

Интеграция FreeIPA с Active Directory

- FreeIPA - «Active Directory» в мире GNU/Linux
- Варианты интеграции. Прямая и непрямая
- Межлесовое доверие «AD» <-> FreeIPA

Управление учётными данными – что это?

- **"Управление учётными данными** ([англ. Identity management](#), сокр. **IdM**, иногда **IDM**) — комплекс подходов, практик, технологий и специальных программных средств для управления учётными данными пользователей, системами контроля и управления доступом (СКУД), с целью повышения безопасности и производительности информационных систем при одновременном снижении затрат, оптимизации времени простоя и сокращения количества повторяющихся задач.

@ Wikipedia

- Учетные записи: Пользователи, компьютеры, сервисы
- Аутентификация: пароли, биометрия, Двухфакторная проверка
- Авторизация: Политики, Списки контроля доступа, правила доступа
- Вручную? На каждом компьютере свои юзеры и пароли? Нет! Только не это!

FreeIPA - «Active Directory» в мире GNU/Linux

- Введение
- История продукта
- Описание возможностей

Почему «AD» так распространено?

- Интегрировано из коробки со всеми продуктами Microsoft
- Относительно легко ставить, настраивать и управлять
- Легко подключать клиентов
- Сложность решения скрыта в типовых задачах и админа и тем более скрыта от пользователя
- Удобные инструменты администрирования

Аналоги функционала Active Directory в мире Open Source

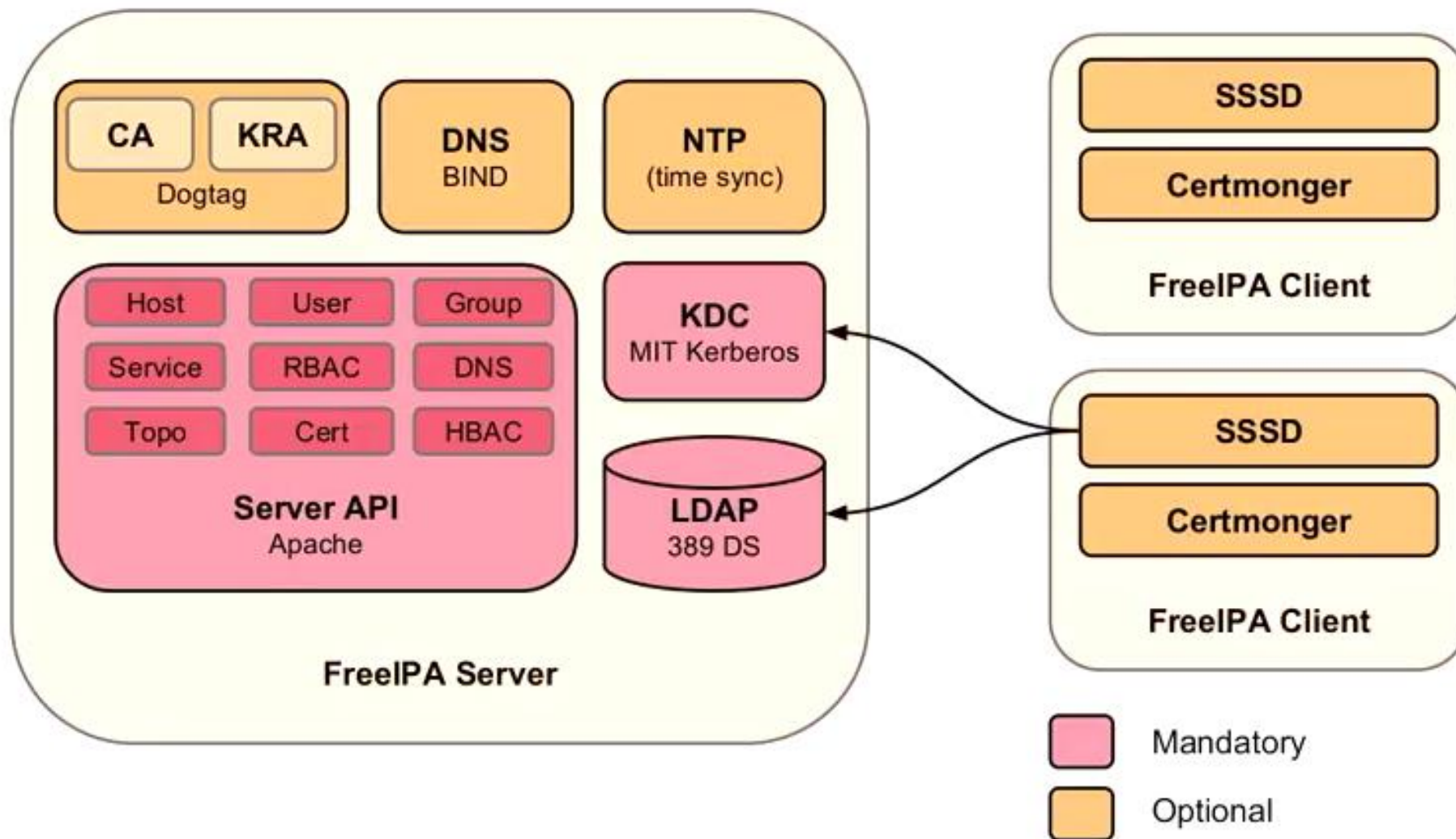
- Много инструментов, каждый для своих задач
 - “принцип linux: делать одну вещь и делать её хорошо”
- Сложно или никак не интегрировать разные реализации
- Много операций по настройке и поддержке
- Вручную поставить Openldap+Kerberos и потом это поддерживать? Только не на предприятии!
- Слишком много возможных вариантов решений и их настройки
- Плохо с инструментами управления

