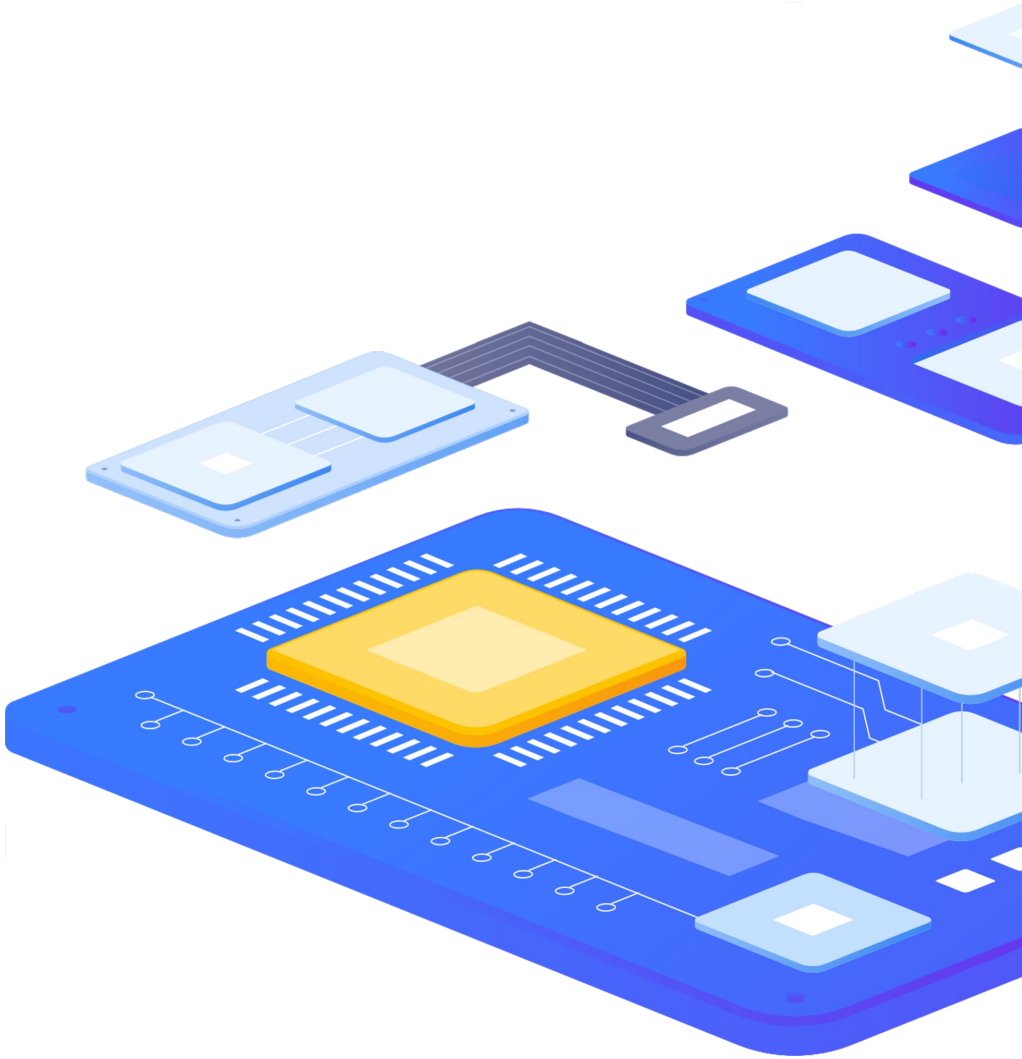
initMAX

Řízení přístupu do PostgreSQL prostřednictvím externího autentizačního providera

initMAX

Úvod

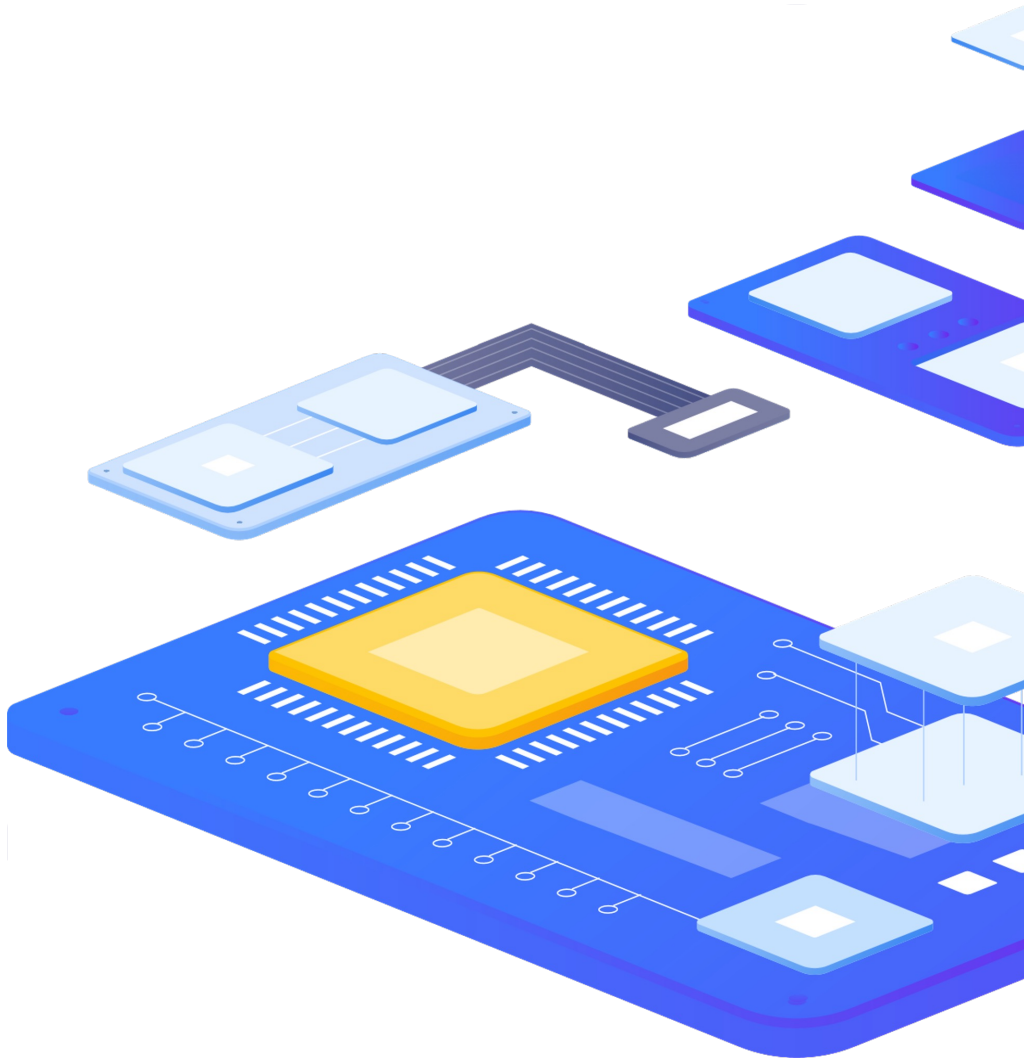
- PostgreSQL podporuje 11 metod ověřování, přičemž mezi základní patří:
  - **Trust authentication**, která jednoduše věří, že uživatelé jsou ti, za které se vydávají.
  - **Password Authentication,** která vyžaduje, aby se uživatelé ověřili heslem.
  - **LDAP Authentication**, která se spoléhá na ověřovací server LDAP.
  - **PAM authentication,** která se spoléhá na knihovnu PAM (Pluggable Authentication Modules).
  - **Certificate authentication**, která vyžaduje připojení SSL a ověřuje uživatele kontrolou obdrženého certifikátu SSL.
  - **GSSAPI authentication**, která se spoléhá na knihovnu kompatibilní s GSSAPI. Obvykle se používá k přístupu k autentizační službě, jako je FreeIPA nebo Microsoft Active Directory a využívá protokol Kerberos.



