

Övning: Konfigurera nginx med självsignerade certifikat

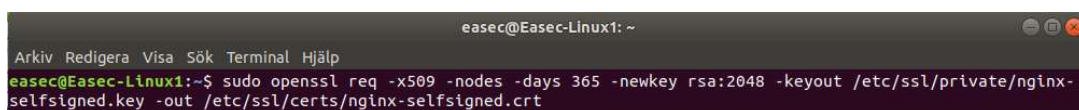
Arbetsuppgift 1: Starta ingående virtuella maskiner

1. På din fysiska maskin, anslut till Hyper-V Manager.
2. Starta Eassec-Router och Eassec-Linux1, genom att högerklicka på respektive virtuell maskin och klicka på alternativet Start.
3. Anslut till Eassec-Linux1 genom att i Hyper-V Manager högerklicka på Eassec-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 installera nginx:
sudo apt-get install nginx
Skriv in ett **J** och klicka på **Enter** för att installera nginx.

Arbetsuppgift 3: Skapa certifikat för SSL



```
eassec@Eassec-Linux1: ~  
Arkiv Redigera Visa Sök Terminal Hjälp  
eassec@Eassec-Linux1:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```

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
```

```
eassec@Eassec-Linux1: ~
Arkiv Redigera Visa Sök Terminal Hjälp
Generating a 2048 bit RSA private key
.....+++
..+++
writing new private key to '/etc/ssl/private/nginx-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU] SE
State or Province Name (full name) [Some-State] SK
Locality Name (eg, city) [] Lomma
Organization Name (eg, company) [Internet Widgits Pty Ltd] easec
Organizational Unit Name (eg, section) [] IT
Common Name (e.g., server FQDN or YOUR name) [] easec-linux1
Email Address [] easec@easec.net
eassec@Eassec-Linux1:~$
```

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

```
eassec@Eassec-Linux1: ~
Arkiv Redigera Visa Sök Terminal Hjälp
eassec@Eassec-Linux1:~$ sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+.....
.....+.....
.....
```

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
```

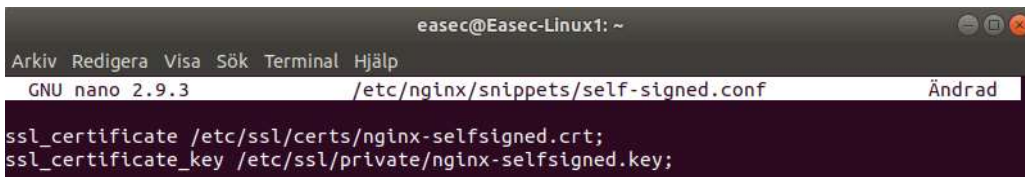
Arbetsuppgift 4: Skapa snippets för SSL

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
```



```
easec@Easec-Linux1: ~  
Arkiv Redigera Visa Sök Terminal Hjälp  
GNU nano 2.9.3 /etc/nginx/snippets/self-signed.conf Ändrad  
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;  
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

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.

```

eassec@Eassec-Linux1: ~
GNU nano 2.9.3 /etc/nginx/snippets/ssl-params.conf
# 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 in
# 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;

```

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

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

Skriv in följande i filen:

```

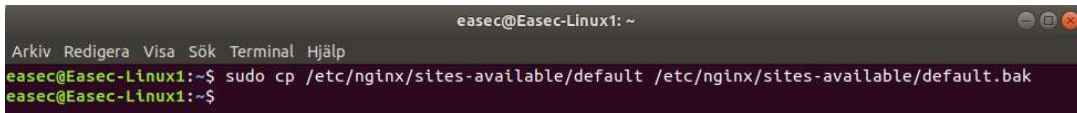
# from https://cipherli.st/
# and
https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html

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.



```
easec@Easec-Linux1: ~
Arkiv Redigera Visa Sök Terminal Hjälp
easec@Easec-Linux1:~$ sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/default.bak
easec@Easec-Linux1:~$
```

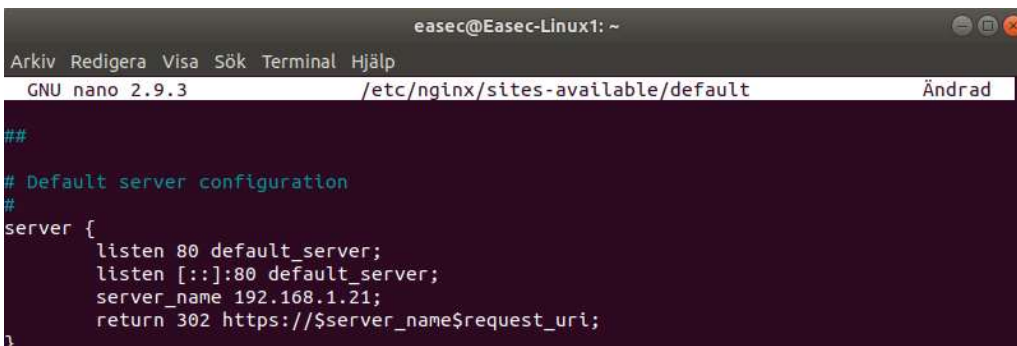
4. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att göra säkerhetskopior av nuvarande snippets:

```
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 inställningar:

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

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

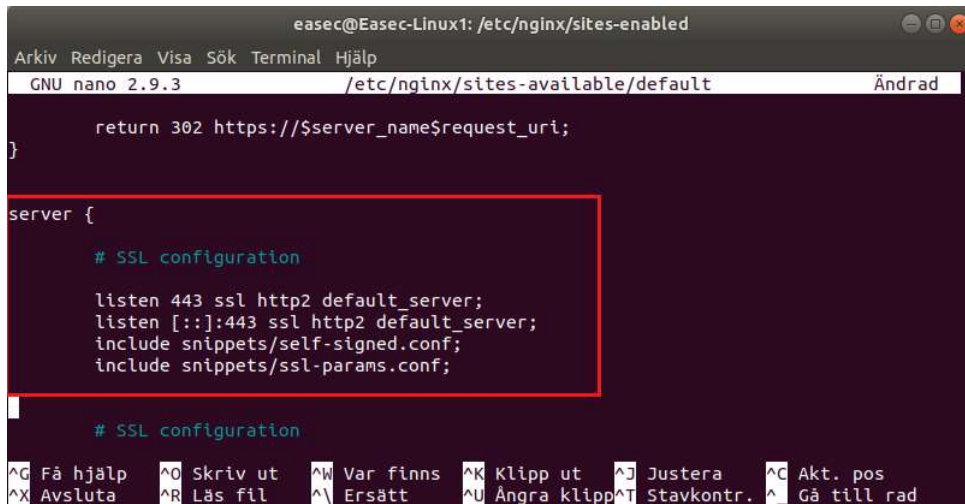


