



Администратор Linux LDAP



Проверить, идет ли запись

Меня хорошо видно && слышно?



Ставим "+", если все хорошо
"-", если есть проблемы

Тема вебинара

LDAP. Централизованная авторизация и аутентификация



Федоров Иван Романович

Технический директор ГК "Илотех"

Опыт:

Более 10 лет в IT-сфере

Аспирант университета ИТМО по направлению "Информационная безопасность"

Многократный победитель различных конкурсов и хакатонов (команда IBI Solutions)

Эл. почта: ifedorov.devops@gmail.com



Правила вебинара



Активно
участвуем



Off-topic обсуждаем
в группе Telegram
OTUS-Linux-2022-12



Задаем вопрос
в чат или голосом



Вопросы вижу в чате,
могу ответить не сразу



Маршрут вебинара

Знакомство

Введение

LDAP

FreeIPA

Практика

Рефлексия



Цели вебинара

К концу занятия вы сможете

1. Понять как работает LDAP и для чего он нужен



-
2. Устанавливать FreeIPA



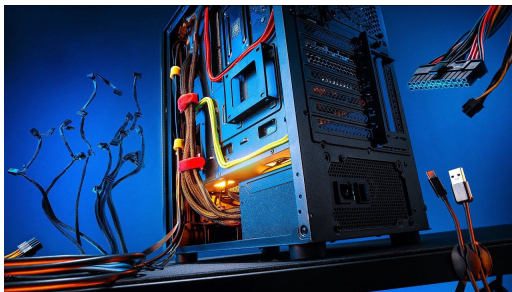
-
3. Создавать пользователей централизованно с помощью “взрослых” решений



Designed by Pngtree

Смысл

Зачем вам это уметь



Введение

Проблема

Большое количество серверов и различных пользователей



Варианты решения

- **синхронизировать все ручками или скриптами:**
 - пользователи (важно помнить про унификацию UID между хостами) — необходимо для того, чтобы была возможность без проблем получать доступ к своим файлам на разных серверах
 - группы (GID)
 - домашние каталоги (не всегда и не везде)
 - общие настройки для хостов
- **“изобретать велосипеды”**, управлять частью данных с помощью систем типа ansible (этот вариант очень часто более практичен, чем настройка чего-то готового)
- **использовать готовые “взрослые” решения**

“Взрослые” готовые решения

LDAP и сетевой каталог



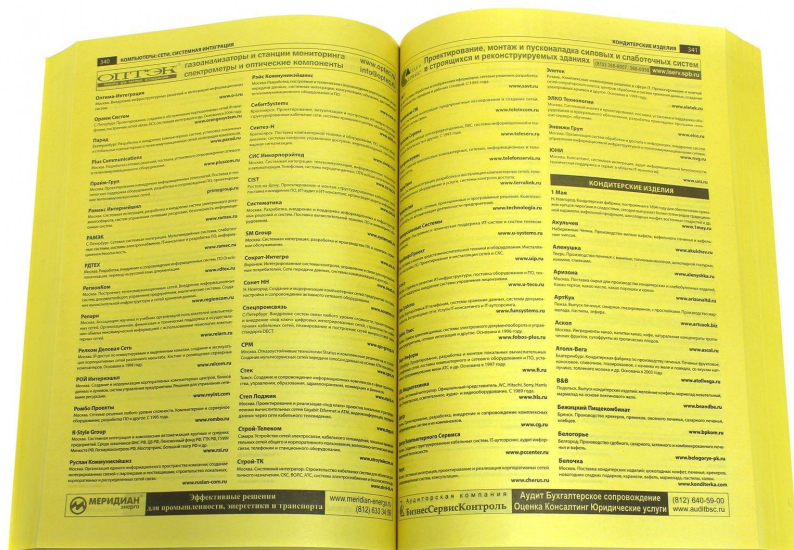
LDAP

LDAP

LDAP (Lightweight Directory Access Protocol) — протокол, определяющий методы, посредством которых осуществляется доступ к данным каталога с иерархической структурой.

