SSL - Let's Encrypt Nginx RockyLinux

Berikut adalah langkah-langkah untuk mengonfigurasi SSL Let's Encrypt di server Nginx :

1. Instal EPEL Repository dan Certbot

Anda perlu menginstal EPEL repository dan Certbot :

```
sudo dnf install epel-release
sudo dnf install certbot python3-certbot-nginx
```

2. Membuka Port 80 dan 443

Pastikan port 80 (HTTP) dan 443 (HTTPS) terbuka di firewall :

```
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https
sudo firewall-cmd --reload
```

3. Mendapatkan Sertifikat SSL

Gunakan Certbot untuk mendapatkan sertifikat SSL untuk domain Anda. Gantikan ilusidgital.com dengan domain Anda, tambahakan -d jika ada domain tambahan lainnya :

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

Certbot akan otomatis mengkonfigurasi Nginx untuk menggunakan sertifikat yang diperoleh.

4. Verifikasi Konfigurasi Nginx

Certbot akan memperbarui konfigurasi Nginx Anda untuk menggunakan sertifikat SSL yang diperoleh. Verifikasi bahwa konfigurasi telah diperbarui dengan benar dengan membuka file konfigurasi Nginx untuk domain Anda. Biasanya berada di /etc/nginx/conf.d/ilusidigital.conf.

Contoh blok server Nginx untuk HTTPS :

```
server {
    listen 443 ssl;
    listen [::]:443 ssl;
    server_name ilusidigital.com www.ilusidigital.com;

    ssl_certificate /etc/letsencrypt/live/ilusidigital.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/ilusidigital.com/privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;

    location / {
        proxy_pass http://localhost:3000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

5. Mengatur Redirect HTTP ke HTTPS

Untuk mengarahkan semua lalu lintas HTTP ke HTTPS, tambahkan blok server berikut :

```
server {
    listen 80;
    listen [::]:80;
    server_name ilusidigital.com www.ilusidigital.com;

    location / {
        return 301 https://$host$request_uri;
    }
}
```

6. Restart Nginx

Setelah semua konfigurasi selesai, restart Nginx untuk menerapkan perubahan :

```
sudo systemctl restart nginx
```

7. Mengatur Pembaruan Otomatis Sertifikat

Let's Encrypt sertifikat hanya berlaku selama 90 hari. Untuk memastikan sertifikat Anda selalu diperbarui, tambahkan cron job untuk menjalankan pembaruan otomatis :

```
echo "0 3 * * * /usr/bin/certbot renew --quiet" | sudo tee -a /etc/crontab > /dev/null
```

8. Dengan langkah-langkah di atas, Anda akan memiliki server Nginx yang dikonfigurasi untuk menggunakan sertifikat SSL dari Let's Encrypt, memastikan bahwa komunikasi antara server dan klien dienkripsi dengan aman.

Revision #4
Created 9 July 2024 02:55:22 by Kevin
Updated 22 October 2024 02:45:43 by Kevin