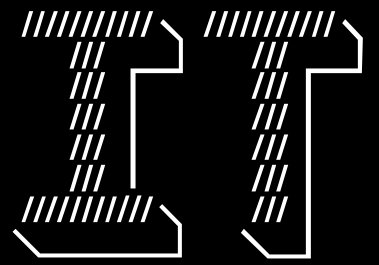
LDAP: туда и обратно

Сергей Печенко

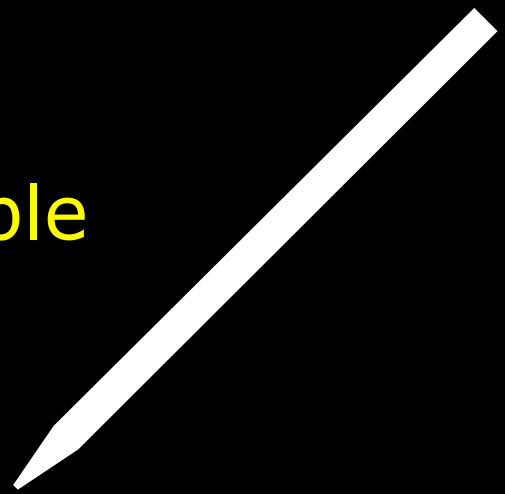
Москва, 2019

Райффайзен



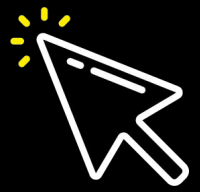
Об авторе

- За клавиатурой 27^{й} год
- Оберегаю разные production’ы с 2013
- Изучаю и воплощаю DevOps-практики с 2014
- @tnt4brain
- @ru_gitlab/@ru_logs/@ru_ldap/@pro_ansible
- bantu.ru



TL;DR

- Истоки
- Почему LDAP?
- Сервер: reOpenLDAP
- Веб-клиент: phpLDAPadmin



One Ring to rule them all,
One Ring to find them,
One Ring to bring them all
And in the Darkness bind them

Истоки

Lightweight Directory Access Protocol

- Древовидная база данных, хранящая контейнеры и объекты
- Формат контейнеров, объектов и доступных фильтров для поиска определяется загруженными схемами
- Большинство реализаций оптимизированы для поиска и чтения
- Часто используется для хранения информации об учётных записях и группах пользователей

Занимательные факты

- LDAP был создан для замены DAP (X.519), потому что тот оказался слишком сложен в реализации
- Существуют штучное число массово используемых реализаций LDAP-сервера
- Существуют клиентские библиотеки как для Top10 языков, так и для множества менее популярных
- Существует несколько вариантов UI

Широко используемые разновидности

ActiveDirectory

- Правит миром Windows, является основой доменов.
- Взаимодействует с массой closed-source компонентов → нерасширяемый

389ds

- Является основой FreeIPA от RedHat.

OpenLDAP

- Поставляется со многими дистрибутивами Linux/Unix.

ReOpenLDAP

- Работает в инфраструктуре мобильного оператора, принимавшего прошлый митап (по информации от мейнтейнера проекта).

Почему LDAP?

Что даёт LDAP Ops’ам?

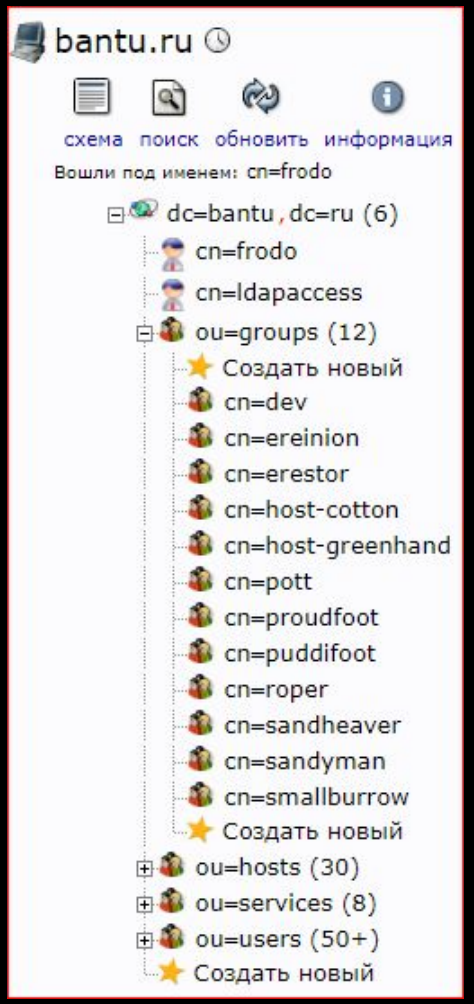
1. Единую точку хранения и управления
2. Возможность поэтапного расширения схемы хранимых данных
3. Возможность хранения и модификации конфигурации базы её же штатными средствами
4. Лёгкую реализацию HA как вида «master-slave», так и «master-master»
5. Один протокол и хранилище для разных систем: Windows, macOS, Linux, Solaris, FreeBSD
6. Мощную систему контроля прав доступа с точностью до атрибута
7. LDIF: инструментарий для поддержки IaaC
8. Ссылки (referrals), раскрываемые как клиентами, так и сервером

Что даёт LDAP Dev’ам?

1. Древовидную БД “на вырост” с гибкой подстройкой под задачи
2. Кроссплатформенность
3. Широкий выбор языков, имеющих клиентские компоненты LDAP
4. «Автомагическая» проверка соответствия данных схеме на уровне сервера

Создание и наполнение дерева: читы

1. LDAP-суффикс = домен компании: dc=bantu,dc=ru
2. УЗ суперадмина - вне ветви, хранящей УЗ пользователей
3. УЗ синхронизации - там же
4. Однородные объекты собираем в свои «ou»
5. RFC2307 читать обязательно!



