Övning: Konfigurera nginx med självsignerade certifikat

Arbetsuppgift 1: Starta ingående virtuella maskiner

1. På din fysiska maskin, anslut till Hyper-V Manager.
2. Starta Easec-Router och Easec-Linux1, genom att högerklicka på respektive virtuell maskin och klicka på alternativet Start.
3. Anslut till Easec-Linux1 genom att i Hyper-V Manager högerklicka på Easec-Linux1 och klicka på Anslut.
4. Logga på som easec med lösenordet Pa$$w0rd.

Arbetsuppgift 2: Installera nginx

1. Starta Terminalfönstret, genom att klicka på ctrl+alt+t.
2. I Terminalfönstret, skriv in följande kommando och klicka på Enter:

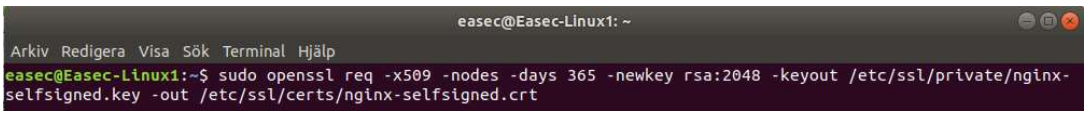
   `sudo apt-get update`

   Ange lösenordet **`Pa$$w0rd`** för sudo.
3. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att installare nginx:

   `sudo apt-get install nginx`

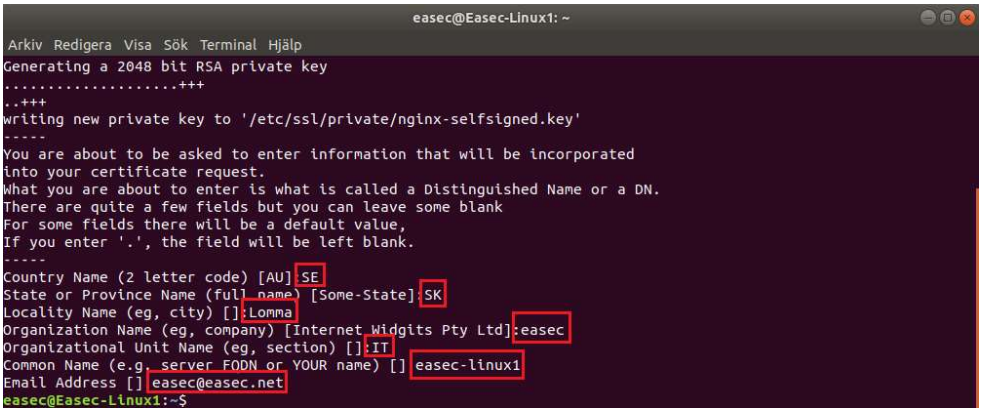
   Skriv in ett **`J`** och klicka på **Enter** för att installera nginx.

Arbetsuppgift 3: Skapa certifikat för SSL



1. I Terminalfönstret, skriv in följande kommando och klicka på Enter:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```



Ange svar enligt följande tabell (klicka på **Enter** efter varje rad):

Country Name: **SE**

State or Province Name: **SK**

Locality Name: **Lomma**

Organization Name: **easec**

Organizational Unit Name: **IT**

Common Name: **easec-linux1**

Email Address: **easec@easec.net**

2. Skriv in följande kommando och klicka på Enter efter varje rad, för att skapa Diffie-Hellman group för användning vid förhandling av Perfect Forward Secrecy mellan klienter (detta kan ta några minuter):

```
sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
```

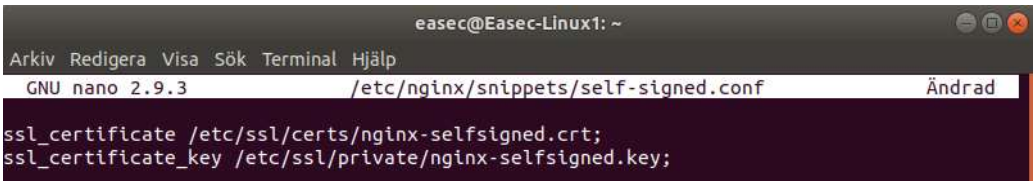
Arbetsuppgift 4: Skapa snippets för SSL

Nästa steg är att modifiera konfiguration för nginx. För detta kommer du att skapa ”configuration snippets” som kommer att innehålla referenser till fil för nyckel och certifikat.

Denna metod för att konfigurera nginx ger dig en möjlighet att lägga samman vanliga konfigurationssegment till återanvändbara moduler.

