Настройка аутентификации LDAP в PostgreSQL

Воронин Д.Л., Муравьёв С.К.

2 декабря 2013

Общие понятия

Служба каталогов — средство иерархического представления ресурсов, принадлежащих некоторой отдельно взятой организации, и информации об этих ресурсах. Под ресурсами могут пониматься материальные ресурсы, персонал, сетевые ресурсы и т. д.
LDAP (*Lightweight Directory Access Protocol* — "облегчённый протокол доступа к каталогам") — протокол прикладного уровня для доступа к службе каталогов.

Протокол LDAP. Основные понятия

Данные в LDAP представлены *иерархией записей*.

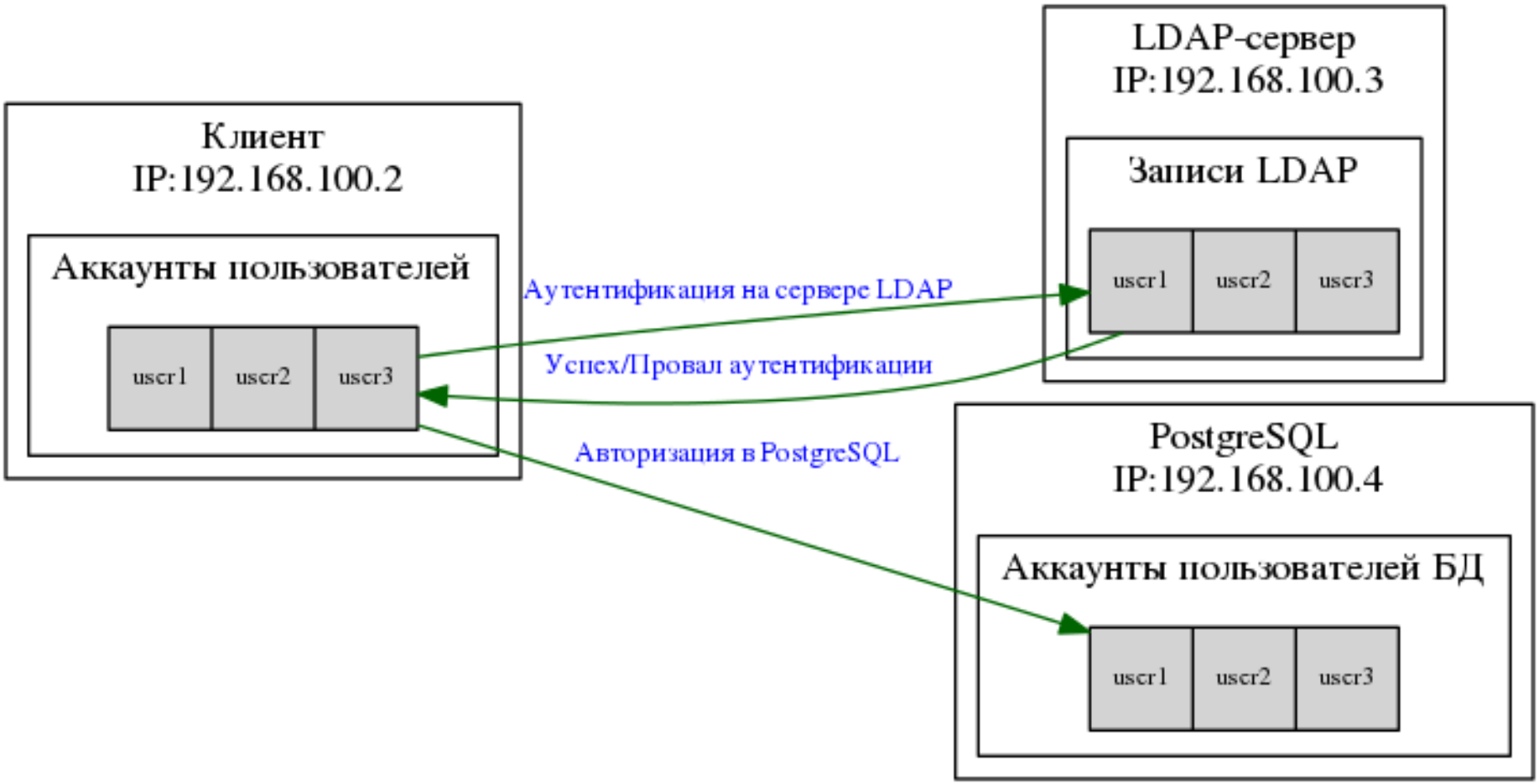
- **DIT**(*Data Information Tree* — "информационное дерево") — вся иерархическая структура каталога.
- **root**(корень) — верхняя часть DIT. Также называется базой (**base**) или суффиксом (**suffix**)
- **object** (объект) — каждая запись дерева. Каждая запись имеет ноль или более дочерних записей.
- **objectclass**(объектный класс) — тип записи. Любая запись является экземпляром одного или нескольких объектных классов.
- **attribute**(атрибут) — поля записи. Каждый объектный класс имеет ноль или более атрибутов.

