**NginX**

NGINX is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server. NGINX is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption.

In basic term it is simply a web server like apache but have rich feature set more than Apache.

**Installation.**

Debian (Ubuntu, Mint, Wheezy/Sid)

Take the following Step

1. Open the bash.

2.Perform all the operation under root permission

***#vi /etc/apt/sources.list***

append the following to the end of the file:

***deb http://nginx.org/packages/ubuntu/ codename nginx***

***deb-src http://nginx.org/packages/ubuntu/ codename nginx***

***:wq!***

3. ***$ apt-get update***

***$ apt-get install nginx***

Fedora (CentOS,Redhat)

Take the following Step

1. Open the bash.

2.Perform all the operation under root permission

create the file named ***/etc/yum.repos.d/nginx.repo*** with the following contents:

***[nginx]***

***name=nginx repo***

***baseurl=http://nginx.org/packages/mainline/OS/OSRELEASE/$basearch/***

***gpgcheck=0***

***enabled=1***

***:wq!***

3. ***$yum clean all***

***$yum repolist***

***$yum update***

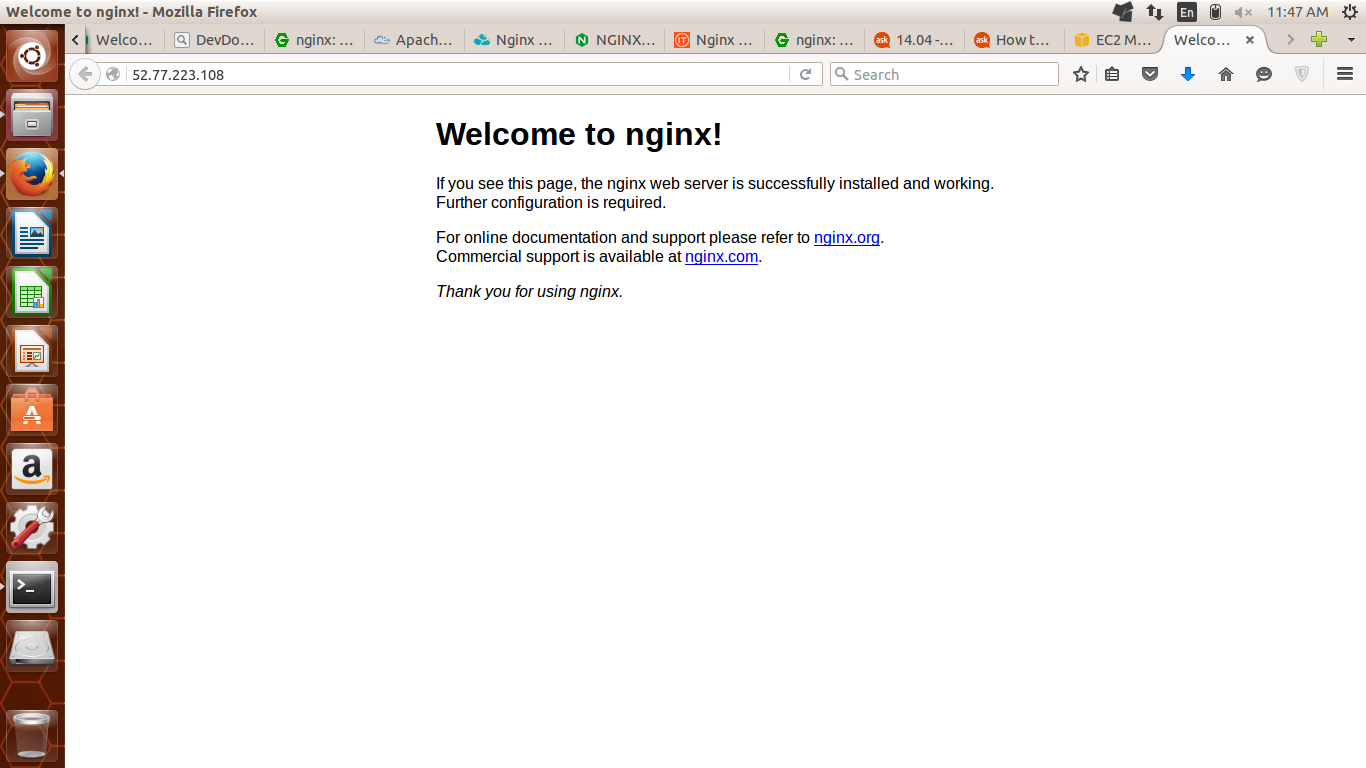
***$yum install nginx\* -y***

Testing the installation in browser

Start the service of nginx

***#service nginx start***

Open the browser with the url [http://localhost](http://localhost/)



