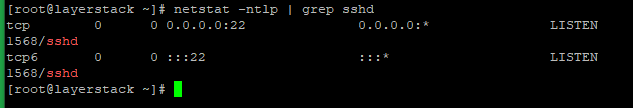
Use the below command to check on the SSH port being used in the server:

# grep -i port /etc/ssh/sshd\_config



You can also use the netstat command to check on the port that is being used by the SSH service. Execute the below command and the output should show up in the SSH port.

# netstat -ntlp | grep sshd



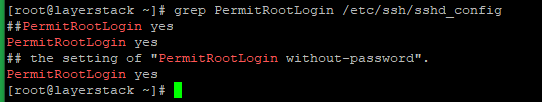
Basic solutions to troubleshoot rejected SSH login

For checking on issues related to SSH rejecting login attempts, the below guidelines can be followed.

1. **Checking whether Root Login is permitted**

SSH service can be configured to disable logins for the root user. To check if root login is permitted or not, run the below command:

# grep PermitRootLogin /etc/ssh/sshd\_config



If it is not permitted, set the value of PermitRootLogin in */etc/ssh/sshd\_config* to yes as in the above image, restart SSH, and try logging in as root again.

Run the below command to restart the SSH service.

# systemctl restart sshd

OR

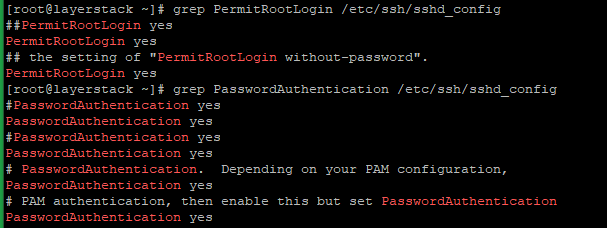
# service ssh restart

sshtbs9

1. **Checking whether Password Authentication is accepted**

SSH can be configured to accept/not accept passwords and instead make use of public-key authentication. To check if password authentication is enabled or not, run the below command:

# grep PasswordAuthentication /etc/ssh/sshd\_config



Set the value of PasswordAuthentication in */etc/ssh/sshd\_config* to yes as in the above image, restart SSH, and try logging in with your password again.

Run the below command to restart the SSH service.

# systemctl restart sshd

OR

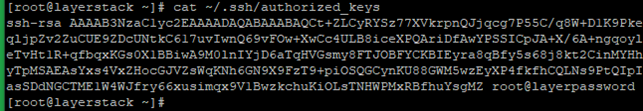
# service ssh restart

sshtbs11

1. **Checking SSH public key stored on the server**

If login attempts to your server using public-key authentication are not working, you need to make sure that the public key has been set inside your server. To view the public keys stored in your server, make use of the below command.

# cat ~/.ssh/authorized\_keys



If your public key is not listed in this file, add it to the file on a new line.

On some servers, the location of the authorized keys may be different. Run the below command to see where the file is located:

# grep AuthorizedKeysFile /etc/ssh/sshd\_config

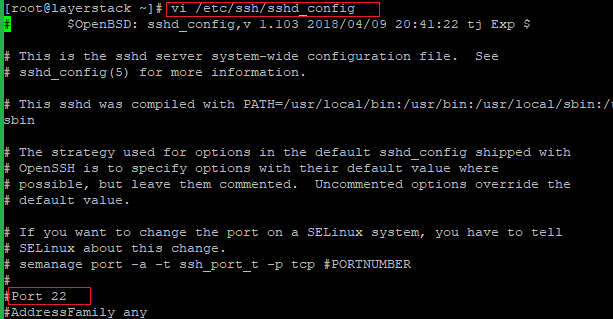
sshtbs13

Change SSH port to increase the server security

The server default SSH port is 22, and changing the server default SSH port means adding an extra layer of security to the server by reducing the risk of automated attacks.

Please note that the port numbers from 0-to-1023 are reserved for various system services. Hence, the recommended ports can use choosing port numbers between 1024 to 65535.

1. Edit the sshd configuration file and add a new Port.
2. # vi /etc/ssh/sshd\_config
3. locate the line
4. Port 22
5. OR
6. #Port 22
7. And
8. Change to the new port number that you want to use and save the file.



1. Now restart the SSH services in the server, using the following commands that depend on the OS system.
2. # systemctl restart sshd
3. OR
4. # service ssh restart

sshtbs15

1. Update the server firewall rules with a new SSH port.

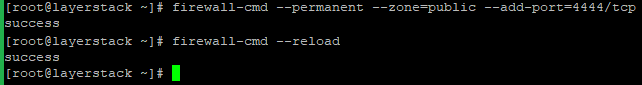
For **Ubuntu**, the default firewall is UFW, and please use the following command to add the new rule.