- **Не является протоколом аутентификации или авторизации**
- Определяет и описывает, как данные **представлены** в службе каталогов
- Определяет, каким образом данные загружаются (импортируются) и выгружаются (экспортируются) из службы каталогов
- **Не определяет, как происходит хранение и манипулирование данными**
- Работает на 389/tcp без SSL/TLS и 636/tcp с SSL/TLS
- Пример данных: записи о пользователях, группах, контактная информация, место работы
- Сложности для понимания:
 - своеобразная терминология и сокращения
 - используется как компонент других систем

Для упрощения понимания

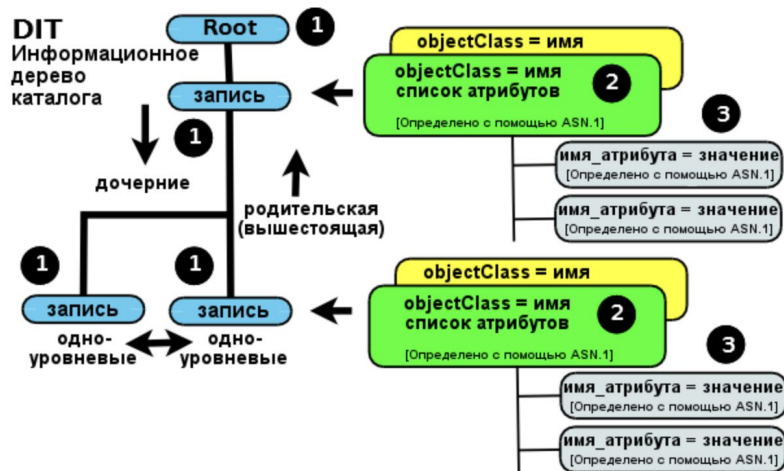


Структура дерева объектов

В LDAP-системе данные представлены как иерархия объектов, каждый из которых называется **записью**. Полученная в результате древовидная структура называется **Информационным деревом каталога (Directory Information Tree, DIT)**. Верхнюю часть данного дерева обычно называют **корнем (root)**, (а также **базой (base)** или **суффиксом (suffix)**).

У каждой записи есть одна **родительская запись (объект)** и ноль или более **дочерних записей (объектов)**. Каждая дочерняя запись (объект) является **одноуровневой (братской)** по отношению к другим дочерним записям своей родительской записи.

Каждая запись состоит из (является экземпляром) одного или нескольких **объектных классов (objectClass)**. Объектные классы содержат ноль или более **атрибутов (attribute)**. Атрибуты имеют имена (и, иногда, аббревиатуры или псевдонимы) и обычно содержат данные.



Объектные классы

Объектные классы — “контейнеры” атрибутов.

- У каждого объектного класса есть уникальное имя.
- Объектный класс определяет, должен (MUST) ли входящий в него атрибут присутствовать в записи (обязательный атрибут), или он может (MAY) присутствовать (необязательный атрибут).
- Каждый объектный класс принадлежит к определённому типу: он может быть структурным (STRUCTURAL), вспомогательным (AUXILIARY) или абстрактным (ABSTRACT). В записи должен быть один и только один структурный (STRUCTURAL) объектный класс и может быть ноль или более вспомогательных (AUXILIARY) объектных классов.
- Объектный класс может быть частью иерархии, в этом случае он наследует все характеристики своего родительского объектного класса (классов) (включая все содержащиеся в них атрибуты).
- Существует огромное число предопределённых объектных классов, в каждом из которых полно атрибутов для почти всех возможных применений каталогов LDAP.

Атрибуты

Атрибуты — пары “ключ-значение”.

- Каждый атрибут имеет имя (а также может иметь короткое имя или псевдоним) и обычно содержит данные.
- Все атрибуты являются членами одного или нескольких объектных классов.
- Каждый атрибут определяет тип данных, которые он может содержать (ключевое слово SYNTAX в определении атрибута).
- Атрибуты могут быть частью иерархии, в этом случае дочерний атрибут наследует все характеристики родительского атрибута.
- У атрибутов может быть одно (SINGLE-VALUE) или несколько (MULTI-VALUE) значений.