initMAX

Úvod

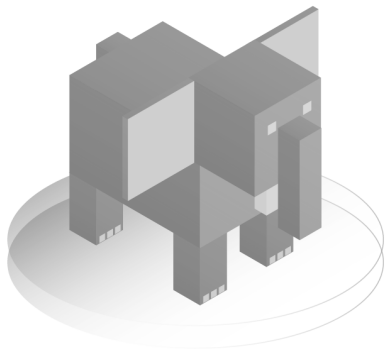
- Co je Kerberos, jak funguje a proč je dobré ho používat
  - Kerberos je síťový autentizační protokol, který slouží pro bezpečné ověření klienta i serveru
  - Klient se ověřuje vůči třetí straně - KDC (Key Distribution Center)
  - Po síti se neposílají žádná hesla, ani nejsou uložena lokálně u klienta
  - Využívá se silných šifrovacích algoritmů
  - KDC je centrálním prvkem a může poskytovat služby mnoha aplikacím a klientům
  - Přístupy lze řídit z jednoho místa
  - **Nefunkčnost centrální ověřovací služby může ovlivnit fungování více systémů**



initMAX

Řízení přístupu do PostgreSQL prostřednictvím externího autentizačního providera

1. Autentizace a žádost o ticket
2. Odeslání Session Key a TGT
3. Žádost o ServiceTicket
4. ServiceTicket



PostgreSQL Client

6. Ověření

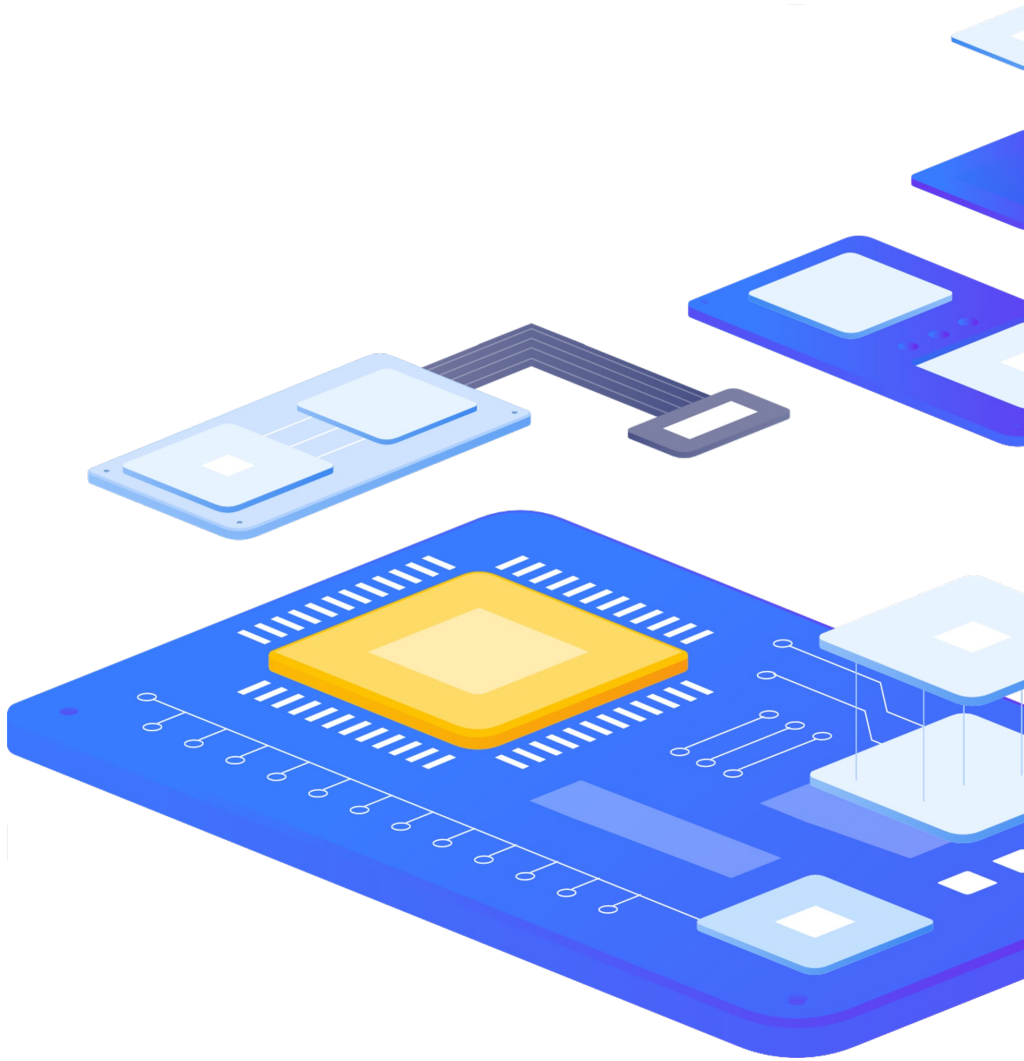
PostgreSQL Server

5. ServiceTicket a požadavek na autentizaci
7. Potvrzení a navázání spojení

initMAX

Základní požadavky

- Nainstalovaný databázový server PostgreSQL
- Podpora a konfigurace pro Kerberos na DB serveru
  - krb5-workstation a krb5-server
  - /etc/krb5.conf
- Uživatelský účet v Active Directory pro PostgreSQL
- Vygenerovaný keytab pro DB server
- Konfigurace PostgreSQL
  - pg_hba.conf
  - postgresql.conf
- Uživatelský účet v PostgreSQL s požadovanými právy
- Kerberos ticket pro DB uživatele (Active Directory nebo kinit)



initMAX

Podpora a konfigurace Kerberos na DB serveru

- Na serveru musí být nainstalované potřebné knihovny a musí být nastavená podpora pro Kerberos
- Instalace potřebných balíčků

```
dnf install krb5-server krb5-workstation
```

- Konfigurace podpory Kerberosu pro klienta
  - Úprava souboru /etc/krb5.conf viz. ukázka
  - Úpravu musí provádět uživatel root

```
[logging]
    default = /var/log/krb5libs.log
    kdc = /var/log/krb5kdc.log
    admin_server = /var/log/kadmind.log

[libdefaults]
    default_realm = DEMO.INITMAX.CZ
    dns_lookup_realm = false
#    ticket_lifetime = 24h
#    renew_lifetime = 7d
    forwardable = true
    udp_preference_limit = 1
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
DEMO.INITMAX.CZ = {
     kdc = demo.initmax.cz
     admin_server = demo.initmax.cz
}

[domain_realm]
.demo.initmax.cz = DEMO.INITMAX.CZ
demo.initmax.cz = DEMO.INITMAX.CZ
```

initMAX

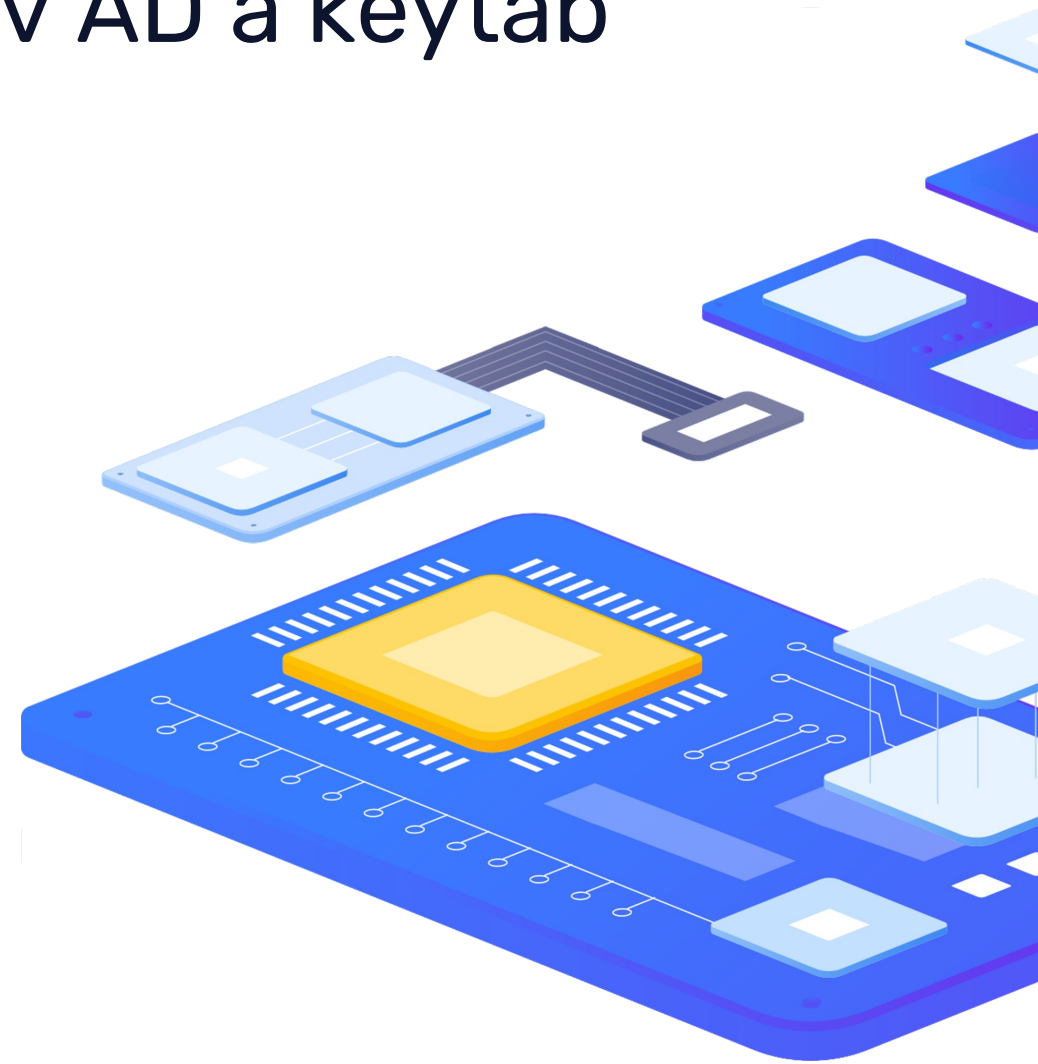
Uživatelský účet pro DB server v AD a keytab

