OCSP Stapling

Az SSL kapcsolatok sebességének növelése Apache, IIS és NginX szerverek esetén

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

1. Tartalomjegyzék

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

2. Bevezető

E tájékoztató célja, hogy a szerveréhez létrehozott SSL tanúsítvány használatának sebességét optimalizálhassa.

Kérjük, olvassa el figyelmesen és kövesse a leírtakat.

Amennyiben bármilyen kérdése vagy problémája van, Ügyfélszolgálatunk az (40) 22-55-22 telefonszámon, az info@netlock.hu e-mail címen vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

3. OCSP Stapling támogatással rendelkező webszerverek

Az alábbi szerverek rendelkeznek OCSP Stapling támogatással:

- NginX 1.3.7 és későbbi verziók
- Windows 2008 vagy későbbi szerveren IIS 7 és annak újabb verziói
- Apache 2.3 és későbbi verziók

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

4. Mi is az OCSP Stapling?

Az OCSP Stapling előnye a Stapling nélküli és a Stapling használatával történő működés bemutatásának különbségein keresztül érzékelhető.

4.1. Kapcsolat felépülése OCSP Stapling nélkül

A visszavonás ellenőrzés OCSP segítségével hagyományos esetben a következőképpen történik:

1. A kliens böngészője felveszi a kapcsolatot a webszerverrel
2. A kliens böngészője a megkapott tanúsítványt lekérdezi a tanúsítványkiadó szerverétől, OCSP vagy CRL esetében
3. Létrejön a kapcsolat…

Mint látható, minden kliens maga kommunikál a tanúsítványkiadóval, ami magas terhelés esetén a felhasználó számára hosszú válaszidőket eredményezhet a kliens oldalon.

4.2. Kapcsolat felépülése OCSP Stapling segítségével

Az OCSP Stapling kihasználja azt, hogy a kapcsolat kiépülésekor a már kiépített kapcsolaton keresztül akár a visszavonási információk lekérését is el lehet küldeni a kliens számára.

A visszavonás ellenőrzés OCSP segítségével hagyományos esetben a következőképpen történik:

Előkészítő lépés: a webszerver időnként letölti a tanúsítványához tartozó OCSP válaszokat, majd meghatározott időnként frissíti azt.

1. A kliens böngészője felveszi a kapcsolatot a webszerverrel
2. A webszerver elküldi az OCSP választ a kliens részére
3. Létrejön a kapcsolat…

Mint látható, a szerver gyakorlatilag „előre betárazza” az OCSP a választ, így

A KAPCSOLAT KIÉPÜLÉSÉNEK SEBESSÉGE TEHÁT NEM FÜGG KÜLSŐ SZERVERTŐL, EZÉRT AZ OCSP STAPLING BEÁLLÍTÁSA KÜLÖNÖSEN AJÁNLOTT!

5. Előzetes követelmények 1 – A tűzfalakon szükséges engedélyezés

Ahhoz, hogy az OCSP Stapling használható legyen, a szervezet tűzfalain a szerver számára engedélyezni kell a következő címek elérését.

http://www.netlock.hu

http://ocsp1.netlock.hu

http://ocsp2.netlock.hu

http://ocsp3.netlock.hu

Javasolt a fenti esetek DNS alapú beállítása, mert a szolgáltatások felhőbe költözése esetén az IP címek változhatnak.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

6. Előzetes követelmények 2 – A gyökértanúsítványok beszerzése

Ahhoz, hogy az OCSP Stapling működjön, egyes szervereken szükséges a gyökértanúsítványok és köztes tanúsítványok szerver számára elfogadható módon történő telepítése.

A tanúsítványok kiadója alapján szükséges a következők tanúsítványok letöltése. Mivel egyes böngészők ezt automatikusan megnyitják, a tanúsítvány letöltéséhez célszerű Internet Explorer-t használni.

Az egyes kiadók elérése a következő alfejezetben olvasható.