If this homepage of nginx will come then all the things are fine

**Hosting a Normal Static Web Page**

The configuration file of Nginx stays in ***/etc/nginx*** or ***/usr/local/etc/nginx.***

First create the Web page which You want to host in a specific directory

***# vi /var/index.html***

<h1> hey, foradians </h1>

:wq!

Then create a separate directory for the configuration file.

***# mkdir conf\_file***

***# cd conf***

***# vi test.conf***

server {

listen 80;

server\_name localhost;

location / {

root /var;

index index.html index.htm;

}

}

:wq

***#vim /etc/nginx/nginx.conf***

then append the following line under http directive

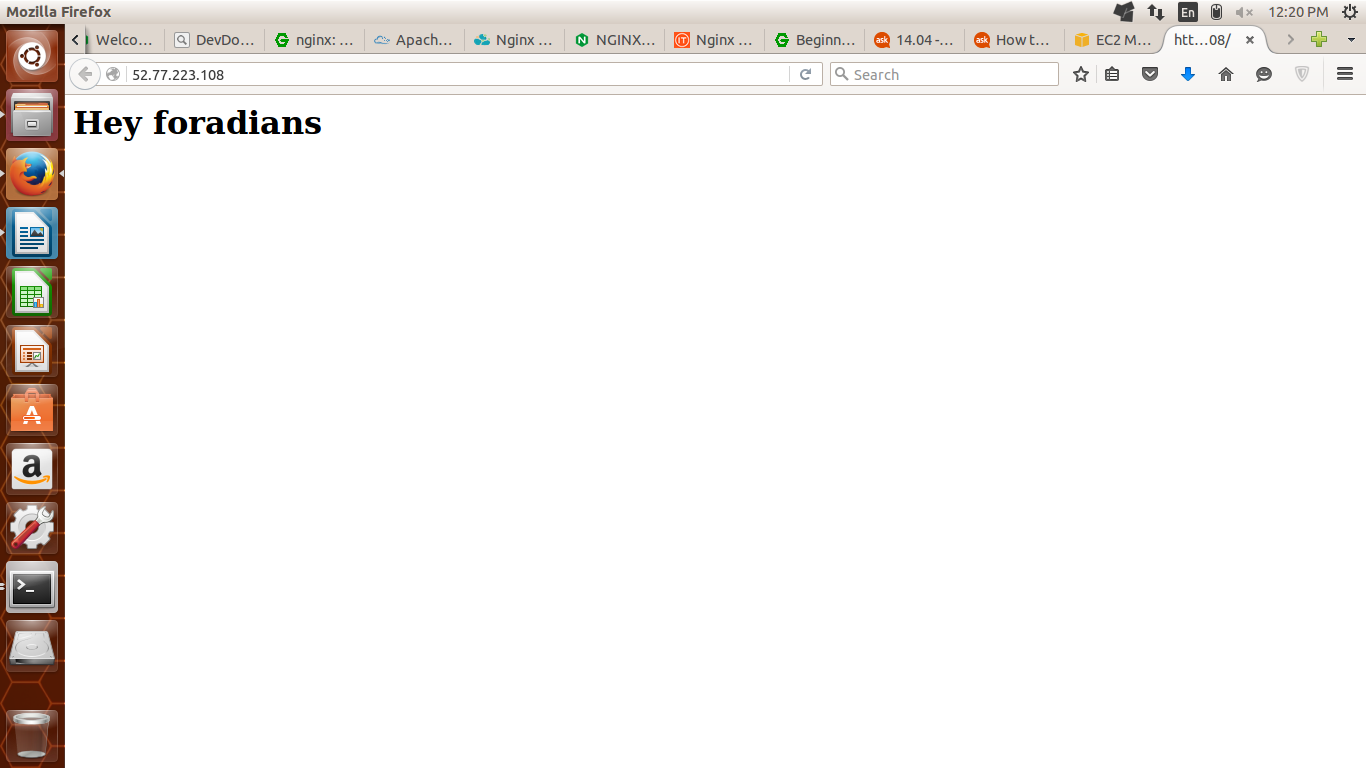
include /etc/nginx/conf\_file/\*.conf;

