How to Install OpenSSH Server In Linux

Oltjano Terpollari | Last Updated: April 24, 2023 | Read Time: 4 mins | SSH | 9 Comments

Being a network administrator requires deep knowledge of remote login protocols such as **rlogin**, **telnet**, and **ssh**. The one I will discuss in this article is **ssh**.

SSH is a secure remote protocol that is used to work remotely on other machines or transfer data between computers using SCP (Secure Copy) command. But, what is **OpenSSH**, and how to install it in your **Linux** distribution?

What is OpenSSH?

OpenSSH is a free open-source set of computer tools used to provide secure and encrypted communication over a computer network by using the **ssh** protocol. Many people, new to computers and protocols, create a misconception about **OpenSSH**, they think it is a protocol, but it is not, it is a set of computer programs that use the **ssh protocol**.

OpenSSH is developed by the **Open BSD** group and it is released under a **Simplified BSD License**. A main factor that has made it possible for **OpenSSH** to be used so much among system administrators is its multi-platform capability and very useful nice features it has.

The latest version is **OpenSSH 9.3** which has been released on **15 March 2023** and comes with many new features and patches, so if you already use **OpenSSH** for administering your machines, I suggest you do an upgrade or install ssh from the source.

Why Use OpenSSH Over Telnet Or Ftp?

The most important reason why one should use **OpenSSH** tools over **ftp** and **Telnet** is that all communications and user credentials using **OpenSSH** are encrypted, and they are also protected from man-in-middle attacks. If a third party tries to intercept your connection, **OpenSSH** detects it and informs you about that.

OpenSSH Features

- Secure Communication
- Strong Encryption (**3DES**, **Blowfish**, **AES**, **Arcfour**)
- **X11** Forwarding (encrypt X Window System traffic)
- Port Forwarding (encrypted channels for legacy protocols)
- Strong Authentication (**Public Key**, One-Time Password, and Kerberos Authentication)
- Agent Forwarding (**Single-Sign-On**)
- Interoperability (Compliance with **SSH 1.3**, **1.5**, and **2.0** protocol Standards)
- SFTP client and server support in both **SSH1** and **SSH2** protocols.
- **Kerberos** and **AFS Ticket Passing**
- Data Compression

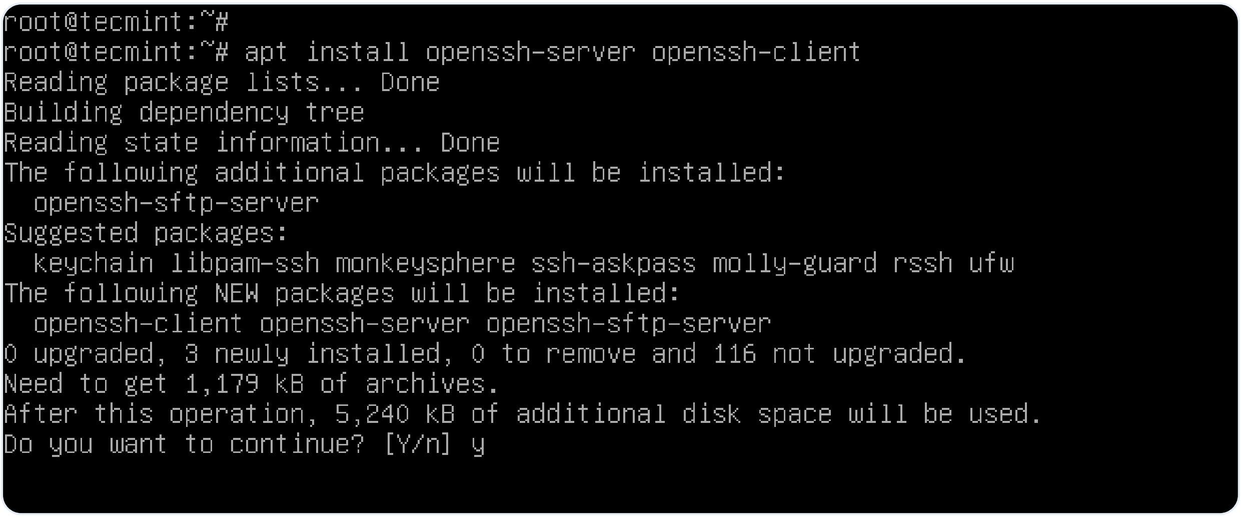
Install OpenSSH Server on Linux

To install **OpenSSH**, open a terminal and run the following commands with superuser permissions.

