SOAL NOMOR 1 - Infrastructure Provisioning

Sevima, sebuah perusahaan yang bergerak di bidang teknologi informasi, memiliki rencana besar untuk mengembangkan infrastuktur mereka dengan membangun sebuah pusat data (data center). Pusat data ini diharapkan mampu menunjang performa aplikasi serta berfungsi sebagai cadangan (backup) sehingga jika terjadi kendala, recovery dapat dilakukan dengan cepat dan efisien. Anda, sebagai calon System Administrator, diberi tugas penting untuk merancang dan mengimplementasikan topologi jaringan untuk pusat data ini menggunakan Cisco Packet Tracer.

Tugas Anda tidak hanya berhenti di situ. Sevima juga berencana untuk memperluas jangkauan operasional mereka dengan membuka cabang di tiga kota besar di Indonesia: Jakarta, Bandung, dan Surabaya. Anda harus memastikan bahwa jaringan di ketiga cabang tersebut terhubung satu sama lain dengan baik.

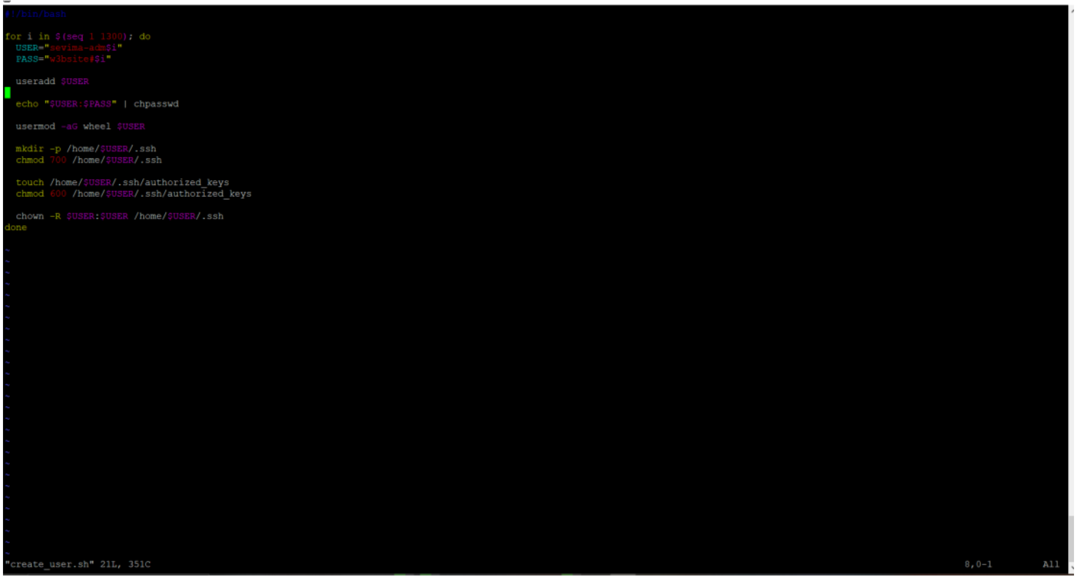
SOAL NOMOR 2: Make Your Web Great Again

A. Konfigurasi Dasar

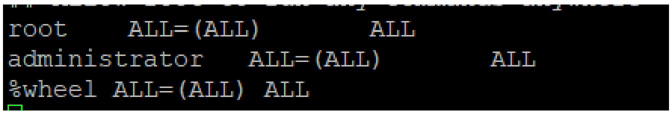
1) Buat user dengan Akses Sudo, Login menggunakan kata sandi dan menggunakan pubkey.

Name	Password
sevima-adm{1..13003	w3bsite#1..1300 (buat password 1-1300 sesuai jumlah user)

Jawab :

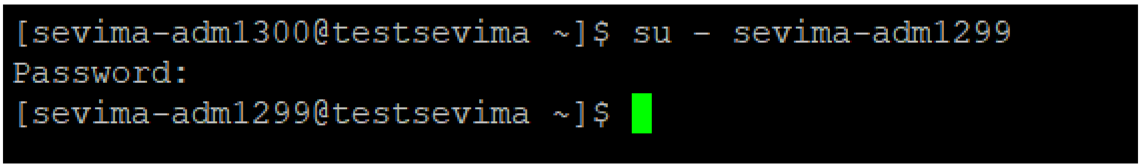


```
#!/bin/bash

for i in $(seq 1 1300); do
  USER="sevima-adm$i"
  PASS="w3bsite#$i"

  useradd $USER

  echo "$USER:$PASS" | chpasswd

  usermod -aG wheel $USER

  mkdir -p /home/$USER/.ssh
  chmod 700 /home/$USER/.ssh

  touch /home/$USER/.ssh/authorized_keys
  chmod 600 /home/$USER/.ssh/authorized_keys

  chown -R $USER:$USER /home/$USER/.ssh
done
~
~
~
"create_user.sh" 21L, 351C                                        8,0-1         All
```

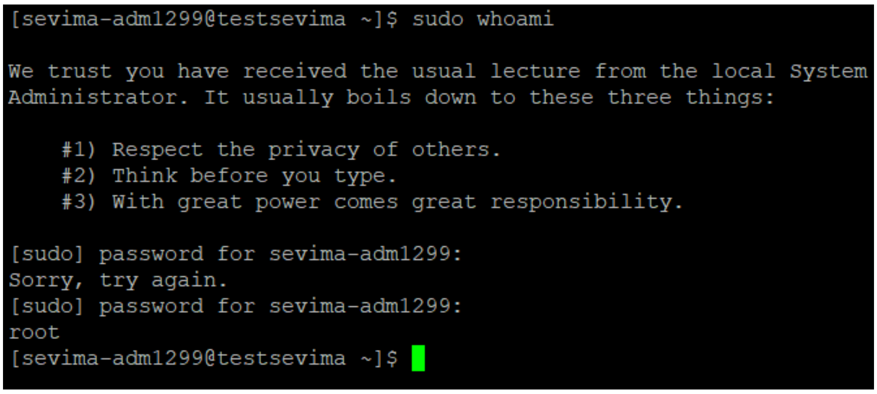


```
root    ALL=(ALL)       ALL
administrator   ALL=(ALL)       ALL
%wheel ALL=(ALL) ALL
```

Hasil :



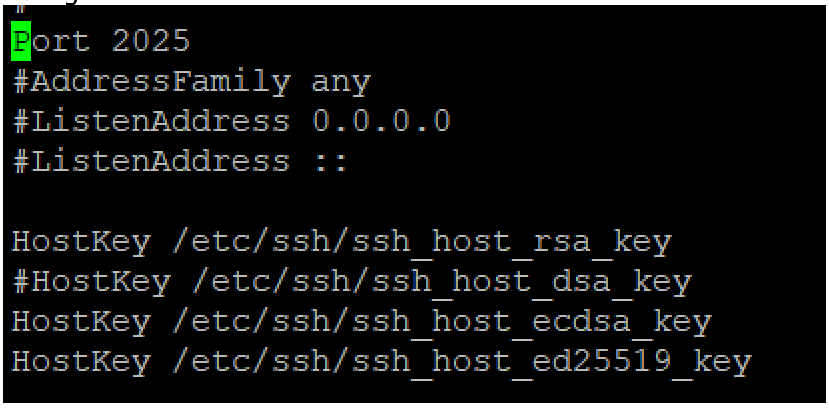
```
[sevima-adm1300@testsevima ~]$ su - sevima-adm1299
Password:
[sevima-adm1299@testsevima ~]$
```



```
[sevima-adm1299@testsevima ~]$ sudo whoami

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for sevima-adm1299:
Sorry, try again.
[sudo] password for sevima-adm1299:
root
[sevima-adm1299@testsevima ~]$
```