6.1. SHA 256 kiadók

Az SHA256 algoritmusú kiadók a következő URL-eken érhetők el.

Legfelső szintű kiadó:

Arany	(SHA256)	www.netlock.hu/index.cgi?ca=gold

Köztes szintű kiadó:

Közjegyzői	(SHA256)	www.netlock.hu/index.cgi?ca=caca
Üzleti	(SHA256)	www.netlock.hu/index.cgi?ca=cbca
Expressz	(SHA256)	www.netlock.hu/index.cgi?ca=ccca
OnlineSSL	(SHA256)	www.netlock.hu/index.cgi?ca=olsslgca

6.2. SHA 1 kiadók

Az SHA1 algoritmusú kiadók a következő URL-eken érhetők el.

Legfelső szintű kiadók:

Közjegyzői	(SHA1)	www.netlock.hu/index.cgi?ca=kozjegyzoi

6.3. Összes kiadó

Természetesen használható egy előre összeállított csomag is erre a célra, amely a következő címen érhető el (javasolt az netlock_osszes_auth_kiado.pem fájl használata a csomagból): http://www.netlock.hu/docs/letoltes/auth_kiadok_csomag.zip

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

7. Az Apache 2.3 és későbbi szerver verziók beállítása

Az Apache 2.3 vagy későbbi verziójú webszerver esetén az apache konfigurációs állományban a következőket kell megadni az OCSP Stapling bekapcsolásához:

1. A Szerveren ellenőrizzük, hogy az OpenSSL legalább 0.9.8h verziója legyen megtalálható, ha ez nem így van, akkor frissítsük azt. Az ellenőrzés elvégezhető a következő paranccsal.

   ```
   openssl –version
   ```

2. A szerver modul betöltő részéhez (általában a httpd.conf fájlban található ez a szakasz) adjuk hozzá a következő szakaszt:

   ```
   LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
   ```

   Ez a beállítás betölti a megfelelő modult. Ellenőrizzük, és szükség esetén telepítsük, ha nem található szerverünkön ez a modul.

3. A szerver SSL részt beállító szakaszához adjuk hozzá a következő bejegyzéseket:

   ```
   #stapling bekapcsolása, cache es cache timeout beallitasa
   SSLUseStapling On
   SSLStaplingCache shmcb:/path/to/datafile[(512000)]
   SSLStaplingStandardCacheTimeout 3600
   SSLStaplingResponseMaxAge 3600
   #a valaszado lekeres timeout beallitasa
   SSLStaplingResponderTimeout 30
   #hibas ocsp eseten a valasz timeoutja
   SSLStaplingErrorCacheTimeout 600
   #ha a szerver nem tud staplingolni, trylater-t küld a kliensnek
   SSLStaplingReturnResponderErrors on
   SSLStaplingFakeTryLater on
   ```

   A „/path/to/datafile” értéket helyettesítsük be, javasolt lehet a következő:

   ```
   /var/cache/mod_shmcb/stapcache
   ```

   Az útvonal és a fájl legyen létrehozva, jogosultsága legyen a webszerver jogosultságával egyező.

   A fentiek megadása és az Apache szerver újraindítása után az OCSP Stapling-nak működnie kell.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

8. Az NginX 1.3.7 és későbbi szerver verziók beállítása

Az Nginx 1.3.7 vagy későbbi verziójú webszerver esetén a konfigurációs állományban a következőket kell megadni az OCSP Stapling bekapcsolásához:

```
## OCSP Stapling
resolver 127.0.0.1;
ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate <file>;
```

- A Resolver értéke a DNS szerver értéke legyen, nem a példában szereplő 127.0.0.1, azaz localhost. Ha a gép tud DNS nevet feloldani, akkor megfelelő lehet a fenti példa is.
- Az SSL Stapling működéséhez és az ellenőrzéshez szükséges, hogy a szerverre a gyökér és köztes tanúsítványok telepítve legyenek.
- Az ssl_trusted_certificate esetén a fájl neve arra a fájlra kell, hogy mutasson, amely a gyökér- és köztes tanúsítványokat tartalmazza.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

9. Az IIS 7 és későbbi szerver verziók beállítása

Figyelem!

