Исследование возможностей сервера OpenLDAP для аутентификации пользователей СУБД PostgreSQL

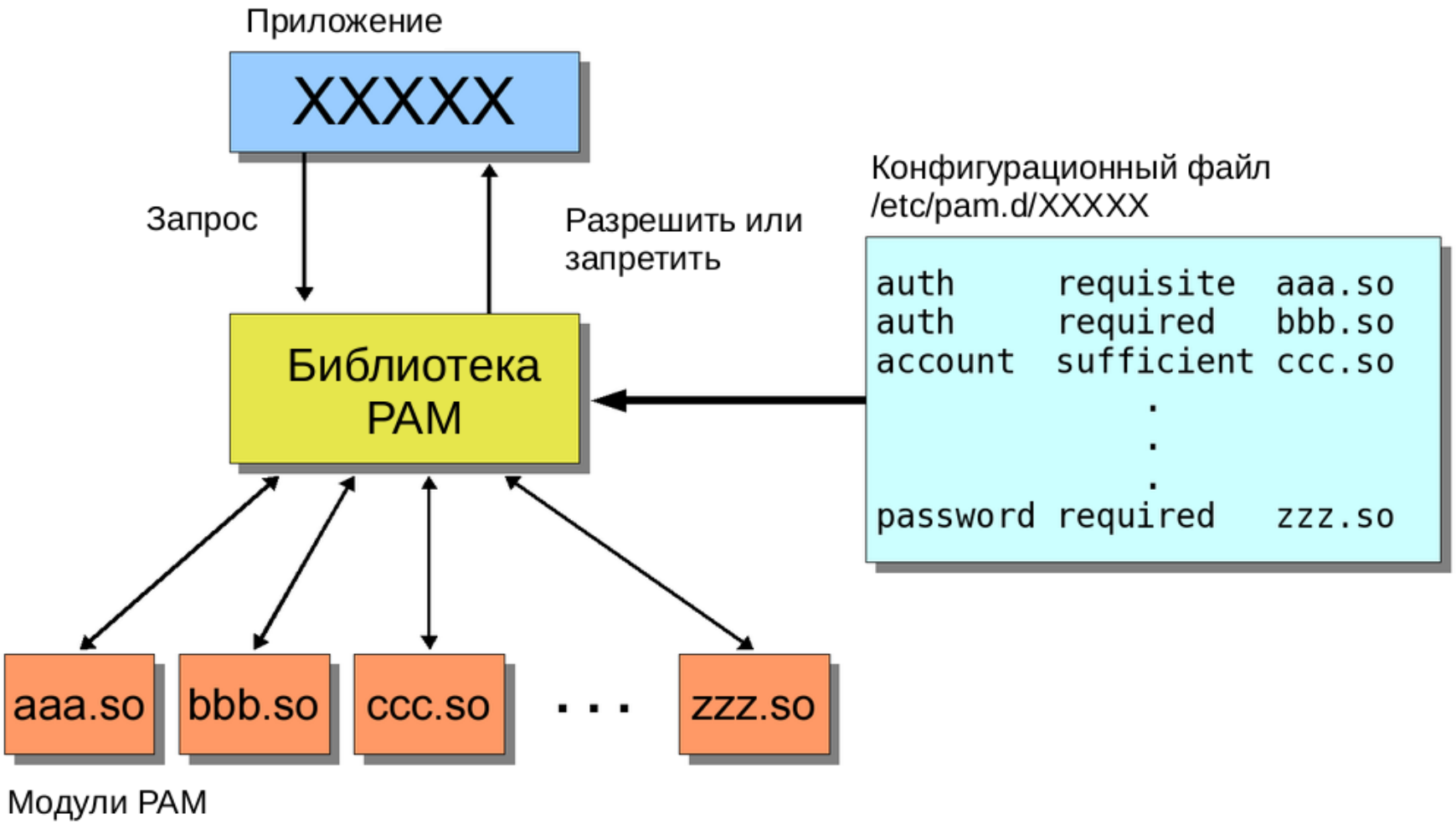
Воронин Д.Л., Муравьёв С.К.