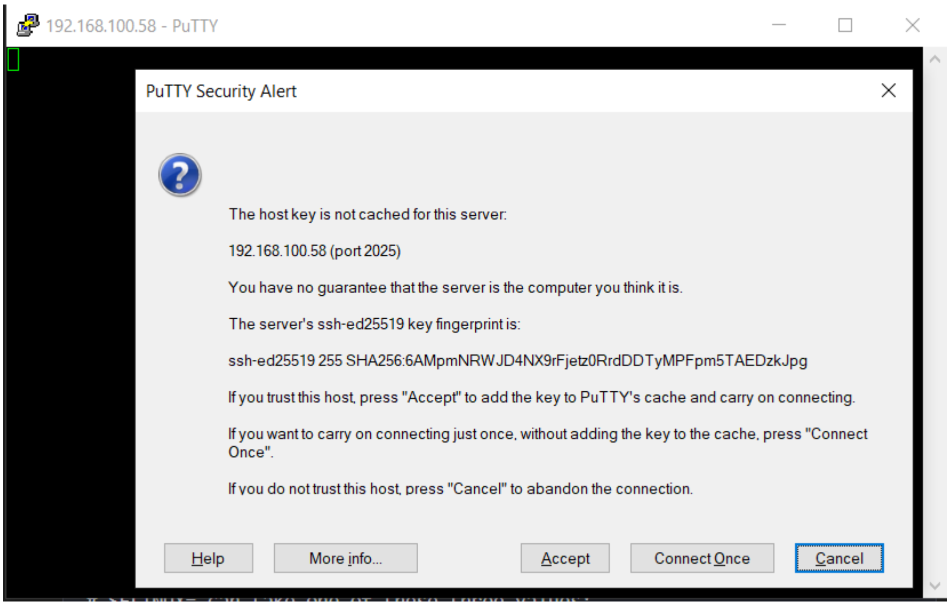
2) Ubah port ssh menjadi 2025

Config :



```
Port 2025
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

Hasil :



The host key is not cached for this server:

192.168.100.58 (port 2025)

You have no guarantee that the server is the computer you think it is.

The server's ssh-ed25519 key fingerprint is:

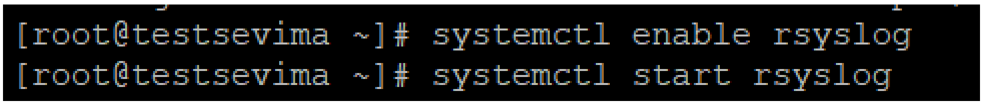
ssh-ed25519 255 SHA256:6AMpmNRWJD4NX9rFjetz0RrdDDTyMPFpm5TAEDzkJpg

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

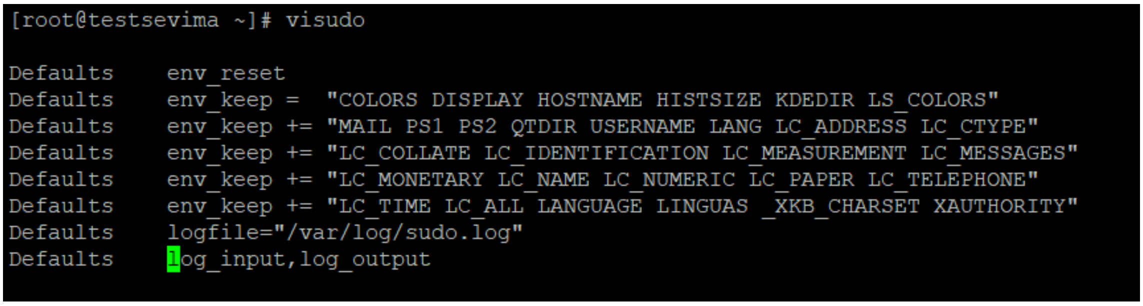
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

3) Aktifkan seluruh log aktivitas

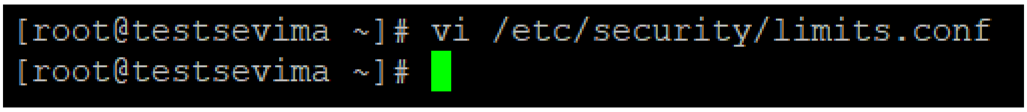


```
[root@testsevima ~]# systemctl enable rsyslog
[root@testsevima ~]# systemctl start rsyslog
```

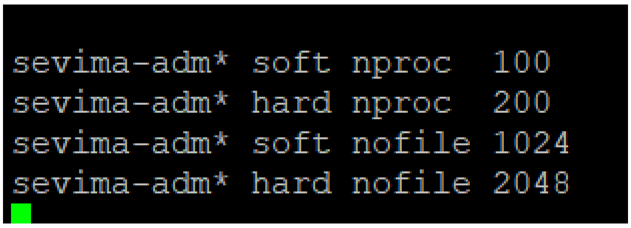


```
[root@testsevima ~]# visudo

Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"
Defaults    logfile="/var/log/sudo.log"
Defaults    log_input,log_output
```

4) Sesuaikan penggunaan sumber daya sesuai kebutuhan dengan ulimit

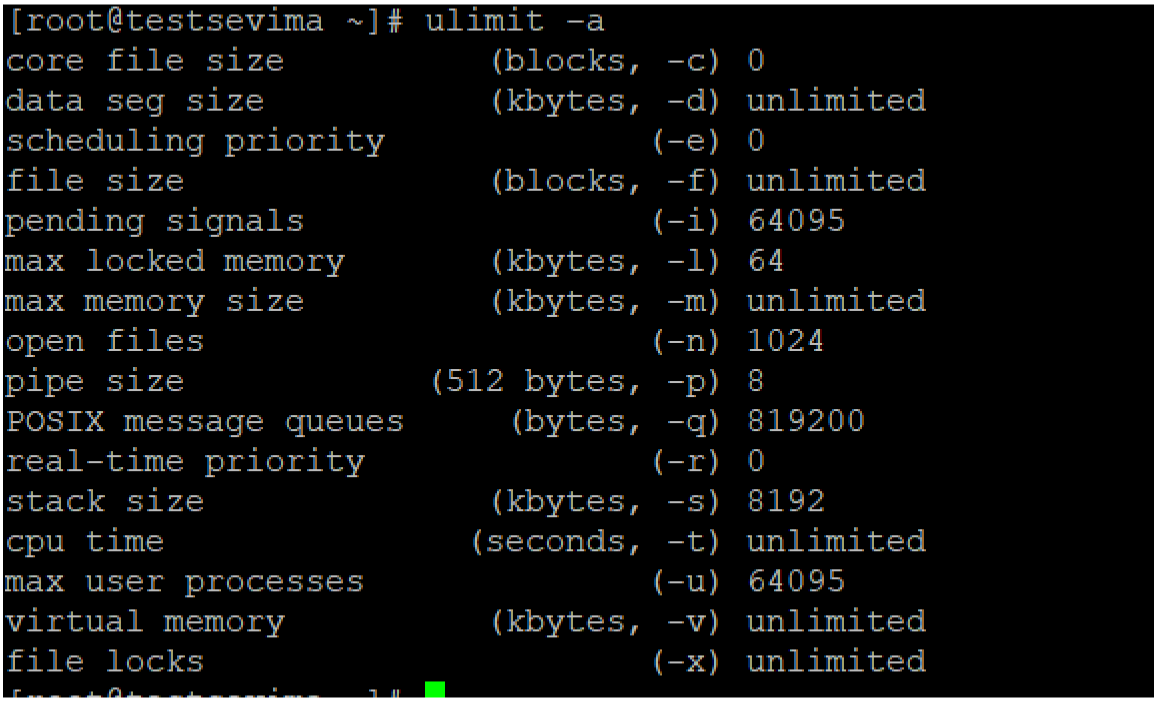