FreeIPA описание

- FreeIPA – сервер каталога, аутентификации, политик доступа, настроек. для GNU/Linux
- IPA – Identity Policy Audit
- Задача – принести в мир GNU/Linux удобное в управлении и развертывании средство для управлению GNU/Linux операционных систем



Компоненты FreeIPA



Средства администрирования: CLI, WEB UI, JSON-RPC REST

```
$ kinit admin
```

Password for admin@EXAMPLE.COM:

```
$ klist
```

Ticket cache: FILE:/tmp/krb5cc_0

Default principal: admin@EXAMPLE.COM

Valid starting Expires Service principal

10/15/12 10:47:35 10/16/12 10:47:34

krbtgt/EXAMPLE.COM@...

```
$ ipa user-add --first=John --last=Doe jdoe --random
```

-----Added user "jdoe"

-----User login: jdoe

First name: John

Last name: Doe

Full name: John Doe

Display name: John Doe

Initials: JD

Home directory: /home/jdoe

GECOS field: John Doe

Login shell: /bin/sh

Kerberos principal: jdoe@EXAMPLE.COM

Email address: jdoe@example.com

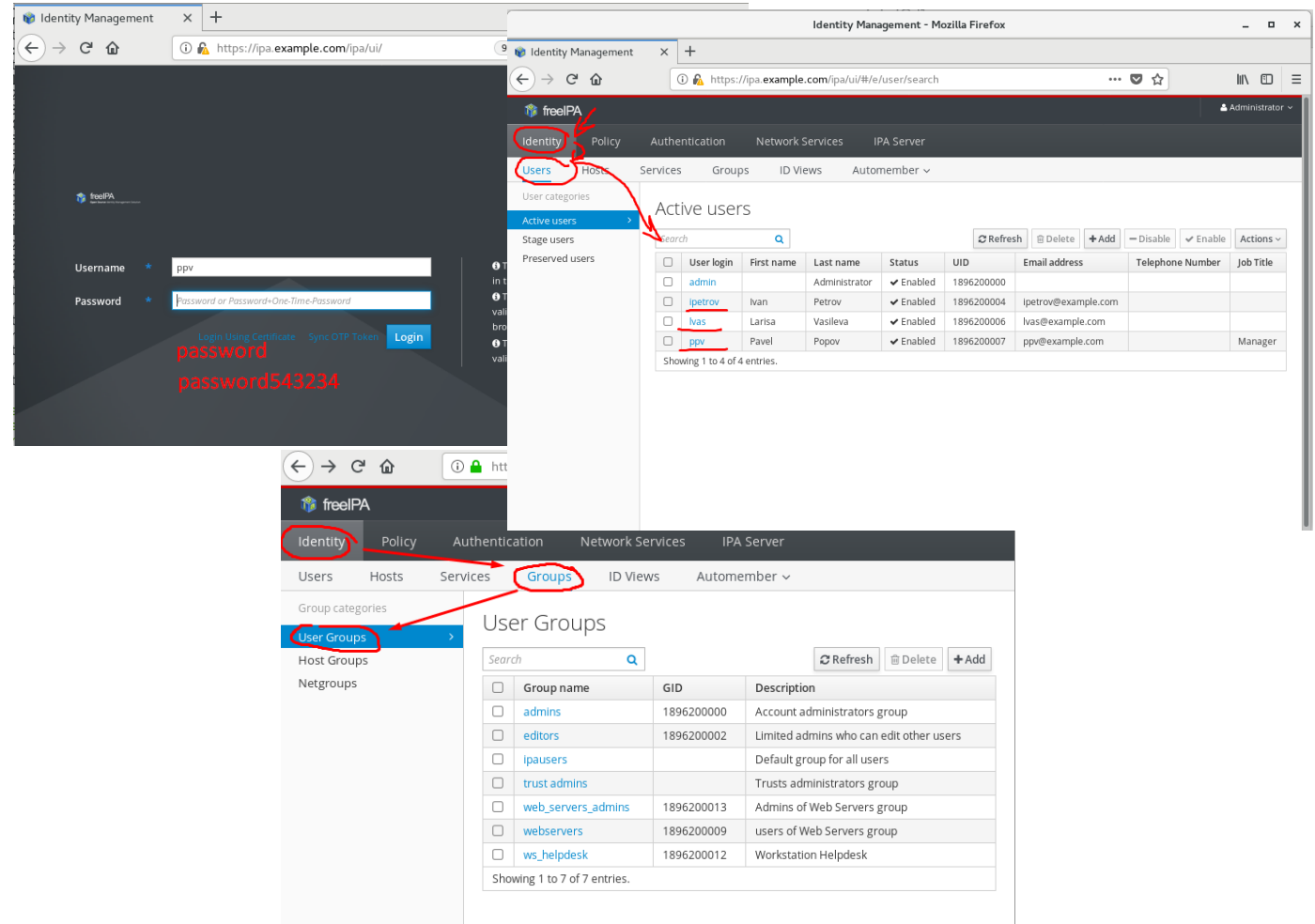
Random password: xMc2XkI=ivVM

UID: 1998400002

GID: 1998400002

Password: True

Kerberos keys available: True



JSON-RPC REST API <https://vda.li/en/docs/freeipa-management-in-a-nutshell/>

Интеграция, что нужно

- **Аутентификация**

Как проверить подлинность? Где она будет проверяться?

- **Учетные записи**

Где они будут храниться и в каком формате? Если в AD, то какие параметры будут использоваться в Linux?