:wq

start the service

***#service nginx start***

then go to browser and type ***localhost***



**Implementing TLS in NginX**

**Generating Certificates and Key with OpenSSL**

1. Generate SSL key.

***#mkdir /etc/nginx/ssl***

***#cd /etc/nginx/ssl***

***#openssl genrsa -des3 -out server.key 2048***

Generating RSA private key, 2048 bit long modulus

...............................................+++

.........................................................................................+++

e is 65537 (0x10001)

Enter pass phrase for server.key: <<<------ Enter the pass phrase

Verifying - Enter pass phrase for server.key:

***#openssl req -new -key server.key -out server.csr***

Enter pass phrase for server.key:

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:IN

State or Province Name (full name) [Some-State]:Karnataka

Locality Name (eg, city) []:Bengaluru

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Foradian

Organizational Unit Name (eg, section) []:DevOps

Common Name (e.g. server FQDN or YOUR name) []:fedena.com

Email Address []:nikit@foradian.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:Nikit12345

An optional company name []:Foradian

***#cp server.key server.key.org***

***#openssl rsa -in server.key.org -out server.key***

***#openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt***

***#vi /etc/nginx/conf\_file/test.conf***

server {

listen 443 ssl;

ssl on;

ssl\_certificate /etc/nginx/ssl/server.crt;

ssl\_certificate\_key /etc/nginx/ssl/server.key;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers HIGH:!aNULL:!MD5;

server\_name 52.77.223.108;

location / {

root /var;

index index.html index.htm;

