# Installation

Installation of the OpenSSH client and server applications is simple. To install the OpenSSH client applications on your Ubuntu system, use this command at a terminal prompt:

sudo apt install openssh-client

To install the OpenSSH server application, and related support files, use this command at a terminal prompt:

sudo apt install openssh-server

The *openssh-server* package can also be selected to install during the Server Edition installation process.

# Configuration

You may configure the default behavior of the OpenSSH server application, *sshd*, by editing the file /etc/ssh/sshd\_config. For information about the configuration directives used in this file, you may view the appropriate manual page with the following command, issued at a terminal prompt:

man sshd\_config

There are many directives in the *sshd* configuration file controlling such things as communication settings, and authentication modes. The following are examples of configuration directives that can be changed by editing the /etc/ssh/sshd\_config file.

Prior to editing the configuration file, you should make a copy of the original file and protect it from writing so you will have the original settings as a reference and to reuse as necessary.

Copy the /etc/ssh/sshd\_config file and protect it from writing with the following commands, issued at a terminal prompt:

sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.original

sudo chmod a-w /etc/ssh/sshd\_config.original

The following are examples of configuration directives you may change:

1. To set your OpenSSH to listen on TCP port 2222 instead of the default TCP port 22, change the Port directive as such:

Port 2222

1. To have *sshd* allow public key-based login credentials, simply add or modify the line:

PubkeyAuthentication yes

If the line is already present, then ensure it is not commented out.

1. To make your OpenSSH server display the contents of the /etc/issue.net file as a pre-login banner, simply add or modify the line:

Banner /etc/issue.net

In the /etc/ssh/sshd\_config file.

After making changes to the /etc/ssh/sshd\_config file, save the file, and restart the *sshd* server application to effect the changes using the following command at a terminal prompt:

sudo systemctl restart sshd.service

# SSH Keys

SSH *keys* allow authentication between two hosts without the need of a password. SSH key authentication uses two keys, a *private* key and a *public* key.

To generate the keys, from a terminal prompt enter:

ssh-keygen -t rsa

This will generate the keys using the *RSA Algorithm*. During the process you will be prompted for a password. Simply hit *Enter* when prompted to create the key.

By default the *public* key is saved in the file ~/.ssh/id\_rsa.pub, while ~/.ssh/id\_rsa is the *private* key. Now copy the id\_rsa.pub file to the remote host and append it to ~/.ssh/authorized\_keys by entering:

ssh-copy-id username@remotehost

Finally, double check the permissions on the authorized\_keys file, only the authenticated user should have read and write permissions. If the permissions are not correct change them by:

chmod 600 .ssh/authorized\_keys

You should now be able to SSH to the host without being prompted for a password.