- **Обнаружение и подключение**

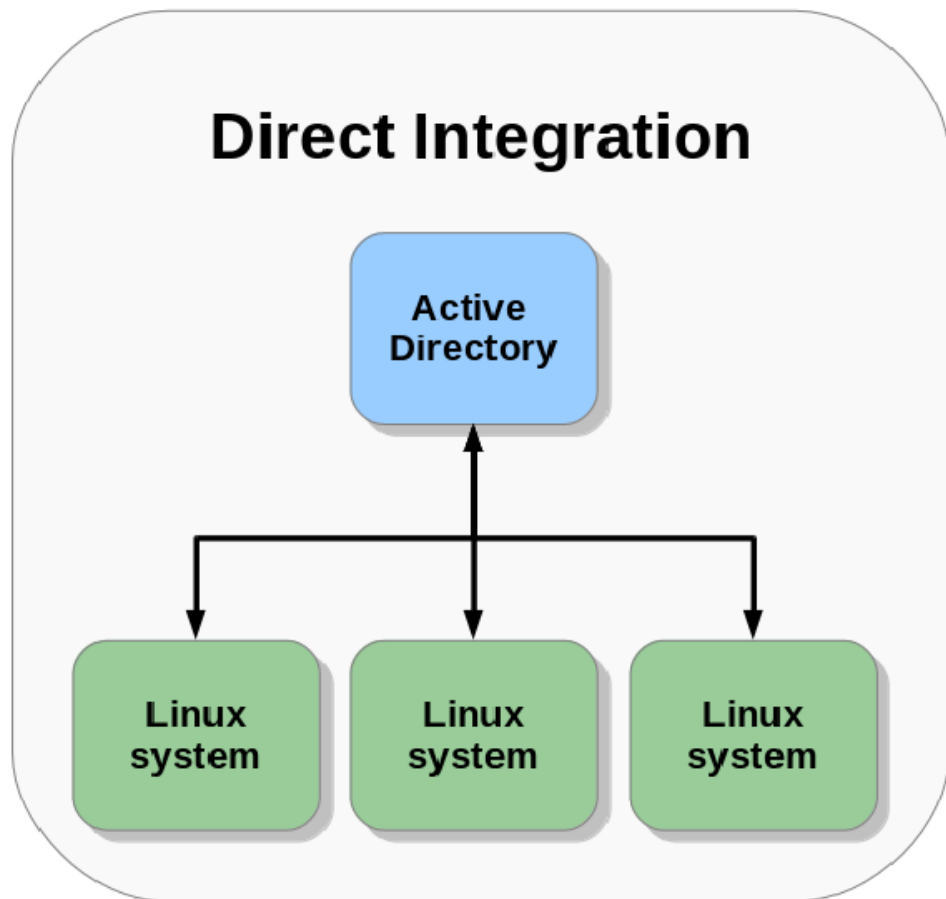
Каким образом разные системы будут обнаруживать и подключаться к сервисам?
Как они их найдут?

