How to Setup SSH Key Authentication to Linux

This how to consolidates several aspects of setting up SSH key access to a Linux server.

> NOTE: We currently have two tutorials for this, that need to be consolidated into one. So, maybe this alternate tutorial fills your use-case: Ubuntu SSH Key Access

> NOTE: If you are creating ssh keys for recent Ubuntu distributions, do not use RSA, as it is no longer an accepted key type (as of Ubuntu 21, I think). Use ecdsa instead.

SSH Server Setup

Follow this link to setup the SSH server on Ubuntu: Ubuntu: Setup SSH Server

Update SSH Config

The SSH service needs to be configured to disallow passwords, and to require SSH key authentication.
The following is list of actions to perform in the service configuration.

SSH Key File Name

> NOTE: Not all ssh configuration files include the naming of the authorizedkeys file for users. And, different flavors of Ubuntu and linux use different naming conventions for the SSH key file of a user.

So, we have to determine the file name for ssh key files, and make sure it is set in the config file, and we use the same name.

To find the ssh key file name, open the ssh config with the following:

```
sudo nano /etc/ssh/sshd_config
```

Locate the line in the config file with, AuthorizedKeysFile. Uncomment the line if necessary.

```
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
```

Make a note of the filename used. This will be needed when installing SSH keys.

Prevent Remote Root Login

This is also done in the ssh config file.

Locate the line with PermitRootLogin, and set it to no, like this:

```
#LoginGraceTime 2m
PermitRootLogin no
```

Disable Password Authentication

This requires three changes in the ssh config file.

Locate the line with ChallengeResponseAuthentication, and set it to no, like this:

```
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

Locate the UsePAM line and set it to no, like this:

```
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM no
```

Locate the PasswordAuthentication line and set it to no, like this:

```
#       ForceCommand cvs server
PasswordAuthentication no
```

Disable interactive keyboard authentication by setting this:

```
KbdInteractiveAuthentication no
```

Save changes to the config file.

Restart SSH

With the changes made above, we need to restart the SSH service, with this:

```
sudo systemctl restart ssh
```

Revision #2
Created 1 September 2025 07:05:55 by glwhite
Updated 28 September 2025 04:32:55 by glwhite