Пример структуры DIT

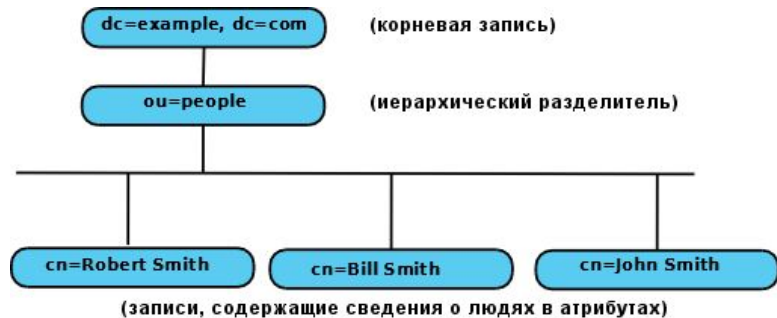
- **dn** — **Distinguished Name**, выделенное или уникальное имя объекта, аналог fqdn (определяется совокупностью атрибутов cn,ou,dc)
- **cn** — **Common Name**, общеупотребительное имя (ФИО , роль , название).
- **dc** — **Domain Component** (компонент доменного имени)
- **ou** — **Organizational Unit** (контейнер для объектов служащий для организации и / или группировки)

Еще немного терминов:

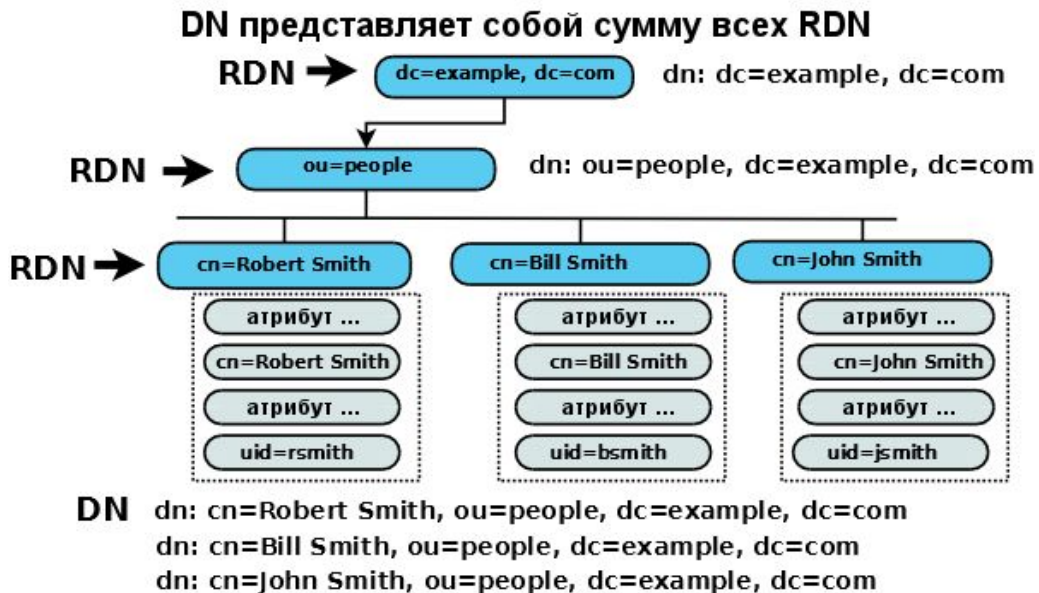
Относительно уникальное имя (**Relative Distinguished Name, RDN**) — имя, уникальное по отношению к родительской записи.

Пример dn:

cn=Robert Smith,ou=people,dc=example,dc=com



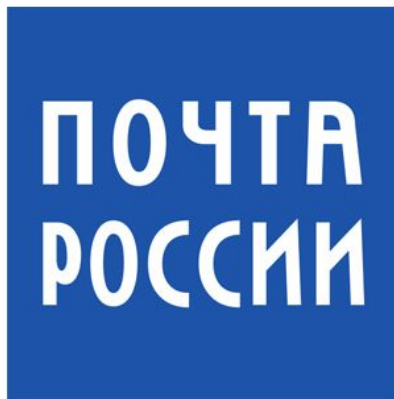
Еще раз закрепим...