```
[root@testsevima ~]# vi /etc/security/limits.conf
[root@testsevima ~]#
```



```

sevima-adm* soft nproc  100
sevima-adm* hard nproc  200
sevima-adm* soft nofile 1024
sevima-adm* hard nofile 2048
```

Hasil :

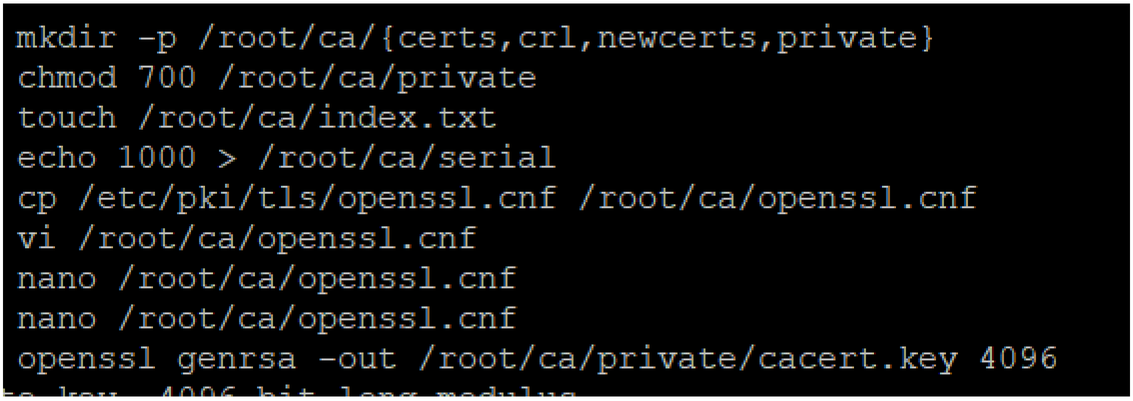


```
[root@testsevima ~]# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 64095
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 64095
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
[root@testsevima ~]#
```

B. Certificate Authority

1) Set up root certificate authority menggunakan OpenSSL pada direktori /root/ca.

Konfigurasi :



```
mkdir -p /root/ca/{certs,crl,newcerts,private}
chmod 700 /root/ca/private
touch /root/ca/index.txt
echo 1000 > /root/ca/serial
cp /etc/pki/tls/openssl.cnf /root/ca/openssl.cnf
vi /root/ca/openssl.cnf
nano /root/ca/openssl.cnf
nano /root/ca/openssl.cnf
openssl genrsa -out /root/ca/private/cacert.key 4096
```

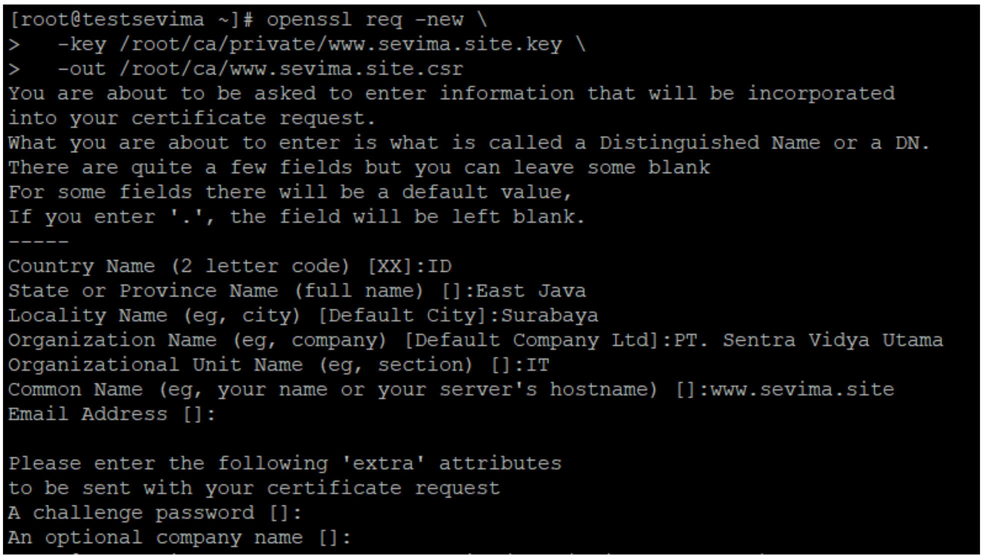
2) Buat Root Certificate cacert.pem and cacert.key dengan menggunakan informasi di bawah ini :

a) Country Code: ID
b) Organization: PT. Sentra Vidya Utama
c) Common Name: SEVIMA CA
d) Create additional certificate

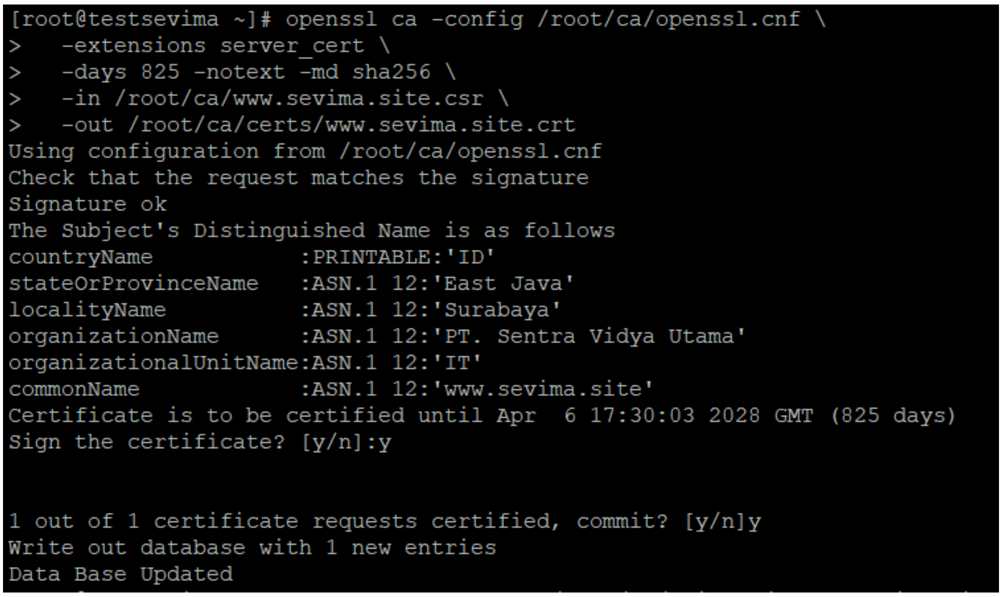
Issued Certificate	Note
www.sevima.site	Web
utara.sevima.site	Web
timur.sevima.site	Web
barat.sevima.site	Web

Konfigurasi :

- www.sevima.site

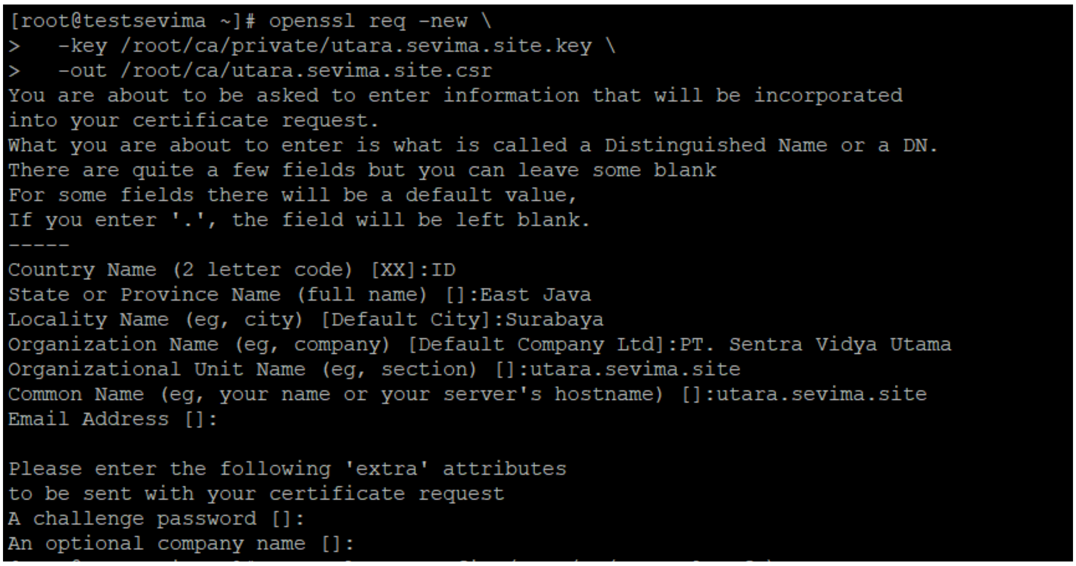


```
[root@testsevima ~]# openssl req -new \
>   -key /root/ca/private/www.sevima.site.key \
>   -out /root/ca/www.sevima.site.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name 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) [XX]:ID
State or Province Name (full name) []:East Java
Locality Name (eg, city) [Default City]:Surabaya
Organization Name (eg, company) [Default Company Ltd]:PT. Sentra Vidya Utama
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:www.sevima.site
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

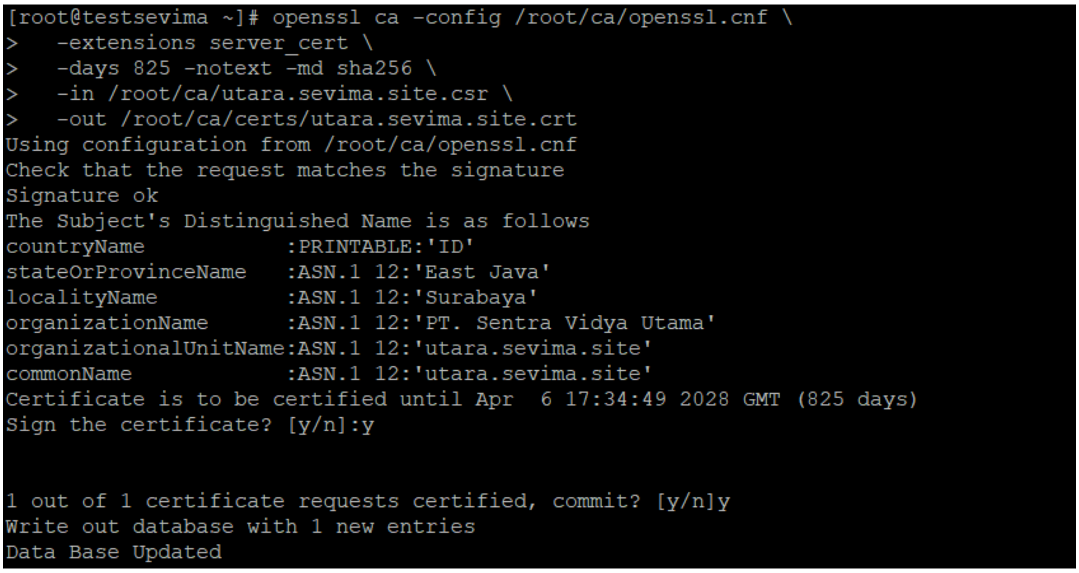


```
[root@testsevima ~]# openssl ca -config /root/ca/openssl.cnf \
>   -extensions server_cert \
>   -days 825 -notext -md sha256 \
>   -in /root/ca/www.sevima.site.csr \
>   -out /root/ca/certs/www.sevima.site.crt
Using configuration from /root/ca/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :ASN.1 12:'East Java'
localityName          :ASN.1 12:'Surabaya'
organizationName      :ASN.1 12:'PT. Sentra Vidya Utama'
organizationalUnitName:ASN.1 12:'IT'
commonName            :ASN.1 12:'www.sevima.site'
Certificate is to be certified until Apr  6 17:30:03 2028 GMT (825 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- utara.sevima.site

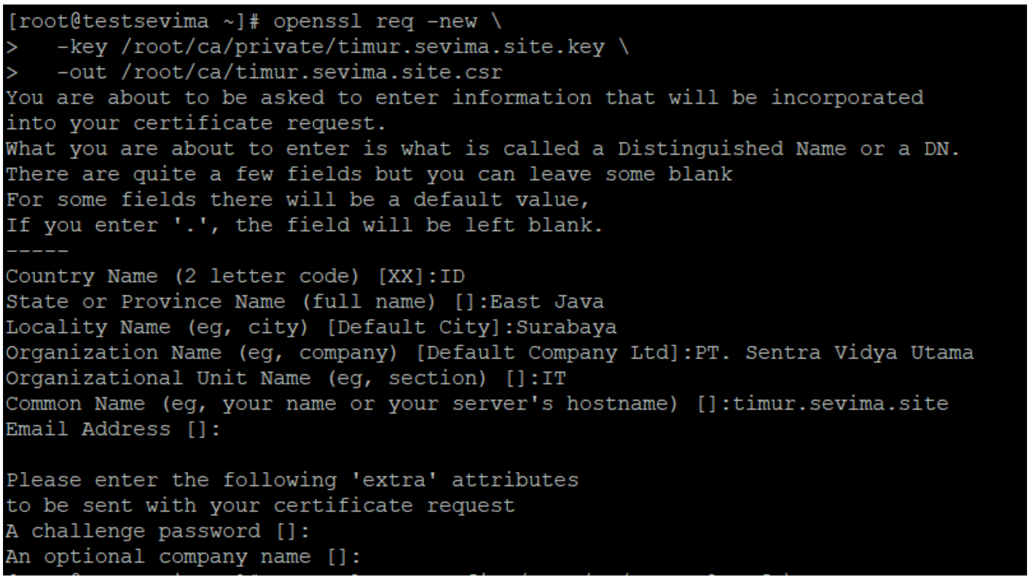


```
[root@testsevima ~]# openssl req -new \
>   -key /root/ca/private/utara.sevima.site.key \
>   -out /root/ca/utara.sevima.site.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name 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) [XX]:ID
State or Province Name (full name) []:East Java
Locality Name (eg, city) [Default City]:Surabaya
Organization Name (eg, company) [Default Company Ltd]:PT. Sentra Vidya Utama
Organizational Unit Name (eg, section) []:utara.sevima.site
Common Name (eg, your name or your server's hostname) []:utara.sevima.site
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

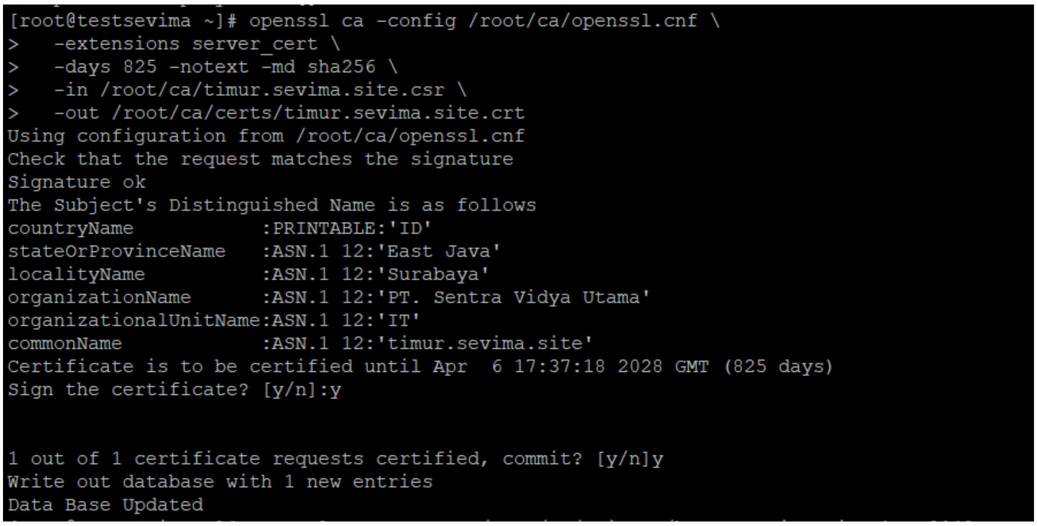


```
[root@testsevima ~]# openssl ca -config /root/ca/openssl.cnf \
>   -extensions server_cert \
>   -days 825 -notext -md sha256 \
>   -in /root/ca/utara.sevima.site.csr \
>   -out /root/ca/certs/utara.sevima.site.crt
Using configuration from /root/ca/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :ASN.1 12:'East Java'
localityName          :ASN.1 12:'Surabaya'
organizationName      :ASN.1 12:'PT. Sentra Vidya Utama'
organizationalUnitName:ASN.1 12:'utara.sevima.site'
commonName            :ASN.1 12:'utara.sevima.site'
Certificate is to be certified until Apr  6 17:34:49 2028 GMT (825 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- timur.sevima.site

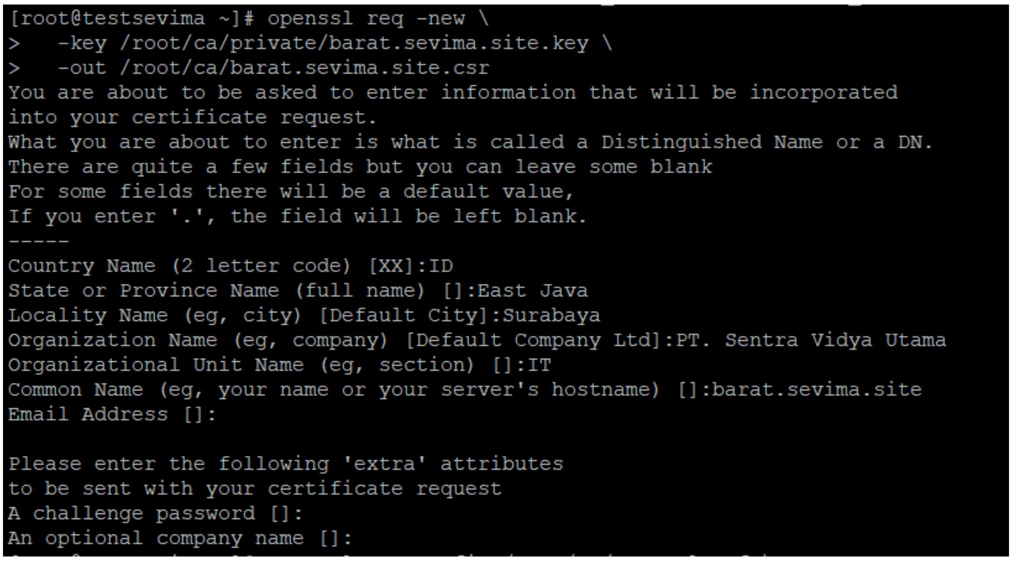


```
[root@testsevima ~]# openssl req -new \
>   -key /root/ca/private/timur.sevima.site.key \
>   -out /root/ca/timur.sevima.site.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name 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) [XX]:ID
State or Province Name (full name) []:East Java
Locality Name (eg, city) [Default City]:Surabaya
Organization Name (eg, company) [Default Company Ltd]:PT. Sentra Vidya Utama
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:timur.sevima.site
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

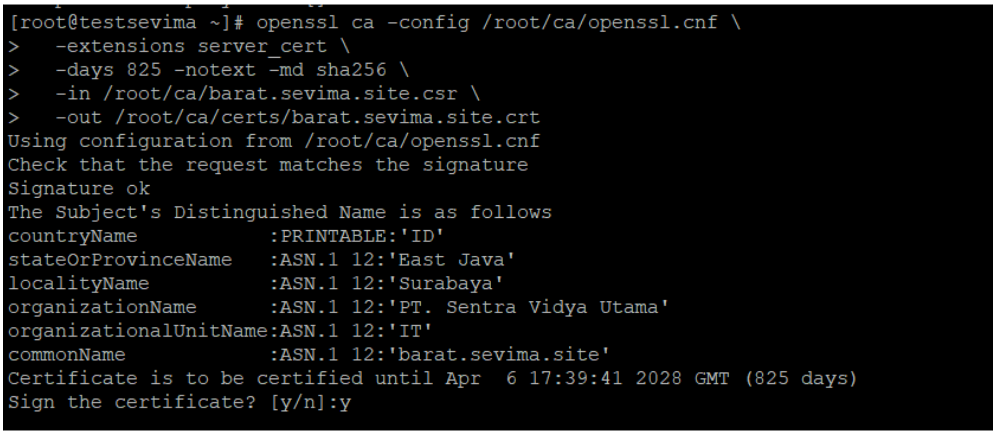


```
[root@testsevima ~]# openssl ca -config /root/ca/openssl.cnf \
>   -extensions server_cert \
>   -days 825 -notext -md sha256 \
>   -in /root/ca/timur.sevima.site.csr \
>   -out /root/ca/certs/timur.sevima.site.crt
Using configuration from /root/ca/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :ASN.1 12:'East Java'
localityName          :ASN.1 12:'Surabaya'
organizationName      :ASN.1 12:'PT. Sentra Vidya Utama'
organizationalUnitName:ASN.1 12:'IT'
commonName            :ASN.1 12:'timur.sevima.site'
Certificate is to be certified until Apr  6 17:37:18 2028 GMT (825 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- barat.sevima.site

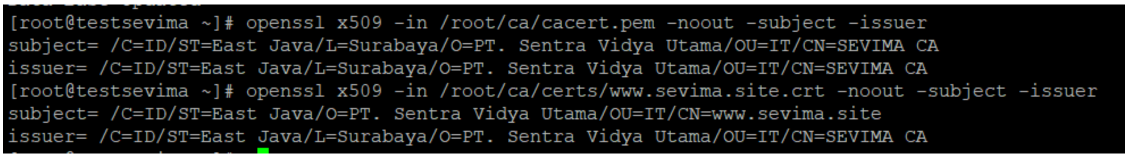


```
[root@testsevima ~]# openssl req -new \
>   -key /root/ca/private/barat.sevima.site.key \
>   -out /root/ca/barat.sevima.site.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name 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) [XX]:ID
State or Province Name (full name) []:East Java
Locality Name (eg, city) [Default City]:Surabaya
Organization Name (eg, company) [Default Company Ltd]:PT. Sentra Vidya Utama
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:barat.sevima.site
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```



```
[root@testsevima ~]# openssl ca -config /root/ca/openssl.cnf \
>   -extensions server_cert \
>   -days 825 -notext -md sha256 \
>   -in /root/ca/barat.sevima.site.csr \
>   -out /root/ca/certs/barat.sevima.site.crt
Using configuration from /root/ca/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'ID'
stateOrProvinceName   :ASN.1 12:'East Java'
localityName          :ASN.1 12:'Surabaya'
organizationName      :ASN.1 12:'PT. Sentra Vidya Utama'
organizationalUnitName:ASN.1 12:'IT'
commonName            :ASN.1 12:'barat.sevima.site'
Certificate is to be certified until Apr  6 17:39:41 2028 GMT (825 days)
Sign the certificate? [y/n]:y
```

Hasil :

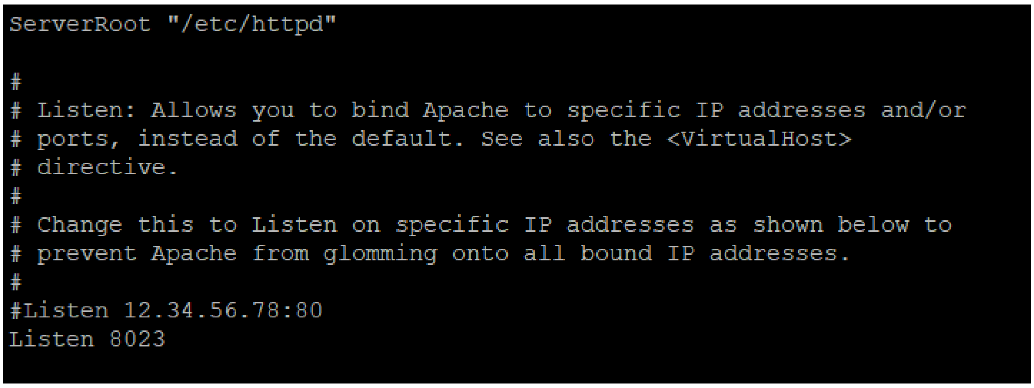


```
[root@testsevima ~]# openssl x509 -in /root/ca/cacert.pem -noout -subject -issuer
subject= /C=ID/ST=East Java/L=Surabaya/O=PT. Sentra Vidya Utama/OU=IT/CN=SEVIMA CA
issuer= /C=ID/ST=East Java/L=Surabaya/O=PT. Sentra Vidya Utama/OU=IT/CN=SEVIMA CA
[root@testsevima ~]# openssl x509 -in /root/ca/certs/www.sevima.site.crt -noout -subject -issuer
subject= /C=ID/ST=East Java/O=PT. Sentra Vidya Utama/OU=IT/CN=www.sevima.site
issuer= /C=ID/ST=East Java/L=Surabaya/O=PT. Sentra Vidya Utama/OU=IT/CN=SEVIMA CA
```

C. Web Server

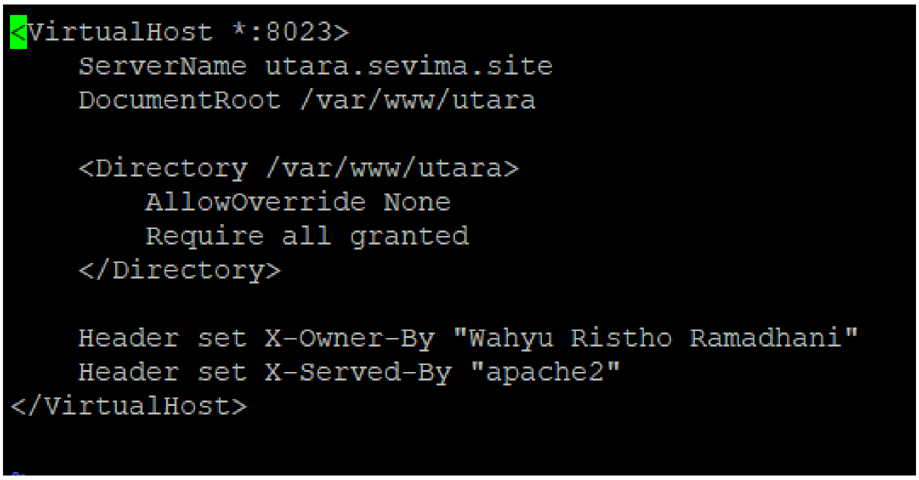
a. Install web server menggunakan apache2 and nginx di host yang sama.

1. Buat virtual host HTTP-only untuk melayani utara.sevima.site menggunakan apache2 pada port 80 + ID peserta Contoh: jika ID peserta adalah 23, maka gunakan port 8023.
   a) Halaman website harus menampilkan "Hello World from Utara Site"
   b) Tambahkan HTTP header berikut:
      - X-Owner-By: diisi dengan nama peserta
      - X-Served-By: diisi dengan jenis web server (apache2)



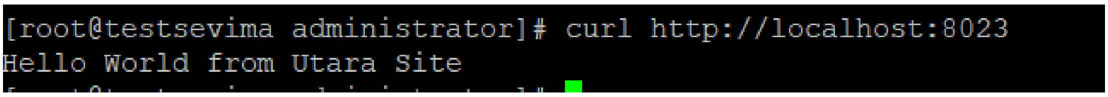
```
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 8023
```

Note: konfigurasi saya tulis 8023 karena saya tidak tau untuk nomor peserta nya maka dari itu saya mengikuti default yaitu 80+23



```
<VirtualHost *:8023>
    ServerName utara.sevima.site
    DocumentRoot /var/www/utara

    <Directory /var/www/utara>
        AllowOverride None
        Require all granted
    </Directory>

    Header set X-Owner-By "Wahyu Ristho Ramadhani"
    Header set X-Served-By "apache2"
</VirtualHost>
```

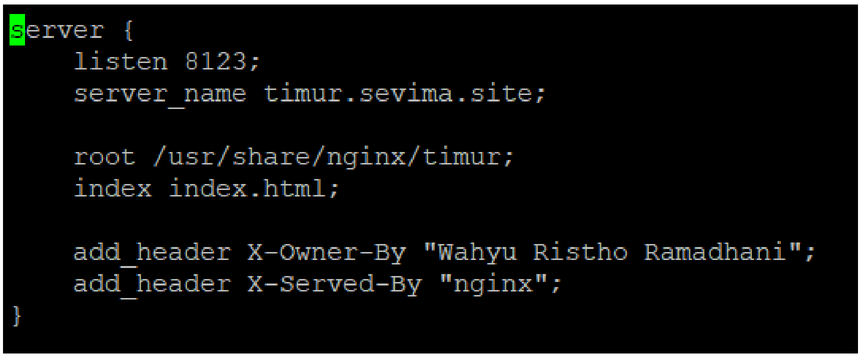
Hasil :



```
[root@testsevima administrator]# curl http://localhost:8023
Hello World from Utara Site
[root@testsevima administrator]#
```

2. Buat virtual host HTTP-only untuk melayani timur.sevima.site menggunakan nginx pada port 81 + ID peserta Contoh: jika ID peserta adalah 23, maka gunakan port 8123.
   a) Halaman website harus menampilkan "Hello World from Timur Site".
   b) Tambahkan HTTP header berikut:
      - X-Owner-By: diisi dengan nama peserta.
      - X-Served-By: diisi dengan jenis web server (apache2).

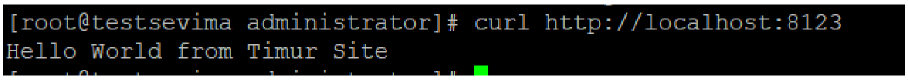
Konfigurasi :



```
server {
    listen 8123;
    server_name timur.sevima.site;

    root /usr/share/nginx/timur;
    index index.html;

    add_header X-Owner-By "Wahyu Ristho Ramadhani";
    add_header X-Served-By "nginx";
}
```

Note: konfigurasi saya tulis 8023 karena saya tidak tau untuk nomor peserta nya maka dari itu saya mengikuti default yaitu 80+23

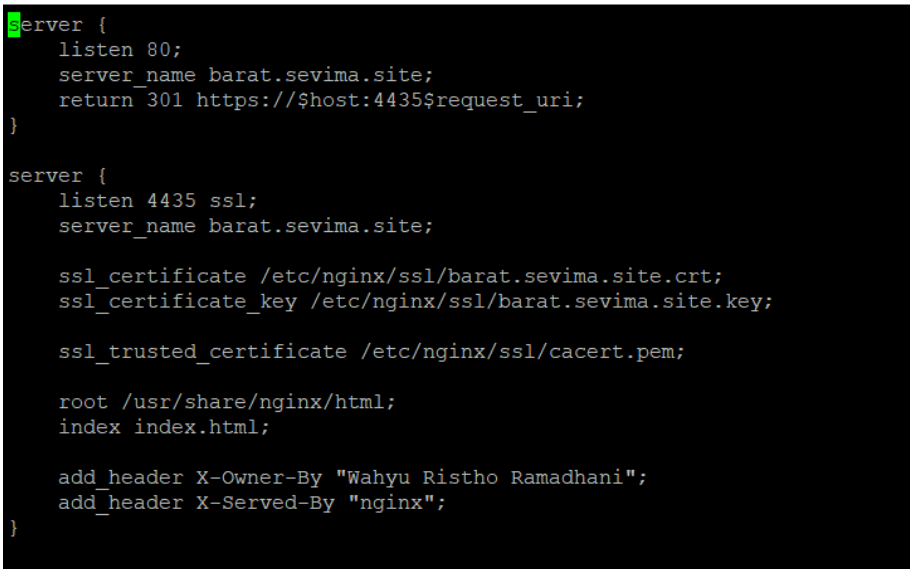
Hasil :



```
[root@testsevima administrator]# curl http://localhost:8123
Hello World from Timur Site
[root@testsevima administrator]#
```

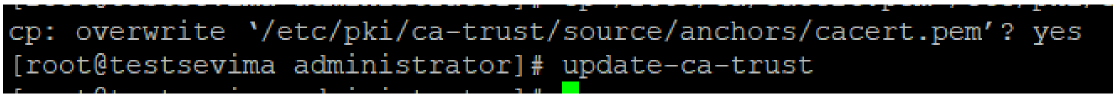
3. Buat virtual host HTTPS untuk melayani `barat.sevima.site` menggunakan nginx dengan port https angka acak (contoh: 4435).
   a) Aktifkan HTTPS menggunakan Certificate Authority dari SEVIMA CA.
   b) Redirect semua permintaan HTTP ke HTTPS.
   c) Pastikan localhost dan laptop kamu dapat mengakses tanpa peringatan apa pun.

Konfigurasi :



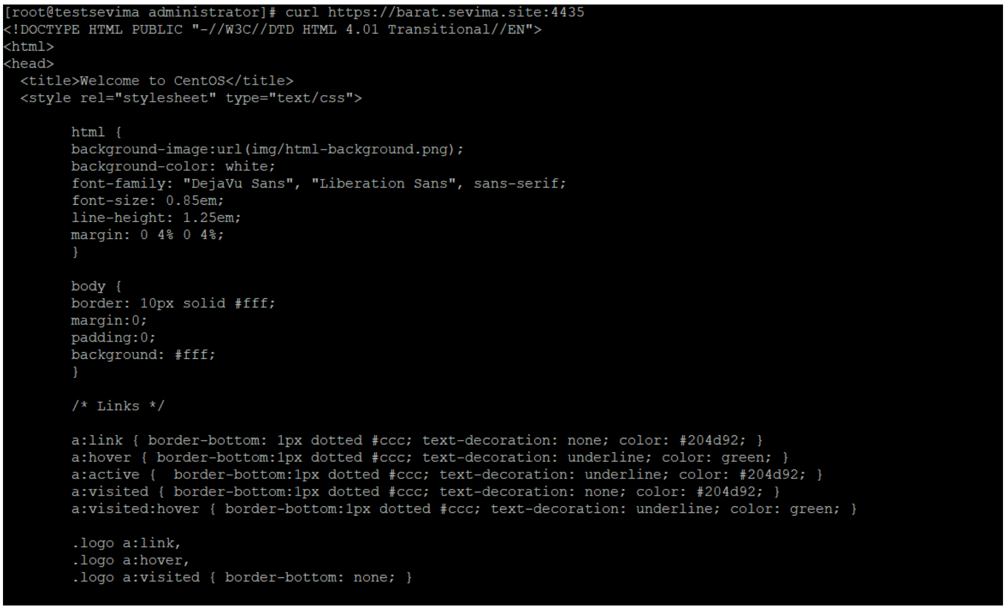
```
server {
    listen 80;
    server_name barat.sevima.site;
    return 301 https://$host:4435$request_uri;
}

server {
    listen 4435 ssl;
    server_name barat.sevima.site;

    ssl_certificate /etc/nginx/ssl/barat.sevima.site.crt;
    ssl_certificate_key /etc/nginx/ssl/barat.sevima.site.key;

    ssl_trusted_certificate /etc/nginx/ssl/cacert.pem;

    root /usr/share/nginx/html;
    index index.html;

    add_header X-Owner-By "Wahyu Ristho Ramadhani";
    add_header X-Served-By "nginx";
}
```

Update SSL ke VM



```
cp: overwrite '/etc/pki/ca-trust/source/anchors/cacert.pem'? yes
[root@testsevima administrator]# update-ca-trust
```

Hasil :

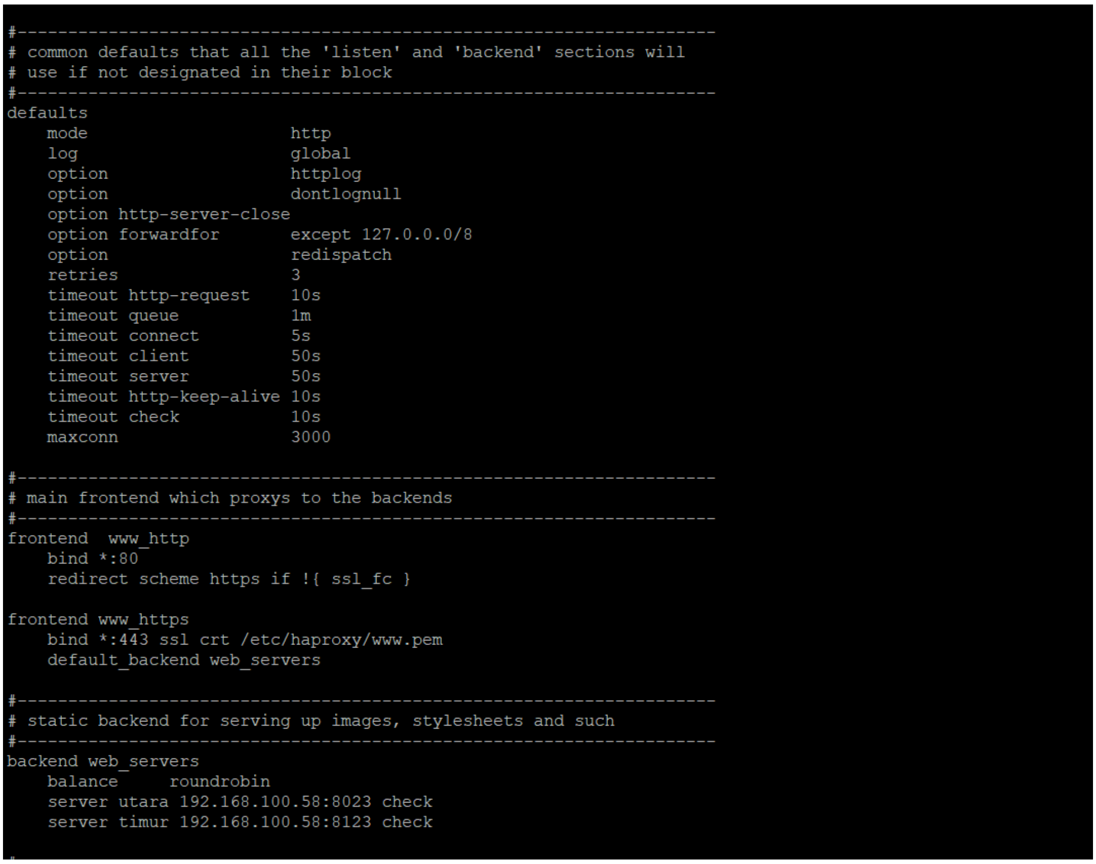


```
[root@testsevima administrator]# curl https://barat.sevima.site:4435
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
  <title>Welcome to CentOS</title>
  <style rel="stylesheet" type="text/css">

        html {
        background-image:url(img/html-background.png);
        background-color: white;
        font-family: "DejaVu Sans", "Liberation Sans", sans-serif;
        font-size: 0.85em;
        line-height: 1.25em;
        margin: 0 4% 0 4%;
        }

        body {
        border: 10px solid #fff;
        margin:0;
        padding:0;
        background: #fff;
        }

        /* Links */

        a:link { border-bottom: 1px dotted #ccc; text-decoration: none; color: #204d92; }
        a:hover { border-bottom:1px dotted #ccc; text-decoration: underline; color: green; }
        a:active {  border-bottom:1px dotted #ccc; text-decoration: underline; color: #204d92; }
        a:visited { border-bottom:1px dotted #ccc; text-decoration: none; color: #204d92; }
        a:visited:hover { border-bottom:1px dotted #ccc; text-decoration: underline; color: green; }

        .logo a:link,
        .logo a:hover,
        .logo a:visited { border-bottom: none; }
```

