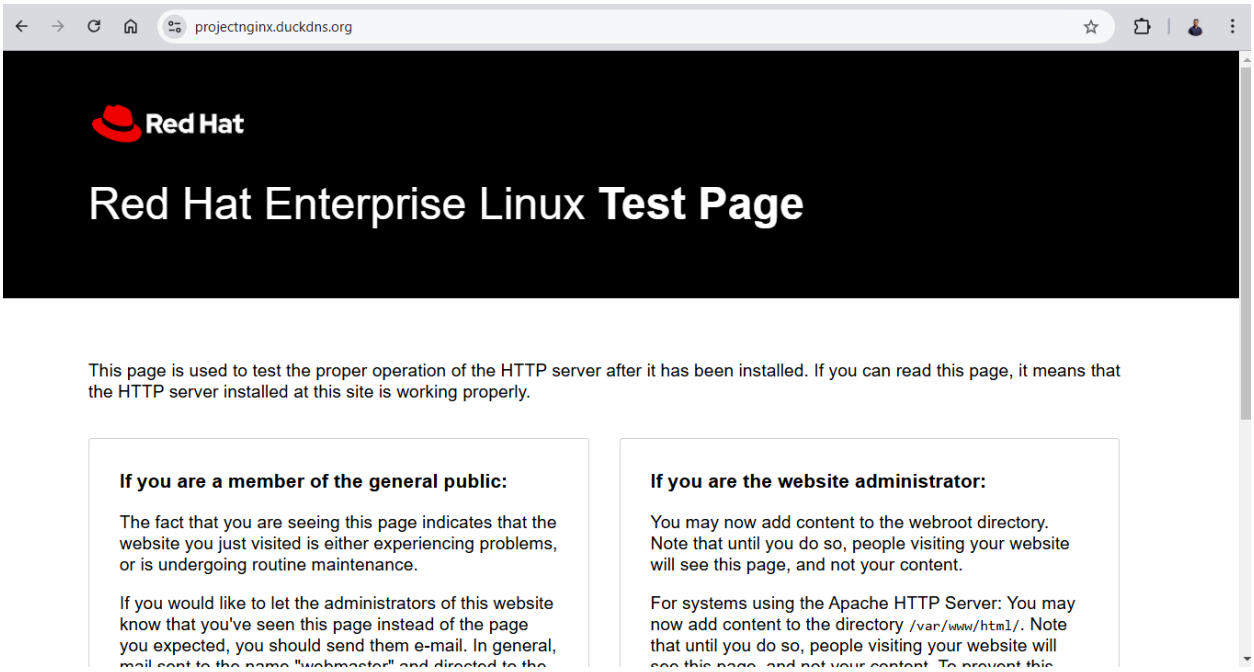
Shrikant Sherkar-Assignment

Response from *curl -I https://projectnginx.duckdns.org*:

```
[ec2-user@ip-172-31-88-244 ~]$ curl -I https://projectnginx.duckdns.org
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Wed, 05 Mar 2025 12:26:08 GMT
Content-Type: text/html
Content-Length: 5909
Last-Modified: Mon, 09 Aug 2021 11:43:42 GMT
Connection: keep-alive
ETag: "611114ee-1715"
Accept-Ranges: bytes
```

On visiting *https://projectnginx.duckdns.org:*

Project-Video-Link



GitHub Repo Link:

GitHub-Repo-Link

Stepwise execution of commands to Secure Web Server Deployment with SSL on RHEL/Rocky Linux 9:

Overview

This project documents the step-by-step process of deploying an Nginx web server on an **AWS EC2 instance** running **RHEL/Rocky Linux 9**, securing it with **Let's Encrypt SSL (Certbot)**, and configuring DNS with **DuckDNS**.

Prerequisites

- **AWS EC2 instance** (RHEL/Rocky Linux 9)
- **Domain/subdomain** (e.g., projectnginx.duckdns.org)
- **DuckDNS Account**
- **Public IP Address of the EC2 instance**

Step 1: Update System Packages

sudo dnf update -y

Step 2: Install Nginx

sudo dnf install nginx -y

sudo systemctl enable --now nginx

sudo systemctl status nginx

Step 3: Open Firewall Ports

sudo firewall-cmd --permanent --add-service=http

sudo firewall-cmd --permanent --add-service=https

sudo firewall-cmd --reload

Step 4: Configure DuckDNS for Dynamic DNS

1. Go to DuckDNS
2. Register your domain/subdomain (projectnginx.duckdns.org)
3. Obtain your **DuckDNS Token**
4. Update DNS TXT record for Let's Encrypt verification:

curl -X GET "https://www.duckdns.org/update?domains=projectnginx&token=YOUR_DUCKDNS_TOKEN&txt=YOUR_CERTBOT_VALUE"

Step 5: Install Certbot (Let's Encrypt)

sudo dnf install epel-release -y

sudo dnf install certbot python3-certbot-nginx -y

Step 6: Generate SSL Certificate

sudo certbot certonly --manual --preferred-challenges dns -d projectnginx.duckdns.org

- Follow the prompts and **add the provided TXT record** to DuckDNS using the API.
- Verify propagation using:

dig -t TXT _acme-challenge.projectnginx.duckdns.org

- After successful verification, Certbot generates the SSL certificate at:
    - /etc/letsencrypt/live/projectnginx.duckdns.org/fullchain.pem
    - /etc/letsencrypt/live/projectnginx.duckdns.org/privkey.pem

---

Step 7: Configure Nginx for SSL

Edit the Nginx configuration file:

sudo vi /etc/nginx/conf.d/default.conf

Add the following configuration:

```
server {
  listen 443 ssl;
  server_name projectnginx.duckdns.org;
  ssl_certificate /etc/letsencrypt/live/projectnginx.duckdns.org/fullchain.pem;
  ssl_certificate_key /etc/letsencrypt/live/projectnginx.duckdns.org/privkey.pem;
```

```
    location / {
        root /usr/share/nginx/html;
        index index.html;
    }
}
server {
    listen 80;
    server_name projectnginx.duckdns.org;
    return 301 https://$host$request_uri;
}
```

Save and exit, then restart Nginx:

```
sudo nginx -t
sudo systemctl restart nginx
```

Step 8: Verify SSL Certificate

```
curl -I https://projectnginx.duckdns.org
```

Check SSL status:

```
sudo certbot certificates
```

Troubleshooting

- **Check Nginx logs:**

```
sudo journalctl -u nginx --no-pager | tail -20
```

- **Check Certbot logs:**

```
sudo cat /var/log/letsencrypt/letsencrypt.log
```

- **Verify DNS record propagation:**

```
dig -t TXT _acme-challenge.projectnginx.duckdns.org
```