1. I Terminalfönstret, skriv in följande kommando och klicka på Enter:

   `sudo nano /etc/nginx/snippets/self-signed.conf`



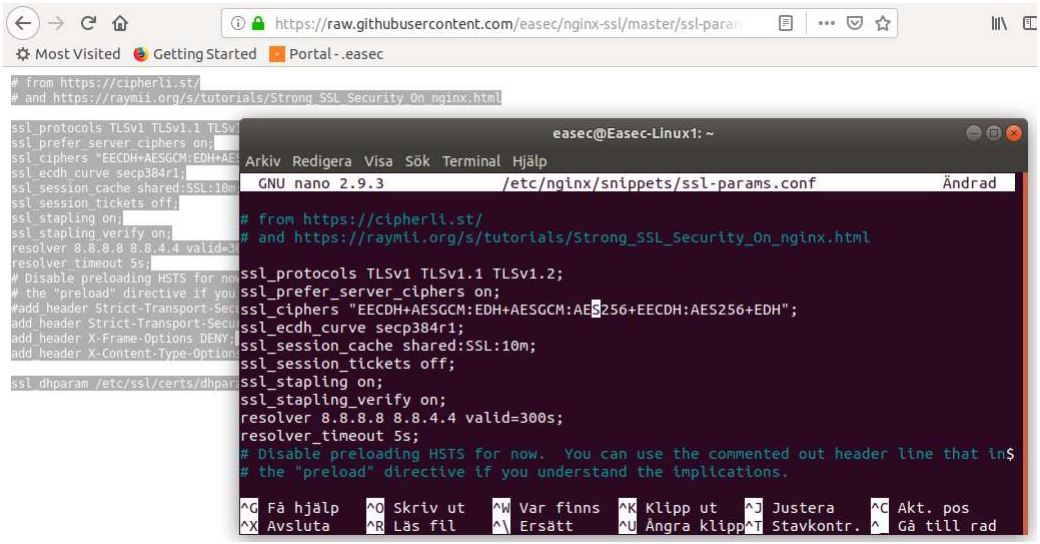
2. I fönstret med nano, lägg till följande rader:

   `ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;`

   `ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;`

   Klicka på ctrl+x, skriv in ett J och klicka på Enter, för att spara dina förändringar.

Nästa steg är att skapa ytterligare en snippet, denna kommer att användas för att definiera inställningar för SSL. Parametrar som sätts, kan återanvändas för andra konfiguration när nginx används. Filinnehåll som skriv in under punkt 3 finns på https://github.com/easec/nginx-ssl, om du kopierar från denna tänk då på att klicka på Raw.



3. I Terminalfönstret, skriv in följande kommando och klicka på Enter:

   sudo nano /etc/nginx/snippets/ssl-params.conf

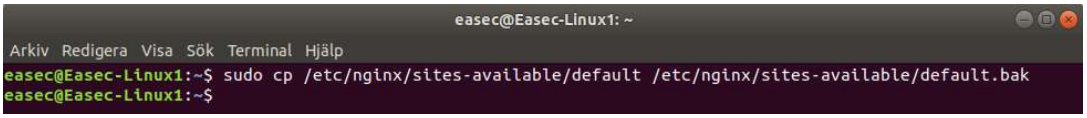
   Skriv in följande i filen:

```
# from https://cipherli.st/
# and
https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";
ssl_ecdh_curve secp384r1;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off;
ssl_stapling on;
ssl_stapling_verify on;
resolver 8.8.8.8 8.8.4.4 valid=300s;
resolver_timeout 5s;
# Disable preloading HSTS for now.  You can use the commented out
header line that includes
# the "preload" directive if you understand the implications.
#add_header Strict-Transport-Security "max-age=63072000;
includeSubdomains; preload";
add_header Strict-Transport-Security "max-age=63072000;
includeSubdomains";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
```

```
ssl_dhparam /etc/ssl/certs/dhparam.pem;
```

Klicka på ctrl+x, skriv in ett **J** och klicka på **Enter**, för att spara filen.



