

Contents

1

Installing and Enabling OpenSSH on CentOS 7

1.1

Step 1: Install OpenSSH Server Software Package

1.2

Step 2: Starting SSH Service

1.3

Step 3: Check sshd status

1.4

Step 4: Enable OpenSSH Service

2

OpenSSH Server Configuration

2.1

Firewall Settings

Introduction

Secure Shell (SSH) is a cryptographic protocol that allows a client to interact with a remote server in a secure environment.

High-level encryption protects the exchange of sensitive information and allows flie trans or issue commands on remote machines securely

How to Enable SSH on CentOS 7



Prerequisites

- CentOS 7 system to act as an SSH server
- A user with necessary permissions
- Access to a command line (Ctrl-Alt-T)
- **yum** utility (included by default)

Contents

- 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings



SSH software packages are included on CentOS by default. However, if these packages are not present on your system, easily install them by completing Step 1, outlined below.

Step 1: Install OpenSSH Server Software Package

Enter the following command from your terminal to start the installation process:

```
sudo yum -y install openssh-server openssh-clients
```

This command installs both the OpenSSH client applications, as well as the OpenSSH server daemon, **sshd**.

```
[phoenixnap@localhost ~]$ sudo yum -y install openssh-server openssh-clients
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: mirror.wufx.net
* extras: mirror.wufx.net
* updates: mirror.slu.cz
Package openssh-server-7.4p1-16.el7.x86_64 already installed and latest version
Package openssh-clients-7.4p1-16.el7.x86_64 already installed and latest version
Nothing to do
```

In this example, the system informs us that the latest version is already present.

Step 2: Starting SSH Service

Contents

- 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings

```
sudo systemctl start sshd
```

When active, **sshd** continuously listens for client connections from any of the client tools. When a connection request occurs, **sshd** sets up the correct connection.

Step 3: Check sshd status

Check the status of the SSH daemon:

```
sudo systemctl status sshd
```

As we have previously started the service, the output confirms that it is active.

```
[phoenixnap@localhost ~]$ systemctl status sshd
■ sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-08-05 02:36:58 MDT; 29min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1094 (sshd)
    CGroup: /system.slice/ssh.service
            └─1094 /usr/sbin/sshd -D

Aug 05 02:36:58 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 05 02:36:58 localhost.localdomain sshd[1094]: Server listening on 0.0.0.0 port 22.
Aug 05 02:36:58 localhost.localdomain sshd[1094]: Server listening on :: port 22.
```

Contents

- 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings



To stop the SSH daemon enter:

```
systemctl stop sshd
```

We can check if the service has stopped by verifying the status. The output shows that the service is inactive and the time and date when the status last changed.

```
[phoenixnap@localhost ~]$ systemctl status sshd
■ sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Mon 2019-08-05 08:55:59 MDT; 14s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 8115 ExecStart=/usr/sbin/sshd -D $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 8115 (code=exited, status=0/SUCCESS)

Aug 05 05:59:41 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 05 05:59:41 localhost.localdomain sshd[8115]: Server listening on 0.0.0.0 port 22.
Aug 05 05:59:41 localhost.localdomain sshd[8115]: Server listening on :: port 22.
Aug 05 05:59:41 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
Aug 05 08:55:59 localhost.localdomain systemd[1]: Stopping OpenSSH server daemon...
Aug 05 08:55:59 localhost.localdomain sshd[8115]: Received signal 15; terminating.
Aug 05 08:55:59 localhost.localdomain systemd[1]: Stopped OpenSSH server daemon.
```

Step 4: Enable OpenSSH Service

Enable SSH to start automatically after each system reboot by using the **systemctl** command:

□ Contents

- 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings



To disable SSH after reboot enter:

```
sudo systemctl disable sshd
```

OpenSSH Server Configuration

Properly configuring the **sshd** configuration file [hardens server security](#). The most common settings to enhance security are changing the port number, disabling root logins, and limiting access to only certain users.

To edit these settings access the **/etc/ssh/sshd_config** file:

```
sudo vim /etc/ssh/sshd_config
```

Once you access the file by using a text editor (in this example we used **vim**), you can disable root logins and edit the default port number:

- To disable root login:

PermitRootLogin no

□ Contents □

- 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings



```
Port 2002
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Remember to uncomment the lines that you edit by removing the hashtag.

Save and close the file. Restart **sshd**:

```
service sshd restart
```

☐ Contents ☐

- ☐ 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- ☐ 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings



After successfully enabling SSH and configuring the **sshd** file, adjust the firewall settings to make sure there are no compatibility issues.

It is also possible to restrict IP access to make the connection even more secure.

To restrict IP access, edit the **iptables** file by typing:

```
sudo vim /etc/sysconfig/iptables
```

To allow access using the port defined in the sshd config file, add the following line to the iptables file:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2002 -j ACCEPT
```

To restrict access to a specific IP, for example 133.123.40.166, edit the line as follows:

```
-A RH-Firewall-1-INPUT -s 133.123.40.166 -m state --state NEW -p tcp --dport 2002 -j ACCEPT
```

☐ Contents ☐

☐ 1 Installing and Enabling OpenSSH on CentOS 7

- 1.1 Step 1: Install OpenSSH Server Software Package
- 1.2 Step 2: Starting SSH Service
- 1.3 Step 3: Check sshd status
- 1.4 Step 4: Enable OpenSSH Service

☐ 2 OpenSSH Server Configuration

- 2.1 Firewall Settings




```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# please do not ask us to add additional ports/services to this default configuration
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 2002 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A RH-Firewall-1-INPUT -s 133.123.40.166 -m state --state NEW -m tcp -p tcp --dport 2002 -j ACCEPT
COMMIT
```

If your site uses IPv6, and you are editing ip6tables, use the line:

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 2002 -j ACCEPT
```

Save and exit the file by pressing Escape (Esc) on your keyboard and typing:

:X

Press Enter to confirm.

Restart iptables to apply the changes:

Contents

- 1 Installing and Enabling OpenSSH on CentOS 7
 - 1.1 Step 1: Install OpenSSH Server Software Package
 - 1.2 Step 2: Starting SSH Service
 - 1.3 Step 3: Check sshd status
 - 1.4 Step 4: Enable OpenSSH Service
- 2 OpenSSH Server Configuration
 - 2.1 Firewall Settings

