# {jcomments on}DHCP-Сервер + OpenLDAP

Перед прочтением этой статьи можно ознакомиться что такое openldap : http://linux-bash.ru/index.php?option=com_content&view=article&id=42:ldap&catid=4:seti&Itemid=4

и простой пример настройки dhcp-сервера: http://linux-bash.ru/index.php?option=com_content&view=article&id=39:dhcp&catid=4:seti&Itemid=4

Ставим dhcp-сервер с хранением настроек в openldap.

***sudo apt-get install dhcp3-server-ldap***

Указываем сетевой адаптер на котором будет работать dhcp:

***sudo nano /etc/default/dhcp3-server***

**INTERFACES="eth0"**

Указываем в конфиге dhcp-сервера данные для работы с openldap (все остальное

ненужно, удаляем):

***sudo nano /etc/dhcp3/dhcpd.conf***

**ldap-server "127.0.0.1";**
**ldap-port 389;**
**ldap-username "cn=admin,dc=mega,dc=local";**
**ldap-password "pass";**
**ldap-base-dn "ou=dhcp,dc=mega,dc=local";**
**ldap-method static;**

Устанавливаем openldap-сервер:

***sudo apt-get install slapd ldap-utils***

Запускаем конфигуратор:

***sudo dpkg-reconfigure slapd***

и отвечаем на вопросы:

невыполнять настройку сервера openldap: **нет**

удалять базу при вычистке slapd: **да**

allow ldapv2 protocol: **да**

Включаем поддержку slapd.conf (с новшеством новой версии, с динамической загрузкой, отношения у меня не сложились):

В /etc/default/slapd переменной SLAPD_CONF указываем путь к файлу конфигу:

**SLAPD_CONF=/etc/ldap/slapd.conf**

Генерим рутовский пароль для доступа к ldap:

***slappasswd -s <ваш pass>***

Получим следующее:

**{SSHA}a2ieiYYJfYMkUHY6RvxjxWu7Nadbpnh9**

копируем, дальше понадобится. Создаем файл конфигурации:

***sudo touch /etc/ldap/slapd.conf***

***sudo nano /etc/ldap/slapd.conf***

Заполняем (у меня также samba использует openldap, поэтому вам строчку "include /etc/ldap/schema/samba.schema" можно убрать, если не нужна):

**include /etc/ldap/schema/core.schema**
**include /etc/ldap/schema/cosine.schema**
**include /etc/ldap/schema/inetorgperson.schema**
**include /etc/ldap/schema/misc.schema**
**include /etc/ldap/schema/nis.schema**
**include /etc/ldap/schema/openldap.schema**
**include /etc/ldap/schema/samba.schema**
**include /etc/ldap/schema/dhcp.schema**
**pidfile /var/run/slapd/slapd.pid**
**argsfile /var/run/slapd/slapd.args**
**modulepath /usr/lib/ldap**
**moduleload back_bdb**
**access to * by * read**
**access to attrs=userPassword**
**{Tab}by self write**
**{Tab}by anonymous auth**
**{Tab}by * none**
**database bdb**
**suffix "dc=mega,dc=local"**
**rootdn "cn=admin,dc=mega,dc=local"**
**rootpw {SSHA}a2ieiYYJfYMkUHY6RvxjxWu7Nadbpnh9**
**directory /var/lib/ldap**
**loglevel 256**
**index objectClass eq**
**index cn eq**

Рассмотрим конфиг подробнее. Сначала добавляем нужные схемы, в зависимости от того какое програмное обеспечение будет использовать ldap (например для интеграции с dhcp исползуется dhcp.schema). Далее указываются пути к Pid-файлу, файлу с аргументами, путь к модулям. Подгружаем модуль bdb, Описываем доступ к информации: указываем, что себе(под кем Вы находитесь в системе) разрешена запись,

анонимам предлагается авторизоваться. Указываем тип базы - bdb (во многих руководствах еще используется ldbm). Описываем корень базы и указываем логин и пароль администратора ldap, указываем директорию хранения БД и индексы, для ускорения поиска по базе.

Нажатие клавиши {Tab} в указанных строках конфига обязательно, иначе будет ошибка.

Копируем файл со схемой ldap из папки dhcp-сервера:

***sudo cp /usr/share/doc/dhcp3-server-ldap/dhcp.schema.gz /etc/ldap/schema/dhcp.schema.gz***

***sudo gzip -d /etc/ldap/schema/dhcp.schema.gz***

Перезапускаем ldap:

***sudo /etc/init.d/slapd restart***

Если выдала система ошибку, смотрим логи:

***cat /var/log/syslog***

Проверяем появился ли процесс:

***ps -ax | grep slap***

Проверяем что 389-ый порт слушается:

***netstat -nap tcp | grep 389***

Если все нормально, значит сервер ldap готов.