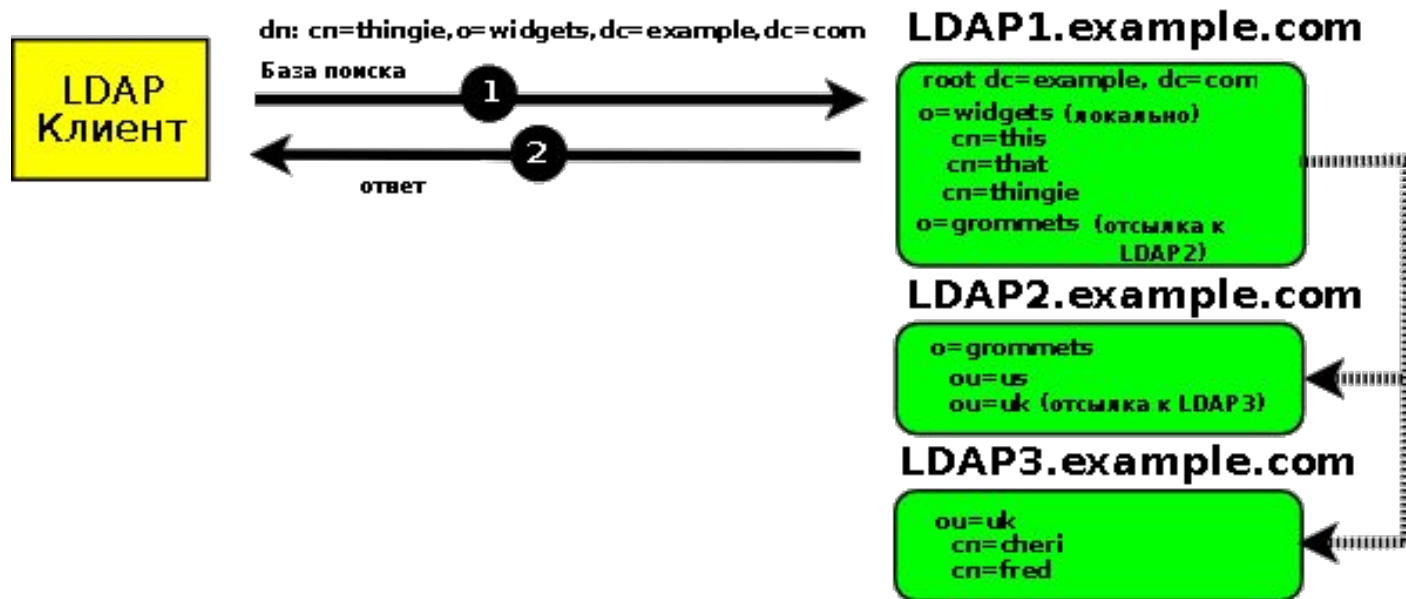
Для упрощения понимания

Получатель: Иванов Иван Иванович, ул. Строителей, д. 25, кв. 12, Москва

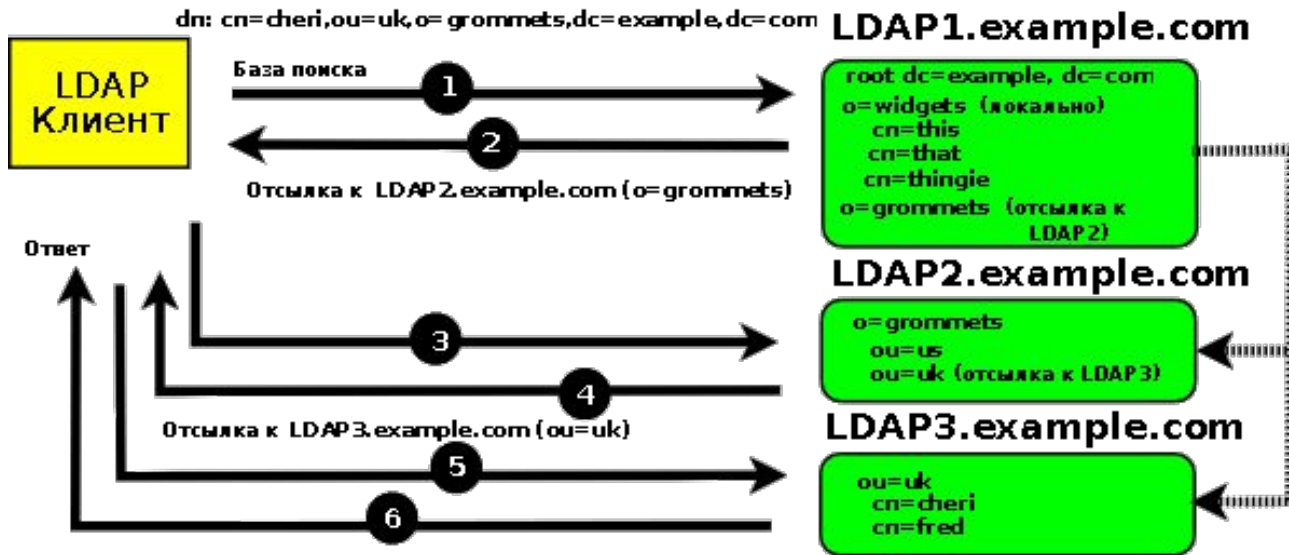
Получатель: Иванов Иван Иванович, ул. Декабристов, д. 54, кв. 3, Санкт-Петербург