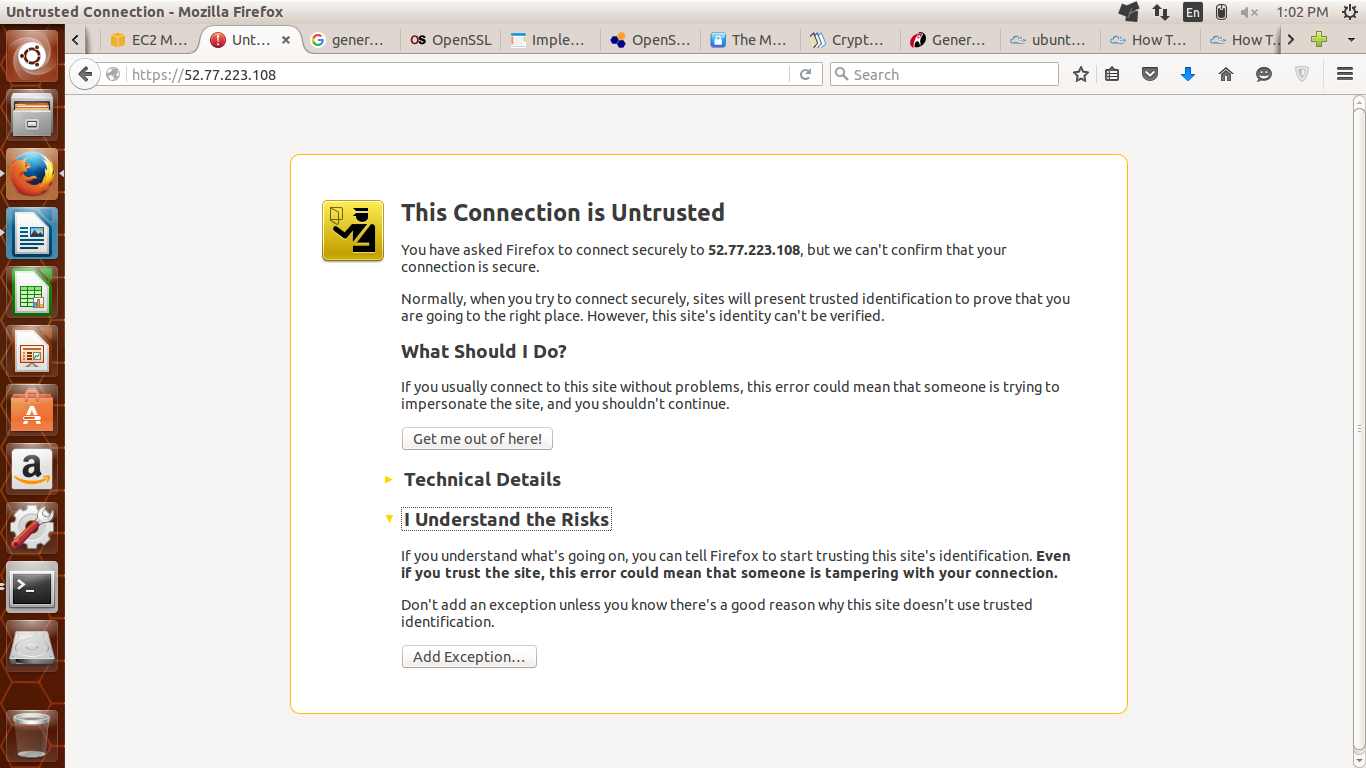
}

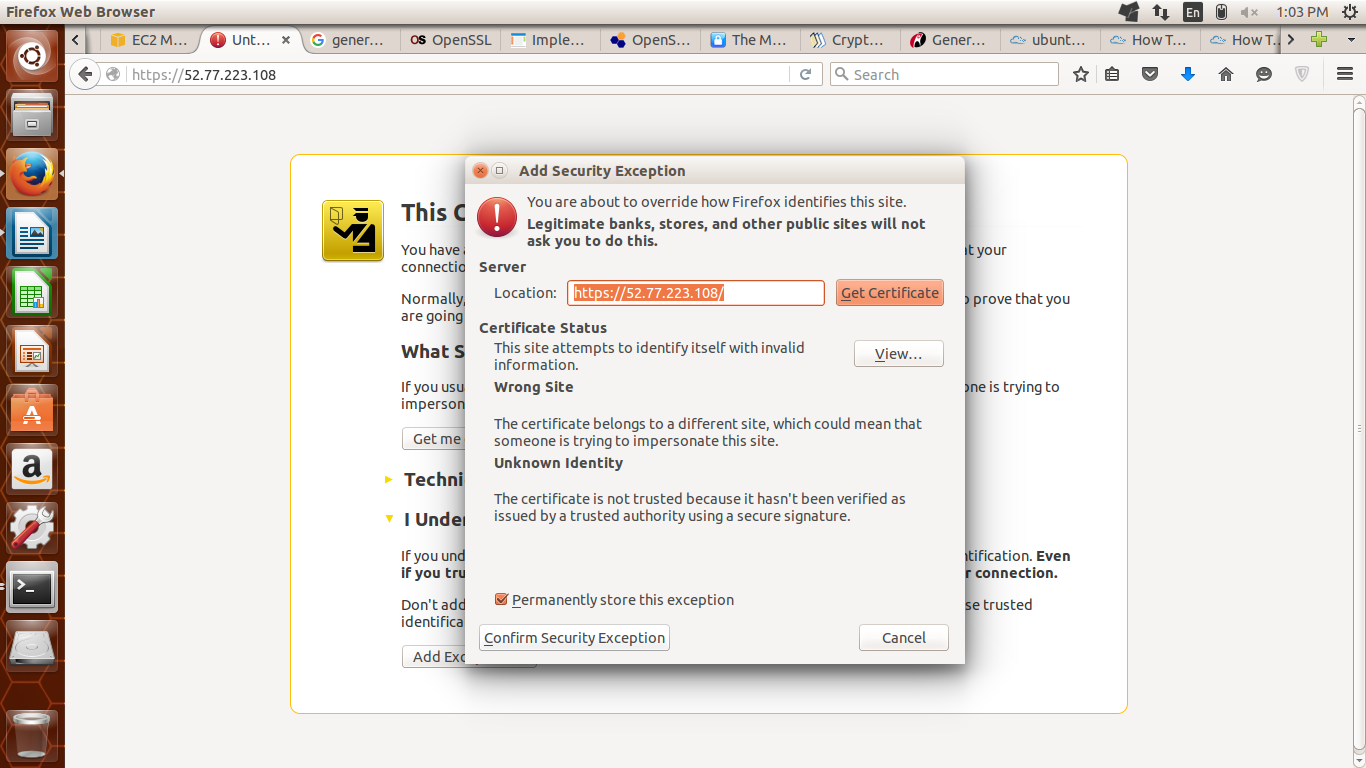
}

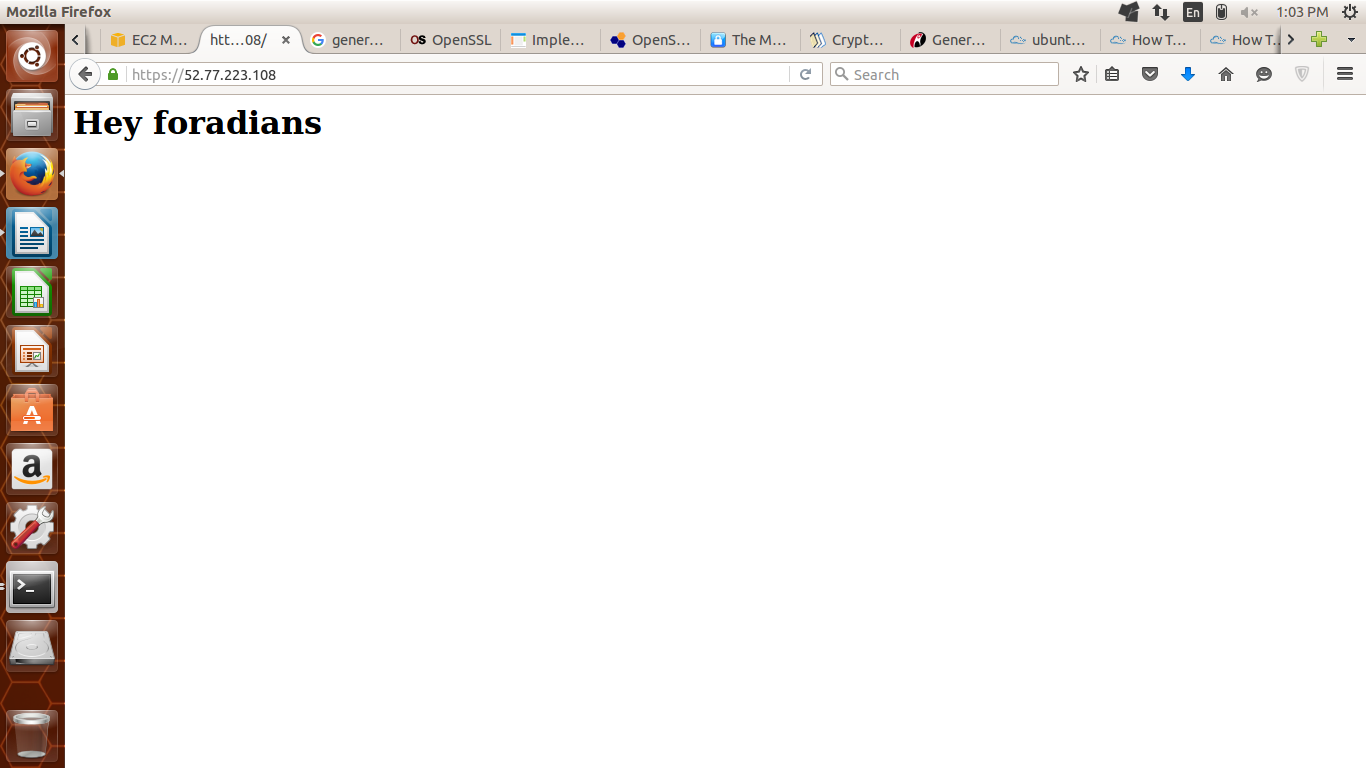
***#service nginx stop***

***#service nginx start***

Then go to browser and type [https://***localhost***](https://localhost/)







**NginX Redirection.**

Redirection is used to redirect or pass the site from one url to another. Lets say if we want that we just type http://www.foradian.com but it redirects to [https://www.foradian.com](https://www.foradian.com/) then we have to redirect it.

This can be done by changing the configuration file and use *rewrite* option

server {

listen 443 ssl;

ssl on;

ssl\_certificate /etc/nginx/ssl/server.crt;

ssl\_certificate\_key /etc/nginx/ssl/server.key;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers HIGH:!aNULL:!MD5;

server\_name 52.77.223.108;

**rewrite ^ https://www.google.com$request\_uri? permanent;**

location / {

root /var;

index index.html index.htm;

}

}

The above configuration file redirects [https://52.77.223.108](https://52.77.223.108/) to [https://www.google.com](https://www.google.com/)