Az IIS 7 szervernek a sikeres beállításhoz Windows 2008 vagy későbbi szerveren kell futnia, és alapesetben az OCSP Stapling bekapcsolt állapotú.

Az IIS esetében a következő lépések szükségesek:

1. A legfelső szintű tanúsítványok telepítése a szerverre.
2. A köztes kiadó tanúsítványok telepítése a szerverre.

A tanúsítványok telepítésének lépései gyökértanúsítványok esetén

(Arany, SHA1 Közjegyzői, SHA1 Üzleti, SHA1 Expressz esetében):

1. Töltse le a kiadó gyökértanúsítványát a szerverre.
2. Telepítse MMC-vel az „Trusted Root Certification Authorities" tárolóba.
   (Ne felejtse el, hogy a Local Computer store-ba kell telepíteni. A függelék bemutatja az MMC használatát.)
3. A telepítés után szükség lehet az IIS újraindítására.

A tanúsítványok telepítésének lépései köztes (intermediate) tanúsítványkiadók esetén

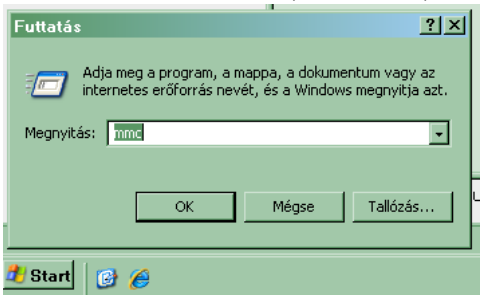
(SHA256 Közjegyzői, SHA256 Üzleti, SHA256 Expressz, SHA1 OnlineSSL, SHA256 OnlineSSL esetében):

1. Töltse le a köztes kiadó gyökértanúsítványát a szerverre.
2. Telepítse MMC-vel az „Intermediate Certification Authorities" tárolóba.
   (Ne felejtse el, hogy a Local Computer store-ba kell telepíteni. A függelék bemutatja az MMC használatát.)
3. A telepítés után szükség lehet az IIS újraindítására.

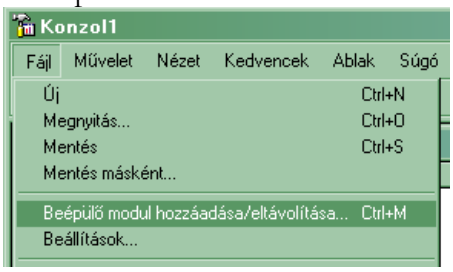
NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

10. Függelék A – Tanúsítvány kezeléséhez MMC konzol létrehozása, mentése Windows operációs rendszeren

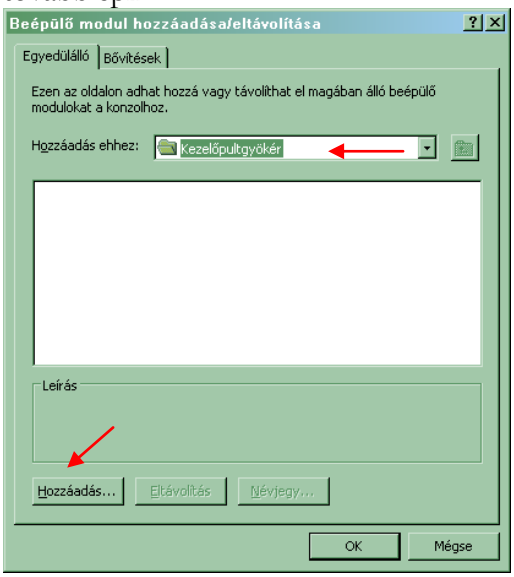
1. Indítsa el a Start menü / Futtatás / MMC parancsot.



