

Sécurisation de l'accès à PostgreSQL

Un client peut souhaiter ouvrir un accès sur son PostgreSQL à partir d'un poste autre que celui du serveur (BI, requêtage, Jasper Studio, etc..). Afin de gérer ce type accès, une documentation complète est disponible sur le sujet :

[Procédure Technique 1Life - Configuration réseau jasper - formation](#)

Les commandes `openprod-config-jasper` & `postgres-config` ont été réécrites dans ce sens.

Commande open-config-jasper

La commande `openprod-config-jasper` permet d'ouvrir l'accès de PostgreSQL à des utilisateurs externes (Power BI, Jasper Studio, etc...). Elle permet de prendre en compte une nouvelle adresse IP et ce, même si le serveur Jasper est installé sur le serveur Open-Prod (config mono serveur).

```
openprod@openprod-028t:~$ openprod-config-jasper
Récupération de l'IP du serveur Jasper.
Attention, les services PostgreSQL peuvent être redémarrés durant l'opération : n'exécutez ce traitement que lorsque la base de données est le moins sollicitée possible ou lors d'une période hors production !
Voulez-vous Continuer ?
Appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
O
Une installation locale de Jasper a été détectée sur ce serveur !
Voulez-vous autoriser une autre adresse IP à se connecter ?
Appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
N
Configuration /etc/postgresql/12/main/pg_hba.conf
Configuration /etc/postgresql/12/main/postgresql.conf
```

Au lancement de la commande, le programme détecte si Jasper est installé localement et propose d'autoriser une autre adresse IP. En répondant « N » à la question « Voulez-vous autoriser une autre adresse IP », le programme se contente de vérifier que le serveur Jasper local a les bons droits dans les fichiers et se termine.

```
openprod@openprod-028t:~$ openprod-config-jasper
Récupération de l'IP du serveur Jasper.
Attention, les services PostgreSQL peuvent être redémarrés durant l'opération : n'exécutez ce traitement que lorsque la base de données est le moins sollicitée possible ou lors d'une période hors production !
Voulez-vous Continuer ?
Appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
O
Une installation locale de Jasper a été détectée sur ce serveur !
Voulez-vous autoriser une autre adresse IP à se connecter ?
Appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
O
Indiquer l'IP du serveur que vous souhaitez autoriser à se connecter sur PostgreSQL : 192.168.10.55
Configuration /etc/postgresql/12/main/pg_hba.conf
Configuration /etc/postgresql/12/main/postgresql.conf
openprod@openprod-028t:~$
```

En répondant « O » à la question « Voulez-vous autoriser une autre adresse IP », le programme demandera de saisir l'adresse IP souhaitée et implémentera automatiquement le fichier `pg_hba.conf`.

```
# "local" is for Unix domain socket connections only
local    all             all                                md5
# IPv4 local connections:
host     all             all                                127.0.0.1/32      md5
# IPv6 local connections:
host     all             all                                ::1/128          md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local    replication     all                                peer
host     replication     all                                127.0.0.1/32      md5
host     replication     all                                ::1/128          md5
host     all             all                                192.168.10.0/24   md5
```

Commande postgres-config

Initialement prévue pour ouvrir tous sous-réseaux à l'accès PostgreSQL (0.0.0.0/0), la commande a été remaniée afin de limiter les accès sur PostgreSQL. Elle demande à présent le sous-réseau que l'on souhaite autoriser.

```
openprod@openprod-u20t:~ $ postgres-config
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Attention, vous êtes en train d'autoriser d'autre sous-réseaux à accéder à PostgreSQL !
Pour un accès plus restreint, privilégier la commande openprod-config-jasper
Voulez vous Continuer ?
Appuyez sur la touche O pour "Oui" ou sur la touche N pour "Non" :
O
Indiquez le sous-réseau désiré sous la forme 192.168.10.0, 10.0.0.0, ou 0.0.0.0 pour tous les sous-réseaux : 192.168.10.0
[sudo] Mot de passe de openprod :
openprod@openprod-u20t:~ $
```

Résultat :

```
# Allow replication connections from localhost, by a user with the
# replication privilege.
local    replication     all                                peer
host     replication     all                                127.0.0.1/32      md5
host     replication     all                                ::1/128          md5
# PostgreSQL open config by MyFab 192.168.10.0
host     all             all                                192.168.10.0/24   md5
```

Dans la mesure du possible, tendre à réduire au maximum le nombre d'utilisateurs pouvant avoir accès à PostgreSQL depuis le réseau. Une bonne connaissance du contexte réseau (VPN, adresse IP publique/locale, etc..) du client reste nécessaire. Le client doit toujours avoir conscience que toutes IP définies dans ce fichier peut avoir accès à PostgreSQL en dehors de l'ERP.

Revision #2

Created 18 April 2023 08:23:17 by Alexis CHAPEL

Updated 19 April 2023 05:15:22 by Alexis CHAPEL