# sudo ufw allow 4444/tcp

For **CentOS**, the default firewall is FirewallD, and please use the following command to add the new rule.

# firewall-cmd --permanent --zone=public --add-port=4444/tcp

# firewall-cmd --reload



1. Connect the server using the new SSH port.

Please use the “-p” option () to specify the port while connecting the server from the SSH client terminal.

# ssh username@server\_ipaddress -p 4444

NOTE: Change the port number 4444 with your original custom port number

Troubleshooting the SSH Connection

If you're unable to connect to a compute instance using SSH, follow these troubleshooting steps to identify common problems.

Verify the connection

In a terminal window, run the following command:

Copy

nc *<public ip>* 22

* **If the SSH banner displays:** You successfully connected to the instance using SSH. The underlying problem might be related to permissions. As a next step, verify your credentials. If the credentials you're using to SSH to the instance are incorrect, the connection fails.

You must have the full path to the private key portion of the SSH key pair that you used when you created the instance. For more information about key pairs, see [Managing Key Pairs on Linux Instances](https://docs.oracle.com/en-us/iaas/Content/Compute/Tasks/managingkeypairs.htm#Managing_Key_Pairs_on_Linux_Instances).

* **If the SSH banner does not display:** A network issue might be preventing the connection from succeeding. Continue with the troubleshooting suggestions on this page.

Add a public IP address

If the connection is routed over the internet and you're not using a [bastion](https://docs.oracle.com/iaas/Content/Bastion/Concepts/bastionoverview.htm), then the instance must have a public IP address to connect to the instance. Without a public IP address, the instance is not reachable. For more information about how to manage public IPv4 addresses on instances, see [Public IP Addresses](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingpublicIPs.htm#Public_IP_Addresses).

Verify the network security lists

Oracle Cloud Infrastructure provisions each cloud network with a default set of security lists to permit SSH traffic. If the security list that permits SSH connections is removed, you can't access the instance. Ensure a security list that opens port 22 is present. For more information about security lists, see [Security Lists](https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm#Security_Lists).

Confirm that the instance is accessible

Check the [instance accessibility status metric](https://docs.oracle.com/en-us/iaas/Content/Compute/References/compute-health-metrics.htm#compute-health-metrics) to determine whether the instance is responding to an Address Resolution Protocol (ARP) request. If the ARP ping fails, the metric shows that the instance is unresponsive. If there isn't an ongoing infrastructure issue, then the instance probably has a software issue or a network misconfiguration that you must resolve yourself.

Confirm that SSH is running on the instance

The steps for confirming that SSH is running vary depending on the operating system. Review the documentation for your operating system to find information that explains how to confirm whether SSH is running.

Capture serial console history

You can capture the instance's [serial console data history](https://docs.oracle.com/en-us/iaas/Content/Compute/Tasks/displayingconsole.htm#Displaying_the_Console_for_an_Instance) in the Console or by using the [console-history](https://docs.oracle.com/iaas/tools/oci-cli/latest/oci_cli_docs/cmdref/compute/console-history.html) resource in the CLI. This information can help determine the cause of connectivity problems.

When using the CLI to capture the instance's serial console data history, include the following option to ensure that full history is captured. Without this option, the data might be truncated: --length 10000000.

Connect to the serial console

Serial console connections let you remotely troubleshoot malfunctioning instances. For more information, see [Troubleshooting Instances Using Instance Console Connections](https://docs.oracle.com/en-us/iaas/Content/Compute/References/serialconsole.htm#Instance_Console_Connections).

From the serial console, you can interrupt the boot process to [boot into maintenance mode](https://docs.oracle.com/en-us/iaas/Content/Compute/References/serialconsole.htm#instcon_linux_trouble__maintenancemode). In maintenance mode, you can [add or reset the SSH key for the opc user](https://docs.oracle.com/en-us/iaas/Content/Compute/References/serialconsole.htm#instcon_linux_trouble__resetsshkey).

Update PuTTY tool

If you are trying to connect to a Linux instance from a Windows system using PuTTY and you receive a failure message stating that the key format is too new, then the PuTTYgen tool and the PuTTY tool are not the same version. Update the PuTTY tool to the latest version.

When connecting an SSH client to an SSH server, the first step is establishing basic network connectivity.

