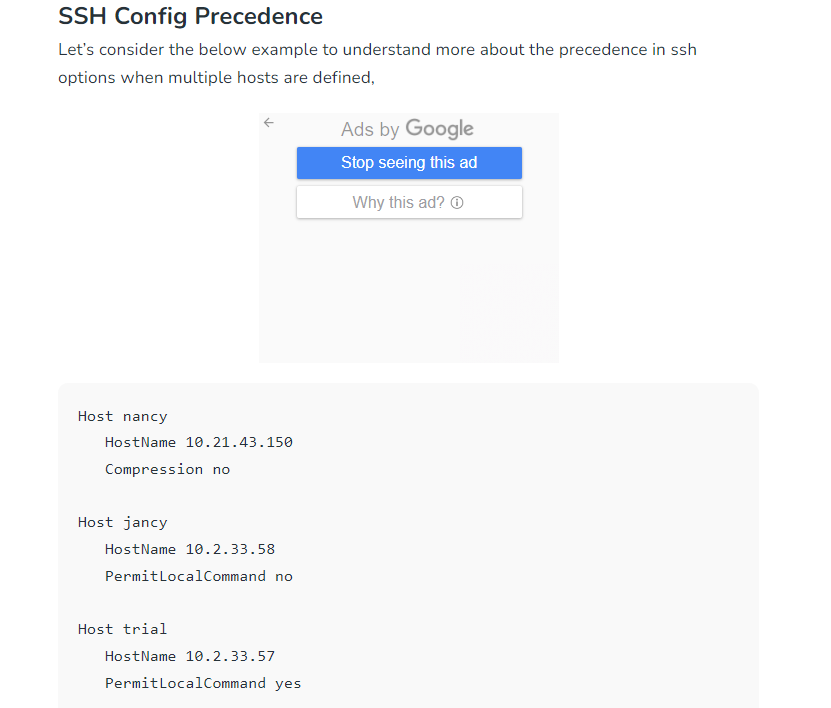
**Setting Up Linux SSH on Ubuntu Linux**

## SSH Config File Example

When a user wants to connect to a remote server through ssh, then he should mention remote username followed by IP address or hostname and port (default port 22 can be ignored). Consider below example,

****

**Override SSH Config File Options**

SSH client reads the configuration file in the following order,

* Options are mentioned in the command line.
* Options mentioned in the ~/.ssh/config file.
* Options mentioned in the /etc/ssh/ssh\_config file.

If SSH does not return an active result, enable the SSH protocol in your systems by typing this utility. You only do this in case your SSH service is not running. Otherwise, you can pass this step if it is running. Ubuntu comes with the Uncomplicated Firewall (UFW), which manages network rules by default. An active UFW will potentially prevent the connection of SSH to your server. You can change UFW settings to allow connection to the SSH server. You should also use this command t open port 22.These commands will help you configure UFW to allow connection;Log in to your Linux computer and test SSH using the following command;

You can proceed to configure the SSH client. Notably, this allows connection to the remote server from your local machine. The procedure for setting up an SSH client is as follows;

You can establish a connection to your remote system from the local computer. To achieve this, you should know the IP address of your local command and use this command;

The above step-by-step guide should help you configure SSH on your system. Once you install and set up SSH on both your server and client machines, you should be able to access your server remotely once you establish a connection.