- **Управление политиками и настройками**

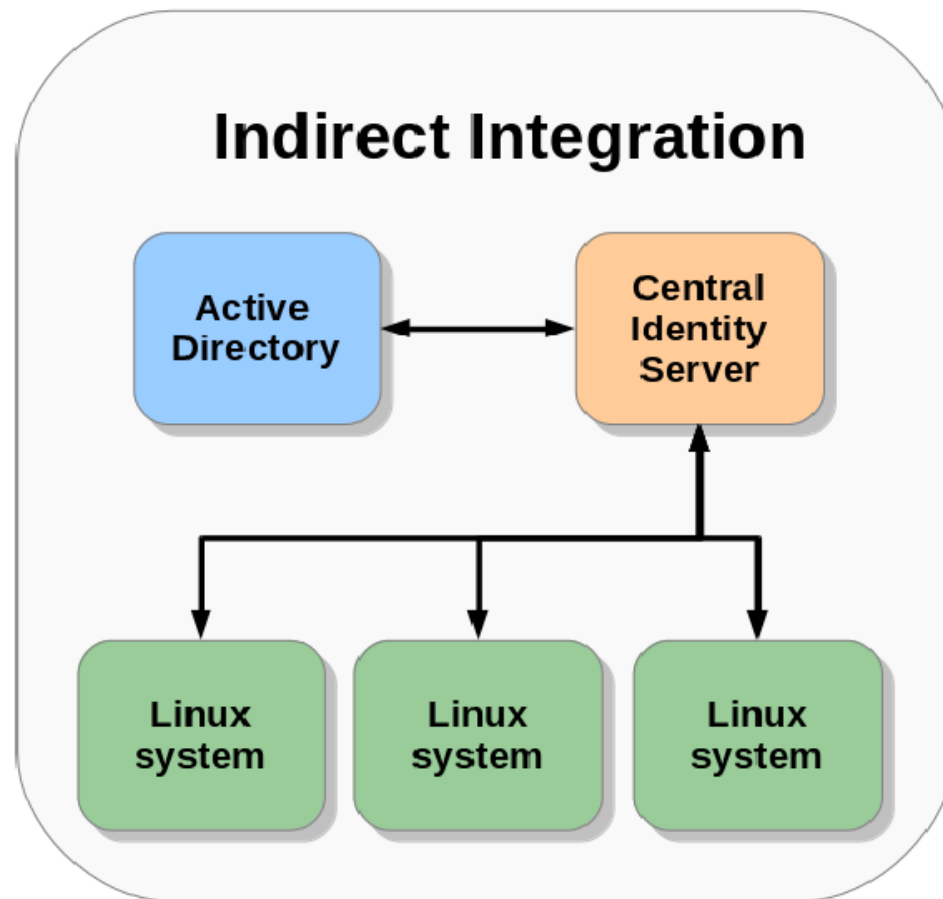
Как будут работать и управляться политики безопасности и другие настройки?

