Apache: SSL ne podržava višestruke virtualne hostove

Apache je jedan od najpopularnijih softvera za web servise, a taj status obično dolazi od činjenice da se takav softver razlikuje od drugih po tome što ima najviše mogućnosti, najfleksibilniji je i slično. U slučaju takvog softvera korisnici imaju dojam da je svemoguć, što naravno zna razočarati kad se dozna da to nije slučaj.

U slučaju Apacheja, to se najviše može vidjeti u činjenici da nije moguće imati više SSL virtualnih hostova, odnosno nije moguće preko HTTPS protokola pristupiti na nekoliko različitih adresa na istom poslužitelju.

Dakle, nije moguće istovremeno imati SSL adrese

https://nesto.institucija.hr

i

https://www.institucija.hr

Ovo, sasvim ozbiljno ograničenje, se može zaobići na nekoliko načina, no nažalost nijedan nije previše praktičan, no nije nemoguće za riješiti. Naravno, potrebno je nešto više iskustva u radu s nekim servisima i samim operativnim sustavom.

Razlog zašto je nemoguće imati više adresa, odnosno virtualnih hostova, leži u činjenici što se SSL nalazi na različitom mrežnom sloju od HTTP protokola, te ga enkapsulira unutar sebe. Ovo znači da nema "Host:" zaglavlja po kojemu se razlikuju virtualni hostovi, te nema mogućnosti da Apache zna o kojem se virtualnom hostu radi (obično se svodi na prvi definirani).

Postoji nekoliko načina rješavanja ovog problema.

1. Jedan SSL poslužitelj za sve potrebe

Ukoliko želite nekoliko servisa osigurati preko SSL-a, možete ih jednostavno staviti unutar nekog dediciranog virtualnog hosta, primjerice secure.institicija.hr:

https://secure.institucija.hr/webmail

ili

https://secure.institucija.hr/prijava

Ovo je najlakše za ostvariti, jer posebnog podešavanja i nema, potrebno je samo definirati jedan VHOST sa SSL-om, te u njegov DOCUMENT_ROOT stavljati webove koje želite zaštititi (ili ih symlinkati s neke druge lokacije). Tipičan izgled SSL VHOST-a, primjerice /etc/apache2/sites-available/ssl:

```
<IfModule mod_ssl.c>

# Since SSL has no NameVirtualHosts, and we don't support machines with
# multiple IP addresses yet, make this a simple default config.
```

```
<VirtualHost _default_:443>
    ServerAdmin admin@institucija.hr
    ServerName server.institucija.hr
    DocumentRoot /var/www/secure
    LogLevel warn
    ErrorLog /var/log/apache2/ssl-secure.institucija.hr-error.log
    CustomLog /var/log/apache2/ssl-secure.institucija.hr-access.log combined

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/secure.institucija.hr.crt
    SSLCertificateKeyFile /etc/ssl/private/secure.institucija.hr.key
    SSLCertificateChainFile /etc/ssl/certs/secure.institucija.hr.chain
    # Needed for older MSIE6 patch levels
    SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown

</VirtualHost>

</IfModule>
```

Kod definiranja ostalih VHOST-ova (koji nisu SSL), rabite ovaj oblik VirtualHost direktive:

```
NameVirtualHost 161.53.XXX.YYY:80
```

Druga dva načina su definiranje joše jedne adrese na mrežnom sučelju, ili stavljanje druge mrežne kartice u poslužitelj, te definiranje SSL VHOST-a na nekom drugom portu (default je 443).

2. druga IP adresa

Ako dodamo dodatnu mrežnu karticu na poslužitelj, ili kreiramo virtualno mrežno sučelje, možemo na novim IP adresama poslužitelja definirati drugi virtualni SSL host, zadržavajući *defaultni* port 443. Ipak, ukoliko vama niti vašim korisnicima nije problem koristiti drugi SSL port, lakši način je definirati SSL VHOST na drugom portu.

3. drugi port

Moguće je definirati virtualni host na drugom portu, ali tada je potrebno navoditi taj port u adresi. Tako primjerice umjesto jednostavnog:

https://webmail.institucija.hr

moramo navesti

https://webmail.institucija.hr:81

Port je naravno, proizvoljan, no pazite da ne uzmete neki koji je već u uporabi.

Za svaki SSL VHOST koji želite definirati stavite:

```
NameVirtualHost 161.53.XXX.ZZZ:81

<VirtualHost 161.53.XXX.ZZZ:81>
  ServerName some.domain.com
  # SSL i druge opcije
</VirtualHost>
```

Ipak, moramo reći da rješenje za više SSL hostova na jednoj adresi postoji, i to u vidu dodatnih modula, primjerice mod_gnutls [1]. Ovaj modul podržava SNI (Server Name Identification [2]) proširenja TLS-a, no još se vodi kao eksperimentalan, pa ga ne možemo preporučiti za uporabu na produkcijskom poslužitelju. Ukoliko ipak želite probati, pogledajte upute na http://www.der-eremit.de/post/13589628448/ssl-enabled-name-based-virtual-hosts-with-mod-gnutls [3].

Dodatno, ukoliko ste napravili certifikat s više FQDN-ova (ili wildcard certifikat, koji nije preporučljiv iz sigurnosnih razloga), *vjerojatno* ćete moći ostvariti da imate više SSL VHOST-ova. Kažemo "vjerojatno" jer neki su webmasteri prijavili da im ovakvo rješenje jednostavno ne radi. Nadalje, ukoliko niste naveli sve VHOST-ove u alt_names sekciji zahtjeva za certifikatom, morat ćete ponoviti cijelu proceduru i možda čak povući (*revokati*) stari certifikat. Na kraju, sve popularniji uređaji za surfanje - mobilni uređaji - najčešće ne podržavaju SNI, što bi nekima moglo biti dosta važno.

Nove inačice OpenSSL-a također obećavaju podršku za SNI (od inačice 0.9.8j koja nije u Lenny distribuciji), pa će problem višestrukih VHOST-ova na jednoj IP adresi vjerojatno biti trajno riješen.

čet, 2010-06-24 13:16 - Željko Borš**Kuharice:** Linux [5]
Kategorije: Servisi [6]
Vote: 0

Source URL: https://sysportal.carnet.hr/node/757

Links
[1] http://www.outoforder.cc/projects/apache/mod_gnutls/
[2] http://en.wikipedia.org/wiki/Server_Name_Indication
[3] http://www.der-eremit.de/post/13589628448/ssl-enabled-name-based-virtual-hosts-with-mod-gnutls
[4] https://sysportal.carnet.hr/sysportallogin
[5] https://sysportal.carnet.hr/taxonomy/term/17
[6] https://sysportal.carnet.hr/taxonomy/term/28