

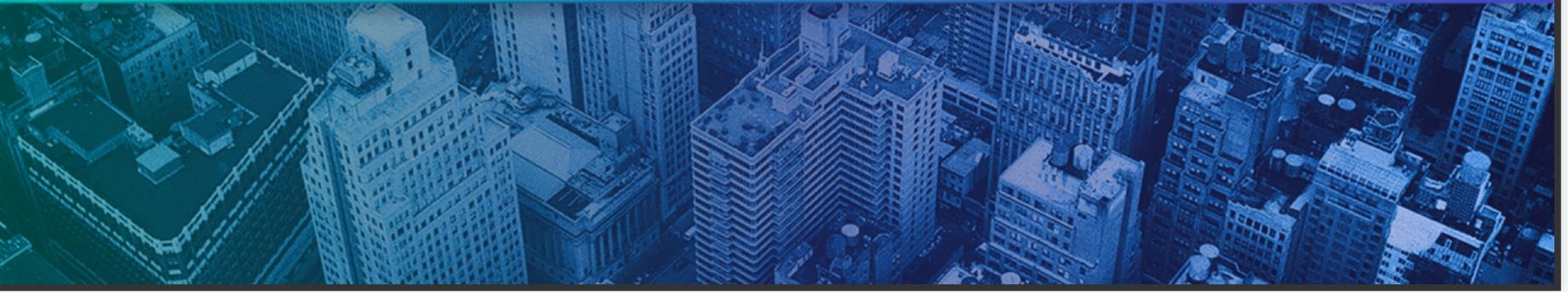


Онлайн-образование



Меня хорошо видно && слышно?

Ставьте  , если все хорошо
Напишите в чат, если есть проблемы



НЕ ЗАБЫТЬ ВКЛЮЧИТЬ
ЗАПИСЬ!!!

AAA, NSS, LDAP

После занятия вы сможете

1. Ориентироваться в терминологии LDAP
2. Подключить клиента freeipa
3. Выбрать систему синхронизации пользователей

Зачем вам это уметь

ВАШ ВАРИАНТ?

Зачем вам это уметь

МОЙ ВАРИАНТ

1. Обслуживание множества хостов
2. Интеграция с Windows LDAP
3. Подготовиться к "внезапной" встрече с LDAP

Централизованное управление доступом

Проблемы масштабирования

- С увеличением количества серверов затрудняется управление пользователями на этих серверах

Что делать? Ваши варианты.

Централизованное управление доступом

Проблемы масштабирования

- С увеличением количества серверов затрудняется управление пользователями на этих серверах

Решения:

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

Готовые 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

Примеры :

```
dn: cn=Alexander Rumyantsev,ou=Teachers,dc=otus,dc=lan  
dn: cn=Pavel Tishkov,ou=Students,dc=otus,dc=lan
```

Инструменты работы с LDAP

- Apache Directory Studio
- Idapvi
- Idapsearch
- ваши варианты?