Отсылки LDAP (1)



Отсылки LDAP (2)



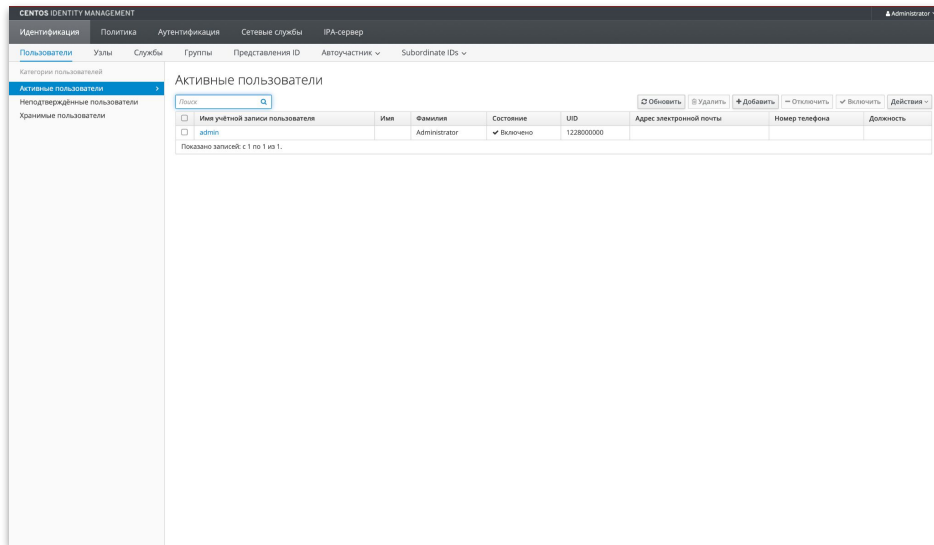
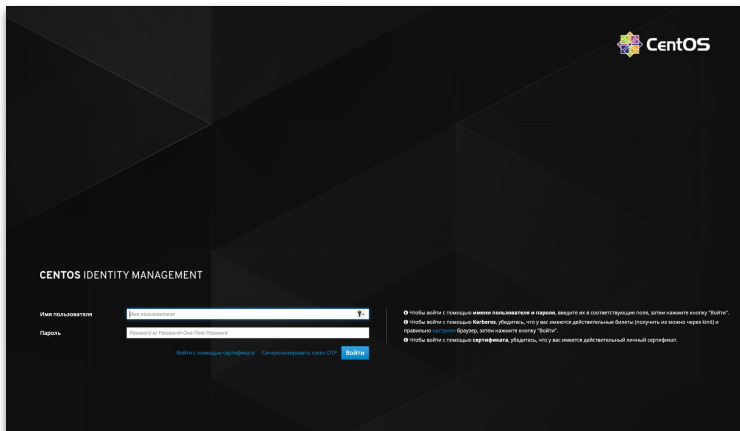
**Все хорошо?
Есть ли вопросы?**

FreeIPA

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-интерфейс управления



Установка

```
$ vim /etc/hosts
10.0.0.11 ipa.ivan-gb.ru ipa
```

```
$ yum install -y @idm:DL1
$ yum install -y ipa-server
$ ipa-server-install
```

```
The log file for this installation can be found in /var/log/ipaserver-install.log
```

```
=====
This program will set up the IPA Server.
Version 4.9.11
```

```
...
```

```
Do you want to configure integrated DNS (BIND)? [no]: no
Server host name [ipa.ivan-gb.ru]:
Please confirm the domain name [ivan-gb.ru]:
Please provide a realm name [IVAN-GB.RU]:
Directory Manager password:
Password (confirm):
IPA admin password:
Password (confirm):
NetBIOS domain name [IVAN-GB]:
Do you want to configure chrony with NTP server or pool address? [no]: no
Continue to configure the system with these values? [no]: yes
```