Прямая и непрямая интеграция

Direct Integration



Indirect Integration



Варианты прямой интеграции

Типовое решение: Samba + winbind

Сторонние продукты - прослойки

Нативные LDAP и Kerberos PAM и NSS модули: pam_ldap, nss_ldap, pam_krb5



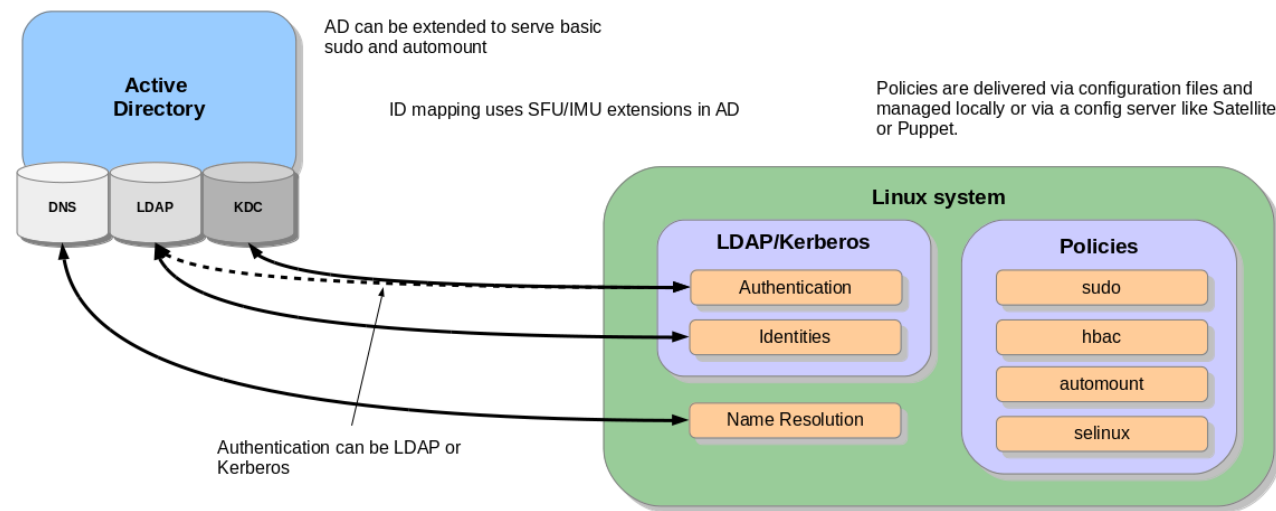
Современный
подход: SSSD

Нативный LDAP клиент, PAM и NSS модули



AaBaby.ru

pam_ldap
nss_ldap
pam_krb5



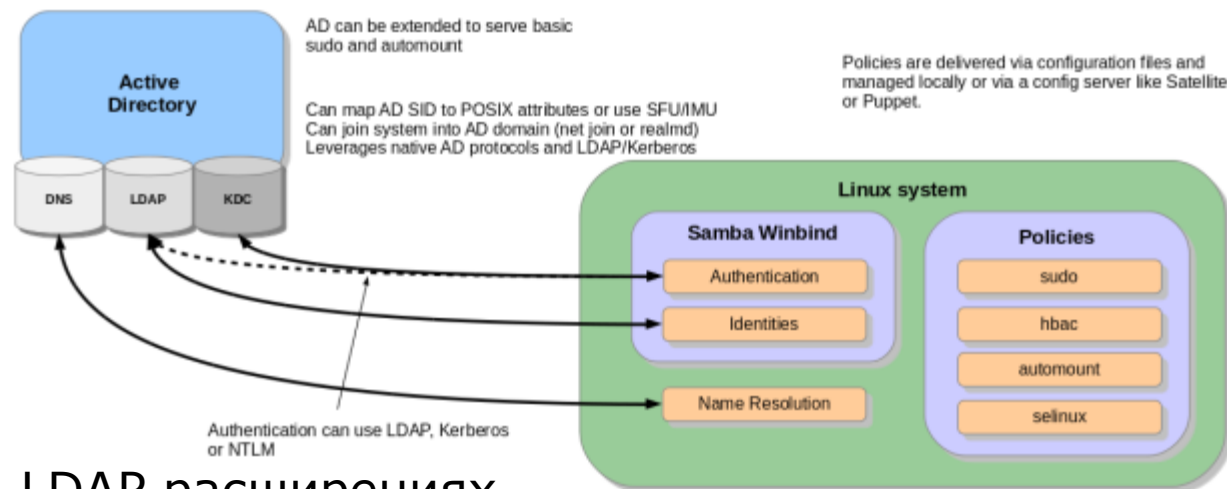
Плюсы:

- Простая и интуитивная настройка
- Это бесплатно + нет сторонних вендоров

Минусы:

- Только один домен. У вас 2 домена или даже лес? Хм, а что это такое? Мы не знаем.
- Пароли админа домена хранятся прямо в конфигах
- Кэширование входа? Его у вас нет! Недоступен сервер, нет и входа.
- В настройках указано имя сервера. У вас 2 контроллера домена и один из них выключен? Это уже проблема. Никаких DNS SRV!
- Чистый LDAP, никаких LDAP расширений
- Требуется создавать и обновлять хранить POSIX атрибуты Linux юзеров внутри AD
- Политики доступа, настройки безопасности Linux в AD? Их нет.

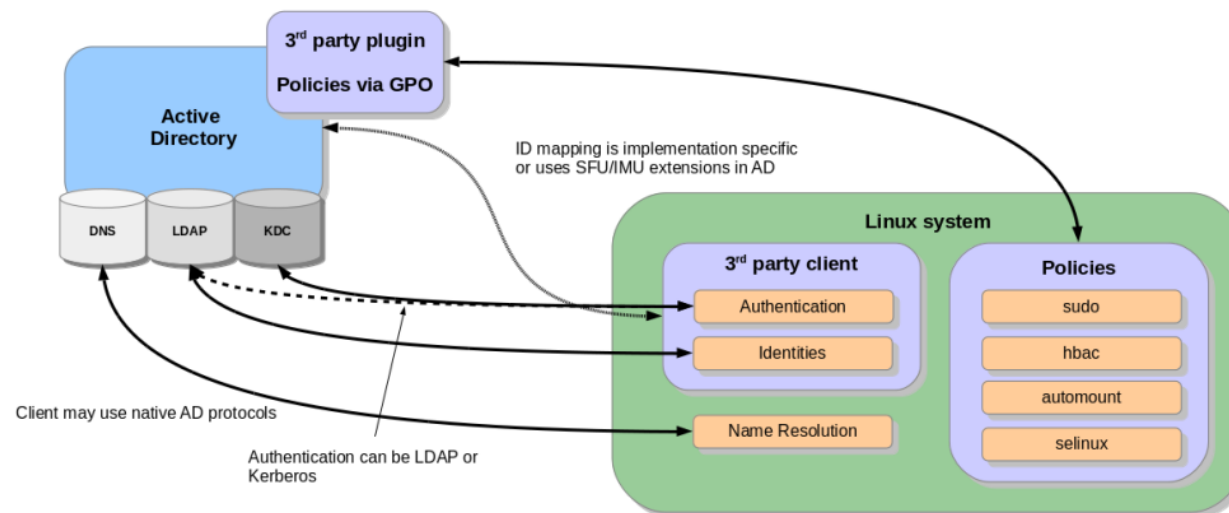
Типовое решение: Samba + winbind



Плюсы:

- Winbind знает о Windows протоколах и LDAP расширениях
- Winbind знает что есть AD домены и леса, может находить контроллеры домена с помощью DNS SRV и умеет переключаться на запасной контроллер домена, если основной недоступен
- Может сам делать маппинг идентификаторов SID или брать POSIX атрибуты из AD, если они там есть (SFU)
- Родной для Samba и cifsclient'a
- Подключается к AD с Kerberos и его токеном безопасности
- Минусы:
- Работает только с AD и не работает с другими каталогами
- Проблемы с качеством программного кода и стабильностью

