Install Nginx Proxy

5. Install and configure Nginx and Let’s Encrypt

5.1. Install Nginx

1. Update package lists:

```
sudo apt update
```

2. Install Nginx:

```
sudo apt install nginx -y
```

3. Start and enable Nginx:

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

5.2. Install Certbot for Let’s Encrypt

1. Add repositories and update:

```
sudo apt install software-properties-common -y
sudo add-apt-repository universe
sudo add-apt-repository ppa:certbot/certbot -y
sudo apt update
```

2. Install Certbot with Nginx plugin:

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

5.3. Obtain a certificate for your domain

1. Make sure your DNS A record for `abeta-proxy.finmars.com` points to your VM `PUBLIC_IP`.

2. Run:

```
sudo certbot --nginx -d abeta-proxy.finmars.com
```

3. Follow the prompts:
   1. Enter your email, then press `Enter`.
   2. Agree to terms by typing `A`, then `Enter`.
   3. Choose option `2` to redirect HTTP to HTTPS, then `Enter`.

Certbot will create an Nginx site file and install the certificate under `/etc/letsencrypt/live/abeta-proxy.finmars.com/`.

---

6. Configure Nginx to proxy to APISIX

1. Open the site file Certbot created:

```
sudo nano /etc/nginx/sites-available/default
```

2. Inside the `server { ... }` block for port 443, find these lines:

```
listen 443 ssl;
server_name abeta-proxy.finmars.com;

ssl_certificate /etc/letsencrypt/live/abeta-proxy.finmars.com/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/abeta-proxy.finmars.com/privkey.pem;
```

3. Right below them, add:

```
location / {
    proxy_pass http://127.0.0.1:9080;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
}
```

   After editing, that `server { }` block looks like:

```
server {
    listen 443 ssl;
    server_name abeta-proxy.finmars.com;

    ssl_certificate /etc/letsencrypt/live/abeta-proxy.finmars.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/abeta-proxy.finmars.com/privkey.pem;
```

```
    location / {
        proxy_pass http://127.0.0.1:9080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
    }
}
```

4. Make sure there is also a block that redirects HTTP to HTTPS. It looks like:

```
server {
    listen 80;
    server_name abeta-proxy.finmars.com;
    return 301 https://$host$request_uri;
}
```

5. Save and close:
   - Press `Ctrl+O`, then `Enter`.
   - Press `Ctrl+X`.
6. Test Nginx configuration:

```
sudo nginx -t
```

   You should see “syntax is ok” and “test is successful”.
7. Reload Nginx so it uses the new config:

```
sudo systemctl reload nginx
```

---

7. Open firewall ports (if you use UFW)

1. Allow HTTP (port 80) and HTTPS (port 443), and APISIX port (9080) in UFW:

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw allow 9080/tcp
```

2. Check UFW status:

```
sudo ufw status
```

Revision #5
Created 2025-06-03 15:47:43 UTC by Sergei Zhitenev
Updated 2025-06-03 15:53:37 UTC by Sergei Zhitenev