## Errors

### Hostname Resolution

Most resolution errors occur when the reference to the SSH host can’t be mapped to a network address. While this is almost exclusively DNS related, the root cause isn’t always a DNS issue.

In an OpenSSH client, a command like ssh user@example.com may return an error like this:

ssh: Could not resolve hostname example.com: Name or service not known

Copy

In PuTTY, you might see an error window with text like this:

Unable to open connection to example.com Host does not exist

Copy

Here are some steps you can take to troubleshoot this error.

* Verify the hostname is properly spelled. Typographical errors can strike at any time.
* Verify that you can resolve the hostname on your client machine using the system ping command. Using third-party sites like [WhatsMyDns.net](https://www.whatsmydns.net/) to check beyond your own DNS caching can also help confirm the results.

If you’re having DNS resolution issues at any level, you can also use the Droplet IP address as an interim solution, as in ssh user@203.0.113.0 instead of ssh user@example.com.

The following tutorials are a good resource to begin working out DNS configuration errors:

* [An Introduction to Managing DNS](https://www.digitalocean.com/community/tutorial_series/an-introduction-to-managing-dns)
* [How to Point to DigitalOcean Name Servers From Common Domain Registrars](https://www.digitalocean.com/community/tutorials/how-to-point-to-digitalocean-nameservers-from-common-domain-registrars)
* [How To Set Up a Host Name with DigitalOcean](https://docs.digitalocean.com/products/networking/dns/)

### Connection Timeout

A connection timeout means that the client attempted to establish a network socket to the SSH server, but the server failed to respond within the timeout period.

In an OpenSSH client, a command like ssh user@203.0.113.0 may give an error like this:

ssh: connect to host 203.0.113.0 port 22: Connection timed out

Copy

In PuTTY, you might see an error window with text like this:

Network error: Connection timed out

Copy

Here are some steps you can take to troubleshoot this error.

* Verify that the host IP address is correct for the Droplet.
* Verify that your network supports connectivity over the SSH port being used. Some public networks may block port 22 or custom SSH ports. You can do this by, for example, testing other hosts using the same port with a known working SSH server. This can help you determine if the issue isn’t specific to your Droplet.
* [Verify the Droplet firewall rules](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#checking-your-firewall). Check that they’re not set to a default policy of DROP **and** the port is not added to allow connections.

### Connection Refused

A connection being refused has some subtle differences from a timeout. This means that the request is being routed to the SSH host, but the host does not successfully accept the request.

In an OpenSSH client, a command like ssh user@203.0.113.0 may return an error like this:

ssh: connect to host 203.0.113.0 port 22: Connection refused

Copy

In PuTTY, you might see an error window with text like this:

Network error: Connection refused

Copy

In this situation, you may have the same root issue as with connection timeout errors, but there are some additional things you can check:

* Verify that the host IP address is correct for the Droplet.
* Verify that your network supports connectivity over the SSH port being used. Some public networks may block port 22 or custom SSH ports. You can do this by, for example, testing other hosts using the same port with a known working SSH server. This can help you determine if the issue isn’t specific to your Droplet.
* [Verify the Droplet firewall rules](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#checking-your-firewall). Check that they’re not set to a default policy of DROP **and** the port is not added to allow connections.
* Verify that the [service is currently running](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#checking-the-ssh-service-status) and [bound to the expected port](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#checking-the-ssh-service-port).

## Solutions

### Checking Your Firewall

Some connectivity problems can be caused by firewall configurations. If your firewall is set up to block certain ports or services, it can prevent you from connecting. You can learn more about firewalls in [What is a Firewall and How Does It Work?](https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work).

If you add a firewall rule that allows your local machine to connect by IP address, verify that the IP address assigned by your ISP has not changed. If it has, then you need to modify that firewall rule to permit the new IP address or address range.

How you check your firewall rules depends on which firewall your Droplet uses. Ubuntu servers usually run [UFW](https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands); CentOS servers often use [FirewallD](https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7). If you’re not using either, it’s likely that you’re using [iptables](https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands).

For whichever firewall your system has, make sure to familiarize yourself with how to modify its rules. You also need to know which port your SSH service is using. By default, it’s 22, but you can follow the [Checking the SSH Service Port](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#checking-the-ssh-service-port) section below to confirm.