Сторонние продукты - прослойки



Плюсы:

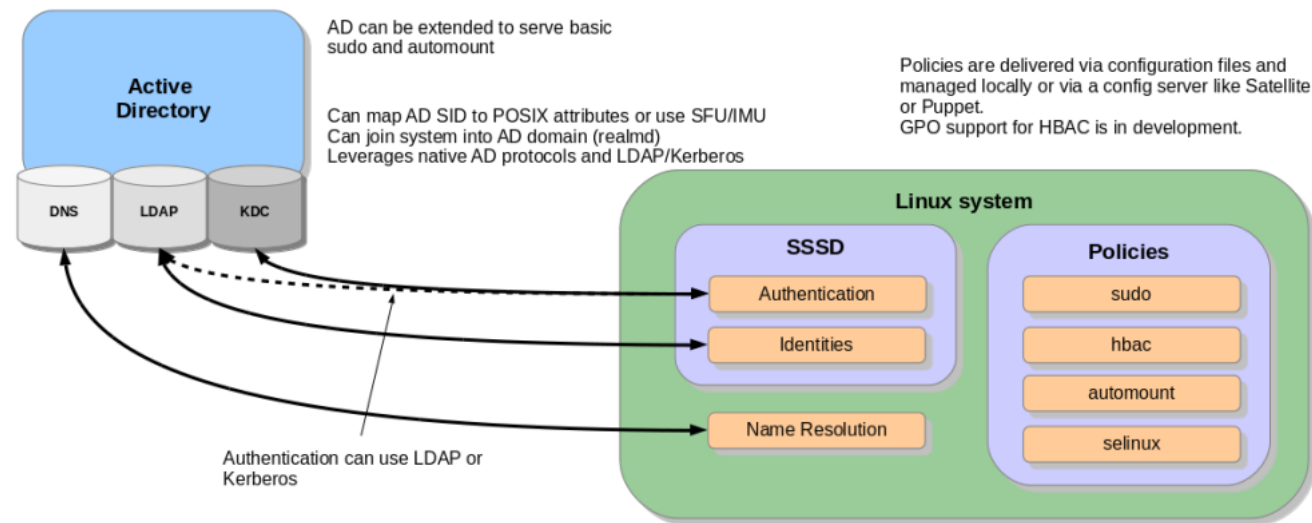
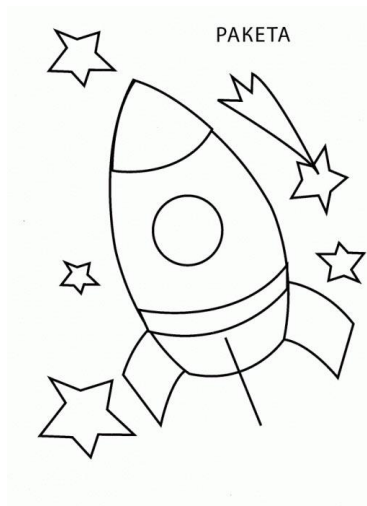
- Управление настройками и доступом для Linux с помощью инструментов управления, используемыми для управления Windows
- Управление HBAC, sudo и другими родными для Linux настройками прямо через GPO.
- Простая и понятная установка и настройка, описана в доке стороннего продукта.

Минусы:

- Плюс ещё один вендор, которому вы будете платить деньги
- Ограничение возможностей и независимости Linux среды
- Сторонний софт на контроллерах домена,
- GNU/Linux в домене AD = +1 учетная запись = надо оплатить +1 CAL
- GNU/Linux машина как белая ворона в AD