Расширения: личный top

1. dynlist
2. memberof
3. ppolicy
4. refint
5. syncprov
6. unique

Полезные схемы

Райффайзен

1. sudoers
2. ssh-pubkey
3. ldapns

Репликация:

```
dn: olcOverlay={0}syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: {0}syncprov
olcSpCheckpoint: 50 5
olcSpSessionLog: 100
olcSpReloadHint: TRUE
```

```
dn: olcDatabase={1}mdb,cn=config
olcSyncrepl: {0}rid=001
  bindmethod=simple
  binddn="cn=frodo,dc=bantu,dc=ru"
  credentials="secret"
  provider="ldap://<master>:389"
  retry="5 100 60 +"
  rid="000"
  searchbase="dc=bantu,dc=ru"
  type=refreshAndPersist
  attrs="*,+"
```

Сервер ReOpenLDAP

Реализация LDAP-сервера

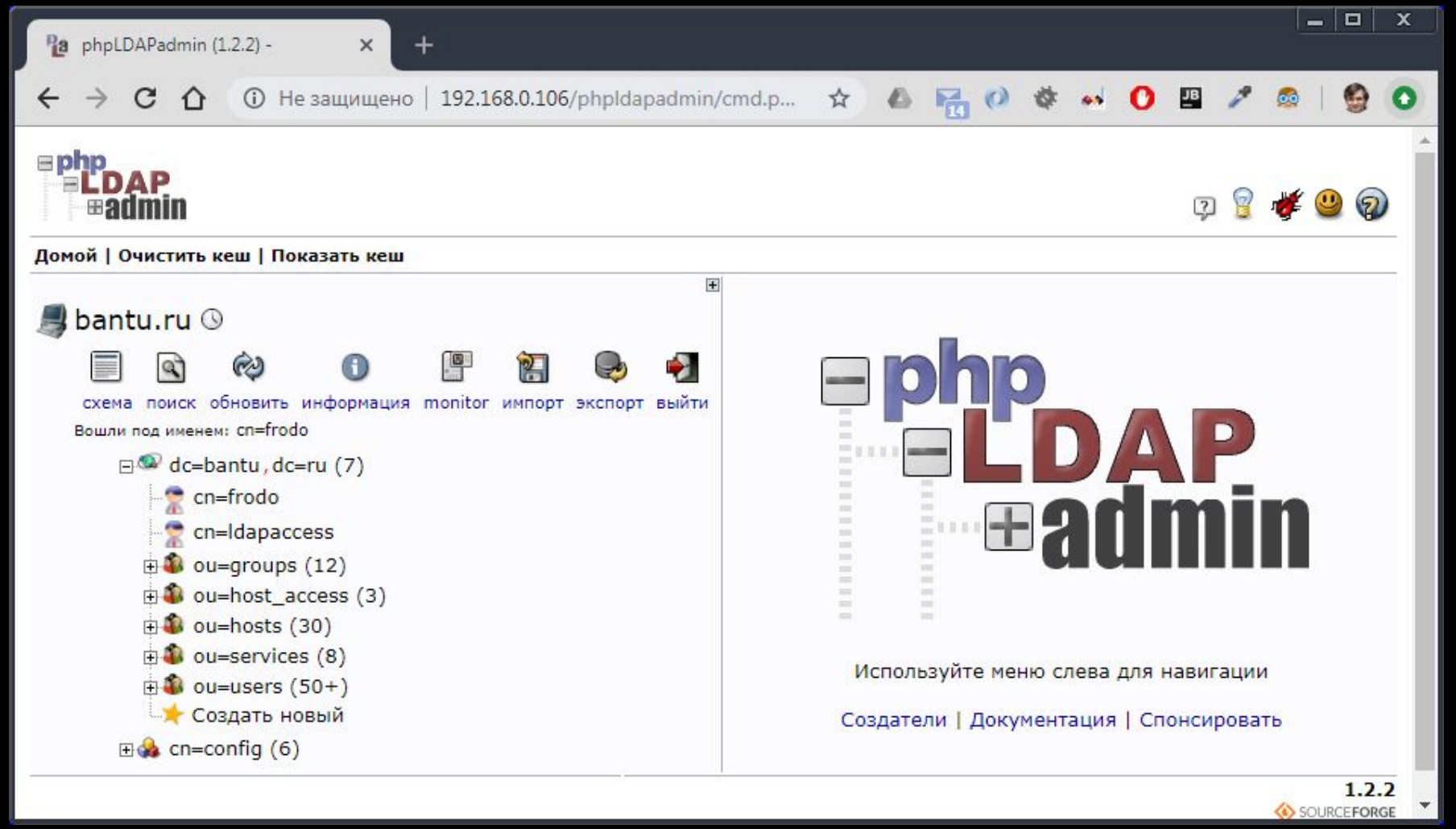
1. Форк OpenLDAP: https://github.com/leo-yuriev/ReOpenLDAP, совместимая по API/протоколу замена
2. Master-master, достаточно надёжный, чтобы работать в серьёзном prod’е
3. 9 issues… OH WAIT!!!…
4. Made in Russia

Веб-клиент phpLDAPadmin

Веб-клиент LDAP

1. Возможность подстройки под бизнес-процессы организации
2. Поддержка работы с атрибутами, требующими уникальности (uid, gid)
3. Поддержка чтения конфигурации непосредственно с сервера

Интерфейс - что это?...



Выводы:

Спасибо
за внимание!

sergey@bantu.ru

Райффайзен