Membuat SSL Certificate [Server Tanpa cPanel]

Bila proses **instalasi SSL Certificate pada server yang sudah dilengkapi dengan cPanel** dapat dilakukan dengan lebih mudah/instan, maka lain hal nya dengan server yang tidak menggunakan cPanel. Proses instalasi yang dilakukan lebih sulit, namun kami akan mencoba berbagi tips instalasinya kepada anda.

Langkah-langkah yang harus dilakukan dalam **instalasi SSL pada server tanpa cPanel**, adalah :

1. **Membuat Key dan Konfigurasi**
    - Pertama-tama, kita definisikan variabel-variabel ini agar tidak perlu terlalu mengulang-ulang:

```
$ export RANDFILE=/tmp/RANDFILE
$ export SERVERNAME=www.namadomain.xyz
$ dd if=/dev/urandom of=$RANDFILE bs=1k count=5
```

    - Selanjutnya kita membuat private key. Hasilnya nanti adalah file **SERVERNAME.key**.

```
$ openssl genrsa -rand $RANDFILE -out $SERVERNAME.key 2048
```

Catatan: rata-rata CA root mendukung hingga 1024 bit saja. Jika ingin dienkrip, tambahkan opsi **-des3** tapi umumnya tidak perlu.

    - Lalu buat **$SERVERNAME.conf**. Buatlah dengan mengkopi paste teks berikut ke teks editor (misal: **saya $SERVERNAME.conf**).

```
[ req ]
default_bits           = 2048
```

```
distinguished_name     = req_distinguished_name
attributes             = req_attributes
prompt                 = no

[ req_distinguished_name ]
C                      = ID
ST                     = DKI
L                      = Jakarta
O                      = PT Namadomain Dot Com
OU                     = IT Division
CN                     = secure.namadomain.xyz
emailAddress           = admin@namadomain.xyz

[ req_attributes ]
challengePassword      = somePassword
```

Penjelasan informasi dari **req_distinguished_name** di atas adalah sebagai berikut:

C: Country Name (2 letter code)
ST: State or Province
L: Locality
O: Organization Name
OU: Organizational Unit Name
CN: Common Name
emailAddress: Your Email Adress

2. Membuat CSR (Certificate Signing Request)

Buat certificate signing request (CSR). Hasilnya adalah **$SERVERNAME.csr** :

```
$ openssl req -x509 -new -key $SERVERNAME.key -out $SERVERNAME.csr -config $SERVERNAME.conf
```

Pembuatan CSR saja selesai pada langkah ini. lalu konfirmasikan CSR anda (.csr) kepada kami melalui Support Ticket.

Selanjutnya anda akan dikirimkan Email Approval untuk aktivasi SSL Certificate ke alamat email **admin@namadomain.xyz**, anda dapat langsung meng-approve email tersebut, setelah itu konfirmasikan kembali melalui Support Ticket.

3. Membuat Sertifikat

Setelah dikonfirmasikan bahwa anda telah meng-approve Email Approval tersebut, maka kami akan menginformasikan sertifikat SSLnya (**$SERVERNAME.crt**). Langkah berikutnya adalah membuat sertifikat SSL itu sendiri dengan cara :

- Buat sebuah file **/etc/apache2/sites-available/namadomain.xyz** yang isinya :

```
# catatan: diasumsikan IP utama server adalah 1.2.3.4
<VirtualHost 1.2.3.4:443>
  ServerName namadomain.xyz
  ServerAlias www.namadomain.xyz
  SSLEngine on
  SSLCertificateFile /etc/apache2/ssl/namadomain_xyz.crt
  SSLCertificateKeyFile /etc/apache2/ssl/namadomain_xyz.key
  <FilesMatch “\.(cgi|shtml|phtml|php3?)$”>
SSLOptions +StdEnvVars
  </FilesMatch>
  <Directory “/usr/lib/cgi-bin”>
    SSLOptions +StdEnvVars
  </Directory>
   CustomLog “|/c/bin/distlog –max-open-files=10 –no-dns –default-log /var/log/apache2/sslaccess.log –virtual-log /s/%0/syslog/https_access.%Y-%m-%d.log –distlog-log /var/log/apache2/distlog_sslaccess.log –distlog-loglevel 1” \
              “\”%{host}n\” %h %l %u %t \”%r\” %>s %b \”%{Referer}i\” \”%{User-Agent}i\””
ErrorLog “|/c/sbin/distlog_sslerror_log”
</VirtualHost>
```

:

Catatan: Jika webserver belum mendukung SNI, maka baris paling pertama :

<VirtualHost 1.2.3.4:443>

harus diganti mejadi:

NameVirtualHost 1.2.3.5:443
<VirtualHost 1.2.3.5:443>

di mana 1.2.3.5 adalah IP dedicated yang telah disiapkan dan berbeda dari IP utama server.

- Taruhlah file **namadomain_xyz.crt** dan **namadomain_xyz.key** ke direktori **/etc/apache2/ssl/** . Demi keamanan, pastikan ownership dan permission file-file tersebut adalah **(root,root,0600) (penting agar user biasa tidak bisa mencuri *.key)**. Lalu aktifkan site tersebut dan reload-lah Apache :

 # a2ensite namadomain.xyz
 # /etc/init.d/apache2 reload

Kadang terjadi apache yang gagal start karena kesalahan saat mengaktifkan situs dengan ssl ini. Solusinya adalah, matikan dulu apache lalu re-enable situs ssl yang dimaksud :

 # /etc/init.d/apache2 stop
 # a2dissite namadomain.xyz && /etc/init.d/apache2 reload
 # a2ensite namadomain && /etc/init.d/apache2 reload

- Langkah terakhir adalah mengarahkan A record **namadomain.xyz** (dan umumnya juga www.**namadomain.xyz**) ke IP 1.2.3.5. Jika tidak, **namadomain.xyz** defaultnya masih mengarah ke IP utama server (mis: 1.2.3.4) dan pengunjung situs masih akan mendapatkan sertifikat SSL default yang diinstal di IP 1.2.3.4, bukan di 1.2.3.5.

Perhatian: hati-hati jika melakukan copy paste, perhatikan nama direktif-direktifnya: **SSLCertificateFile vs SSLCACertificateFile vs SSLCertificateKeyFile**.

Jika masih terdapat permasalahan yang berhubungan dengan aktivasi SSL pada server tanpa cPanel, dapat dikonsultasikan kepada pihak pengelola server anda, atau kepada tim teknis kami melalui Support Ticket.

Semoga membantu ^.^