On Debian/Ubuntu/Linux Mint

On Debian-based distributions, you can use the following apt command to install the openssh server and client as shown.

```
$ sudo apt install openssh-server openssh-client
```



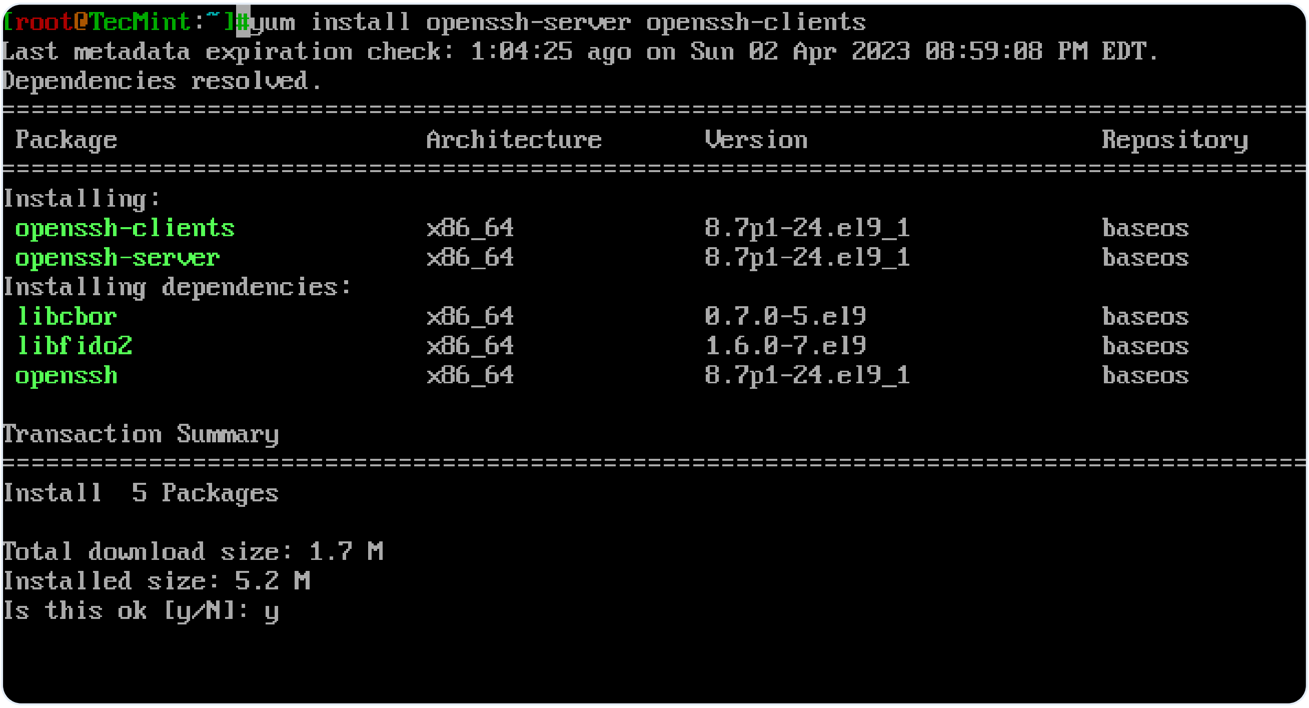
```
root@tecmint:~#
root@tecmint:~# apt install openssh-server openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  openssh-sftp-server
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard rssh ufw
The following NEW packages will be installed:
  openssh-client openssh-server openssh-sftp-server
0 upgraded, 3 newly installed, 0 to remove and 116 not upgraded.
Need to get 1,179 kB of archives.
After this operation, 5,240 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Install OpenSSH in Debian Systems

On RHEL/Centos/Fedora

On RedHat-based distribution, type the following yum command to install the openssh server and client.

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



```
[root@TecMint:~]#yum install openssh-server openssh-clients
Last metadata expiration check: 1:04:25 ago on Sun 02 Apr 2023 08:59:08 PM EDT.
Dependencies resolved.
================================================================================
 Package                Architecture      Version                    Repository
================================================================================
Installing:
 openssh-clients        x86_64            8.7p1-24.el9_1             baseos
 openssh-server         x86_64            8.7p1-24.el9_1             baseos
Installing dependencies:
 libcbor                x86_64            0.7.0-5.el9                baseos
 libfido2               x86_64            1.6.0-7.el9                baseos
 openssh                x86_64            8.7p1-24.el9_1             baseos