- V Active Directory vytvoříme servisní účet pro databázový server – například pg_db_srv01
- Dále musíme vygenerovat na Active Directory serveru **Kerberos keytab** svázaný s účtem z předešlého kroku

```
ktpass –princ POSTGRES/pgsql.demo.initmax.cz@DEMO.INITMAX.CZ –pass heslo –mapuser pg_db_srv01
-crypto ALL –ptype KRB5_NT_Principal –out pgsql.demo.initmax.cz.keytab
```

- Takto získaný keytab nakopírujeme na DB server například do složky /etc
- A můžeme ověřit jeho funkčnost na PotgreSQL serveru

```
kinit -k -t /etc/pgsql.demo.initmax.cz.keytab POSTGRES/pgsql.demo.initmax.cz@DEMO.INITMAX.CZ -V
Using existing cache: 0
Using principal: POSTGRES/pgsql.demo.initmax.cz@DEMO.INITMAX.CZ
Using keytab: /etc/pgsql.demo.initmax.cz.keytab
Authenticated to Kerberos v5
```



initMAX

Konfigurace PostgreSQL

- V konfiguračním souboru PostgreSQL serveru upravíme parametr **krb_server_keyfile**

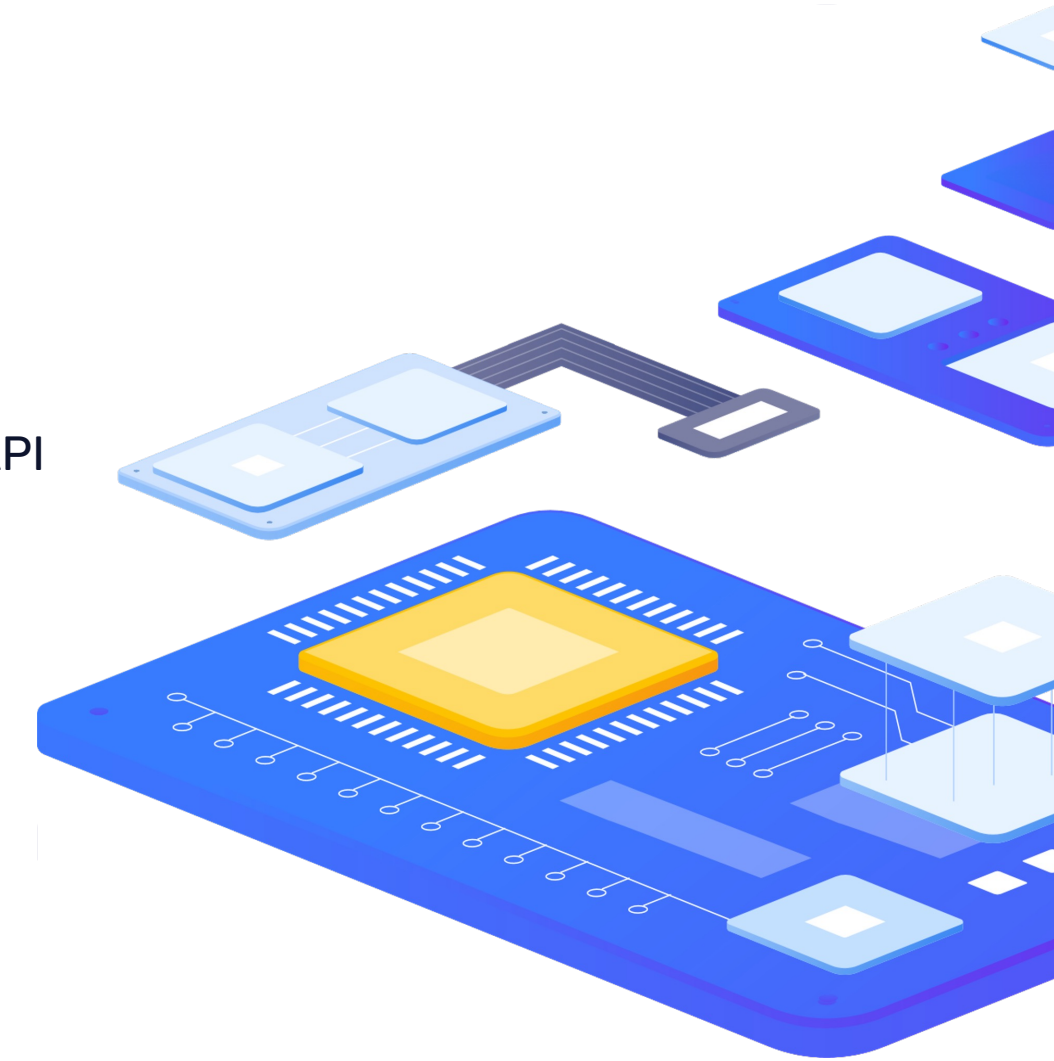
```
krb_server_keyfile=/etc/pgsql.demo.initmax.cz.keytab
```

- V souboru **pg_hba.conf** povolíme přihlašování metodou GSSAPI

```
# IPv4 local connections:
#host   all   all   127.0.0.1/32   ident
host   all   all   0.0.0.0/0       gss include_realm=0 krb_realm=DEMO.INITMAX.CZ
```

- A vytvoříme uživatele v PostgreSQL
  - Uživatel musí odpovídat skutečnému uživateli v AD

```
pgsqldemo=# create user "ad_user" superuser;
```



initMAX

Přihlášení do PostgreSQL

- Získání ticketu z Active Directory

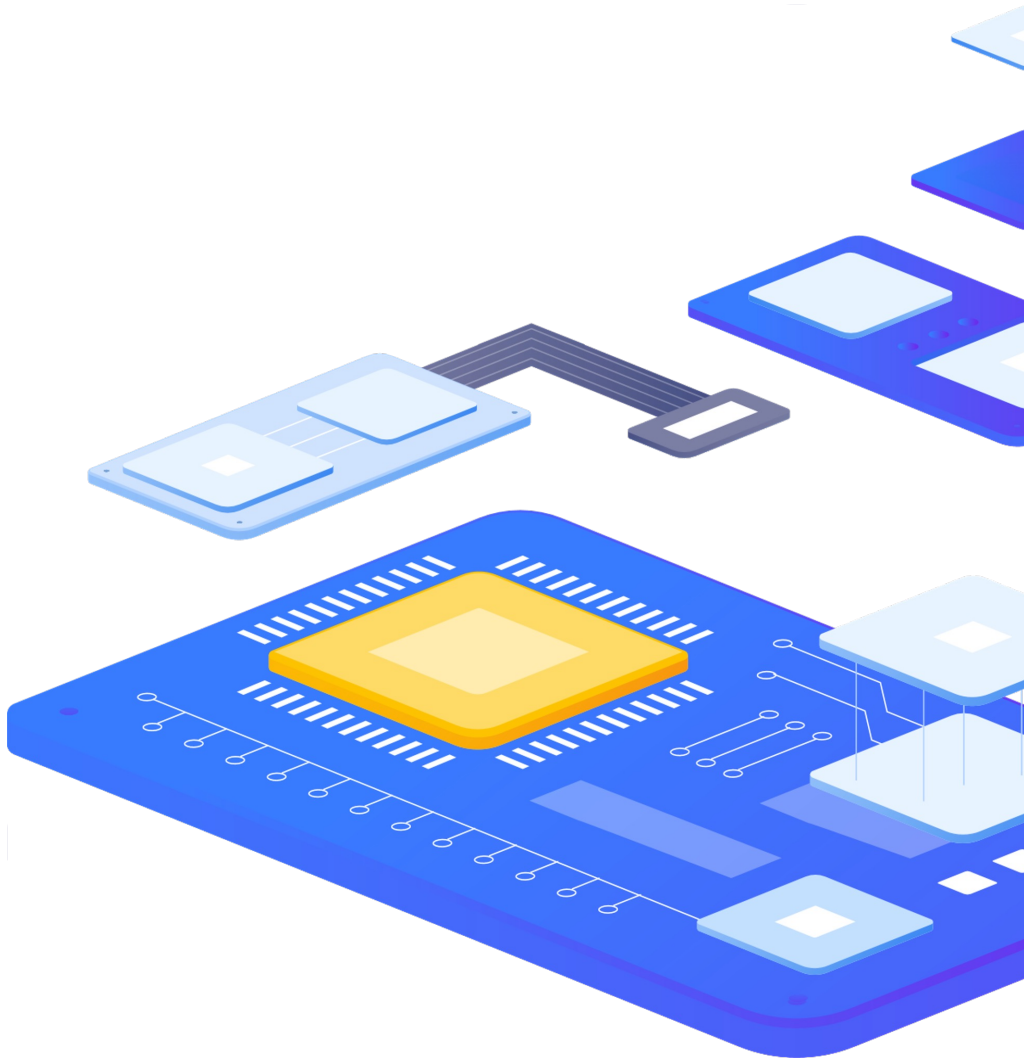
```
kinit ad_user
```

- Přihlášení do PostgeSQL

```
psql -U "ad_user" -h csas-pgsql.win.initmax.cz postgres
```