27 января 2014

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust
- Password
- Ident
- Peer
- PAM
- LDAP

Схема работы метода PAM



Информационное дерево каталога LDAP

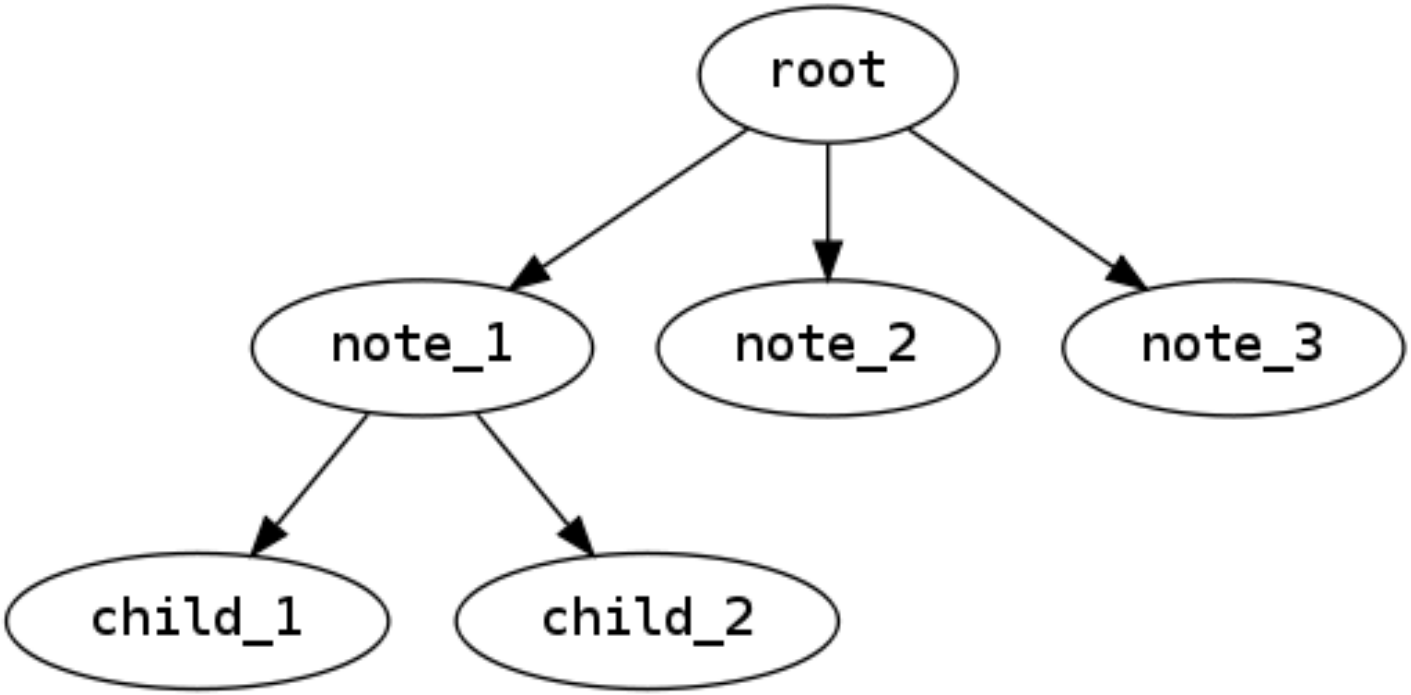
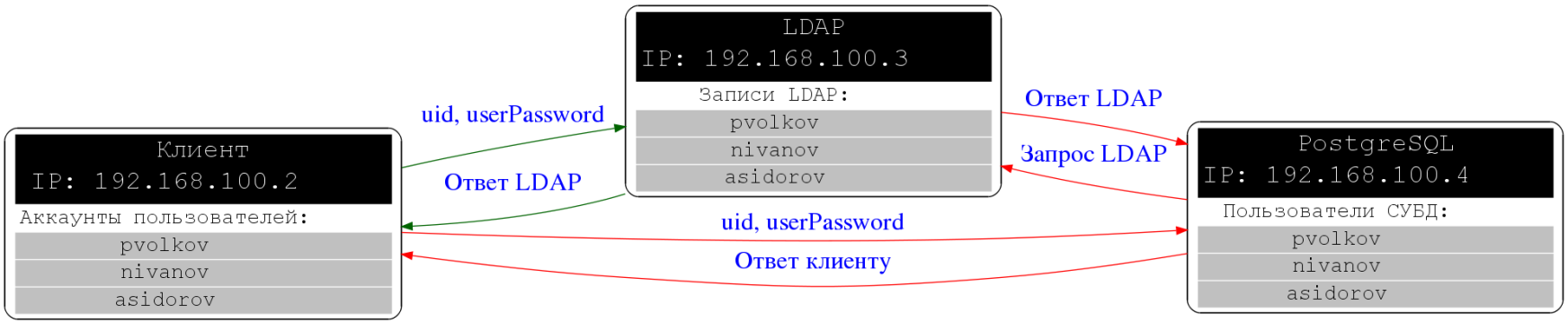