Transaction Summary
================================================================================
Install  5 Packages

Total download size: 1.7 M
Installed size: 5.2 M
Is this ok [y/N]: y
```

Install OpenSSH in RedHat Systems

Configure OpenSSH Server in Linux

It's time to configure our **OpenSSH** behavior through the **ssh config** file, but before editing the **/etc/ssh/sshd_config** file we need to back up a copy of it, so in case we make any mistake we have the original copy.

Open a terminal and run the following cp command to make a copy of the original **sshd** configuration file.

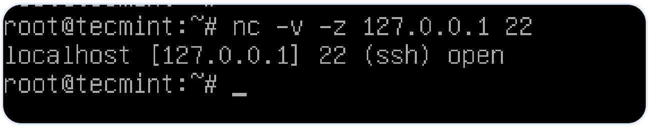
```
$ sudo cp /etc/ssh/sshd_config  /etc/ssh/sshd_config.original_copy
```

As you can see from the command I typed, I added the **original_copy suffix**, so every time I see this file I know it is an original copy of the sshd config file.

How Do I Connect to OpenSSH

Before we go further, we need to verify if our **openssh** server is working or not. How to do that? You can try to connect to the **openssh** server from your **localhost** through your **openssh client** or do a **portscan** with nmap, but I like to use a small tool called netcat, also known as the TCP/IP Swiss army knife. I love working with this amazing tool on my machine, so let me show it to you.

```
# nc -v -z 127.0.0.1 22
```



```
root@tecmint:~# nc -v -z 127.0.0.1 22
localhost [127.0.0.1] 22 (ssh) open
root@tecmint:~# _
```

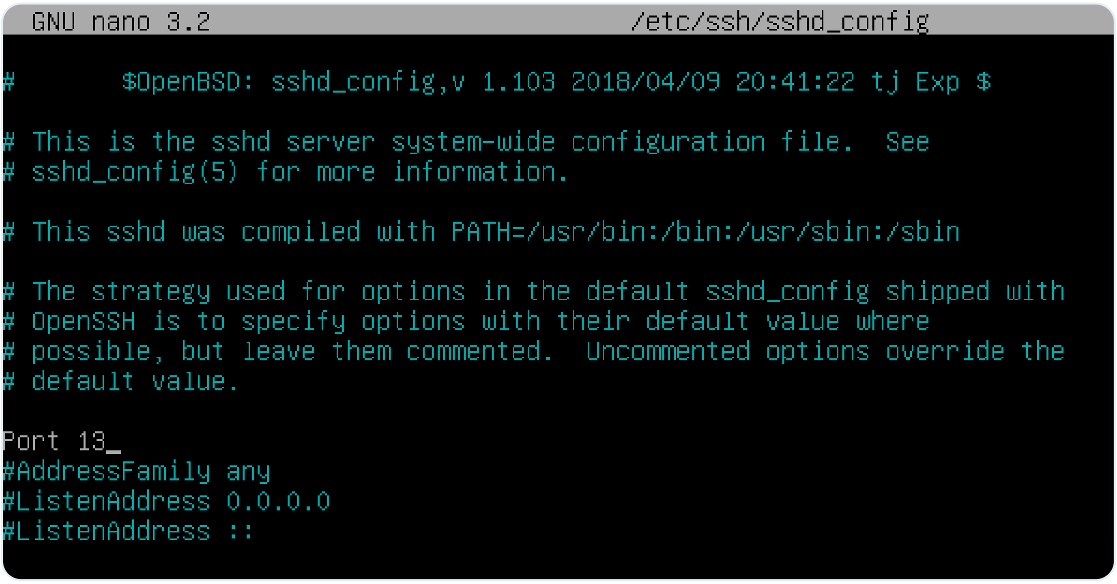
Verify SSH Connection

Referring to the **netcat** results, the **ssh** service is running on port **22** on my machine. Very good! What if we want to use another port, instead of 22? We can do that by editing the sshd configuration file.

Change SSH Port

Set your **OpenSSH** to listen on **TCP** port **13** instead of the default TCP port **22**. Open the **sshd_config** file with your favorite text editor and change the port directive to 13.

