*PostGreSQL User Guide*

*Secure TCP/IP Connections with SSL*

Table of Contents

[Objective 2](#_Toc500496726)

[Prerequisites 2](#_Toc500496727)

[Process 3](#_Toc500496728)

[Create certificate 3](#_Toc500496729)

[Install certificate 5](#_Toc500496730)

[Configure PostGreSQL 5](#_Toc500496731)

[Remember 7](#_Toc500496732)

[Related documentation 7](#_Toc500496733)

# Objective

This document describes the installation process of a ssl encrypt connection.

The first part of the document describes the way to create a new VM on SG Cloud and to automatically create the corresponding PostgreSQL Server.

The second part of the document describes the operational process to complete the installation.

# Prerequisites

Search the Organisational Unit name.

This information is required to generate a CSR.

Ask customer for his billing CA.

This information is required to request a certificate on “MKT certification request portal”.

# Process

## Create certificate

#### Request a certificate

Certificate is provided by SAFE API. Documentation is here : [Requesting a Production Certificate](http://api.fr.world.socgen/docs/en/latest/api/tutorials/certificates/prod-csr.html#submitting-csr)

1. Download [manual\_req\_prompt.conf](https://secnet.fr.world.socgen/datas/OpenSSL/manual_req_prompt.conf) in your unix home
2. Connect to server

*ssh <target server name>*

1. Sudo as postgres

*sudo su - postgres*

1. Create a directory KEY in /home/postgres

*mkdir KEY*

*cd KEY*

1. Copy manual\_req\_prompt.conf in KEY directory

*cp /.users/mount/yourhome/manual\_req\_prompt.conf .*

1. Modify manual\_req\_prompt.conf
   1. uncomment the following line in [req\_ext] part

subjectAltName = DNS:foo,DNS:foo.fr.world.socgen

* 1. change foo with your server name

1. On an unix server (PAACT server or target server) launch the following command:

|  |
| --- |
| openssl req -config manual\_req\_prompt.conf -new -keyout <target server name>.key -out <target server name>.csr |

1. Fill in the requested fields helping [iAppli](https://iappli.fr.world.socgen/iappli/login.jsp) or [wwwdba](https://wwwdba.fr.world.socgen/):

|  |
| --- |
| Common Name []:<target server name>.fr.world.socgen  Organisational Unit [MKT]:SGCIB-SEC  Organisation [GROUPE SOCIETE GENERALE]:GROUPE SOCIETE GENERALE  Locality [Paris]:Paris  State [Ile de France]:Ile de France  Country [FR]:FR |

two files are generated in current KEY directory

<target server name>.key and <target server name>.csr

1. Open url <https://secnet.fr.world.socgen/pages/tools/unipass.php> and fill the fields

You can find help in [iAppli](https://iappli.fr.world.socgen/iappli/login.jsp) or [wwwdba](https://wwwdba.fr.world.socgen/) to fill the fields

|  |
| --- |
| **APPLICATION IDENTIFICATION** |
| iAppli = 167578  Application Name = ARM ACTIVITY RISK MONITORING FOR SEGL  Application Trigram = ARM  Application Manager = denis.duyck ( sesame login : firstname.lastname )  Billing CA = 16476 CA DCC/SGL : 3000316476 les 5 derniers chiffres  Application department = ITEC/DCC/SGL |
| **TECHNICAL CONTACT** |
| login = lionel.fremondiere ( sesame login : firstname.lastname )  Email = list.par-resg-gts-mkt-gdi-postgresql@sgcib.com  Service Now Group = gts\_emea\_gdi\_chg\_mng |
| TECHNICAL DATA |
| Certificate Signing Request (CSR) ( <target server name>.csr content )  -----BEGIN CERTIFICATE REQUEST-----  MIIDVDCCAjwCAQAwgZExJDAiBgNVBAMTG2FybWRldmRiMDAxLmZyLndvcmxkLnNv  Y2dlbjESMBAGA1UECxMJU0dDSUItU0VDMSAwHgYDVQQKExdHUk9VUEUgU09DSUVU  RSBHRU5FUkFMRTEOMAwGA1UEBxMFUGFyaXMxFjAUBgNVBAgTDUlsZSBkZSBGcmFu  Y2UxCzAJBgNVBAYTAkZSMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA  ncLZXg/Zrgvs6NGudH5+X4lVs7JEIvONsTXHDectpHezZYs0PDLPMX2aqGfzdsG3  p+/tkFaU6eoLAC2LAXU2crPVPT7KTwQohs/gOo4OvThw80QmJkGse+5b/vkmVnhj  o23Cc1ygEzTHwlYv5PHIeBgWXxd2OdEr8l7Z9eg8fajK0hc+VN/M+jeUSVNGqLjK  tN1/pozNfVbogoBJOVdQFPKIQN0aO6gbI4jdCeJyLqk5mg6A5ILKkyqJtl7t+f40  Rk6MnW8vXyQitIIeBkV2UIxk+03xgp89hAI1tQyVO2YEX8nw/insHSLtMJQJSens  m8e6h0BC36N+Uf46QD9jLQIDAQABoH0wewYJKoZIhvcNAQkOMW4wbDAJBgNVHRME  AjAAMAsGA1UdDwQEAwIF4DAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw  MwYDVR0RBCwwKoILYXJtZGV2ZGIwMDGCG2FybWRldmRiMDAxLmZyLndvcmxkLnNv  Y2dlbjANBgkqhkiG9w0BAQUFAAOCAQEAm7Do93sUhMlvcK9yMxIQ1JMPs5aul1RI  Ax+eMTFdO8bD36YzeSxKNrLvEh4xYNEJZNVfWTSvYNxdFIZdiNI+JwuVIcir/ZCl  XnE4sz1Wbu5lU81mo/VVrCu3E0T5zPKtYjULsbIxA4oglaqa+jOFgZkECz8REAPM  ztaYlFObzcZ+LCdPqXIpthzbCK8mvq8fpdSnIGgC8bDigRqjgzGyo+L/DIii0bEu  i2y2a0a6b0Pu8a0OidrUSZpve8Nk7u0k9/pgPrtO/b8Hr17IAXYpuNoEukuSk4v+  H3mkL5fBu2eqsGH4PXmPqdWs+1iVp9+LKtKEWpG/HY9vI2Zqqy82/A==  -----END CERTIFICATE REQUEST----- |

