

Installation

- [Installation of Nginx on Ubuntu](#)
- [Nginx with Let's Encrypt](#)

Installation of Nginx on Ubuntu

Introduction

Nginx is one of the most popular web servers in the world and is responsible for hosting some of the largest and highest-traffic sites on the internet. It is more resource-friendly than Apache in most cases and can be used as a web server or reverse proxy.

In this guide, we'll explain how to install Nginx on your Ubuntu 18.04 server and use that as a reverse proxy for microservices created in flask and other applications.

Prerequisites

Before you begin this guide, you should have the following:

An Ubuntu 18.04 server and a regular, non-root user with sudo privileges. Additionally, you will need to enable a basic firewall to block non-essential ports. You can learn how to configure a regular user account and set up a firewall by following our initial server setup guide for Ubuntu 18.04.

<https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-18-04>

Step 1 – Installing Nginx

You can install it using the apt packaging system.

Update your local package index:

```
sudo apt update
```

```
sudo apt install nginx
```

Step 2 – Adjusting the Firewall

```
sudo ufw app list
```

Output

Available applications:

Nginx Full

Nginx HTTP

Nginx HTTPS

OpenSSH

permitting traffic on port 80 :

```
sudo ufw allow 'Nginx HTTP'
```

Verify the change:

Output

Status: active

To Action From

-- --

OpenSSH ALLOW Anywhere

Nginx HTTP ALLOW Anywhere

OpenSSH (v6) ALLOW Anywhere (v6)

Nginx HTTP (v6) ALLOW Anywhere (v6)

Step 3 – Checking your Web Server

```
systemctl status nginx
```

Finally access your website using your localIP address.

```
http://your_server_ip
```

You should see the default Nginx landing page:

[image-1613123355266.png](#)

Conclusion

Now you have installed Nginx server on your Ubuntu. Now you can do the following steps.

1. Server Blocking which I will explain in other chapter.
2. Install Letsencrypt for Https Access.
3. Use this as reverse proxy for your existing webservice such as flask etc..
4. Host your website in Nginx.

Nginx with Let's Encrypt

Introduction

In this tutorial we will discuss about installing certbot on ubuntu to install Let's Encrypt SSL on to your ubuntu server.

Prerequisites

Before we start you need to make sure you have followings:

1. Your own domain for example (www.example.com)
2. DNS management credentials.
3. Update A records in DNS, your A records should look like below.
 1. A --- > www.example.com ---> 103.x.x.x (your public IP)
 2. A --- > example.com ---> 103.x.x.x (your public IP)

Let's Encrypt can be installed for the subdomain to. I have personally tried that and it was working fine.

In case you want to do it for subdomain your A records should look like below.

1. A ---> subdomain.example.com --- > 103.x.x.x (your public IP)

Step 1 — Installing Certbot

We will be using Certbot to install Let's Encrypt, Lets start by adding the repository.

First, add the repository:

```
sudo add-apt-repository ppa:certbot/certbot
```

Install Certbot's Nginx package with `apt` :

```
sudo apt install python-certbot-nginx
```

Now Certbot is ready, before we proceed we need to do some configuration on Nginx server default file.

Open the Nginx default website file.

```
sudo nano /etc/nginx/sites-available/default
```