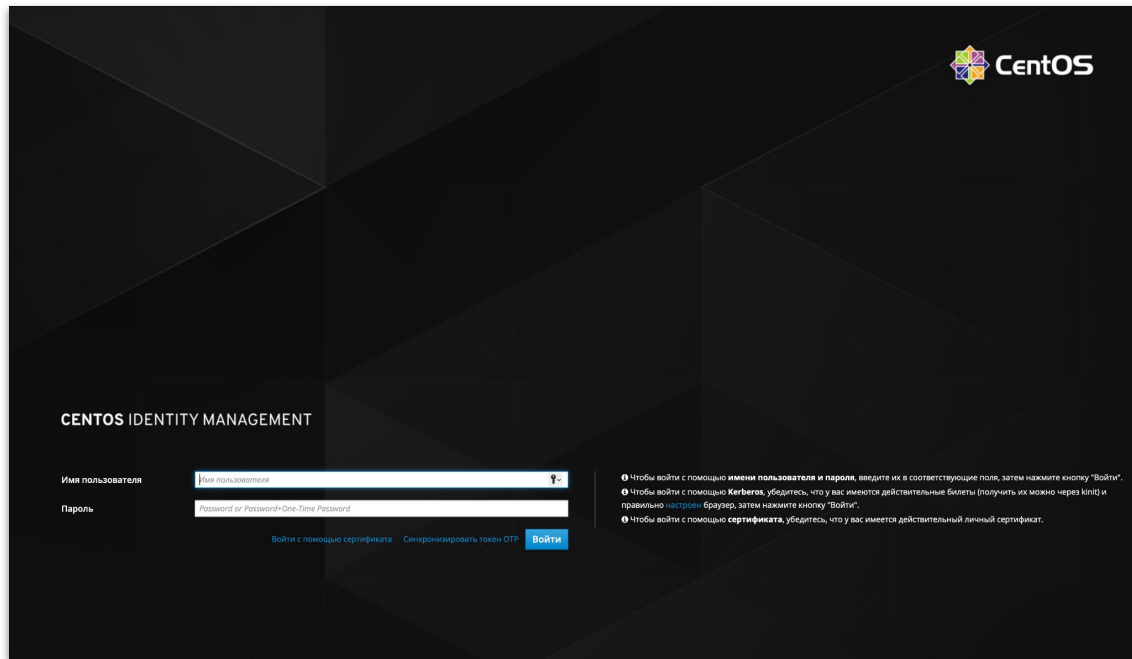
```
=====
Setup complete
```

```
...
```

```
The ipa-server-install command was successful
```

Проверка

http://<hostname>/ipa/ui



The image shows the login interface for CentOS Identity Management. The background is dark with a geometric pattern. In the top right corner is the CentOS logo. The main heading is "CENTOS IDENTITY MANAGEMENT". Below it are two input fields: "Имя пользователя" (Username) and "Пароль" (Password). The password field has a hint: "Password or Password-Only-Time Password". Below the password field are three links: "Войти с помощью сертификата", "Синхронизировать токен OTP", and a blue "Войти" (Login) button. To the right of the login fields is a list of instructions in Russian.

CENTOS IDENTITY MANAGEMENT

Имя пользователя

Пароль

[Войти с помощью сертификата](#) [Синхронизировать токен OTP](#) [Войти](#)

- ❶ Чтобы войти с помощью имени пользователя и пароля, введите их в соответствующие поля, затем нажмите кнопку "Войти".
- ❷ Чтобы войти с помощью **Keycloak**, убедитесь, что у вас имеются действительные билеты (получить их можно через kinit и правильно настроен браузер, затем нажмите кнопку "Войти").
- ❸ Чтобы войти с помощью **сертификата**, убедитесь, что у вас имеется действительный личный сертификат.