```
Port 13
```



```
GNU nano 3.2                              /etc/ssh/sshd_config

#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 13_
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

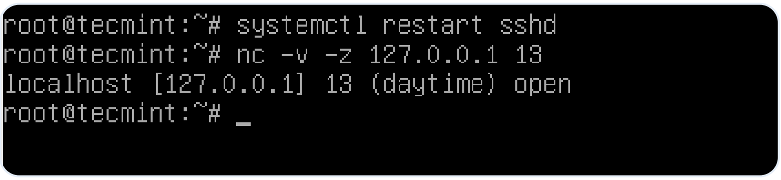
Change SSH Port

Restart the **OpenSSH** server so the changes in the config file can take place by typing the following command and running **netcat** to verify if the port you set for listening is open or not.

```
$ sudo systemctl restart sshd
```

Should we verify if our openssh server is listening on port 13, or not? This verification is necessary, so I am calling my lovely tool **netcat** to help me do the job.

```
# nc -v -z 127.0.0.1 13
```



```
root@tecmint:~# systemctl restart sshd
root@tecmint:~# nc -v -z 127.0.0.1 13
localhost [127.0.0.1] 13 (daytime) open
root@tecmint:~# _
```

Check SSH Connection

Do you like to make your [openssh server display a nice login banner](https://www.tecmint.com/)? You can do it by modifying the content of the **/etc/issue.net** file.

```
$ nano /etc/issue.net
```

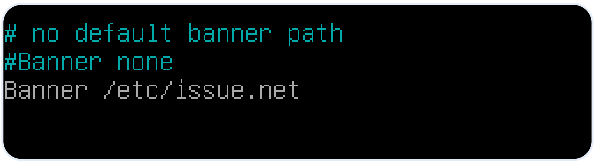
Paste the following banner message.

```
Authorized access only!

If you are not authorized to access or use this system, disconnect now!
```

Next, add the following line inside the sshd configuration file.

```
Banner /etc/issue.net
```



```
# no default banner path
#Banner none
Banner /etc/issue.net
```

Add SSH Banner

After making changes to the SSH configuration, make sure to restart.

```
$ sudo systemctl restart sshd
```

You might also like:

- [*How to Secure and Harden OpenSSH Server*]
- [*5 Best OpenSSH Server Best Security Practices*]
- [*How to Block SSH Brute Force Attacks Using SSHGUARD*]
- [*Basic SSH Command Usage and Configuration in Linux*]
- [*How to Setup Two-Factor Authentication For SSH In Linux*]

Conclusion

There are many things you can do with the **openssh** tools when it comes to the way you configure your **openssh server**, I can say that your imagination is the limit!

Hey TecMint readers,

Exciting news! Every month, our top blog commenters will have the chance to win fantastic rewards, like free Linux eBooks such as **RHCE**, **RHCSA**, **LFCS**, **Learn Linux**, and **Awk**, each worth **$20**!

Learn more about the contest and stand a chance to win by sharing your thoughts below!

PREVIOUS ARTICLE:

MimiPenguin – Display (Hack) Login Passwords of Linux Users

NEXT ARTICLE:

How to Compile and Install OpenSSH from Source in Linux

Oltjano Terpollari

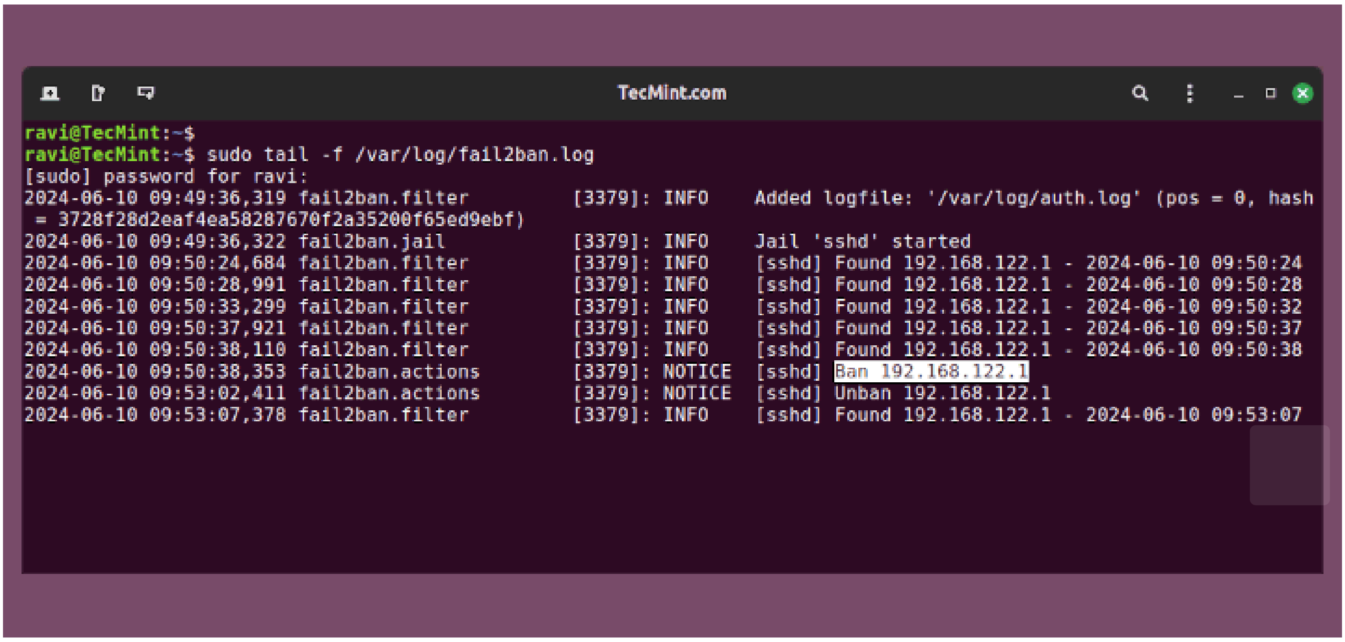
Hi guys, I am a computer Geek and I go by the name Ambition. I do security stuff and I am studying computer engineering. I love programming and Linux.

Each tutorial at TecMint is created by a team of experienced Linux system administrators so that it meets our high-quality *standards.*

Join the TecMint Weekly Newsletter (More Than 156,129 Linux Enthusiasts Have Subscribed)

Was this article helpful? Please add a comment or buy me a coffee to show your appreciation.

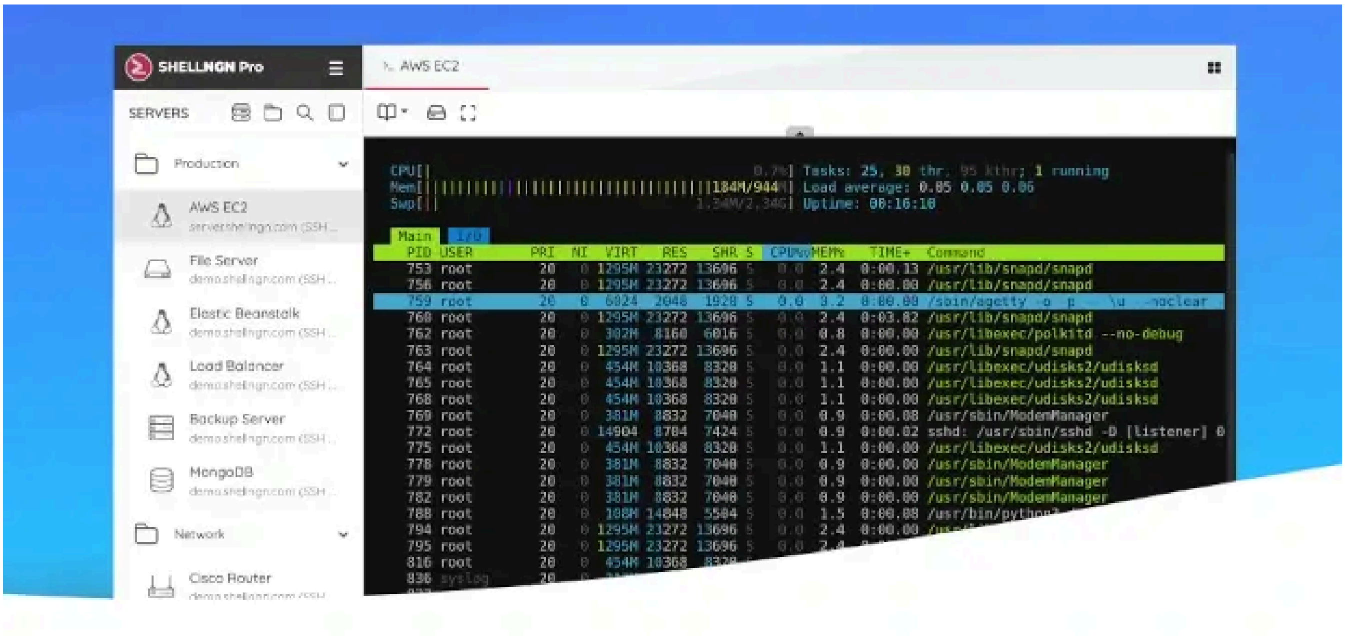
Related Posts



```
ravi@TecMint:~$
ravi@TecMint:~$ sudo tail -f /var/log/fail2ban.log
[sudo] password for ravi:
2024-06-10 09:49:36,319 fail2ban.filter         [3379]: INFO    Added logfile: '/var/log/auth.log' (pos = 0, hash
 = 3728f28d2eaf4ea58287670f2a35200f65ed9ebf)
2024-06-10 09:49:36,322 fail2ban.jail           [3379]: INFO    Jail 'sshd' started
2024-06-10 09:50:24,684 fail2ban.filter         [3379]: INFO    [sshd] Found 192.168.122.1 - 2024-06-10 09:50:24
2024-06-10 09:50:28,991 fail2ban.filter         [3379]: INFO    [sshd] Found 192.168.122.1 - 2024-06-10 09:50:28
2024-06-10 09:50:33,299 fail2ban.filter         [3379]: INFO    [sshd] Found 192.168.122.1 - 2024-06-10 09:50:32
2024-06-10 09:50:37,921 fail2ban.filter         [3379]: INFO    [sshd] Found 192.168.122.1 - 2024-06-10 09:50:37
2024-06-10 09:50:38,110 fail2ban.filter         [3379]: INFO    [sshd] Found 192.168.122.1 - 2024-06-10 09:50:38
2024-06-10 09:50:38,353 fail2ban.actions        [3379]: NOTICE  [sshd] Ban 192.168.122.1
2024-06-10 09:53:02,411 fail2ban.actions        [3379]: NOTICE  [sshd] Unban 192.168.122.1
2024-06-10 09:53:07,378 fail2ban.filter         [3379]: INFO    [sshd] Found 192.168.122.1 - 2024-06-10 09:53:07
```

