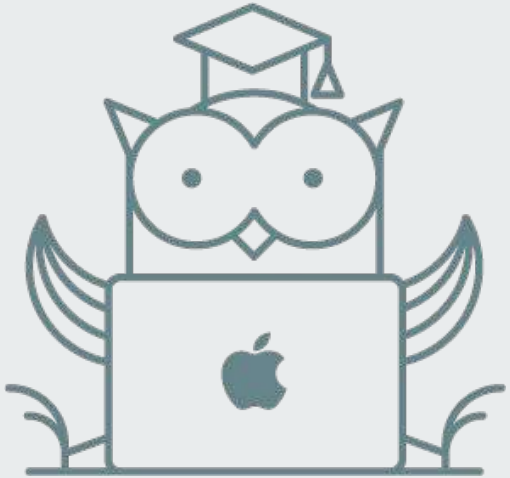
Курс «Администратор Linux»

LDAP, nsswitch

Занятие # 16

Дмитрий Молчанов
Григорий Ожегов



План

- LDAP
- nsswitch
- Настройка pam_ldap,openldap (занятие 2)

Проблемы роста

С увеличением количества серверов затрудняется управление пользователями на этих серверах.

Мы можем:

- “синхронизировать” все ручками или скриптами.
- “изобретать велосипеды” и управлять частью данных с помощью систем типа ansible. Этот вариант очень часто более практичен, чем что-то готовое и “взрослое”
- Использовать “взрослые” готовые решения..

Что же необходимо синхронизировать?

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

Проблемы роста: “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.

Проблемы роста: “взрослые” решения

Эти продукты позволяют решать вопросы управления пользователями в больших сетях, но у них есть свои “нюансы”. Например не все работает из коробки у бесплатных версий, а те, у которых все работает - платные.

Сетевой каталог и 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=Dmitry Molchanov,ou=Teachers,dc=otus,dc=lnx
- dn: cn=Pavel Tishkov,ou=Students,dc=otus,dc=lnx

Структура LDAP

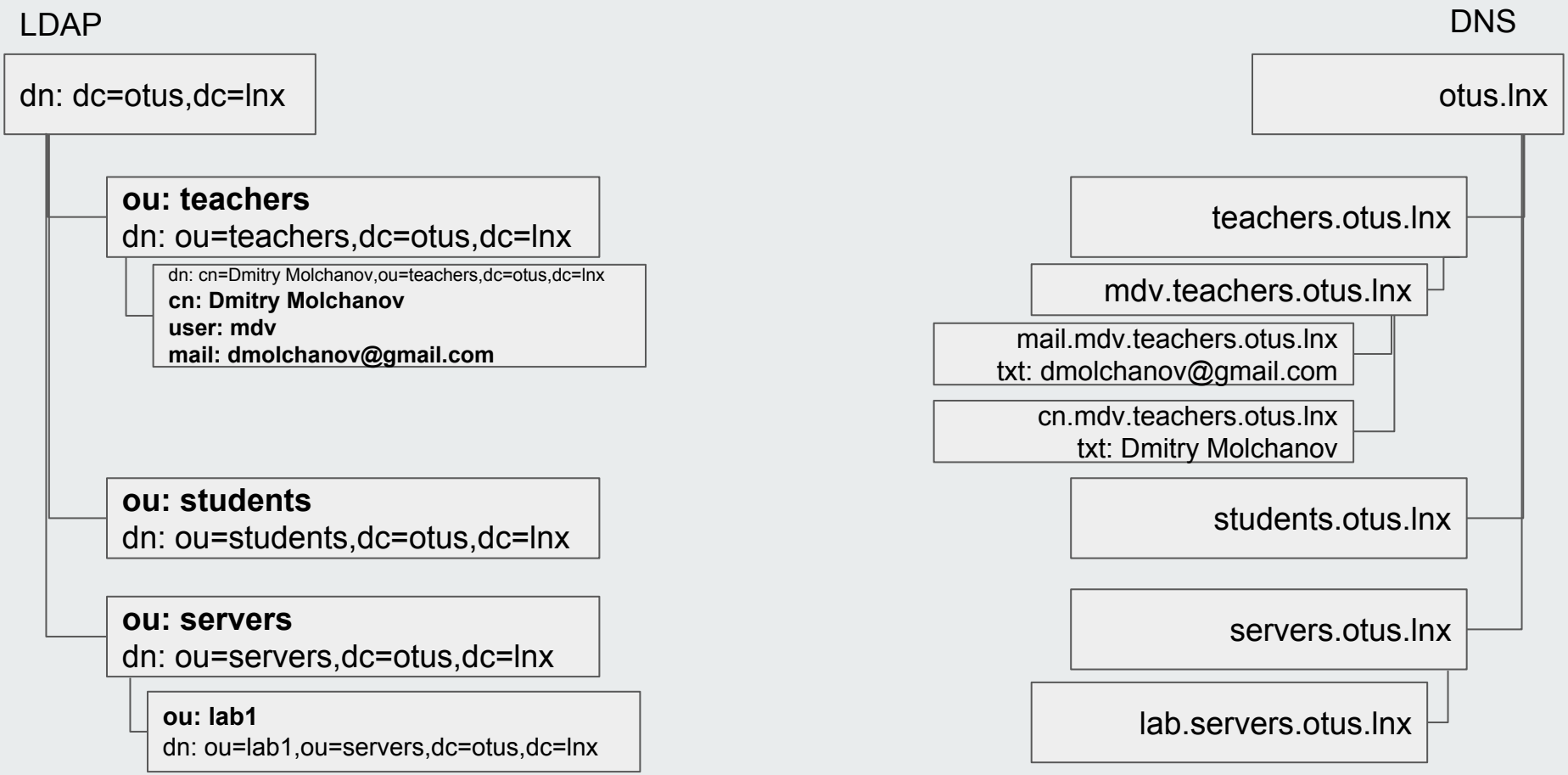


Схема LDAP

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

Результирующим объектом будет:

- dn: cn=Dmitry Molchanov,ou=users,dc=otus,dc=lnx
  DN - уникальный путь к объекту в каталоге LDAP
  - objectClass: unix_user
  - objectClass: inet_user
  - cn: Dmitry Molchanov
  - uid: 1000
  - gid: 1000
  - shell: /usr/bin/bash
  - email: dmolchanov@gmail.com
  - jabber: (nil)
  - telegram: @dmolchanov

Таким образом набор свойств объекта с данным DN равен сумме свойств схем подключенных к объекту. Не все свойства (атрибуты) обязательны.

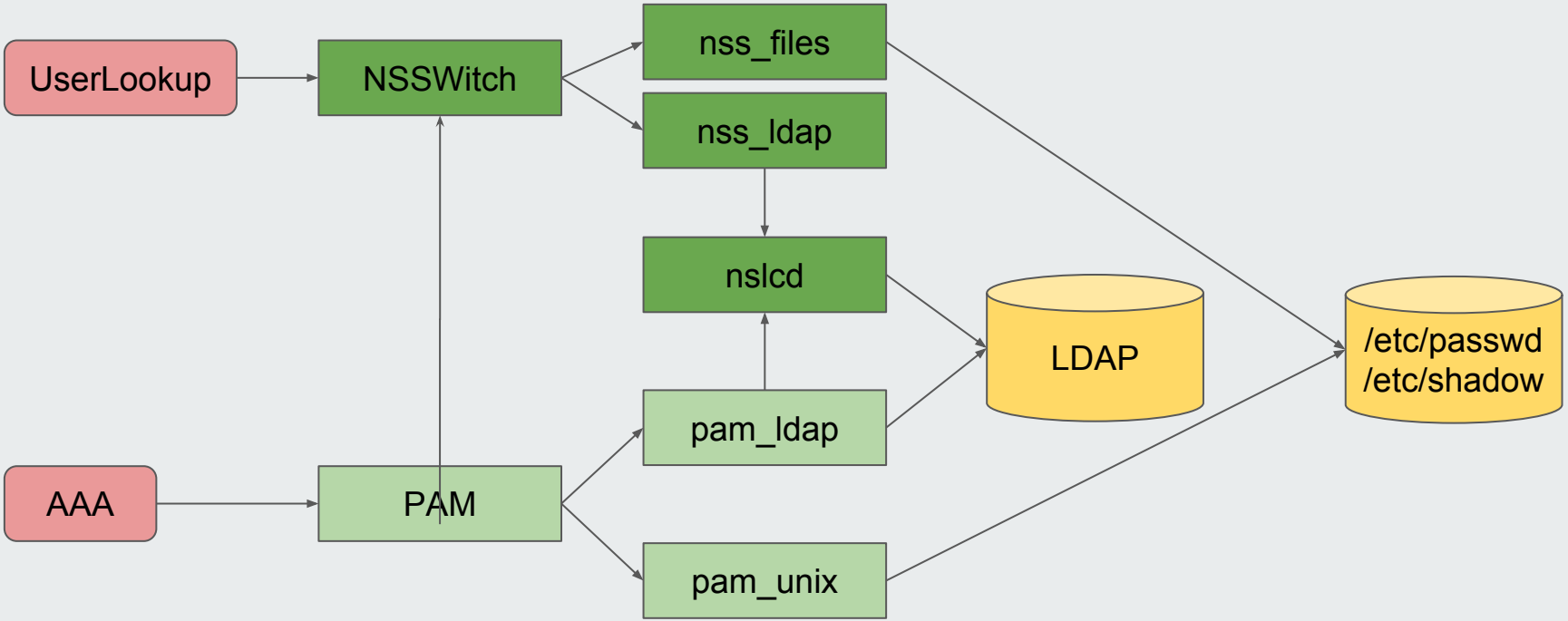
Возможности LDAP

LDAP-каталог позволяет хранить не только информацию о пользователях, группах, но и различную другую информацию:

- mail aliases
- ip services
- информацию для /etc/hosts

Также для пользователей можно хранить множество дополнительных атрибутов расширяя объекты пользователей новыми шаблонами (objectClass). Например можно определять на какие сервера можно ходить пользователю, а на какие - нет.

Поиск пользователя и AAA



NSSwitch

NSSwitch (Name Service Switch) - подсистема которая позволяет делать разрешения имен в разных источниках. Например именно там настраивается в каком порядке разрешать имя в ip-адрес (/etc/hosts и DNS-запрос) или наоборот. Или в каком порядке смотреть базы для поиска пользователей или групп.

Настраивается в файле /etc/nsswitch.conf

nslcd

Демон который выполняет часть функций общения с ldap для NSS и pam_ldap.

настраивается в /etc/nslcd.conf, содержит настройки для доступа к ldap-серверу.

Спасибо за внимание

Дмитрий Молчанов
Григорий Ожегов