- Ve větších prostředích lze vytváření uživatelů automatizovat
- Lze využít například kombinaci
  - LDAP (Active Directory, FreeIPA, OpenLDAP,…)

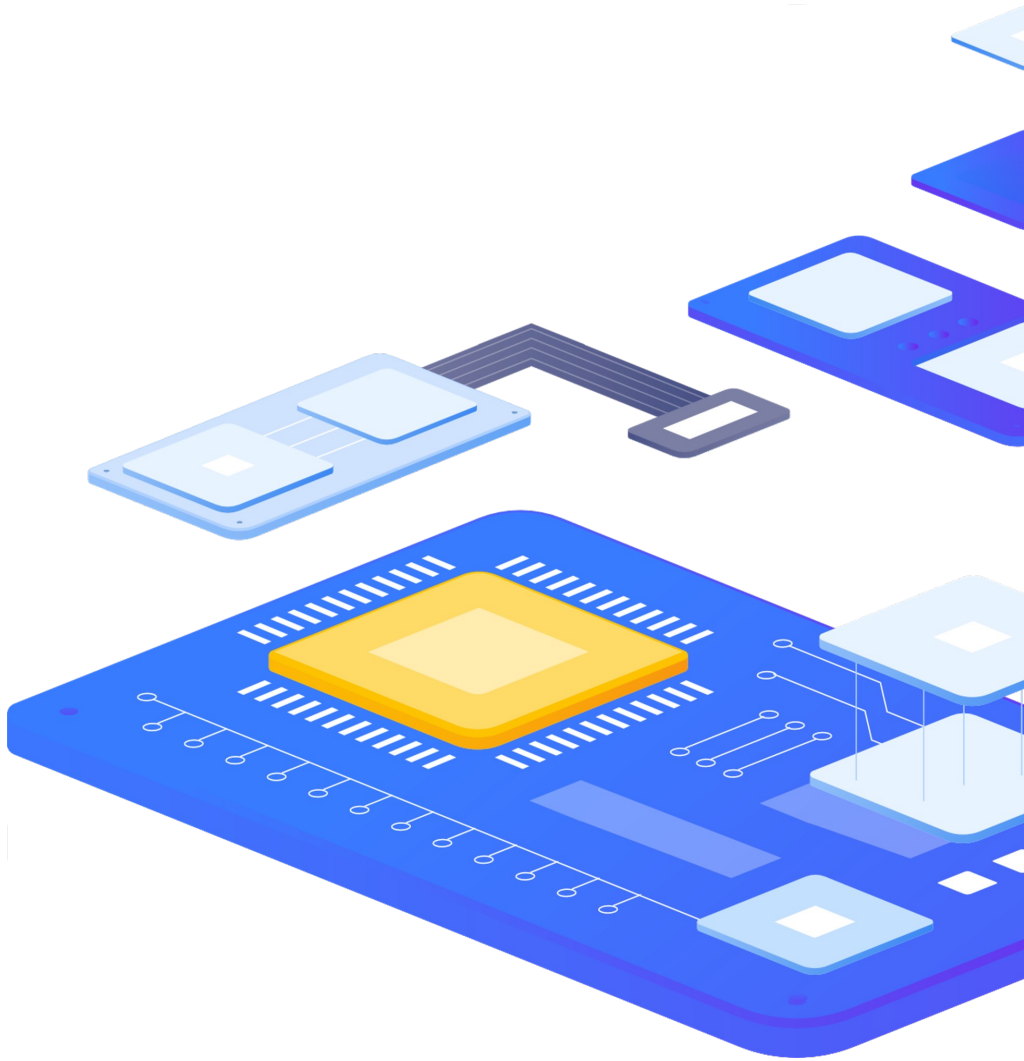
  a
  - ldap2pg



initMAX

ldap2pg

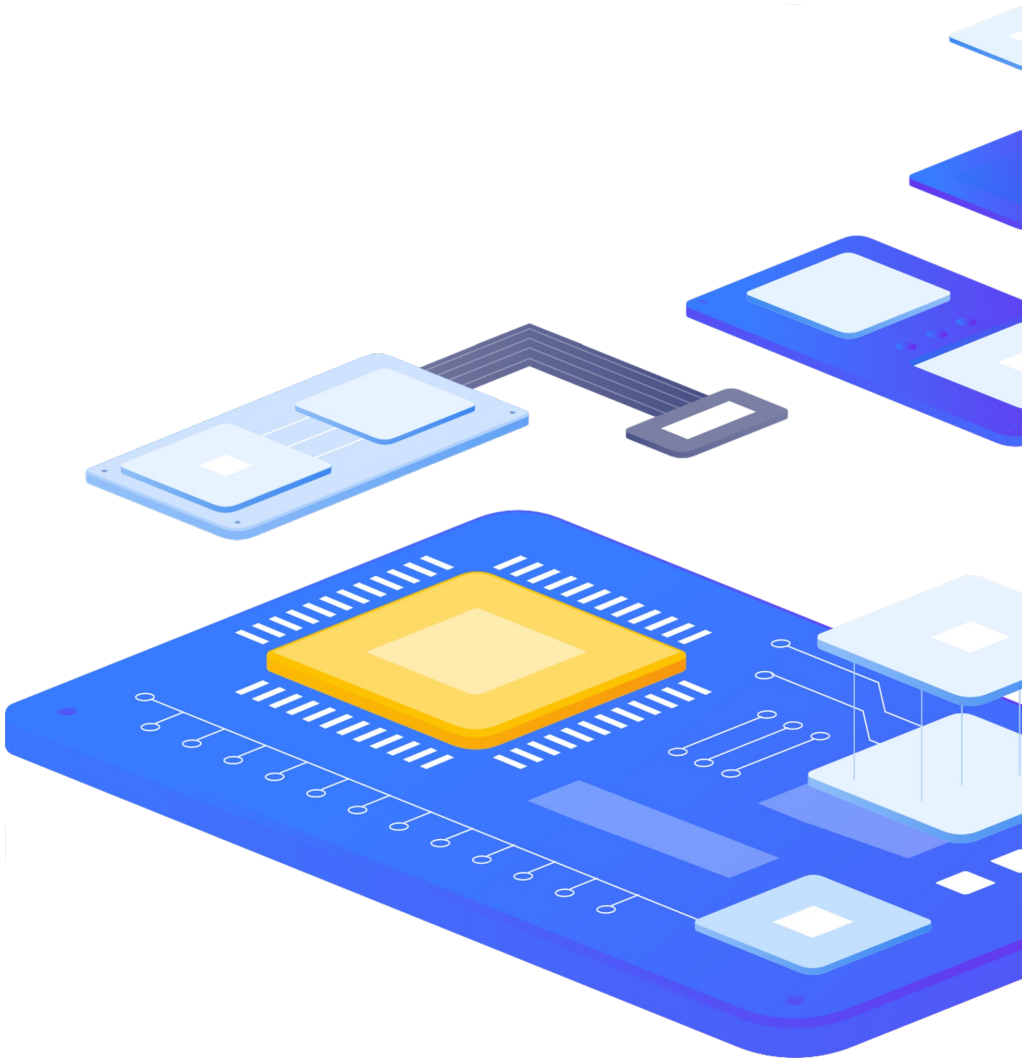
- ldap2pg automatizuje vytváření, aktualizaci a odebírání rolí a uživatelů PostgreSQL
- Ke konfiguraci se používá YAML soubor
- Vytváří, mění a ruší role v PostgreSQL podle nastavení v LDAP
- Umí nastavovat nebo odebírat oprávnění staticky nebo podle nastavení v LDAP
- Může spravovat členství v rolích
- Umí provádět ověření nastavení před jeho ostrým nasazením pomocí parametrů
- Dry run je implicitní nastavení. Pokud chceme aplikovat musíme použít přepínač **--real**