* [**iptables**](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#firewalls-0)
* [FirewallD](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#firewalls-1)
* [UFW](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#firewalls-2)

For Linux systems not running UFW or FirewallD, list your firewall rules using the iptables command with sudo or as the **root** user.

iptables -nL

Copy

The following output would indicate that there are no rules in place that would block SSH traffic:

Chain INPUT (policy ACCEPT)

target prot opt source destination

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Copy

If you see rules or a default policy of REJECT or DROP, you should ensure that the INPUT chain allows the port your SSH service is running on, which is 22 by default.

### Checking the SSH Service Status

If you can’t SSH to your Droplet, you should check that the SSH service is running. How to very the service is running varies from system to system.

On older OS versions (Ubuntu 14 and below, CentOS 6, Debian 6) this may use the service command backed by [Upstart](https://www.digitalocean.com/community/tutorials/the-upstart-event-system-what-it-is-and-how-to-use-it). More modern distributions with [systemd](https://www.digitalocean.com/community/tutorials/how-to-use-systemctl-to-manage-systemd-services-and-units) use the systemctl command. Red Hat-based distributions (for example, CentOS and Fedora) call the service sshd while Debian and Ubuntu call it ssh.

* [**Using systemctl**](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#ssh-service-status-0)
* [Using service](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#ssh-service-status-1)

Similarly, on a server using systemd (like CentOS 7), use the systemctl command to check the status:

systemctl status sshd

Copy

A running service shows output like this, with **active (running)** on the **Active:** line.

sshd.service - OpenSSH server daemon

Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)

Active: active (running) since Mon 2017-03-20 11:00:22 EDT; 1 months 1 days ago

Process: 899 ExecStartPre=/usr/sbin/sshd-keygen (code=exited, status=0/SUCCESS)

Main PID: 906 (sshd)

CGroup: /system.slice/sshd.service

├ 906 /usr/sbin/sshd -D

├26941 sshd: [accepted]

└26942 sshd: [net]

Copy

If the service is not running, the **Active** line displays **inactive** followed by recent journal entries for the service:

sshd.service - OpenSSH server daemon

Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)

Active: inactive (dead) since Fri 2017-04-21 08:36:13 EDT; 2s ago

Process: 906 ExecStart=/usr/sbin/sshd -D $OPTIONS (code=exited, status=0/SUCCESS)

Process: 899 ExecStartPre=/usr/sbin/sshd-keygen (code=exited, status=0/SUCCESS)

Main PID: 906 (code=exited, status=0/SUCCESS)

Copy

In this case, restart it with systemctl start sshd.

### Checking the SSH Service Port

There are two general ways to check which port the SSH service is running on. One is checking the SSH configuration file, and the other is examining the running process.

On most systems, the SSH configuration file is /etc/ssh/sshd\_config. The default port is 22, but can be overridden by any configuration line in this file specifying a Port directive with a number.

You can search lines like this [using grep](https://www.digitalocean.com/community/tutorials/using-grep-regular-expressions-to-search-for-text-patterns-in-linux):

**grep** Port /etc/ssh/sshd\_config

Copy

You’ll see output like this with the port number:

Port 22

Copy

If you know [the service is running](https://docs.digitalocean.com/support/how-to-troubleshoot-ssh-connectivity-issues/#checking-the-ssh-service-status), you can confirm that the service is running on the expected port using ss (run with sudo or as the **root** user). Similar output is provided for the netstat -plnt command as well, but ss is the preferred command for querying socket information from the kernel.

ss -plnt

Copy

The output you are looking for should reference the program name listening on the configured port. For example, this output shows that the SSH service is listening on all interfaces, \*, on port 22.

State Recv-Q Send-Q Local Address:Port Peer Address:Port

LISTEN 0 128 \*:22 \*:\* users:(("sshd",pid=1493,fd=3))

LISTEN 0 128 :::22 :::\* users:(("sshd",pid=1493,fd=4))

Copy

The interface references \* and 0.0.0.0 indicate all interfaces on the Droplet. 127.0.0.1 indicates that the service is not publicly accessible. The relevant sshd\_config directive is ListenAddress and should be commented out to default to all interfaces, or set to the public IP address of the Droplet.

## Conclusion

If you need further help, you can [open a support ticket](https://cloudsupport.digitalocean.com/). Make sure to include the following information:

* The username, host, and port you are using to connect.
* The authentication mechanism you expect to use.
* The full output of the errors linked to the stage of error, including verbose output of the SSH client
* All of the information you’ve gathered from troubleshooting so far.
* Anything you were unclear about while referencing this article.

Including all the above diagnostic information and clarifying where you are encountering the issue when trying to connect can help us quickly get up to speed with where your need on the issue is.