2. A megjelenő konzolon a File menüből válassza a Beépülő modul hozzáadása/eltávolítása menüpontot.

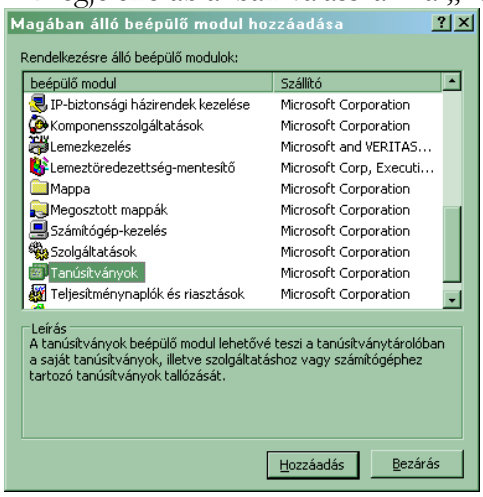


3. A következő ablakban a Kezelőpultgyökér -hez a Hozzáad… gomb megnyomásával kell továbblépni.

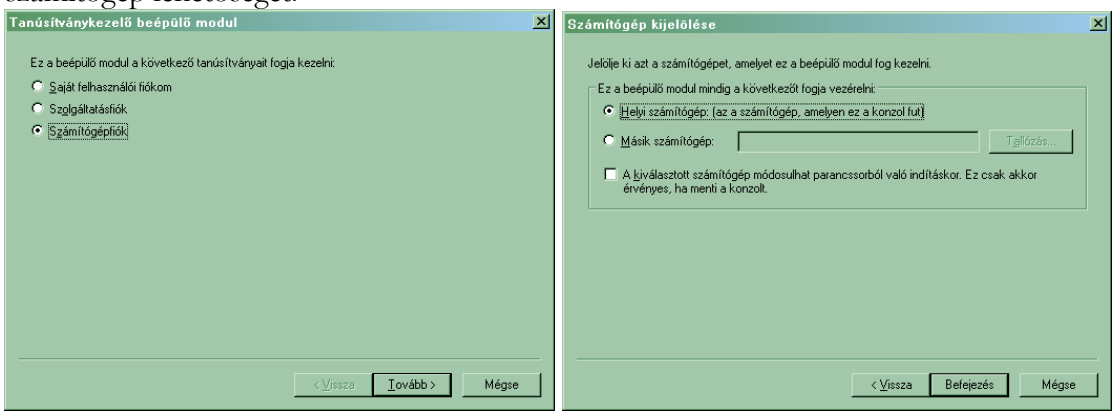


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

4. A megjelenő ablakban válassza ki a „Tanúsítványok” lehetőséget.



5. Ezután a megjelenő ablakban a Számítógépfiók lehetőséget kell választani, majd a Helyi számítógép lehetőséget.

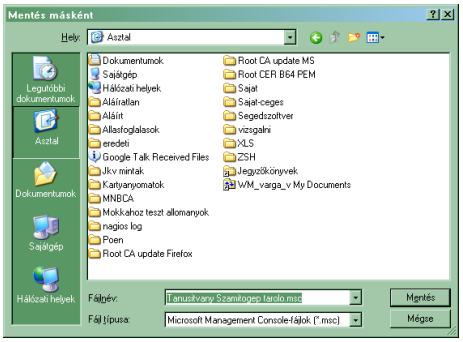


6. Ezt követően kattintson a Befejezés (Finish) gombra az ablak bezárásához.

Mentse el a létrejött panelt az alábbi lépések szerint.

1. Válassza a File / Mentés másként, majd adja meg a helyet, ahova menteni kívánja a konzolt.

2. Ezt követően az új ikonnal bármikor újraindíthatjuk a konzolt.



NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu