

Procedura pozyskania i instalacji certyfikatu SSL dla PostgreSQL 8.x

Spis treści:

Wstęp	2
Przygotowanie.....	2
Generowanie wniosku o certyfikat.....	2
Proces pobierania certyfikatu z CC Signet.....	3
Instalacja certyfikatu.....	3
Podsumowanie i uwagi.....	3

Wstęp

Jest to dokument, który pokaże Ci, jak poprawnie skonfigurować PostgreSQL 8.x, do zestawiania szyfrowanych połączeń w protokole SSL/TLS. Kolejne rozdziały pomogą Ci przejść przez wszystkie etapy tworzenia wniosku o certyfikat oraz instalacji certyfikatu. W efekcie będziesz mógł z łatwością zabezpieczyć swój serwer korzystając z certyfikatów wystawionych przez **Centrum Certyfikacji Signet**.

Przygotowanie

Zakładamy, że posiadamy bazę danych z obsługą SSL (jeżeli kompilujemy źródła bazy danych należy mieć włączoną opcję: **--with-openssl**). Możemy wtedy wystartować serwer z obsługą SSL ustawiając parametr **ssl** na **true** w pliku konfiguracyjnym **postgresql.conf**. Kiedy serwer startuje z tą opcją, szuka dwóch plików **server.key** i **server.crt** w katalogu z danymi. Te dwa pliki muszą zawierać odpowiednio klucz prywatny i certyfikat serwera. Jeśli klucz prywatny jest chroniony poprzez hasło, serwer zapyta o nie i nie wystartuje, aż do momentu jego poprawnego wprowadzenia. Serwer będzie przyjmował zarówno połączenia standardowe, jak i połączenia SSL na tym samym porcie.

Żeby wygenerować pliki **server.key** i **server.crt** potrzebny będzie nam pakiet OpenSSL.

Generowanie wniosku o certyfikat

Tworzymy katalog, w którym będziemy generowali wniosek CSR i przygotowujemy plik z certyfikatem, np.:

```
$ mkdir /tmp/certtmp
$ chmod 600 /tmp/certtmp
$ cd /tmp/certtmp
```

Tworzymy plik konfiguracyjny **postgres.cnf** dla OpenSSL. Zawartość pliku jest następująca:

```
[ req ]
default_bits           = 1024
default_keyfile        = server.key
distinguished_name     = req_distinguished_name

[ req_distinguished_name ]
commonName             = Nazwa podmiotu (nazwa serwera lub adres IP)
commonName_default    = localhost
emailAddress           = Adres Email
emailAddress_default   = postmaster@moja.domena.pl
```

Wykonujemy następujące polecenie generujące żądanie CSR:

```
$ openssl req -new -nodes -config postgres.cnf > postgres.csr
```

gdzie:

postgres.csr jest plikiem zawierającym żądanie wystawienia certyfikatu. Jego zawartość powinna wyglądać mniej więcej tak:

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIBfTCB5wIBADA+MRIwEAYDVQQDEwlsb2NhbGhvc3QxKDAmBgkqhkiG9w0BCQEW  
GXBvc3RtYXN0ZXJAbW9qYS5kb21lbmEucGwwZ8wDQYJKoZIhvcNAQEBBQADgY0A  
MIGJAoGBAMcfWcQ3T2dAE994qgzuniPNqcgqebb2YaE9ATkN6uIA9ZVspjxYqID7  
/JJcPsygteO12Aw0yLJdzq5aQrSEE6Sw14ZP5X8mBai4G+0W8Nomt/VGHYqXPYAK  
/q9N408GaMyaE10X6n71HUBBxCW/TmbFv+QcvPRizJ0hEZQmM6MJAgMBAAGgADAN  
BgkqhkiG9w0BAQQFAAOBgQDA3kqRWxH70Bakmlu7hhuu3UKgAMCpT/XbjkONQbps  
9peC92vT+xH40MlJRZGzin5RtVtWaumxyusrp0QrTxNPOPXNJtAu7712/lk1pG8T  
qPyo1c3k6tpB99SLSvfl+YAgqjSMJvXKSn8D9dtqHv6ctDAVkJyWpGrSUC5BlxoJ  
zg==  
-----END CERTIFICATE REQUEST-----
```

W wyniku polecenia jest też tworzony plik **server.key** który zawiera klucz prywatny w postaci niezaszyfrowanej.

Możemy sprawdzić poprawność wniosku następującym poleceniem:

```
$ openssl req -text -noout < postgres.csr
```

Proces pobierania certyfikatu z CC Signet

Następnym krokiem jest uzyskanie certyfikatu za pośrednictwem stron WWW Centrum Certyfikacji Signet (www.signet.pl). Otrzymany certyfikat zapisujemy w pliku server.crt.

Instalacja certyfikatu

Po uzyskaniu certyfikatu z CC Signet możemy przystąpić do jego instalacji w systemie PostgreSQL. W tym celu pobrany certyfikat i klucz prywatny kopiujemy do katalogu z danymi serwera:

```
$ cp server.crt $PGDATA/server.crt  
$ cp server.key $PGDATA/server.key
```

i zabezpieczamy plik certyfikatu i klucza przed niepowołanym dostępem:

```
$ chown postgres:postgres $PGDATA/server.*  
$ chmod 400 $PGDATA/server.*  
$ chattr +i $PGDATA/server.*  
$ rm -fr /tmp/certtmp
```

Po wykonaniu powyższych czynności możemy przystąpić do uruchomienia bazy danych z obsługą SSL.

Podsumowanie i uwagi

Powyższa procedura pozyskiwania certyfikatu i zabezpieczenia serwera PostgreSQL w wersji 7.x jest bardzo podobna do przedstawionej powyżej.