OpenLDAP

OpenLDAP — открытая реализация протокола LDAP.

`slapd` — сервер службы каталогов, реализующую 3ю версию протокола LDAP. В качестве хранилища поддерживаются механизмы манипуляции данных. Одним из самых распространенных является BDB (высокопроизводительный механизм манипуляции с поддержкой транзакций) на базе **Berklery DB**.

Механизм работы



Настройка сервера LDAP

1. Настройка клиентской машины.
2. Настройка сервера OpenLDAP.
3. Настройка сервера PostgreSQL.

Установка сервера OpenLDAP

На сервере LDAP требуется установить пакеты OpenLDAP:

```
# yum install openldap openldap-clients -y
```

Добавить демон slapd в список автозагрузки:

```
# chkconfig slapd on
```

Установка имени DIT

При установке сервера OpenLDAP устанавливается имя информационного дерева dc=example,dc=com. Для установки своего имени информационного каталога необходимо создать `root.ldif`:

```
1 dn: olcDatabase={2}bdb,cn=config
2 changetype: modify
3 replace: olcSuffix
4 olcSuffix: dc=ldap-server,dc=ru
```

В данном случае имя DIT сменится на `dc=ldap-server,dc=ru`

Создание учётной записи администратора DIT

Администратор информационного каталога DIT позволяет манипулировать информацией пользователей и добавлять новых пользователей. Создайте запрос `admin.ldif`:

```
1 dn: olcDatabase={2}bdb,cn=config
2 changetype: modify
3 replace: olcRootDN
4 olcRootDN: cn=admin,dc=ldap-server,dc=ru
```

При выполнении запроса будет создан администратор информационного каталога `admin`

Назначение пароля администратору admin DIT

Создать зашифрованный пароль администратора командой:

```
# slappaswd
```

Чтобы назначить пароль администратору информационного каталога требуется создать запрос admin_password.ldif:

```
1 dn: olcDatabase={2}bdb,cn=config
2 changetype: modify
3 add: olcRootPW
4 olcRootPW: encrypt_password
```

где вместо encrypt_password записать хэш пароля, сгенерированный командой slappaswd

Списки контроля доступа

ACL (*Access Control List* — списки контроля доступа) — последовательность правил, с помощью которых разграничиваются права пользователей LDAP на атрибуты. Правила работают последовательно, в том порядке, в котором они записаны в конфигурационных файлах.

Изменение политики безопасности контроля доступа

Создать файл политик acl.ldif:

```
dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to attrs=userPassword by self write
by dn.base="cn=admin,dc=ldap-server,dc=ru" write
by anonymous auth by * none

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {1}to * by dn.base="cn=admin,dc=ldap-server,dc=ru"
write by self write by * read

dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,
cn=peercred,cn=external,cn=auth" read
by dn.base="cn=admin,dc=ldap-server,dc=ru" read by * none
```

Описание правил

Первое правило описывает доступ к атрибуту `userPassword`. Второе правило описывает правила доступа к остальным атрибутам. Третье правило описывает правила доступа к мониторингу LDAP.

Загрузка созданных LDIF в LDAP

Для загрузки изменений в LDAP используется команда:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f filename.ldif
```

Таким образом для настройки изменений сервера OpenLDAP выполнить:

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f root.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f admin.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f admin_password.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f acl.ldif
```

При успешном выполнении каждой команды будет выведена следующая строка:

```
modifying entity <entity_name>
```

Настройка клиентской машины

Для аутентификации с использованием сервера LDAP требуется выполнить миграцию пользовательских аккаунтов в LDAP. Для этих целей используется пакет утилит `migrationtools`. Для установки пакета требуется выполнить команду:

```
# yum install migrationstools -y
```

Создание схем пользовательских аккаунтов

Скрипты пакета `migrationtools` создают LDIF(*LDAP Data Interchange Format* — "формат обмена данными LDAP") файлы с данными аккаунтов операционных систем.

