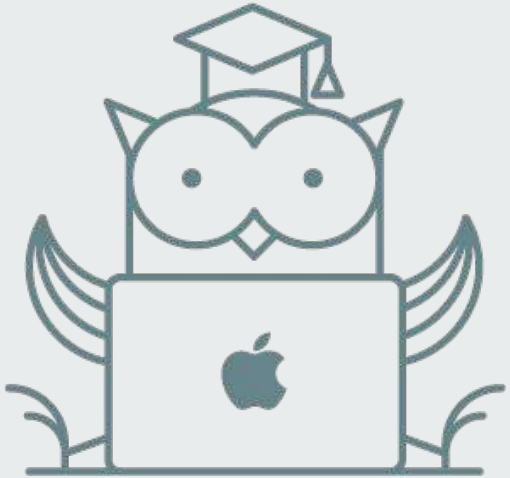
Курс «Администратор Linux»

Установка и настройка LDAP

Занятие # 17 (16.2)

Дмитрий Молчанов
Григорий Ожегов



План

- Подготовительные шаги
  - Проектирование каталога
- Настройка сервера
  - Установка пакетов
  - Генерация сертификатов
  - Конфигурирование базы
  - Импорт схем
  - Импорт начального каталога
  - Настройка доступов
  - Добавление пользователей
- Настройка клиента
  - Установка пакетов
  - настройка nsswitch/nscd
  - настройка nslcd
  - настройка pam

Подготовка: Проектирование каталога

Вводные данные.

Домен: otus.lnx
Серверов: 3+
Пользователей: ~20+2
Орг элементов: 5 - группы, люди (студенты и преподаватели) и сервера
Группы: 2 - students, teachers
Служебные аккаунты: 1 - ldapadm

Требования:

- общая база пользователей для доступа к серверам.
- безопасный обмен данными

Подготовка: Проектирование каталога

- dc=otus,dc=lnx
  - ou=Groups,dc=otus,dc=lnx
  - ou=People,dc=otus,dc=lnx
    - ou=Teachers,ou=People,dc=otus,dc=lnx
    - ou=Students,ou=People,dc=otus,dc=lnx
  - ou=Servers,dc=otus,dc=lnx

Подготовка: Проектирование каталога

- dc=otus,dc=lnx
  - cn=ldapadm,dc=otus,dc=lnx
  - cn=ldapauth,dc=otus,dc=lnx
  - ou=Groups,dc=otus,dc=lnx
    - cn=wheel,ou=Groups,dc=otus,dc=lnx
  - ou=People,dc=otus,dc=lnx
    - ou=Teachers,ou=People,dc=otus,dc=lnx
      - cn=Dmitry Molchanov,ou=Teachers,ou=People,dc=otus,dc=lnx
      - cn=Grigory Ozhegov,ou=Teachers,ou=People,dc=otus,dc=lnx
    - ou=Students,ou=People,dc=otus,dc=lnx
  - ou=Servers,dc=otus,dc=lnx

Обзор необходимых пакетов

- Сервер:
  - openldap-servers
  - openldap-clients
  - openldap
- Клиент:
  - nss-pam-ldapd
  - openldap
  - nscd (опционально)

LDIF

LDIF (LDAP Data Interchange Format) - формат обмена (получение информации/изменение информации) данными с LDAP-сервером.

```
dn: unique_name
[changetype: (add|modify|delete)]
attribute_name: 7bit_attribute_value
attribute_name:: base64_attribute_value
attribute_name:< url_reference
```

LDIF

LDIF (LDAP Data Interchange Format) - формат обмена (получение информации/изменение информации) данными с LDAP-сервером.

```
dn: unique_name
attribute_name: 7bit_attribute_value
attribute_name:: base64_attribute_value
attribute_name:< url_reference



dn: unique_name
changetype: (add|modify|delete)
[modification_type: attribute]
attribute_name: 7bit_attribute_value
-
[modification_type: attribute]
attribute_name: 7bit_attribute_value
```

Установка сервера

- Установка пакетов

```
yum install openldap-servers
```

После установки конфигурация находится в /etc/openldap.

За обслуживание клиентов отвечает сервис slapd.

Начальное управление происходит через интерфейс ldapi с помощью утилит:

```
ldapmodify
ldapadd
```

Также будут необходимы утилиты:

```
slappaswd
```

Генерация пароля для rootDN

```
# slappasswd
New password:
Re-enter new password:
{SSHA}wH5821SDVaRn/SiVz894vFwUcpul68zv
```

Инициализация базы: step1.ldif

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=otus,dc=lnx                          ← установка нашего домена

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=ldapadm,dc=otus,dc=lnx               ← Установка пользователя который будет управлять каталогом (rootDN)

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}wH5821SDVaRn/SiVz894vFwUcpul68zv  ← Установка пароля для пользователя

dn: olcDatabase={1}monitor,cn=config               ← Установка прав на доступ к конектсту мониторинга
changetype: modify
replace: olcAccess
olcAccess: to *
      by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read
      by dn.base="cn=ldapadm,dc=otus,dc=lnx" read
      by * none
```

Инициализация базы, сертификат