initMAX

ldap2pg - instalace

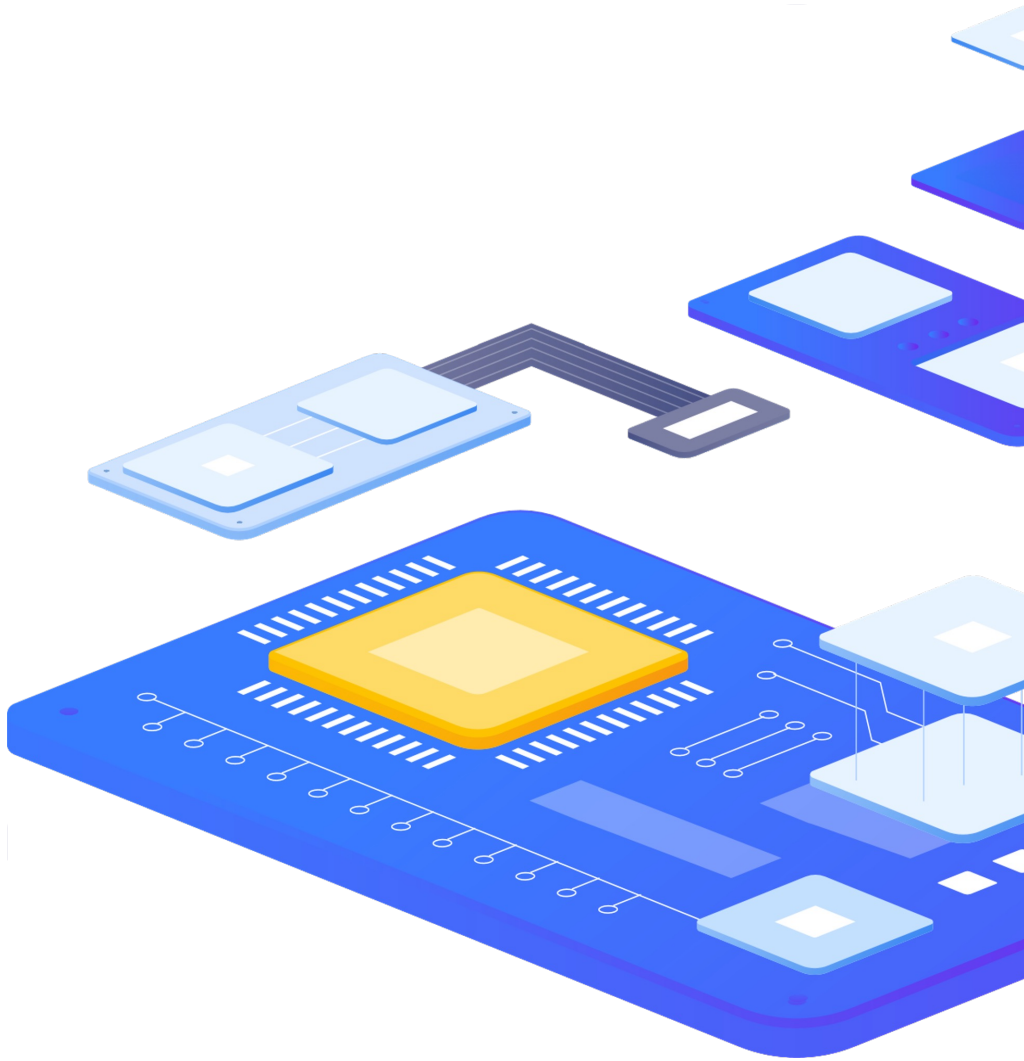
- ldap2pg je dostupný jako balíček pro Python
- ldap2pg vyžaduje:
  - Python 2.6+ nebo Python 3.4+
  - Pyyaml
  - python-ldap
  - python-psycopg2
- Autoři doporučují používat distribuční balíčky jak pro instalaci závislostí tak pro samotný ldap2pg, pokud jsou k dispozici.
- Od verze 6.0 je projekt přepsaný do jazyka GO



initMAX

ldap2pg - instalace

- Instalace na RHEL 6/7/8/9 kompatibilních OS
  - K dispozici jsou dva repozitáře
    - PGDG YUM repository
      - Officiální PostgreSQL repozitář
      - Na serveru s PostgreSQL jej již můžete mít k dispozici
    - Dalibo Labs YUM repository
      - Je upstream
      - Balíčky jsou aktuálnější
- Debian 8/9/10/11
  - Je nutné instalovat pře pip



initMAX

ldap2pg - instalace

- Postup pro RHEL 6/7/8/9 kompatibilní a Dalibo Labs YUM repository
  - Nainstalujeme repozitář a obnovíme dnf cache

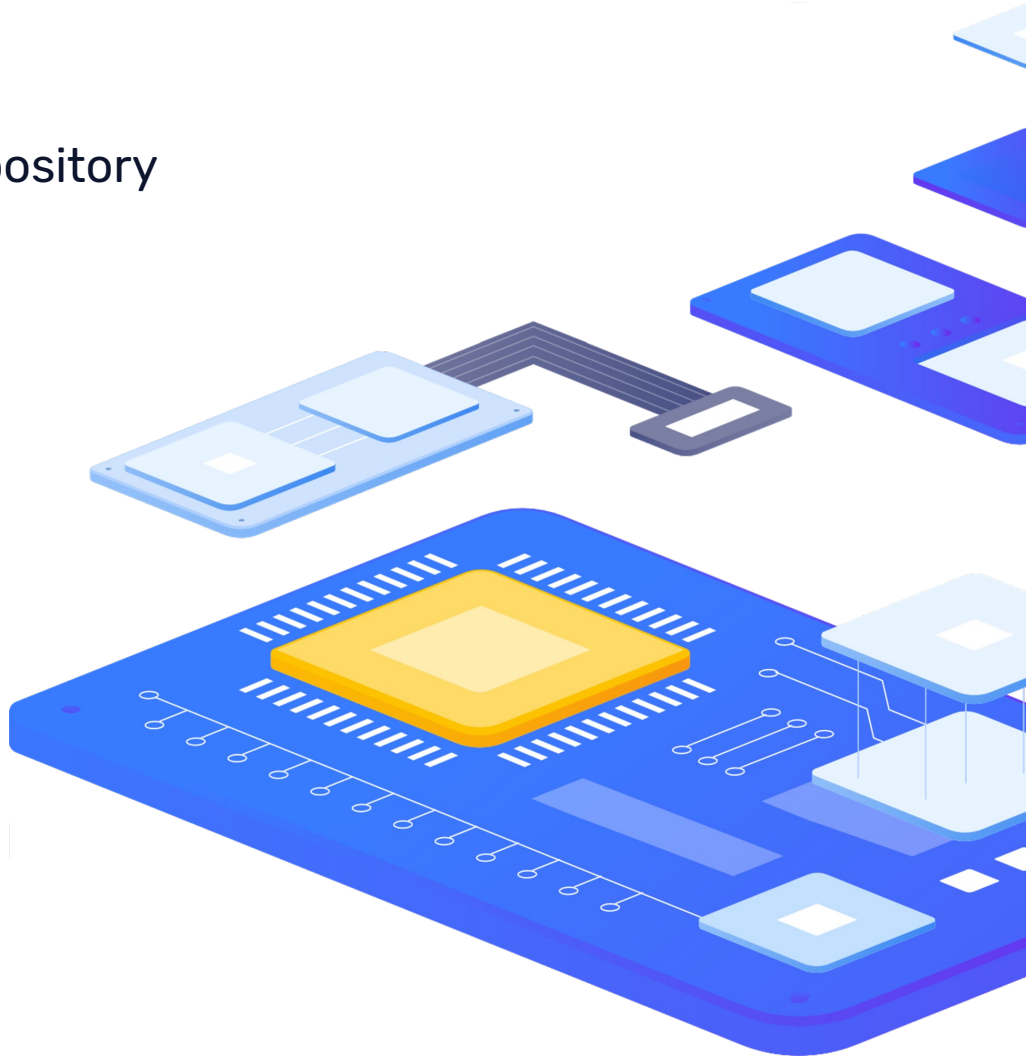
```
dnf install -y https://yum.dalibo.org/labs/dalibo-labs-4-1.noarch.rpm
dnf makecache fast
```

  - Alternativně můžeme repozitář také nainstalovat ručně

```
vi /etc/yum.repos.d/dalibolabs.repo

# do souboru vložit
[dalibolabs]
name = Dalibo Labs - RHEL/CentOS/Rockylinux $releasever - $basearch
baseurl = https://yum.dalibo.org/labs/RHEL$releasever-$basearch
gpgcheck = 1
enabled = 1

# uložit a obnovit dnf cache
dnf makecache fast
```

```
dnf install ldap2pg
```