Установка клиента

```
$ vim /etc/hosts  
10.0.0.11 ipa.ivan-gb.ru ipa
```

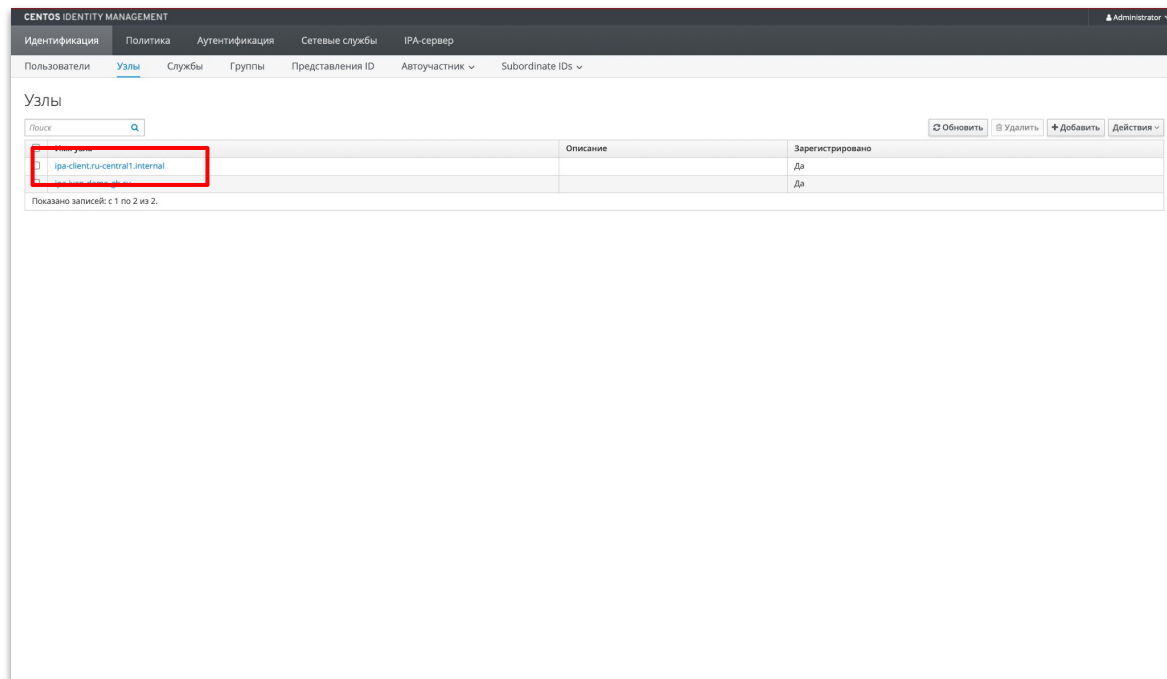
```
$ yum install -y freeipa-client  
$ ipa-client-install --mkhomedir --domain=IVAN-GB.RU --server=ipa.ivan-gb.ru --no-ntp -p  
admin -w <password>
```

...

```
The ipa-client-install command was successful
```

Проверка

`http://<hostname>/ipa/ui/#/e/host/search`



Управление пользователями

Создание пользователя

```
$ ipa user-add otus-user --first=Otus --last=User --password
```

Вывод всех пользователей

```
$ ipa user-find --all
```

Поиск

```
$ ipa user-find otus
```

Изменение

```
$ ipa user-mod USERNAME --shell=/bin/bash
```

Удаление

```
$ ipa user-del USERNAME
```

**Как настроение?
Есть ли вопросы?**

Kerberos

Kerberos

Kerberos предоставляет как сетевую аутентификацию, так и безопасный метод, посредством которого может быть проведена авторизация без необходимости повторного ввода пароля или предоставления других удостоверяющих данных.

Используется для обеспечения работы **технологии единого входа (Single Sign-on, SSO)**



Вопросы?



Ставим “+”,
если вопросы есть



Ставим “-”,
если вопросов нет



Рефлексия

Цели вебинара

К концу занятия вы сможете

1. Понять как работает LDAP и для чего он нужен



-
2. Устанавливать FreeIPA



-
3. Создавать пользователей централизованно с помощью “взрослых” решений



Designed by Pngtree

Рефлексия



С какими впечатлениями уходите с вебинара?



Как будете применять на практике то, что узнали на вебинаре?

**Заполните, пожалуйста,
опрос о занятии
по ссылке в чате**