Для выполнения миграции требуется перейти в каталог с скриптами:

```
# cd /usr/share/migrationtools
```

Выполнить команды преобразования файлов аккаунтов ОС в формат LDIF:

```
# ./migrate_base.pl > /path_to_save/base.ldif
# ./migrate_group.pl > /path_to_save/groups.ldif
# ./migrate_hosts.pl > /path_to_save/hosts.ldif
# ./migrate_passwd.pl > /path_to_save/passwd.ldif
```

Эти скрипты требуется скопировать с клиентской машины на сервер LDAP.

Удаление локальных аккаунтов пользователей с клиентской машины

Так как аутентификация пользователей будет проходить с использованием сервера LDAP, то требуется удалить учётные записи пользователей с клиентской машины:

```
# userdel user1
# userdel user2
# userdel user3
```

SSSD

SSSD (System Security Services Daemon) позволяет обращаться к удаленным механизмам аутентификации, называемым поставщиками. Таким образом стирается граница между аутентификацией локального и сетевого доступа и допускается использование разных механизмов. Информацию о пользователях предоставляет база данных, называемая доменом, которая может служить источником данных для поставщика. Допускается использование нескольких поставщиков данных идентификации, что разрешает нескольким серверам реализовать различные пространства имен. Полученная информация будет предоставлена внешним приложениям с помощью стандартных интерфейсов PAM и NSS.

Установка SSSD на клиентской машине

Для установки SSSD на клиентской машине выполнить команду:

```
# yum install -y sssd
```

Добавить демон sssd в список автозагрузки:

```
# chkconfig sssd on
```

Установка метода аутентификации с использованием LDAP

```
# authconfig --updateall \
             --passalgo=sha512  \
             --enableldap \
             --enableldapauth
             --ldapserver=192.168.100.3 \
             --ldapbasedn=dc=ldap-server,dc=ru
             --enablesssd \
             --enablesssdauth
```

Данная команда устанавливает метод аутентификации клиента LDAP с использованием LDAP-сервера по IP 192.168.100.3, который имеет DIT `dc=ldap-server,dc=ru` и демона `sssd`.

На этом настройка клиента завершена.

Загрузка данных аккаунтов клиентской машины в сервер LDAP

Для загрузки данных, полученных с помощью скриптов пакета `migrationtools` выполнить следующие команды:

```
# ldapadd -a -f /path_to_file/base.ldif -D \
cn=admin,dc=ldap-server,dc=ru -W
# ldapadd -a -f /path_to_file/groups.ldif -D \
cn=admin,dc=ldap-server,dc=ru -W
# ldapadd -a -f /path_to_file/hosts.ldif -D \
cn=admin,dc=ldap-server,dc=ru -W
# ldapadd -a -f /path_to_file/users.ldif -D \
cn=admin,dc=ldap-server,dc=ru -W
```

При выполнении каждой из команд требуется ввести пароль администратора `admin` DIT `dc=ldap-server,dc=ru`.

На этом закончена настройка сервера LDAP.

Установка сервера PostgreSQL

Установить пакеты сервера PostgreSQL:

```
# yum install -y postgresql93 postgresql93-server
```

Инициализировать сервер базы данных:

```
# service postgresql93 initdb
```

Установить спектр адресов, с которых возможно подключение к серверу:

```
listen_addresses = '*'
```

в файле `/var/lib/pgsql/9.3/data/postgresql.conf`.

Редактирование pg_hba.conf

Установить метод аутентификации пользователей LDAP в pg_hba.conf:

```
host all all 192.168.100.2/32 ldap
ldapserver=192.168.100.3
ldapprefix="uid="
ldapsuffix=",ou=People,dc=ldap-server,dc=ru"
```

Таким образом разрешается подключение с IP 192.168.100.2 всем пользователям, прошедшие аутентификацию в LDAP сервере по IP 192.168.100.3 из группы `ou=People,dc=ldap-server,dc=ru`.

Изменение конфигурационных файлов PostgreSQL требуют перезапуска сервера:

```
# service postgresql93 restart
```

Проверка работы