  - Nainstalujeme samotný ldap2pg

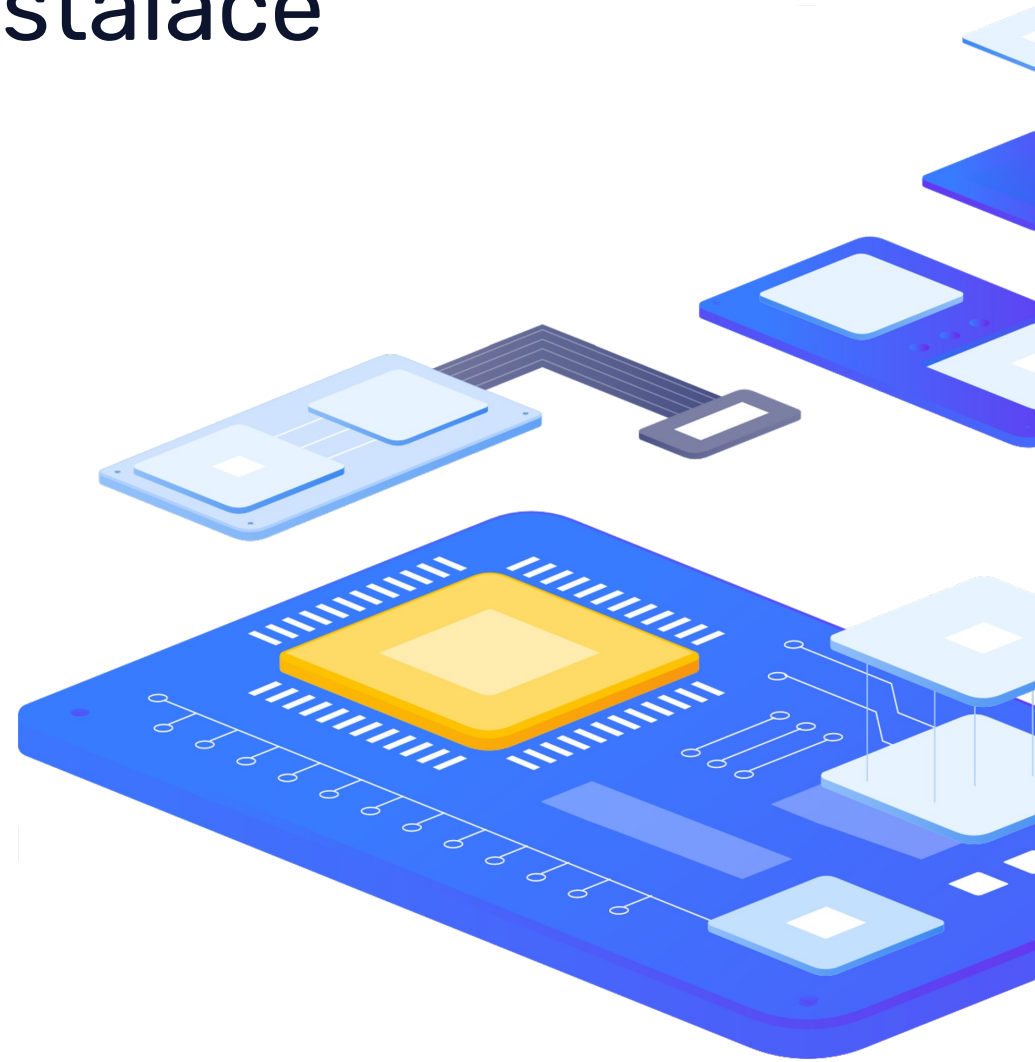


initMAX

ldap2pg – ověření správnosti instalace

```
ldap2pg -V
ldap2pg 5.8
psycopg2 2.8.6 (dt dec pq3 ext lo64) libpq 12.4
python-ldap 3.3.1
Python 3.6.8 (default, Nov  9 2021, 14:44:26)
[GCC 8.5.0 20210514 (Red Hat 8.5.0-3)]ld
```

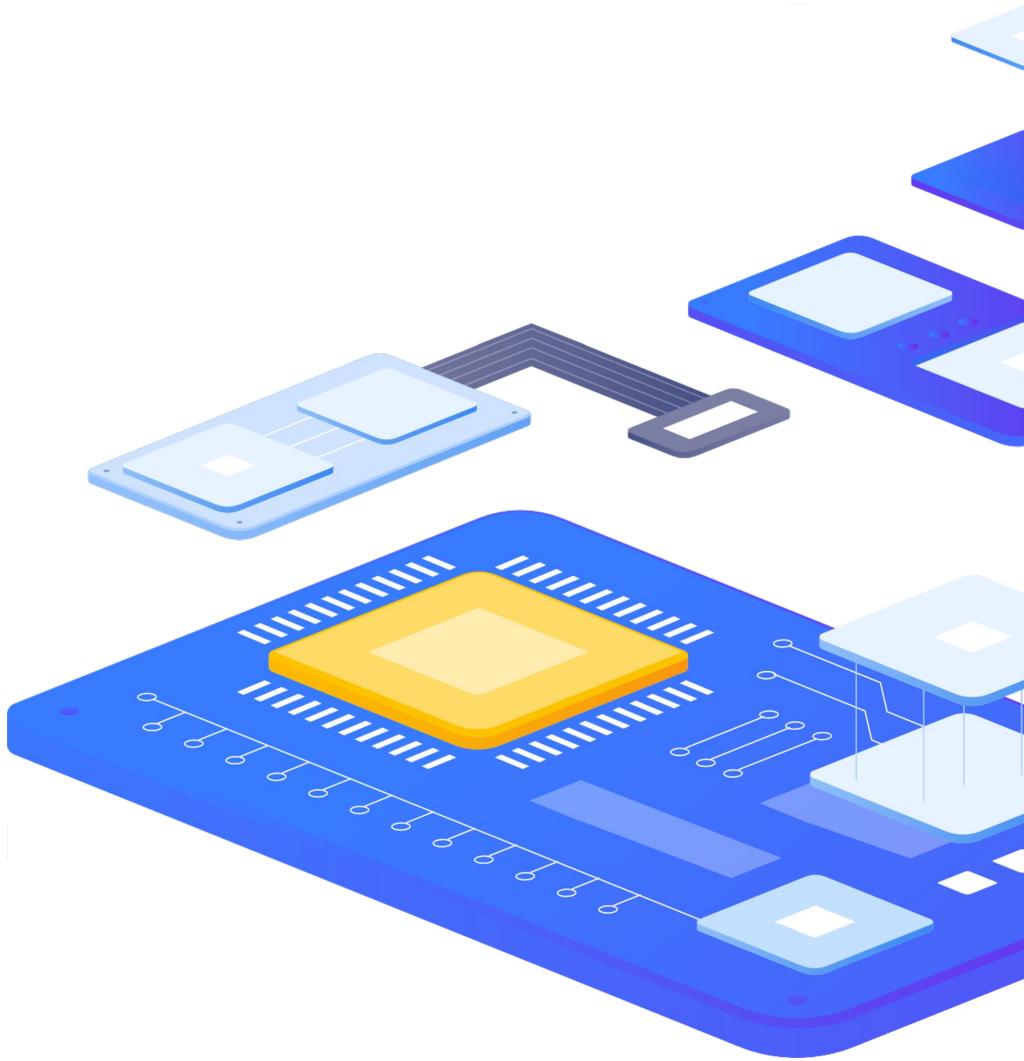
```
ldap2pg --help
usage: ldap2pg [-c PATH] [-C] [-n] [-N] [-q] [-v] [--color] [--no-color] [-?]
               [-V]

PostgreSQL roles and privileges management.

optional arguments:
  -c PATH, --config PATH
                        path to YAML configuration file (env: LDAP2PG_CONFIG).
                        Use - for stdin.
  -C, --check           check mode: exits with 1 on changes in cluster
  -n, --dry             don't touch Postgres, just print what to do (env:
                        DRY=1)
  -N, --real            real mode, apply changes to Postgres (env: DRY='')
  -q, --quiet           decrease log verbosity (env: VERBOSITY)
  -v, --verbose         increase log verbosity (env: VERBOSITY)
  --color               force color output (env: COLOR=1)
  --no-color            force plain text output (env: COLOR='')
  -?, --help            show this help message and exit
  -V, --version         show version and exit

ldap2pg requires a configuration file to describe LDAP searches and role
mappings. See https://ldap2pg.readthedocs.io/en/latest/ for further details.
By default, ldap2pg runs in dry mode.
```