How to Install Fail2ban to Stop Brute-Force Attacks on Ubuntu 24.04

How to Get Root and User SSH Login Email Alerts

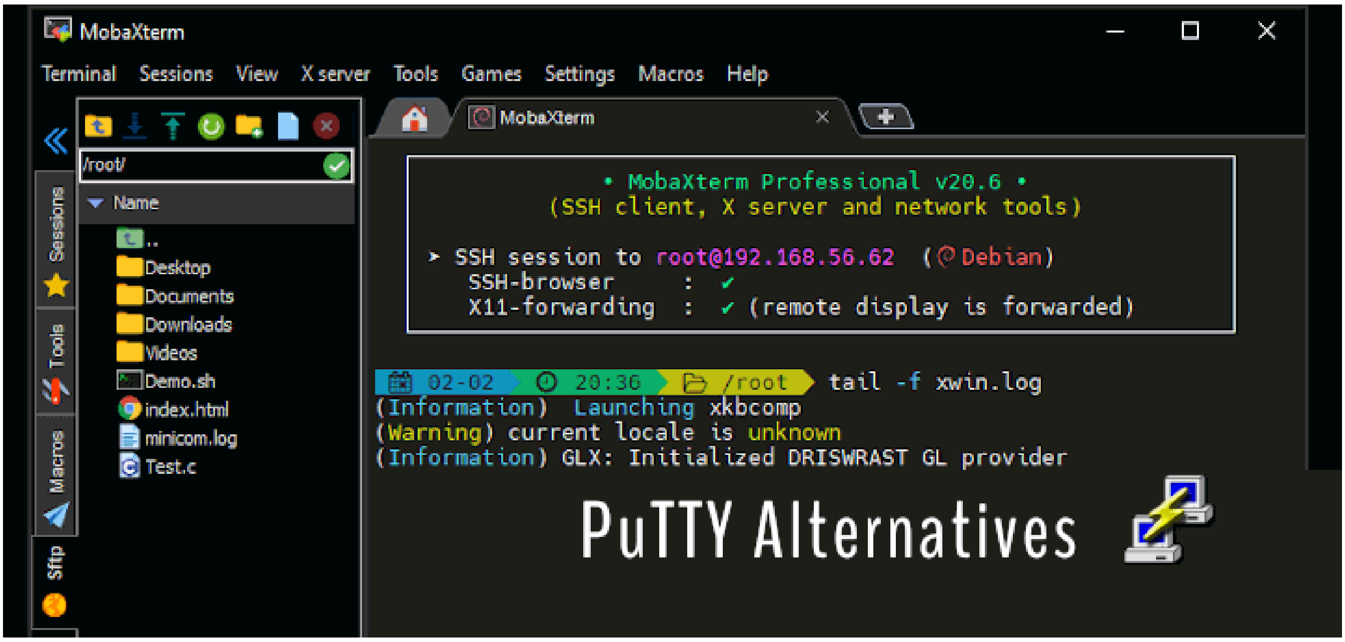

SHELLNGN Pro
SERVERS
Production
AWS EC2
server.shellngn.com (SSH...
File Server
demo.shellngn.com (SSH...
Elastic Beanstalk
demo.shellngn.com (SSH...
Load Balancer
demo.shellngn.com (SSH...
Backup Server
demo.shellngn.com (SSH...
MongoDB
demo.shellngn.com (SSH...
Network
Cisco Router
AWS EC2

```
CPU[|                                  0.7%] Tasks: 25, 30 thr, 95 kthr; 1 running
Mem[||||||||||||||||||||||||||||||||184M/944M] Load average: 0.05 0.05 0.06
Swp[||                           1.34M/2.34G] Uptime: 00:16:10

 Main  I/O
  PID USER       PRI  NI  VIRT   RES   SHR S  CPU% MEM%   TIME+  Command
  753 root        20   0 1295M 23272 13696 S   0.0  2.4  0:00.13 /usr/lib/snapd/snapd
  756 root        20   0 1295M 23272 13696 S   0.0  2.4  0:00.00 /usr/lib/snapd/snapd
  759 root        20   0  6024  2048  1928 S   0.0  0.2  0:00.00 /sbin/agetty -o -p -- \u --noclear
  760 root        20   0 1295M 23272 13696 S   0.0  2.4  0:03.82 /usr/lib/snapd/snapd
  762 root        20   0  302M  8160  6016 S   0.0  0.8  0:00.00 /usr/libexec/polkitd --no-debug
  763 root        20   0 1295M 23272 13696 S   0.0  2.4  0:00.00 /usr/lib/snapd/snapd
  764 root        20   0  454M 10368  8320 S   0.0  1.1  0:00.00 /usr/libexec/udisks2/udisksd
  765 root        20   0  454M 10368  8320 S   0.0  1.1  0:00.00 /usr/libexec/udisks2/udisksd
  768 root        20   0  454M 10368  8320 S   0.0  1.1  0:00.00 /usr/libexec/udisks2/udisksd
  769 root        20   0  381M  8832  7040 S   0.0  0.9  0:00.08 /usr/sbin/ModemManager
  772 root        20   0 14904  8704  7424 S   0.0  0.9  0:00.02 sshd: /usr/sbin/sshd -D [listener] 0
  775 root        20   0  454M 10368  8320 S   0.0  1.1  0:00.00 /usr/libexec/udisks2/udisksd
  778 root        20   0  381M  8832  7040 S   0.0  0.9  0:00.00 /usr/sbin/ModemManager
  779 root        20   0  381M  8832  7040 S   0.0  0.9  0:00.00 /usr/sbin/ModemManager
  782 root        20   0  381M  8832  7040 S   0.0  0.9  0:00.00 /usr/sbin/ModemManager
  788 root        20   0  108M 14848  5504 S   0.0  1.5  0:00.08 /usr/bin/python3
  794 root        20   0 1295M 23272 13696 S   0.0  2.4  0:00.00
  795 root        20   0 1295M 23272 13696 S   0.0  2.4
  816 root        20   0  454M 10368  8320
  836 syslog      20
```

Shellngn – Best Online SSH Client with SFTP, VNC, RDP

8 Best SSH Clients for Linux in 2024



```
        • MobaXterm Professional v20.6 •
      (SSH client, X server and network tools)

 ➤ SSH session to root@192.168.56.62  (Debian)
   SSH-browser     :  ✓
   X11-forwarding  :  ✓ (remote display is forwarded)

 02-02  20:36  /root  tail -f xwin.log
(Information)  Launching xkbcomp
(Warning) current locale is unknown
(Information) GLX: Initialized DRISWRAST GL provider
```

10 Best PuTTY Alternatives for SSH Remote Connection

How to Setup SSH Passwordless Login in Linux [3 Easy Steps]

9 Comments

Leave a Reply

Ravi Soni

March 12, 2017 at 12:38 pm

Hey,

Trouble here .. : (

After I changed the ssh port to 13 I'm not able to login via putty (Connection timeout error) what to do now ?