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

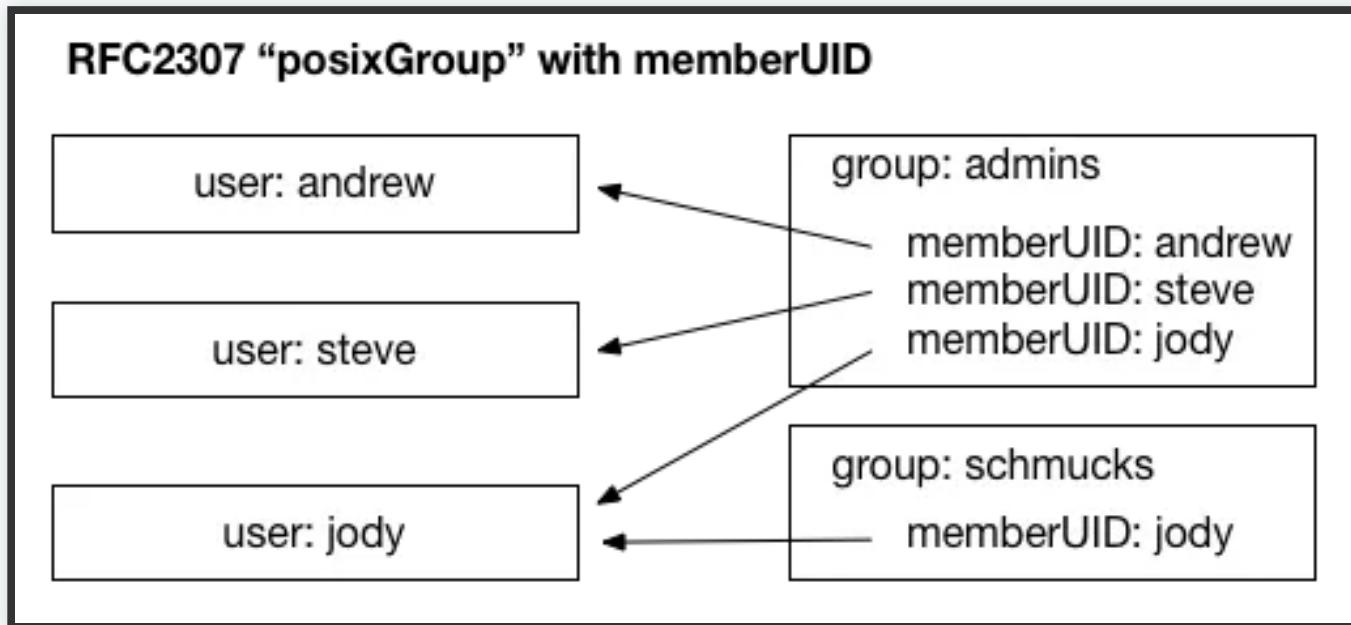
LDAP Schema

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

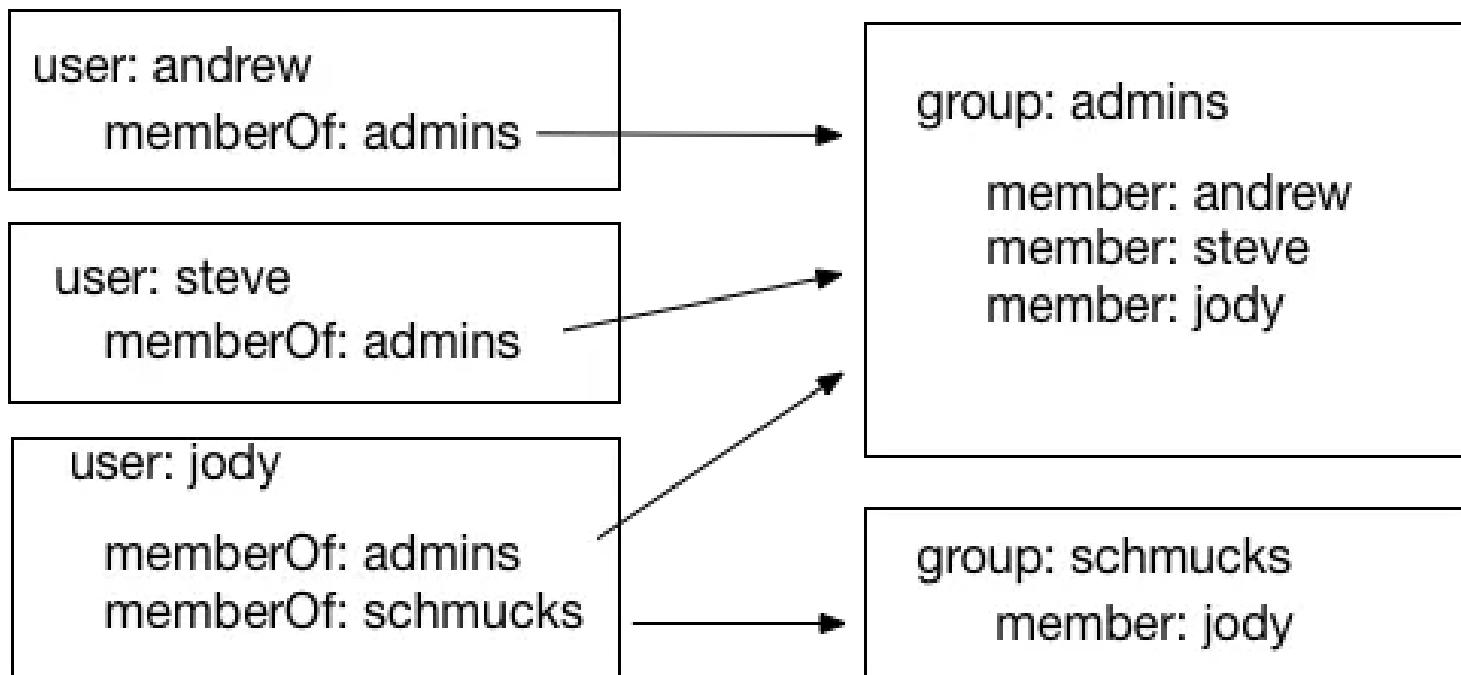
Пример влияния схемы RFC2307



<https://i0.wp.com/unofficialaciguide.com/wp-content/uploads/2019/07/ldap-schema-1.png?w=540&ssl=1>

Пример влияния схемы RFC2307bis

RFC2307bis “memberOf” with groupOfNames, groupOfMembers, etc



Аутентификация vs Авторизация

	Authentication	Authorization
Meaning	"Are you allowed to access X app?"	"What are you allowed to <i>modify</i> in X app?"
Methods	Password, 2FA, MFA, X509 Certificates, Biometric authenticators, WebAuthN	Access control for URI, Access control lists etc.

Напомните каю роль играет PAM и NSS

NSS (Name Service Switch)

Для GLIBC- функций

- gethostbyname()
- getpwname()
