

Aktualizacja bazy danych PostgreSQL do wersji 12 lub nowszej

1. Hasła scram-sha-256 lub md5

Od wersji 12 PostgreSQL domyślnie ustawia wartość dla hasel:

```
password_encryption = scram-sha-256
```

Po ustawieniu hasel w PostgreSQL wygląda to następująco:

username	usesysid	usecreatedb	usesuper	userepl	usebypassrls	
http	16385	f	f	f	f	SCRAM-SHA-256\$4096:D1NPKy+ZDiGGF1/E8q5M/g==\$kD4a
edokumenty	16384	f	f	f	f	SCRAM-SHA-256\$4096:9Q2v9SU06DQ2bHV/tCu1XA==\$GqC
postgres	10	t	t	t	t	SCRAM-SHA-256\$4096:2gkT6r1hnnvIWi9K5L403Q==\$J3bm

Jeśli wykonujemy pg_upgradecluster z wersji gdzie domyślnie korzystaliśmy szyfrowania md5. Do nowego PostgreSQL zostanie przeniesione to samo ustawienia. Dlatego jeśli chcemy przejść na scram-sha-256 należy zmienić ustawienie w PostgreSQL

```
vim /etc/postgresql/12/main/postgresql.conf
password_encryption = scram-sha-256
:wq
```

A następnie restart usługi postgresql

Po zalogowaniu os psql wykonać polecenie

```
SELECT
  rolname, rolpassword ~ '^SCRAM-SHA-256\$$' AS has_upgraded
FROM pg_authid
WHERE rolcanlogin;
```

Jeśli zwróci nam FALSE, konieczne będzie zmiana hasła np:

```
ALTER user postgres with encrypted password 'hasło';
```

Zmiana konfiguracji pg_hba.conf

```
vim /etc/postgresql/13/main/pg_hba.conf
```

```
# "local" is for Unix domain socket connections only
local edokumenty edokumenty scram-sha-256
local edokumenty http scram-sha-256
```

2. Konfiguracja pgbouncer

Zmiana konfiguracji w przypadku skorzystania z szyfrowania scram-sha-256 została opisana tym artykule

<http://support.edokumenty.eu/trac/wiki/AdminGuide/pgbouncer>