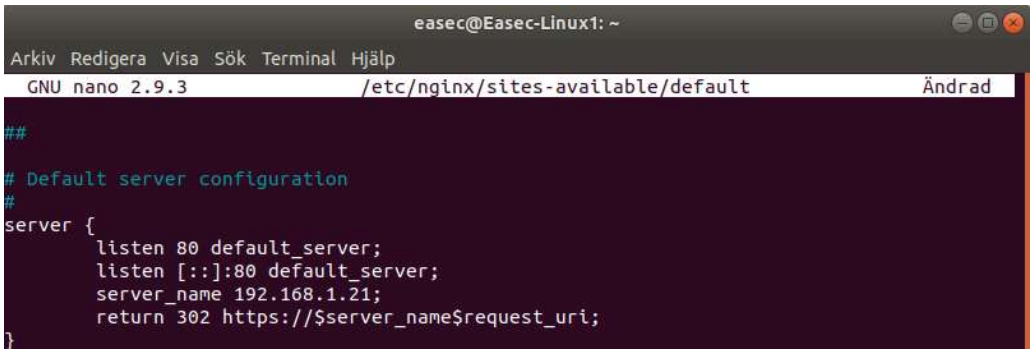
4. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att göra säkerhetskopia av nuvarande snippets:

   sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/default.bak

5. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att justera inställngar:

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

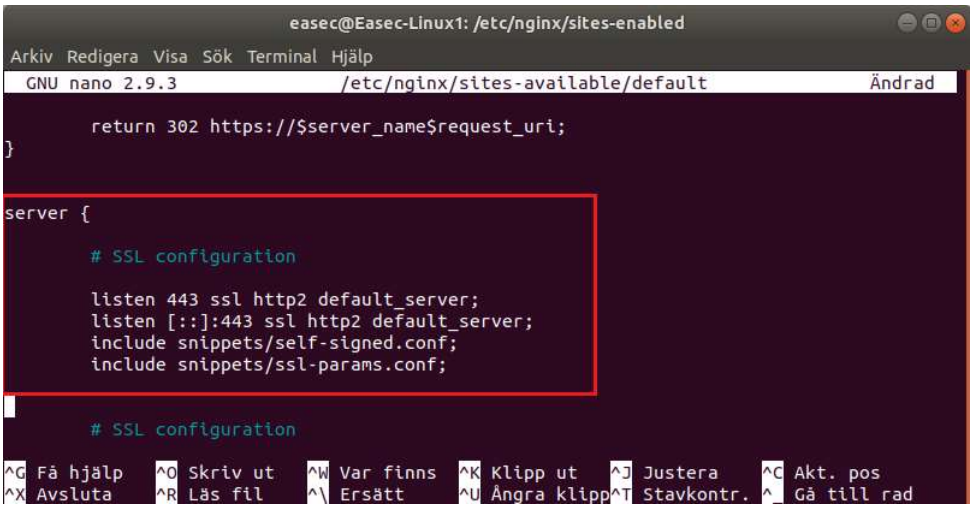
Du kommer att modifiera konfigurationen så att förfrågningar via HTTP kommer automatiskt att omdirigeras till HTTPS.



6. Lägg till markerade rader:

```
server {

 listen 80 default_server;
 listen [::]:80 default_server;
 easec-linux1 192.168.1.21;
 return 302 https://$server_name$request_uri;
 }
```



7. Lägg till följande direkt efter föregående direktiv:

```
server {

 # SSL configuration


 listen 443 ssl http2 default_server;

 listen [::]:443 ssl http2 default_server;

 include snippets/self-signed.conf;

 include snippets/ssl-params.conf;
```

Klicka på ctrl+x, skriv in ett **J** och klicka på **Enter**, för att spara filen.

Arbetsuppgift 5: Konfigurera brandvägg

1. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att visa nuvarande inställningar för `ufw`:

```
sudo ufw status
```

För att tillåta HTTPS-trafik, kan du tillåta profilen ”Nginx Full” och om du har profilen ”Nginx HTTP” kan du ta bort denna.

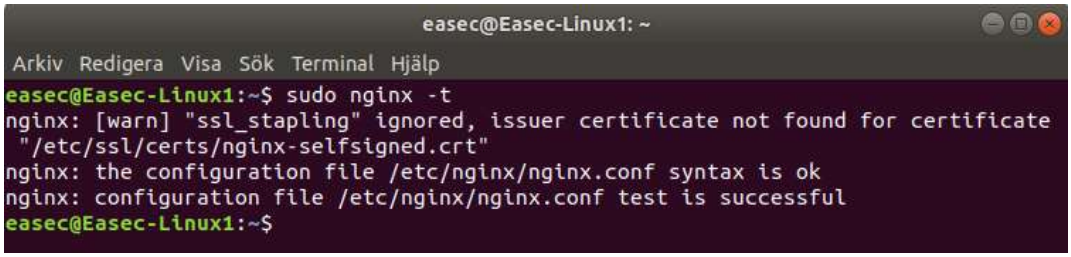
2. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att tillåta HTTPS och ta bort HTTP (om du inte hade profilen ”Nginx HTTP”, behöver du inte skriva det sista kommandot):

   sudo ufw allow 'Nginx Full' && sudo ufw delete allow 'Nginx HTTP'

3. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att visa verifiera att inställningar för `ufw` har ändrats:

   sudo ufw status

Arbetsuppgift 6: Slå på förändringar för nginx



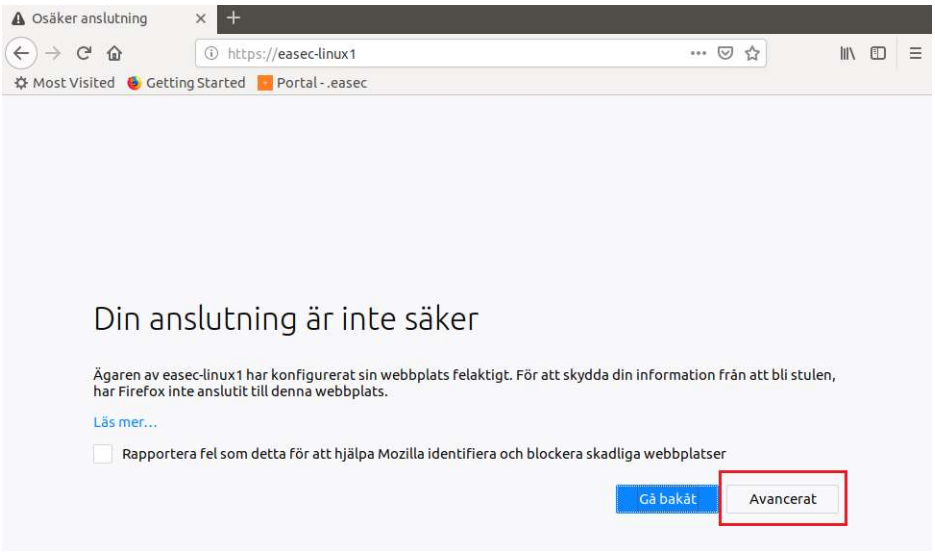
1. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att kontrollera så att det inte finns syntaxfel i konfigurationsfiler:

   sudo nginx -t

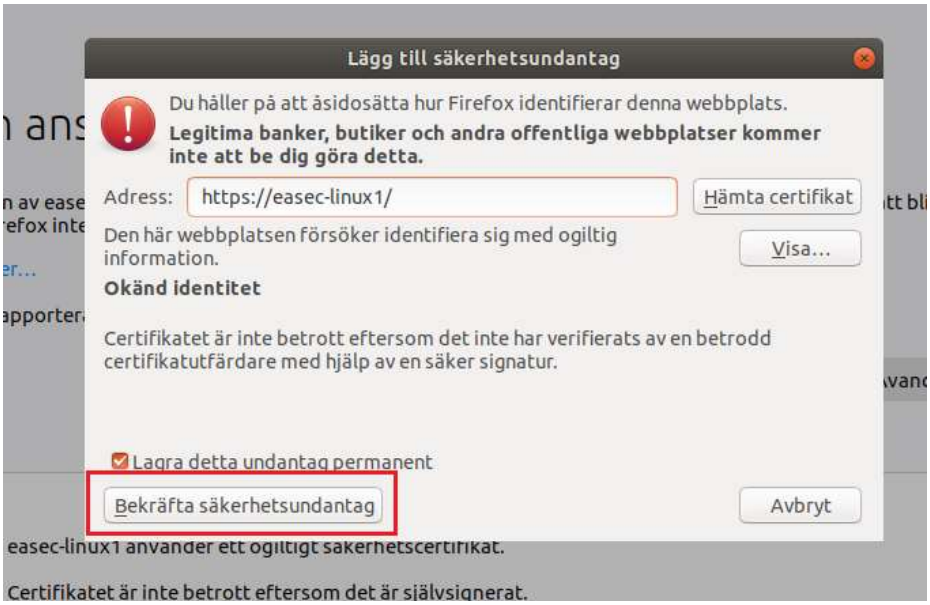
2. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att starta om nginx:

   sudo systemctl restart nginx

Arbetsuppgift 7: Testa funktionen



1. Öppna webbläsare, skriv in url: https:/easec-linux1 och klicka på Enter. Kontrollera att sidan öppnas med ett varningsmeddelande, detta beror på att du använder ett självsignerande certifikat.



2. Klicka på Avancerat – Bekräfta säkerhetsundantag.

3. Standardsida för nginx kommer att visas.