How to enable SSL for a subdomain on Nginx

To enable SSL for a subdomain on Nginx, you can follow these steps:

Obtain an SSL certificate for your subdomain. You can use a free certificate from Let's Encrypt or purchase a certificate from a certificate authority.

Install the certbot utility on your server, which is used to automate the process of obtaining and renewing Let's Encrypt certificates:

```
sudo apt-get update
```

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

Run the certbot command with the --nginx flag to automatically generate a new SSL certificate and configure Nginx to use it:

```
sudo certbot --nginx -d example.com -d www.example.com
```

Make sure to replace example.com with your subdomain name.

Follow the prompts to enter your email address and agree to the Let's Encrypt terms of service. Certbot will automatically configure Nginx to use the new SSL certificate for your subdomain.

Test that SSL is working by visiting your subdomain with https:// at the beginning of the URL. You should see a green padlock icon in your web browser, indicating that the site is secured with SSL.

If you already have an SSL certificate for your subdomain, you can skip step 2 and use the appropriate ssl_certificate and ssl_certificate_key directives in your Nginx configuration to specify the path to your existing certificate and key files.

Revision #1
Created 20 February 2023 16:37:03 by Daniel Azimi
Updated 3 June 2023 06:29:04 by Daniel Azimi