1. Clic on verify
2. If verify submit has been done, clic on Send button.

You should see that



#### Receive certificate

You receive several email by the process

* [UniPass][SHA2] Step 1/4 Reception of your certificate request for 123456
* [UniPass][SHA2] Step 2/4 Approbation of your certificate request for 123456
* [UniPass][SHA2] Step 4/4 Certificate of the new instance / Certificat de la nouvelle instance. / <target server name>.fr.world.socgen / 5a1801def2bb37.12345678

Step 3/4 is integrated in Step 4/4 as Step 3/4 is the reception of certificate and Step 4/4 is implementation.

## Install certificate

1. You receive 3 files ( file.txt ; file.cer ; file.p7b ) by email
2. Copy file.cer to your unix home directory
3. Connect to server

*ssh <target server name>*

1. Sudo as postgres

*sudo su - postgres*

1. From directory KEY copy <target server name>.key in $PGDATA

*cd KEY*

*cp <target server name>.key $PGDATA*

1. Copy file.cer to $PGDATA\<target server name>.crt

*cp /.users/mount/yourhome/file.cer $PGDATA\<target server name>.crt*

1. Apply security on both files

*chmod 600 <target server name>.crt <target server name>.key*

## Configure PostGreSQL

#### Enable SSL connections for Postgres

1. Edit file postgresql.conf in $PGDATA
   1. In the following part : listener process configuration
   2. Uncomment line #ssl=true
   3. Just after this line, add the following lines with adequate path

* ssl\_cert\_file = '/<hostname>/postgres/<clustername>/<target server name>.crt'
* ssl\_key\_file = '/<hostname>/postgres/<clustername>/<target server name>.key'

#### Restrict to SSL connections

1. Edit file pg\_hba.conf
2. In section # IPv4 remote secured connections:
   1. Comment the following line

*#host all all 0.0.0.0/0 md5*

* 1. Add the following

*hostssl all all 0.0.0.0/0 md5*

#### Reload config settings

By shell command : */usr/bin/pg\_ctl reload*

or

By sql command : *SELECT pg\_reload\_conf();*

#### Test SSL

*psql --host=<host name>.fr.world.socgen --port=5433 --user=<user name> --password --dbname=<database name>*

You should see :

SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)

#### Restart PostgreSQL (in case)

*pg\_ctl stop*

*pg\_ctl start*

# Remember

Service Now group :

* gts\_emea\_gdi\_chg\_mng

email in Technical Contact part for MKT certification request

* Par-Resg-Gts-Mkt-Gdi-Postgresql [list.par-resg-gts-mkt-gdi-postgresql@sgcib.com](mailto:list.par-resg-gts-mkt-gdi-postgresql@sgcib.com)
* Par-Resg-Gts-Mkt-Gdi-Mssql [PAR-RESG-GTS-MKT-DBA-Mssql@sgcib.com](mailto:PAR-RESG-GTS-MKT-DBA-Mssql@sgcib.com)
* Par-Resg-Gts-Mkt-Gdi-Sybase [PAR-RESG-GTS-MKT-DBA-Sybase@sgcib.com](mailto:PAR-RESG-GTS-MKT-DBA-Sybase@sgcib.com)

# Related documentation

<https://www.postgresql.org/docs/9.6/static/ssl-tcp.html>

<https://www.postgresql.org/docs/9.6/static/auth-pg-hba-conf.html>

<https://gosane.fr/mettre-en-place-ssl-pour-postgresql/>

<http://api.fr.world.socgen/docs/en/latest/api/tutorials/certificates/prod-csr.html#submitting-csr>  
<https://secnet.fr.world.socgen/pages/tools/unipass.php>  
<https://sbc.safe.socgen/docs/DOC-185301>