D. Load Balancer HAProxy

1) Konfigurasikan load balancer HTTP/HTTPS untuk www.sevima.site, yang dihosting oleh utara.sevima.site dan timur.sevima.site menggunakan apache2 dan nginx.
2) Gunakan sertifikat dari SEVIMA CA.
3) Gunakan algoritma round-robin.
4) Pastikan localhost dapat mengakses tanpa peringatan apa pun.

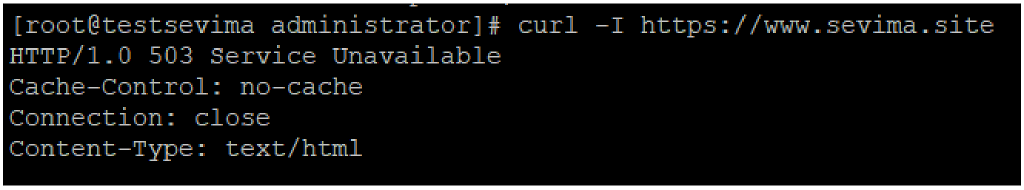
Konfigurasi :



```
#---------------------------------------------------------------------
# common defaults that all the 'listen' and 'backend' sections will
# use if not designated in their block
#---------------------------------------------------------------------
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option http-server-close
    option forwardfor       except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         5s
    timeout client          50s
    timeout server          50s
    timeout http-keep-alive 10s
    timeout check           10s
    maxconn                 3000

#---------------------------------------------------------------------
# main frontend which proxys to the backends
#---------------------------------------------------------------------
frontend  www_http
    bind *:80
    redirect scheme https if !{ ssl_fc }

frontend www_https
    bind *:443 ssl crt /etc/haproxy/www.pem
    default_backend web_servers

#---------------------------------------------------------------------
# static backend for serving up images, stylesheets and such
#---------------------------------------------------------------------
backend web_servers
    balance     roundrobin
    server utara 192.168.100.58:8023 check
    server timur 192.168.100.58:8123 check
```

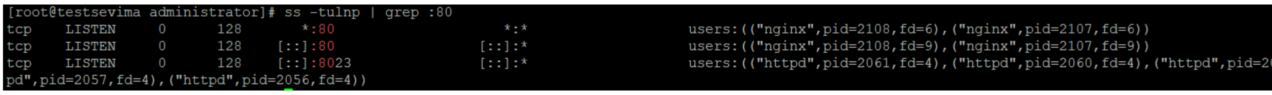
Hasil :

Jika service Nginx dan Httpd dimatikan haproxy tersebut berhasil running

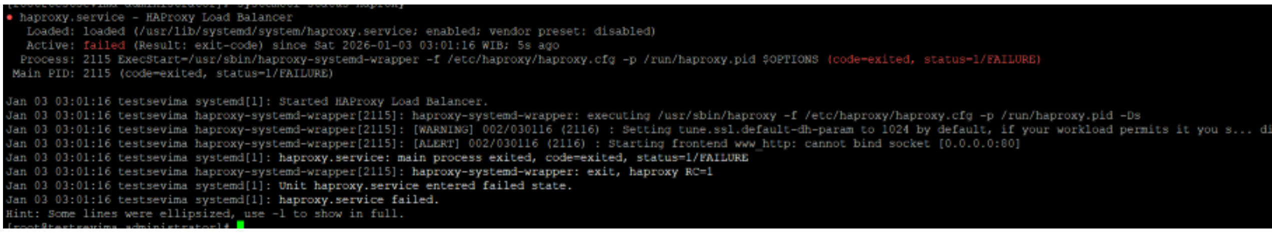


```
[root@testsevima administrator]# curl -I https://www.sevima.site
HTTP/1.0 503 Service Unavailable
Cache-Control: no-cache
Connection: close
Content-Type: text/html
```

Namun jika Nginx dan Httpd di start maka service haproxy bentrok antar port nya dan menyebabkan service mati



```
[root@testsevima administrator]# ss -tulnp | grep :80
tcp    LISTEN     0      128        *:80                  *:*                   users:(("nginx",pid=2108,fd=6),("nginx",pid=2107,fd=6))
tcp    LISTEN     0      128     [::]:80               [::]:*                   users:(("nginx",pid=2108,fd=9),("nginx",pid=2107,fd=9))
tcp    LISTEN     0      128     [::]:8023             [::]:*                   users:(("httpd",pid=2061,fd=4),("httpd",pid=2060,fd=4),("httpd",pid=2
pd",pid=2057,fd=4),("httpd",pid=2056,fd=4))
```



```
[root@testsevima administrator]# systemctl status haproxy
● haproxy.service - HAProxy Load Balancer
   Loaded: loaded (/usr/lib/systemd/system/haproxy.service; enabled; vendor preset: disabled)
   Active: failed (Result: exit-code) since Sat 2026-01-03 03:01:16 WIB; 5s ago
  Process: 2115 ExecStart=/usr/sbin/haproxy-systemd-wrapper -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid $OPTIONS (code=exited, status=1/FAILURE)
 Main PID: 2115 (code=exited, status=1/FAILURE)

Jan 03 03:01:16 testsevima systemd[1]: Started HAProxy Load Balancer.
Jan 03 03:01:16 testsevima haproxy-systemd-wrapper[2115]: haproxy-systemd-wrapper: executing /usr/sbin/haproxy -f /etc/haproxy/haproxy.cfg -p /run/haproxy.pid -Ds
Jan 03 03:01:16 testsevima haproxy-systemd-wrapper[2115]: [WARNING] 002/030116 (2116) : Setting tune.ssl.default-dh-param to 1024 by default, if your workload permits it you s... di
Jan 03 03:01:16 testsevima haproxy-systemd-wrapper[2115]: [ALERT] 002/030116 (2116) : Starting frontend www_http: cannot bind socket [0.0.0.0:80]
Jan 03 03:01:16 testsevima systemd[1]: haproxy.service: main process exited, code=exited, status=1/FAILURE
Jan 03 03:01:16 testsevima haproxy-systemd-wrapper[2115]: haproxy-systemd-wrapper: exit, haproxy RC=1
Jan 03 03:01:16 testsevima systemd[1]: Unit haproxy.service entered failed state.
Jan 03 03:01:16 testsevima systemd[1]: haproxy.service failed.
Hint: Some lines were ellipsized, use -l to show in full.
[root@testsevima administrator]#
```