



ОНЛАЙН-ОБРАЗОВАНИЕ

AAA, NSS, LDAP

Централизация управления доступом

Александр Румянцев



Проблемы масштабирования

С увеличением количества серверов затрудняется управление пользователями на этих серверах.

Мы можем:

- “синхронизировать” все ручками или скриптами; важно помнить про унификацию UID между хостами
- “изобретать велосипеды” и управлять частью данных с помощью CM систем типа `ansible`; этот вариант очень часто более практичен, чем что-то готовое и “взрослое”
- Использовать “взрослые” готовые (и не очень) решения



Синхронизируемые данные

- **пользователей (UID)** - необходимо для того, чтобы пользователи могли без проблем получать доступ к своим файлам на разных серверах.
- **группы (GID)**
- **домашние каталоги (не всегда и не везде)**
- **общие настройки для хостов**



Взрослые решения

Изобретено не так уж много механизмов позволяющих решить эту проблему. один из современных - LDAP и Сетевой Каталог.

На основе LDAP работает и Microsoft Active Directory, которая является, по факту, корпоративным стандартом на текущий момент.

В мире opensource есть несколько реализаций ldap-каталогов, например openldap или apache directory server.

Есть и другие, например NIS (Network Information Service) он же Yellow Pages.



LDAP

LDAP (Lightweight Directory Access Protocol) не является протоколом аутентификации или авторизации. Он является протоколом доступа к централизованной базе о пользователях, группах и прочих объектах безопасности.

LDAP функционирует на 389/tcp без SSL/TLS и 636/tcp с SSL/TLS.



LDAP Терминология

- **dn - distinguished name**, выделенное или уникальное имя объекта, аналог **fqdn**. определяется совокупностью атрибутов **cn,ou,dc**
- **cn - common name**, общеупотребительное имя - ФИО, роль, название.
- **dc - domain component** - компонент доменного имени
- **ou - Organizational Unit** - контейнер для объектов служащий для организации и/или группировки

Пример:

dn: cn=Alexander Rumyantsev,ou=Teachers,dc=otus,dc=lan

dn: cn=Pavel Tishkov,ou=Students,dc=otus,dc=lan



Инструменты работы с Idap

- **Apache Directory Studio**
- **Idapvi**



LDAP Schema

В Каталоге LDAP хранятся объекты, свойства которых определяют схемы/шаблоны.

Например к каталогу подключены схемы содержащие шаблоны:

- **unix_user**
- **uid**
- **gid**
- **shell**
- **inet_user**
- **email**
- **jabber**
- **telegram**

Каждая их этих схем может быть подключена к хранимому объекту и предоставит ему свои свойства

Схема - это тоже ветка ldap с dn: cn=schema.

Принадлежность объекта шаблону определяется стандартным массивом атрибутов objectClass

Подключая разные схемы, мы можем хранить что угодно в LDAP, например конфигурацию почтовой системы

Есть несколько стандартных схем для хранения данных пользователей, базовой считается RFC2307bis



NSS (Name Service Switch)

Для GLIBC-функций

- `gethostbyname()`
- `getpwnam()`
- ...etc

существует "обёртка" (`wrapper`) - NSS, позволяющий определить, где и в каком порядке искать пользователей, группы, хосты

Настраивается в файле `/etc/nsswitch.conf`



FreeIPA

Готовое решение, сочетающее в себе

- Сервер LDAP на базе Novell 389 DS с предустановленными схемами
- Сервер Kerberos
- Преднастроенный bind с хранением зон в LDAP
- Web-консоль управления

```
# yum install ipa-server  
# ipa-server-install
```

В процессе установки мы вводим домен, kerberos realm и два пароля.

- IPA Administrator (dn: uid=admin,cn=users,cn=accounts,dc=otus,dc=lan)
- первый пользователь, админ
- Directory Manager (dn: cn=directory manager) - админ LDAP, под ним мы подключаемся к LDAP



Настройка хоста

Этапы настройки:

- OpenLDAP Client
- SSSD
- PAM
- SSH
- NSSwitch
- oddjob



SSSD

Демон, пришедший на замену NSLCD, предоставляющий интерфейс для общения с LDAP, а так же кеширующий запросы

/etc/sss/sss.conf

```
[domain/default]
cache_credentials = True
# debug = 9
ldap_search_base = cn=users,cn=accounts,dc=otus,dc=lan?subtree?
ldap_group_search_base = cn=groups,cn=accounts,dc=otus,dc=lan?subtree?
ldap_sudo_search_base = ou=sudoers,dc=otus,dc=lan?subtree?
# ldap_access_filter = (|(trustmodel=fullaccess)(accessto=vpn1))
ldap_access_filter = (objectClass=*)
id_provider = ldap
auth_provider = ldap
sudo_provider = ldap
access_provider = ldap
ldap_uri = ldaps://192.168.27.110/
## ldap_backup_uri = ldap://192.168.27.110/
ldap_default_bind_dn = uid=reader,cn=users,cn=accounts,dc=otus,dc=lan
ldap_default_authtok = reader
ldap_id_use_start_tls = True
ldap_tls_cacertdir = /etc/openldap/cacerts
ldap_tls_reqcert = allow
[sss]
services = nss, pam, ssh, sudo
config_file_version = 2
domains = default
[nss]
homedir_substring = /home
[pam]
[sudo]
[ssh]
[pac]
[ifp]
```



OpenLDAP Client

SSSD работает через OpenLDAP Client, и не все настройки предоставляет в конфиге. Некоторые приходится править в штатном конфиге клиента

/etc/openldap/ldap.conf

```
URI ldaps://ipa.otus.lan/  
BASE dc=otus,dc=lan  
TLS_CACERTDIR /etc/openldap/cacerts  
TLS_REQCERT allow  
TLS_CRLCHECK none
```



NSSwitch

```
passwd:      files sss
shadow:      files sss
group:       files sss
hosts:       files dns

bootparams:  nisplus [NOTFOUND=return] files

ethers:      files
netmasks:    files
networks:    files
protocols:   files
rpc:         files
services:    files sss

netgroup:    files sss

publickey:   nisplus

automount:   files sss
aliases:     files nisplus

sudoers:     files sss
```



Интеграция SSH с SSSD

/etc/ssh/sshd_config:

```
AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys  
AuthorizedKeysCommandUser nobody
```



oddjobd

Пришел на замену `ram_mkhome_dir`. Представляет из себя демон, работающий от рута и выполняющий некоторые задачи для `ram`
Нас интересует создание домашней директории



PAM

Настраивается стандартной утилитой `authconfig`, либо напрямую файлами

password-auth и **system-auth**:

`auth` `sufficient` `pam_sss.so forward_pass`

`account` `[default=bad success=ok user_unknown=ignore]` `pam_sss.so`

`password` `sufficient` `pam_sss.so use_authtok`

`session` `optional` `pam_oddjob_mkhomedir.so umask=0077`

`session` `optional` `pam_sss.so`



IPA client

Всё это делает за вас
`ipa-client-install --mkhomedir`
из пакета
`freeipa-client`
Но так же не интересно, да?





**Спасибо
за внимание!**

Вопросы?