```
# ldapmodify -Y EXTERNAL -H ldapi:/// -f ./step1.ldif
# openssl req -new -x509 -nodes -out /etc/openldap/certs/otus.lnx.cert.pem -keyout /etc/openldap/certs/otus.lnx.key.pem -days 3650
Generating a 2048 bit RSA private key
.....................................................................+++
.....................................+++
writing new private key to '/etc/openldap/certs/otus.lnx.key.pem'
-----
[...]
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:Moscow
Organization Name (eg, company) [Default Company Ltd]:Otus Linux Course
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:ldap-server.otus.lnx
Email Address []:dmolchanov@gmail.com
```

Сертификат: step2.ldif , Схемы

```
dn: cn=config
changetype: modify
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/otus.lnx.cert.pem

dn: cn=config
changetype: modify
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/otus.lnx.key.pem
```

Для изменения конфигурации согласно ldif надо выполнить команду. Затем добавить ‘ldaps:///’ в SLAPD_URLS в файле /etc/sysconfig/slapd

```
# ldapmodify -Y EXTERNAL -H ldapi:/// -f ./step2.ldif
```

Для импорта схем выполняем:

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

Импорт начального каталога: otus.ldif

```
dn: dc=otus,dc=lnx
dc: otus
objectClass: top
objectClass: domain

dn: cn=ldapadm ,dc=otus,dc=lnx
objectClass: organizationalRole
cn: ldapadm
description: LDAP Manager

dn: ou=People,dc=otus,dc=lnx
objectClass: organizationalUnit
ou: People

dn: ou=Teachers,ou=People,dc=otus,dc=lnx
objectClass: organizationalUnit
ou: Teachers
```

```
dn: ou=Students,ou=People,dc=otus,dc=lnx
objectClass: organizationalUnit
ou: Students

dn: ou=Group,dc=otus,dc=lnx
objectClass: organizationalUnit
ou: Group

dn: cn=wheel,ou=Group,dc=otus,dc=lnx
objectClass: posixGroup
cn: wheel
gidNumber: 10
```

ldapadd -x -W -D ‘cn=ldapadm,dc=otus,dc=lnx’ -f otus.ldif

Настройка доступа: step3.ldif

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: to *                         ← Ко всем атрибутам
       by self write                    ← владельцу - писать
       by users read                    ← всем - читать
       by anonymous auth                ← остальным только аутентифицироваться
```

Для изменения конфигурации согласно ldif надо выполнить команду

```
# ldapmodify -Y EXTERNAL -H ldapi:/// -f ./step3.ldif
```

Добавление пользователей: step4.ldif

```
dn: cn=Dmitry Molchanov,ou=teachers,dc=otus,dc=lnx
givenName: Dmitry
sn: Molchanov
cn: Dmitry Molchanov
uid: mdv
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
uidNumber: 1001
userPassword: {SSHA}TxGdhET/imat9oyHyyYpBYAsOTXFxyT
homeDirectory: /home/mdv
loginShell: /bin/bash
gidNumber: 0
```

Добавление пользователей: step4.ldif

```
dn: cn=Grigory Ozhegov,ou=teachers,dc=otus,dc=lnx
givenName: Grigory
sn: Ozhegov
cn: Grigory Ozhegov
uid: gozhegov
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
uidNumber: 1002
userPassword: {SSHA}qkMr28yNckOVqc3pquGYftqBCVpkf44U
homeDirectory: /home/gozhegov
loginShell: /bin/bash
gidNumber: 10
```

Для изменения конфигурации согласно ldif надо выполнить команду

```
# ldapadd -x -W -D ‘cn=ldapadm,dc=otus,dc=lnx’ -f ./step4.ldif
```

Конфигурация Клиента.

Пакеты: nss-pam-ldapd+зависимостиб nscd

```
# yum install nss-pam-ldapd nscd
```

“волшебная команда”:

```
# authconfig --enableldap --enableldapauth --ldapserver=ldaps://ldap-server.otus.lnx
--ldapbasedn="dc=otus,dc=lnx" --enablemkhomedir --update
```

Что же она делает “под капотом”?!

Конфигурация клиента: pam,nslcd

- добавление pam_ldap:

```
auth        sufficient    pam_ldap.so use_first_pass
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
password    sufficient    pam_ldap.so use_authtok
session     optional      pam_ldap.so
```

- Конфигурация nslcd:

```
uid nslcd
gid ldap
uri ldaps://ldap-server.otus.lnx
base dc=otus,dc=lnx
binddn cn=ldapadm,dc=otus,dc=lnx
bindpw gfhjkm
tls_reqcert never
ssl no
tls_cacertdir /etc/openldap/cacerts
```

Конфигурация клиента: nsswitch, nscd, ldap.conf

/etc/nsswitch.conf:

```
passwd:     files sss ldap
shadow:     files sss ldap
group:      files sss ldap
netgroup:   files sss ldap
automount:  files ldap
```

Дополнительно, для экономии “времени” можно поставить пакет nscd (Name Services Caching Daemon), он будет кэшировать вызовы getpwnam, getspnam, gethostbyname и подобные, что уменьшит количество сетевых обращений и позволит пережить короткий сетевой сбой, но у этой штуки есть свои “спецэффекты”.

/etc/openldap/ldap.conf

```
URI ldaps://ldap-server.otus.lnx
BASE dc=otus,dc=lnx
TLS_REQCERT never
```

Спасибо за внимание

Дмитрий Молчанов
Григорий Ожегов