```
easec@Easec-Linux1: ~
Arkiv Redigera Visa Sök Terminal Hjälp
GNU nano 2.9.3 /etc/nginx/sites-available/default Ändrad
##
# Default server configuration
#
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name 192.168.1.21;
    return 302 https://$server_name$request_uri;
}
```

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;
}
```



```
easec@Easec-Linux1: /etc/nginx/sites-enabled
GNU nano 2.9.3 /etc/nginx/sites-available/default
return 302 https://$server_name$request_uri;
}

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;

# SSL configuration

^G Få hjälp   ^O Skriv ut  ^W Var finns ^K Klipp ut  ^J Justera   ^C Akt. pos
^X Avsluta   ^R Läs fil   ^\ Ersätt     ^U Ångra klipp ^T Stavkontr. ^_ Gå till rad
```

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.

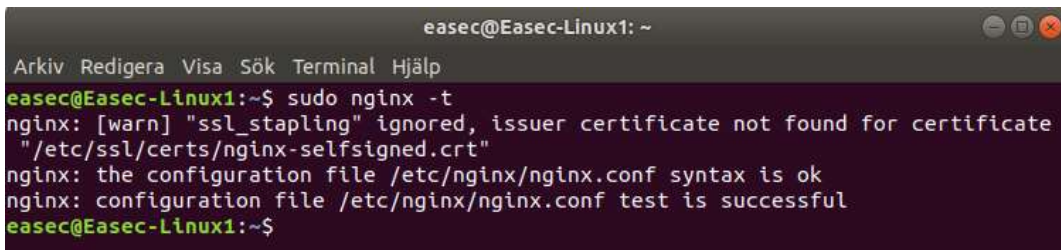
2. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att tillåta HTTPS och ta bort HTTP (om du inte hade profilen "Nginx HTTP", behöver du inte skriva det sista kommandot):

```
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

A terminal window titled 'easec@Easec-Linux1: ~' with a menu bar containing 'Arkiv Redigera Visa Sök Terminal Hjälp'. The terminal shows the command 'sudo nginx -t' being executed. The output is: 'nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/ssl/certs/nginx-selfsigned.crt"', 'nginx: the configuration file /etc/nginx/nginx.conf syntax is ok', and 'nginx: configuration file /etc/nginx/nginx.conf test is successful'. The prompt returns to 'easec@Easec-Linux1:~\$'.

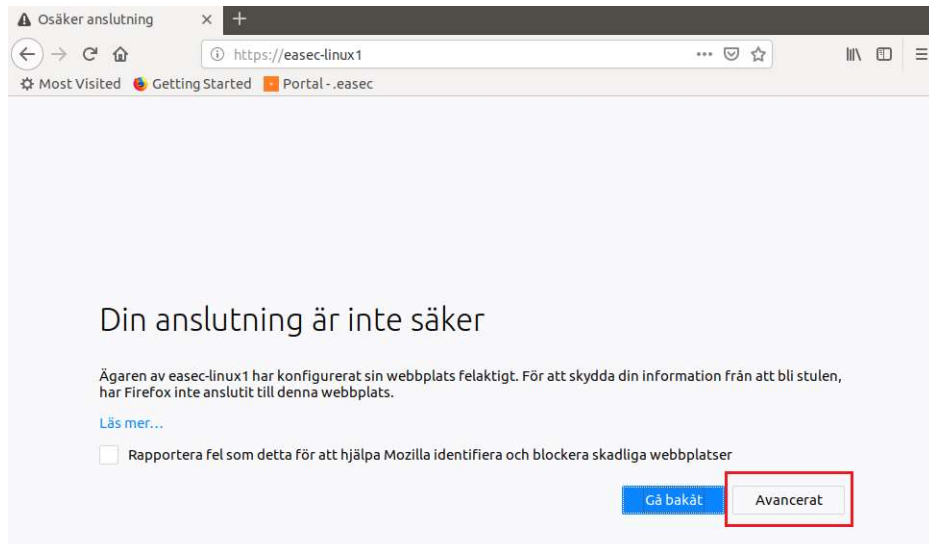
1. I Terminalfönstret, skriv in följande kommando och klicka på Enter, för att kontrollera så att det inte finns syntaxfel i konfigurationsfiler:

```
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://eassec-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.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

Thank you for using nginx.

3. Standardsida för nginx kommer att visas.