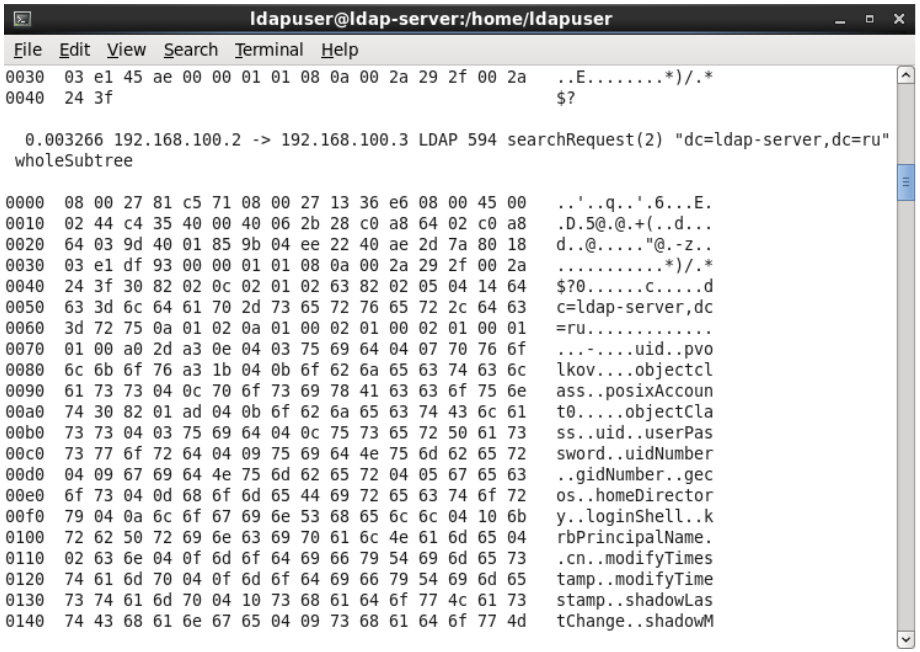
Схема работы стенда

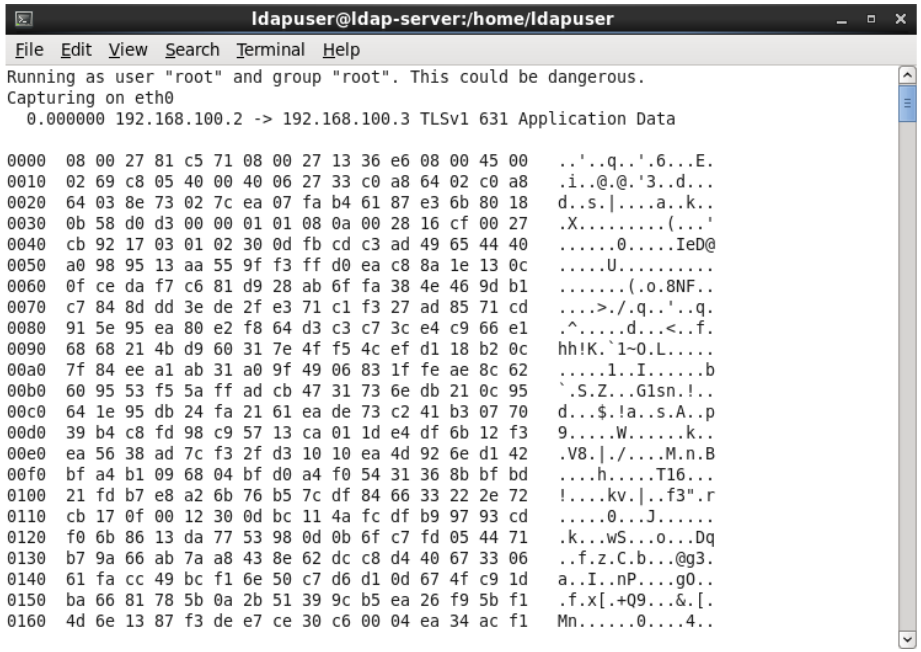


Запись аккаунта пользователя LDAP

```
dn: uid=pvolkov,ou=People,dc=ldap-server,dc=ru
uid: pvolkov
cn: pvolkov
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {SSHA}US0VGNxhxro/QD3B4wIbjRa5re9i8cX1
shadowLastChange:15997
shadowMin:0
shadowMax:99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/pvolkov
```

Соединение клиента с сервером LDAP





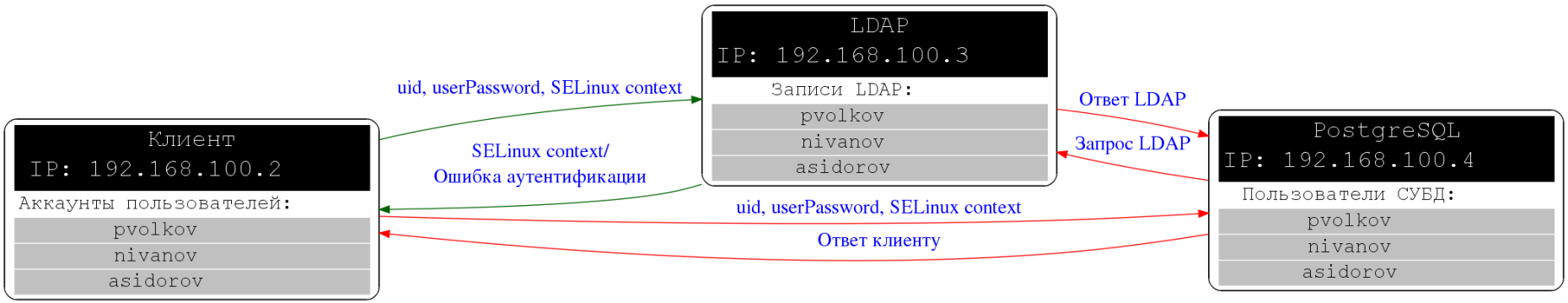
Слева представлен вывод утилиты `tethreal` для соединение клиента и сервера LDAP по протоколу `ldap`, справа — по протоколу `ldaps` (*LDAP security*)

Аутентификация клиентов СУБД PostgreSQL по методу LDAP

В файл `/var/lib/pgsql/9.3/data/pg_hba.conf` требуется добавить строку:

```
hostssl all all 192.168.100.0/24 ldap
ldapserver=192.168.100.3
ldapprefix="uid="
ldapsuffix=",ou=People,dc=ldap-server,dc=ru"
```

Предполагаемая схема работы стенда с использованием SELinux



Достигнутые результаты

- Произведено исследование основных методов аутентфиикации СУБД PostgreSQL. Выявлены их достоинства и недостатки.
- Исследованы возможности сервера OpenLDAP.
- Описан процесс настройки метода аутентификации LDAP в PostgreSQL.