initMAX

ldap2pg - konfigurace

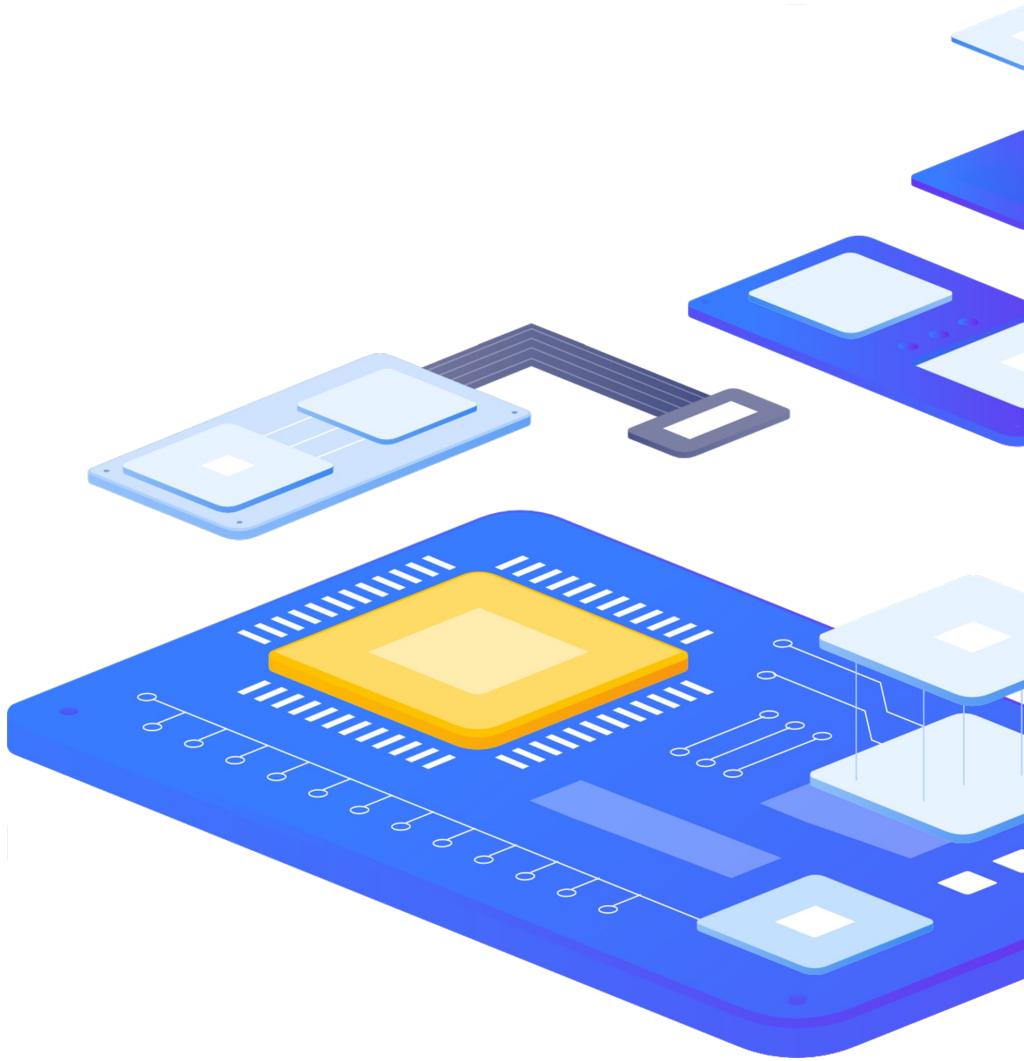
- Konfigurace ldap2pg je uložena v souboru ldap2pg.yml
- Konfigurace je ve formátu YAML – pozor na chyby
- Může obsahovat vše, co je potřebné pro běh ldap2pg
- Konfigurační soubor je hledán v těchto standardních umístěních:
  - ldap2pg.yml v aktuálním pracovním adresáři
  - ~/.config/ldap2pg.yml
  - /etc/ldap2pg.yml
- Pokud je nastavena proměnná LDAP2PG_CONFIG nebo parametr --config <cesta ke konfiguraci>, ldap2pg přeskočí prohledávání standardních umístění souborů
- Je možné zadat i ldap2pg - (s pomlčkou) pro čtení konfigurace ze standardního vstupu



initMAX

ldap2pg - ukázka konfigurace

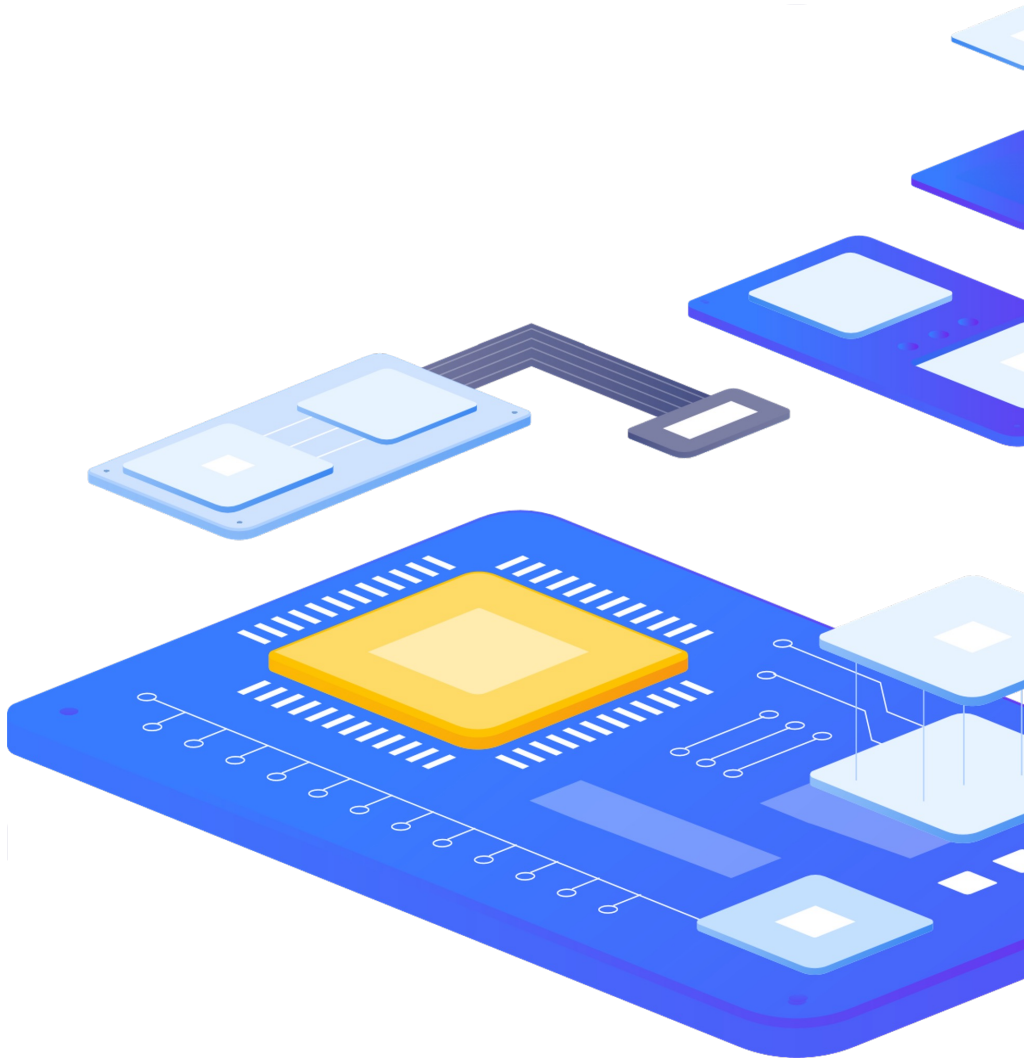
```
postgres:
  dsn: postgres://alfa@csas-pgsql.win.initmax.cz:5432/postgres
  roles_blacklist_query:
    - postgres
    - "pg_*"
    - "rds_*"

ldap:
  uri: ldap://dc1.win.initmax.cz
  binddn: CN=Test User Alfa,OU=Users,OU=testAcounts,DC=win,DC=initmax,DC=cz
  password: "heslo"

sync_map:
- role:
    name: alfa
    options: LOGIN SUPERUSER
    names:
     - ad_roles
    comment: "LDAP role managed by ldap2pg."

- ldapsearch:
    base: CN=pg_DBA_users,OU=Groups,OU=testAcounts,DC=win,DC=initmax,DC=cz
  role:
    name: 'dba_{member.samaccountname}'
    options: LOGIN SUPERUSER
    parent: ad_roles
    comment: "Synced from AD: {dn}"


- ldapsearch:
    base: CN=pg_RO_users,OU=Groups,OU=testAcounts,DC=win,DC=initmax,DC=cz
  role:
    name: '{member.samaccountname}'
    options: LOGIN
    parent: ad_roles
    comment: "Synced from AD: {dn}"
```



initMAX

ldap2pg - ukázka konfigurace

```
version: 6
postgres:
  roles_blacklist_query: [postgres, pg_*]
rules:
- description: "Search LDAP to create roles from all groups found."
  ldapsearch:
    base: OU=pg.initmax.local,OU=Postgres,DC=initmax,DC=local
  role:
    name: "{member.sAMAccountName}"
    options: LOGIN INHERIT
    parent: "{description.lower()}"
    comment: "Generated from LDAP entry {member}"
    config:
      temp_file_limit: 100000

- description: "Search LDAP to create superusers."
  ldapsearch:
    base: CN=DBAs,OU=Postgres,DC=initmax,DC=local
  role:
    name: "{member.sAMAccountName}"
    options:
      SUPERUSER: yes
      LOGIN: yes
      CONNECTION LIMIT: 2
```