Command : nc -v -z 127.0.0.1 13
Ran succeed..

Reply

Ravi Soni

March 12, 2017 at 12:45 pm

I think you article is missing that the port you change to should be open first to connect from outside, it could lock down servers for newbies.

Reply

clay

January 22, 2015 at 5:36 am

nice simple article. I would go into a little more detail about why to and why not to change the port. This is a very debated thing.

Reply

Admin

Ravi Saive

January 22, 2015 at 12:39 pm

@Clay,
Surely, we will come up with a SSH security article soon, stay tuned for that..till then keep reading..

Reply

rockwallably

October 3, 2014 at 5:34 pm

One problem I notice with your post is that you say 'How Do I Connect to OpenSSH' and then you promptly say 'Before we go further, we need to verify….' and then you proceed to give your conclusion without ever detailing anything about how to connect.

You simply show how to verify via netcat and then talk about a nice banner.

Please tell me my eyes don't fail me ?

I think you should provide a lot more detail and examples for this post to be of any value.

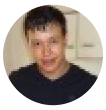
Reply

Mian Anjum Ghaffar

August 12, 2014 at 12:47 pm

Use yum install nc.x86_64 for netcat Red hat and centos .It worked for me in case of Red hat.
Sometime you need net cat for openssh

Reply



Wellington Torrejais da Silva

June 24, 2014 at 8:40 pm

Thanks!!

Reply

Mahesh

April 22, 2014 at 11:51 am

Lots of Thanks.. Your all posts are reliable guide for every linux professional and newbie.
Please guide to install Squid proxy server with Dansguardian content filter on

Ubuntu 14.04..so please post a stepwise procedure on How to Install and Configure Squid with Dansguardian on Ubuntu 14.04 soon. Please post asap……. I've read, searched and tried so many forums/sites/blogs for the same but can't find any reliable source.

Reply

Paul Corr

March 17, 2014 at 5:39 am

Nicely done. I am working with two computers on a home LAN to fully explore SSH and your page concisely puts the basics together. I am running Ubuntu 12.04 LTS and OpenSSH on an old Mac mini and connecting via my new Mac mini running OS X Mavericks (10.9.) Some reference books leave out details like the script that starts the server which you need to know to do a restart after configuration change or how to simply verify that the server is listening on a port, for example. Thanks again.

Reply

Got Something to Say? Join the Discussion…

Thank you for taking the time to share your thoughts with us. We appreciate your decision to leave a comment and value your contribution to the discussion. It's important to note that we moderate all comments in accordance with our comment policy to ensure a respectful and constructive conversation.

Rest assured that your email address will remain private and will not be published or shared with anyone. We prioritize the privacy and security of our users.

Name *

Email *

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search...

Linux Commands and Tools

How to Add New Disks Using LVM to an Existing Linux System

11 Lesser Known Useful Linux Commands

8 Partx Command Usage Examples in Linux

How to Delete Root Mails (Mailbox) File in Linux

Translate rwx Permissions into Octal Format in Linux

5 Ways to Empty or Delete a Large File Content in Linux

Linux Server Monitoring Tools

How to Install Nagios Core in Rocky LInux and AlmaLinux

How to Monitor Node.js Applications Using PM2 Web Dashboard

How to Monitor Apache Performance using Netdata on CentOS 7

3 Tools to Monitor and Debug Disk I/O Performance in Linux

10 Strace Commands for Troubleshooting and Debugging Linux Processes

A Shell Script to Send Email Alert When Memory Gets Low

Learn Linux Tricks & Tips

How to Change Linux Partition Label Names on EXT4 / EXT3 / EXT2 and Swap

Assign Read/Write Access to a User on Specific Directory in Linux

How to Check Bad Sectors or Bad Blocks on Hard Disk in Linux

How to Boot into Single User Mode in CentOS/RHEL 7

How to Set Static IP Address and Configure Network in Linux

How to Show Asterisks While Typing Sudo Password in Linux

Best Linux Tools

9 Best Microsoft Excel Alternatives for Linux

10 Best Flowchart and Diagramming Software for Linux

10 Top Open Source Reverse Proxy Servers for Linux

13 Free and Open-Source Video Editing Software for Linux in 2024

6 Most Notable Open Source Centralized Log Management Tools

10 Best Open Source Forum Software for Linux in 2024