

Membuat Server Support SSL Multidomain dalam Satu Server

Oleh Adi Sumaryadi



SSL (Secure Socket Layer) saat ini sudah menjadi bagian yang tak terpisahkan dari sebuah website, sebagian kita mengenalnya dengan HTTPS atau HTTP yang berjalan dalam mode secure (aman). Jadi semua data yang dikirim ke server akan di enkripsi terlebih dahulu

SSL (Secure Socket Layer) saat ini sudah menjadi bagian yang tak terpisahkan dari sebuah website, sebagian kita mengenalnya dengan HTTPS atau HTTP yang berjalan dalam mode secure (aman). Jadi semua data yang dikirim ke server akan di enkripsi terlebih dahulu. Lalu bagaimana bila dalam satu server yang menggunakan webserver Apache terdapat banyak domain yang harus dipasang SSL. Berikut tutorialnya:

Pertama, ada beberapa aplikasi dasar yang harus disiapkan sebelum kita menggunakan SSL untuk multidomain, saya menggunakan fitur SNI. beberapa syarat yang harus dipenuhi antara lain:

- Apache harus diatas apache versi 2.2 keatas
- OpenSSL sudah terinstall
- Saya menggunakan Server debian 7 (whezee)
- Saya menggunakan SSL free dari Letscript

Sebelum melakukan konfigurasi pastikan mod_ssl sudah aktif untuk apache anda, caranya:
`a2enmod ssl`

Kemudian restart apache anda menggunakan

service apache2 restart atau */etc/init.d/apache2 restart*

Untuk setingan yang terdapat di */etc/apache/ports.conf* silahkan beberapa tambahan berikut ini:

```
NameVirtualHost *:80
Listen 80
<IfModule mod_ssl.c>
    NameVirtualHost *:443
    Listen 443
    SSLStrictSNIVHostCheck off
</IfModule>
```

Selanjutnya untuk setingan Virtual Host di */etc/apache2/site-enabled* adalah sebagai berikut untuk domain pertama:

```
<VirtualHost *:443>

    ServerAdmin    root@adisumaryadi.com
    DocumentRoot  /var/www/domain1.com/

    ServerName     domain1.com
    ServerAlias    www.domain1.com

    ErrorLog       /var/log/apache2/domain1.com-error.log
    TransferLog    /var/log/apache2/domain2.com-access.log

    <Directory //var/www/domain1.com/>
        Options Indexes Includes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        Allow from all
    </Directory>

    SSLEngine on
    SSLProtocol All -SSLv2 -SSLv3
    SSLHonorCipherOrder on
    SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
&lt;EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4 RC4"

    SSLCertificateFile /etc/letsencrypt/live/domain1.com/cert.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/domain1.com/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/domain1.com/chain.pem

</VirtualHost>
```

Sementara untuk setingan VirtualHost domain kedua atau selanjutnya adalah sebagai berikut:

```
<VirtualHost *:443>
```

```
ServerAdmin    root@adisumaryadi.com
DocumentRoot  /var/www/domain2.com/
```

```
ServerName    domain2.com
ServerAlias   www.domain2.com
```

```
ErrorLog      /var/log/apache2/domain2.com-error.log
TransferLog   /var/log/apache2/domain2.com-access.log
```

```
<Directory //var/www/domain2.com/>
```

```
Options Indexes Includes FollowSymLinks MultiViews
AllowOverride All
Order allow,deny
Allow from all
```

```
</Directory>
```

```
SSLEngine on
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
```

```
EECDH+ECDSA+SHA384
```

```
ECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4
```

```
EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4
RC4"
```

```
SSLCertificateFile /etc/letsencrypt/live/domain2.com/cert.pem
```

```
SSLCertificateKeyFile /etc/letsencrypt/live/domain2.com/privkey.pem
```

```
SSLCertificateChainFile /etc/letsencrypt/live/domain2.com/chain.pem
```

```
</VirtualHost>
```

Selamat mencoba, semoga berhasil

Kata Kunci : SSL Multidomain