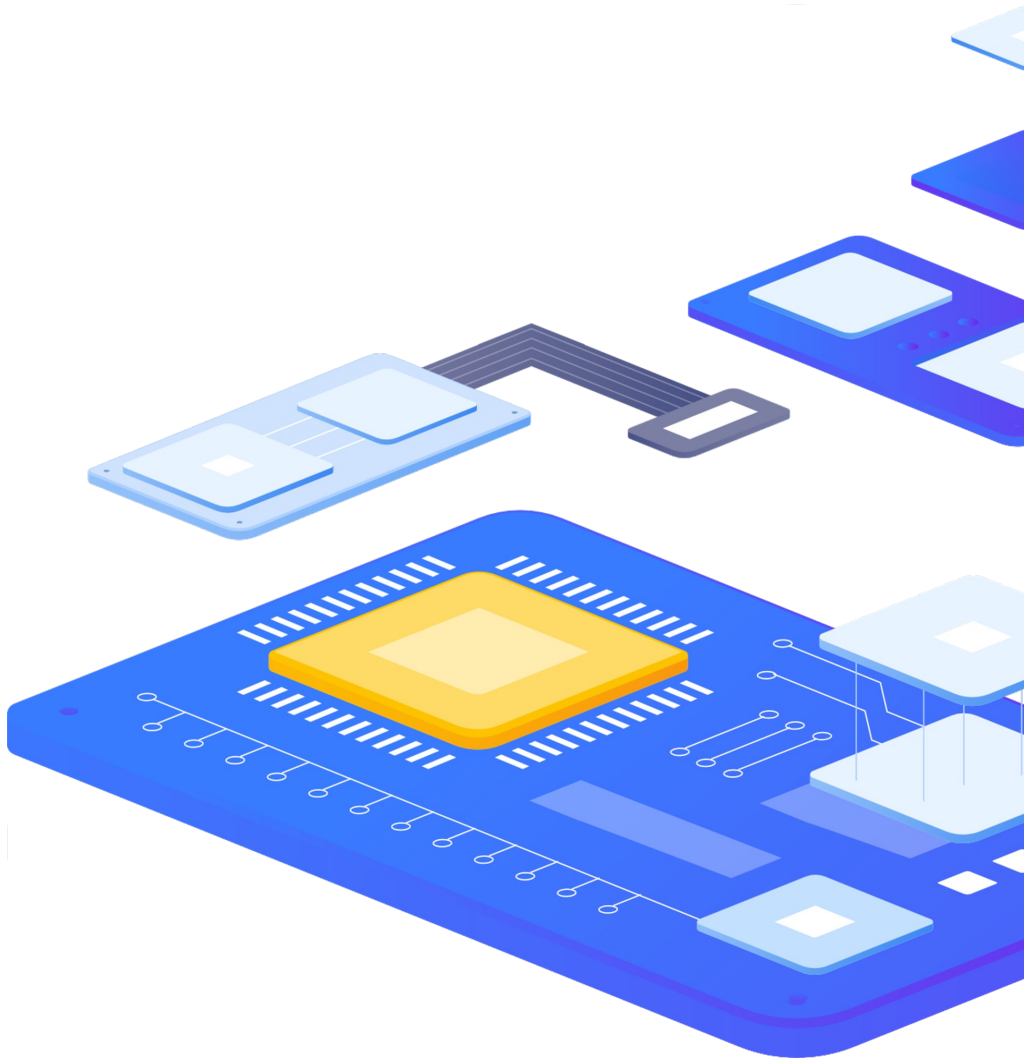


initMAX

ldap2pg - použití

```
# ldap2pg --dry
Starting ldap2pg 5.8.
Using /root/ldap2pg.yml.
Connecting to LDAP server ldap://dc1.win.initmax.cz.
Trying simple bind.
Running in dry mode. Postgres will be untouched.
Inspecting roles in Postgres cluster...
Querying LDAP CN=pg_DBA_users,OU=Group... (objectClass...
Missing 'member' from CN=pg_DBA_users,OU=Groups,OU=testAcounts,DC=win,DC=initmax,DC=cz. Considering
it as an empty list.
Querying LDAP CN=pg_RO_users,OU=Groups... (objectClass...
Missing 'member' from CN=pg_RO_users,OU=Groups,OU=testAcounts,DC=win,DC=initmax,DC=cz. Considering
it as an empty list.
Nothing to do.
Comparison complete.
```

```
$ ldap2pg --real
Starting ldap2pg 5.8.
Using /root/ldap2pg.yml.
Connecting to LDAP server ldap://dc1.win.initmax.cz.
Trying simple bind.
Running in real mode.
Inspecting roles in Postgres cluster...
Querying LDAP CN=pg_DBA_users,OU=Group... (objectClass...
Missing 'member' from CN=pg_DBA_users,OU=Groups,OU=testAcounts,DC=win,DC=initmax,DC=cz. Considering
it as an empty list.
Querying LDAP CN=pg_RO_users,OU=Groups... (objectClass...
Missing 'member' from CN=pg_RO_users,OU=Groups,OU=testAcounts,DC=win,DC=initmax,DC=cz. Considering
it as an empty list.
Nothing to do.
Synchronization complete.
```



initMAX

- Ukázka

Řízení přístupu do PostgreSQL prostřednictvím externího autentizačního providera

Certifikovaná školení

Základní certifikovaná školení

Základy SQL

Tento kurz byl navržen pro lidi, kteří se chtějí seznámit s SQL. Na konkrétních příkladech z každodenní praxe se naučíte jak SQL funguje a jak správně psát SQL dotazy.

4 DNY

48 000,-

Bez DPH

Požadavky: Žádné
Možnost absolvovat online kurz: Ano
Certifikace: Ano

Termíny kurzu:

Na dotaz

REGISTROVAT

Více info a termínů

Úvod do PostgreSQL

Seznámení se s PostgreSQL, popis základních i pokročilých SQL příkazů potřebných nejen pro každodenní práci s PostgreSQL, a to na praktických příkladech.

4 DNY

48 000,-

Bez DPH

Požadavky: Žádné
Možnost absolvovat online kurz: Ano
Certifikace: Ano

Termíny kurzu:

Na dotaz | 19.–22. 2. 24

REGISTROVAT

Více info a termínů

Pokročilá certifikovaná školení

PostgreSQL Professional

Tento kurz poskytuje hluboký vhled do pokročilých témat PostgreSQL, jako je indexování, parametry úložiště, optimalizace, replikace, monitorování a mnoho dalších.

3 DNY

36 000,-

Bez DPH

Požadavky: Žádné
Možnost absolvovat online kurz: Ano
Certifikace: Ano

Termíny kurzu:

Na dotaz | 4.–6. 3. 24

REGISTROVAT

Více info a termínů

PostgreSQL – správa a ladění výkonu

Tento kurz je určen převážně pro databázové adminy a systémové správce. Zabývat se zde budeme tématy konfigurace, správy, provozu a ladění výkonu PostgreSQL.

4 DNY

48 000,-

Bez DPH

Požadavky: základní znalost PostgreSQL a základní znalost OS Linux
Možnost absolvovat online kurz: Ano
Certifikace: Ano

Termíny kurzu:

Na dotaz | 18.–21. 3. 24

REGISTROVAT

Více info a termínů

PostgreSQL – vysoká dostupnost a Patroni

Kurz je určený pro pokročilé uživatele PostgreSQL, které zajímá provozování PostgreSQL v režimu plně automatizované vysoké dostupnosti.

3 DNY

36 000,-

Bez DPH

Požadavky: pokročilá znalost PostgreSQL a základní znalostí OS Linux
Možnost absolvovat online kurz: Ano
Certifikace: Ano

Termíny kurzu:

Na dotaz | 8.–10. 4. 24

REGISTROVAT

Více info a termínů

initMAX

Kontaktujte nás:

Telefon:	+420 800 244 442
Web:	https://www.initmax.cz
Email:	tomas.hermanek@initmax.cz
LinkedIn:	https://www.linkedin.com/company/initmax
Twitter:	https://twitter.com/initmax
Tomáš Heřmánek:	+420 732 447 184