

# Setup Nginx

## Login and User Setup

1. SSH into Your Machine
2. : Use an SSH client to log into your server.
- 3.

...

Copy `ssh your_user@your_server_ip`

...

## Update System Packages

Frist, ensure that all packages are up to date. This can prevent security vulnerabilities.

...

Copy `sudo apt update && sudo apt upgrade && sudo apt autoremove`

...

## Install Monitoring and Web Server Tools

1. Install Glances
2. : An advanced system monitor for Linux.
- 3.

...

Copy `sudo apt install glances`

...

1. Install Nginx
2. : A high-performance web server and a reverse proxy, often used for load balancing.
- 3.

...

Copy `sudo apt install nginx`

...

1. Configure UFW Firewall for Nginx
2. : Make sure Nginx can receive HTTP and HTTPS traffic.
- 3.

...

Copy `sudo ufw allow 'Nginx HTTP' sudo ufw allow 'Nginx HTTPS'`

...

## Set Up Nginx Configuration

1. Remove Existing Nginx Configuration
2. :
- 3.

...

Copy `sudo rm -rf /etc/nginx/nginx.conf`

...

1. Edit New Configuration
2. : Use a text editor like nano to create a new configuration file.
- 3.

...

Copy `sudo nano /etc/nginx/nginx.conf`

...

- Replace the contents with your load balancer configuration. You can use the [Example Nginx config](#) as a starting point.
- Modify RPC/LCD/gRPC server entries and domain names as required.
- Save and exit the editor (CTRL + X , then Y to confirm, and Enter to save).
- 
- Test Nginx Configuration
  - : Ensures your syntax is correct.
  -

...

Copy `sudo nginx -t`

...

1. Enable and Start Nginx
2. : This will make sure Nginx starts on boot and starts running immediately.
- 3.

...

Copy `sudo systemctl enable nginx`  
`sudo systemctl start nginx`

...

Secure with SSL/HTTPS

1. Install Certbot
2. : This tool automates obtaining free SSL/TLS certificates from Let's Encrypt.
- 3.

...

Copy `sudo apt-get install certbot`  
`sudo apt-get install python3-certbot-nginx`

...

1. Obtain the SSL Certificate for your domain
2. :
- 3.

...

Copy `sudo certbot --nginx -d your_domain.com`

...

1. Finally, you can add a cronjob to crontab to enable auto-renewing of the certificates:
- 2.

...

Copy `crontab -e`  
`0 12 * * * /usr/bin/certbot renew --quiet`

...

Last updated 2 months ago On this page \* [Login and User Setup](#) \* [Update System Packages](#) \* [Install Monitoring and Web Server Tools](#) \* [Set Up Nginx Configuration](#) \* [Secure with SSL/HTTPS](#)

Was this helpful? [Edit on GitHub](#) [Export as PDF](#)