создаем файлы, содержащие структуру openldap, для последующего экспорта:

***sudo mkdir /etc/ldap/my_ldif***

***sudo touch /etc/ldap/my_ldif/base.ldif***

***sudo nano /etc/ldap/my_ldif/base.ldif***

**dn: dc=mega,dc=local**
**objectClass: dcObject**
**objectclass: organization**
**dc: mega**
**o: mega**

**dn: ou=Users,dc=mega,dc=local**
**objectClass: organizationalUnit**
**ou: Users**

**dn: ou=Groups,dc=mega,dc=local**
**objectClass: organizationalUnit**
**ou: Groups**

**dn: ou=Computers,dc=mega,dc=local**
**objectClass: organizationalUnit**
**ou: Computers**

(dhcp будет использовать только Groups, а Users и Computers для контроллера домена (он у меня тоже использует openldap), поэтому если вам не нужно, Users и Computers можно удалить)

Добавляем этот каталог в базу:

***ldapadd -x -D "cn=admin,dc=mega,dc=local" -W -f /etc/ldap/my_ldif/base.ldif***

Настройки dhcp.

Все данные будут храниться в группе dhcp

***sudo touch /etc/ldap/my_ldif/dhcp.ldif***

***sudo nano /etc/ldap/my_ldif/dhcp.ldif***

**dn: ou=dhcp,dc=mega,dc=local**
**ou: dhcp**
**description: configuration information for DHCP**
**objectClass: top**
**objectClass: organizationalUnit**

**dn: cn=gate,ou=dhcp,dc=mega,dc=local**
**dhcpServiceDN: cn=conf,cn=gate,ou=dhcp,dc=mega,dc=local**
**objectClass: top**
**objectClass: dhcpServer**
**cn: gate**

**dn: cn=conf,cn=gate,ou=dhcp,dc=mega,dc=local**
**dhcpStatements: ddns-update-style none**
**dhcpStatements: ddns-updates off**
**dhcpStatements: client-updates off**
**dhcpStatements: use-host-decl-names on**
**dhcpStatements: always-reply-rfc1048 on**

**dhcpStatements: default-lease-time 86400**
**dhcpStatements: max-lease-time 129600**
**objectClass: top**
**objectClass: dhcpService**
**objectClass: dhcpOptions**
**dhcpPrimaryDN: cn=gate,ou=dhcp,dc=mega,dc=local**
**dhcpOption: domain-name "gate"**
**dhcpOption: netbios-scope ""**
**dhcpOption: netbios-node-type 8**
**dhcpOption: time-offset 10800**
**dhcpOption: ip-forwarding off**
**dhcpOption: netbios-name-servers 10.10.10.4**
**cn: conf**

**dn: cn=10.10.10.0,cn=conf,cn=gate,ou=dhcp,dc=mega,dc=local**
**objectClass: top**
**objectClass: dhcpSubnet**
**objectClass: dhcpOptions**
**dhcpNetMask: 24**
**dhcpRange: 10.10.10.50 10.10.10.200**
**dhcpOption: domain-name-servers 10.10.10.4**
**dhcpOption: routers 10.10.10.4**
**dhcpOption: ntp-servers 10.10.10.4**
**dhcpOption: broadcast-address 10.10.10.255**
**dhcpOption: default-ip-ttl 64**
**dhcpOption: default-tcp-ttl 64**
**cn: 10.10.10.0**

На свои нужно изменить имя сервера (gate) и ip-адреса. 10.10.10.0 - это локальная сеть, 10.10.10.4 - адрес самого сервера.

Если необходимо, присваиваем машине постоянный ip. (ip привязывается к MAC)

***sudo touch /etc/ldap/my_ldif/av_dhcp.ldif***

***sudo nano /etc/ldap/my_ldif/av_dhcp.ldif***

**dn: cn=AV,cn=10.10.10.0,cn=conf,ou=dhcp,dc=mega,dc=local**
**dhcpHWAddress: ethernet 6C:F0:49:6E:59:A1**
**dhcpStatements: fixed-address 10.10.10.9**
**objectClass: top**
**objectClass: dhcpHost**
**objectClass: dhcpOptions**
**cn: AV**

Экспортируем в базу:

**ldapadd -x -D "cn=admin,dc=mega,dc=local" -W -f /etc/ldap/my_ldif/dhcp.ldif**
**ldapadd -x -D "cn=admin,dc=mega,dc=local" -W -f /etc/ldap/my_ldif/av_dhcp.ldif**

Перезапускаем dhcp-сервер:

***sudo /etc/init.d/dhcp3-server restart***

Все должно работать.

P.S.

Для удаления внесенных данных из базы (если где-то ошиблись) используем следующие команды:

***ldapdelete -W -x -D cn=admin,dc=mega,dc=local***
***"cn=AV,cn=10.10.10.0,cn=conf,cn=gate,ou=dhcp,dc=mega,dc=local"***
***ldapdelete -W -x -D cn=admin,dc=mega,dc=local***
***"cn=10.10.10.0,cn=conf,cn=gate,ou=dhcp,dc=mega,dc=local"***
***ldapdelete -W -x -D cn=admin,dc=mega,dc=local***
***"cn=conf,cn=gate,ou=dhcp,dc=mega,dc=local"***
***ldapdelete -W -x -D cn=admin,dc=mega,dc=local "cn=gate,ou=dhcp,dc=mega,dc=local"***
***ldapdelete -W -x -D cn=admin,dc=mega,dc=local "ou=dhcp,dc=mega,dc=local"***