- ...etc
- существует " обёртка " (wrapper) - NSS, позволяющий определить , где и в каком порядке искать пользователей , группы , хосты
- Настраивается в файле /etc/nsswitch.conf

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

FreeIPA Client Demo

<https://www.freeipa.org/page/Demo>

- можно подключить любой хост
- сервер раз в сутки очищается
- доступны web interface, cli
- в том числе sudo, selinux и прочее

```
yum -y install freeipa-client
```

Шаги установки FreeIPA

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

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

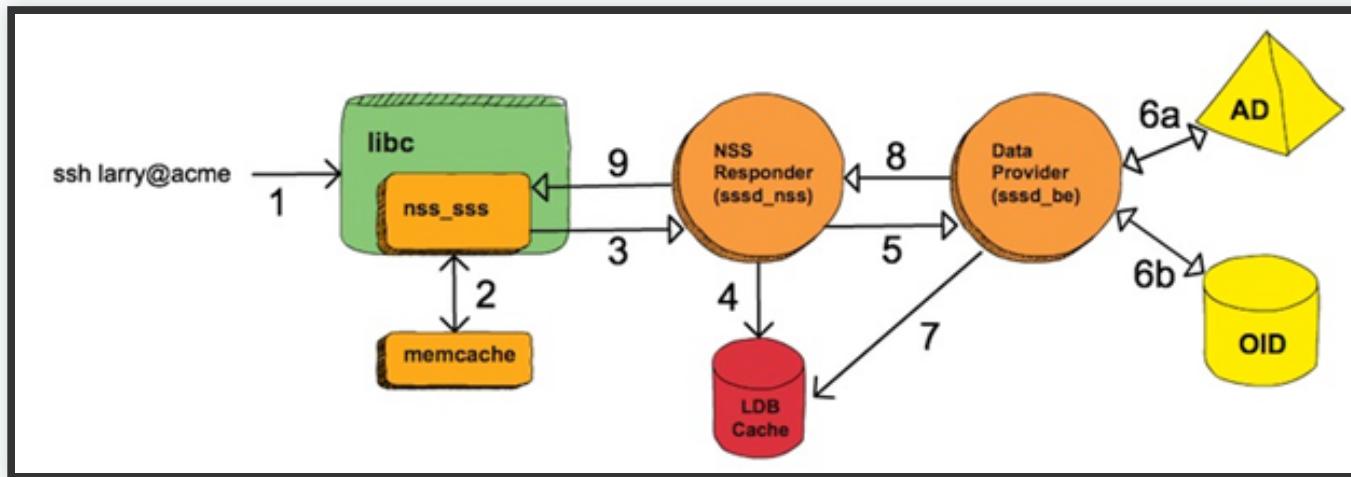
- IPA Administrator (dn: uid=admin,cn=users,cn=accounts,dc=otus,dc=lan) первый пользователь админ
- Directory Manager (dn: cn=directory manager) - админ LDAP, под ним мы подключаемся к LDAP

Этапы настройки хоста

- OpenLDAP Client
- SSSD
- PAM
- SSH
- NSS
- oddjob

Понимание при отладке и настройке.

System Security Services Daemon



- Хранилище: AD, OID (Oracle), OpenLDAP
- Аутентификация пользователей, Авторизация доступа к файлам и директориям по группам
- offline аутентификация, когда хранилище недоступно

System Security Services Daemon

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

```
[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_authzok = reader
```

OpenLDAP Client

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

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

```
/etc/openldap/ldap.conf
```

NSSwitch

```
grep sss /etc/nsswitch.conf
```

```
passwd: files sss
shadow: files sss
group: files sss
hosts: files dns
services: files sss
netgroup: files sss
sudoers: files sss
```

Интеграция SSH с SSSD

```
/etc/ssh/sshd_config:
```

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

oddjobd

Пришел на замену **ram_mkhomedir**. Представляет из себя демон , работающий от рута и выполняющий некоторые задачи для **ram**

Нас интересует создание домашней директории

PAM

Настраивается стандартной утилитой **authconfig**,
authselect (CentOS 8) 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=
session optional pam_sss.so
```

IPA client

Всё шаги делает за вас

```
ipa-client-install --mkhomedir
```

из пакета freeipa-client

Настраивает:

- OpenLDAP Client
- SSSD
- PAM
- SSH
- NSS
- oddjob

IPA жизненный цикл пользователя

Создание, удаление, модификация

- ipa user-find --all
- ipa user-find jdoe
- ipa user-mod USERNAME --shell=/bin/bash
- ipa user-del USERNAME

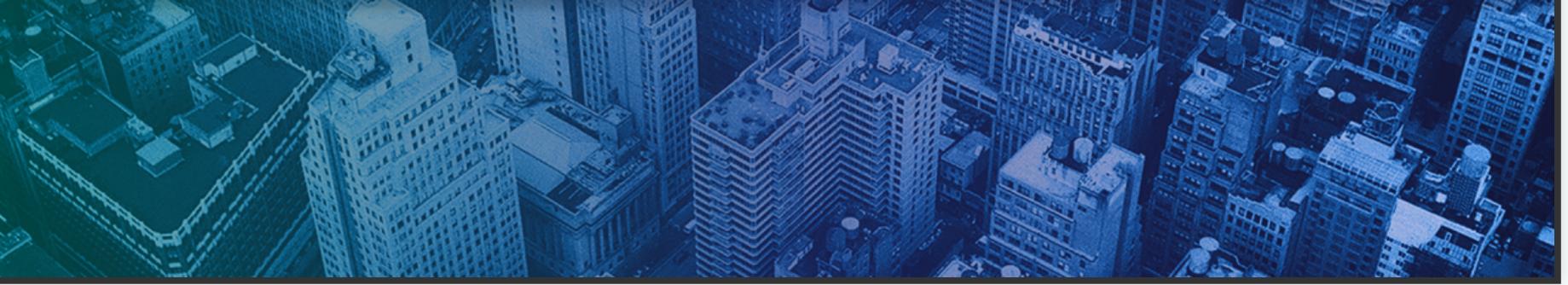
Рефлексия



Отметьте 3 пункта, которые вам запомнились с вебинара



Что вы будете применять в работе из сегодняшнего вебинара?



Заполните, пожалуйста,
опрос о занятии по ссылке в чате