Современный подход: SSSD



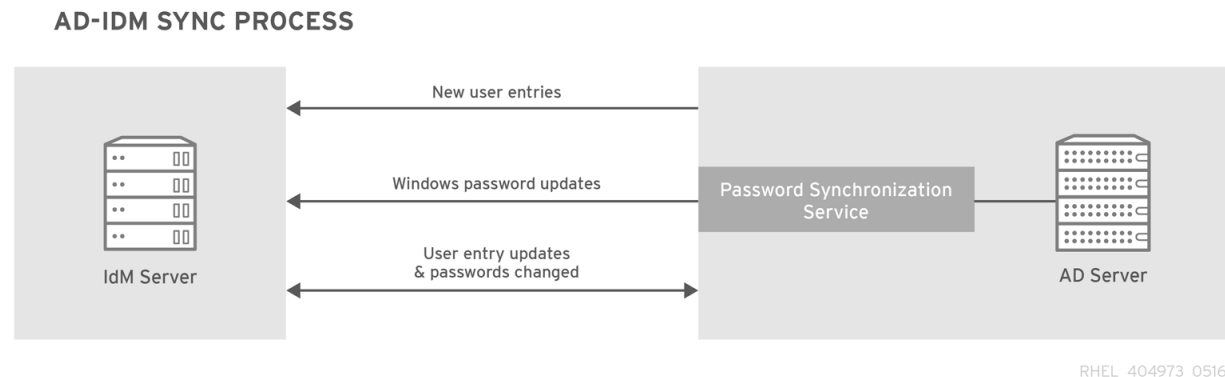
Плюсы:

- Умеет взять HBAC политики из AD
- Может работать не только с AD, но и с FreeIPA
- Полная поддержка DNS SRV, в том числе scavenger и refresh
- SSSD работает с шиной D-Bus, через неё может передать приложениям на машине информацию об учетках. Лучше интеграция с такими приложениями.

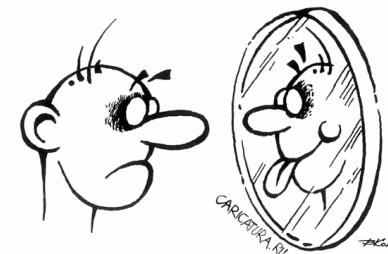
Минусы:

- Недавно появился, его нет в старых системах
- Нет NTLM и нет NETBIOS name lookup (Сетевое окружение)

Интеграция с помощью синхронизации учетных записей



- Учетные записи хранятся в разных каталогах и требуют синхронизации. Это 2 записи в 2 разных каталогах.
- Необходимость синхронизировать и пароли тоже. А перед этим пароли нужно сбросить, чтобы перехватить изменение пароля.
- Дополнительный софт на каждом DC, чтобы захватить изменение пароля
- 2 разных инструментария управления
- Проблемы аудита доступа. 2 каталога = двойной аудит.
- Только один из DC – точка синхронизации с FreeIPA



Интеграция с межлесовыми доверительными отношениями AD - IPA

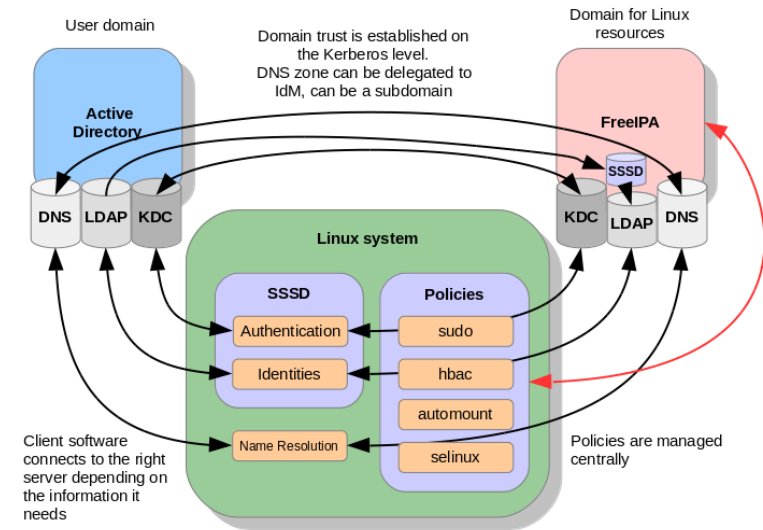


Плюсы:

- Нет синхронизации учетных записей и паролей
- Аутентификация проходит там, где и находится учетная запись.
- Родная для Linux среда управления, есть политики доступа, настройки, и тд.
- Свои Linux администраторы, своя RBAC модель делегирования полномочий
- Расширяемость и высокая доступность серверов, легко масштабируется

Минусы:

- Нужен выделенный IPA сервер.
- Нужен обновлённый SSSD (но обеспечивается совместимость со старыми Linux)
- Пока ещё нет Global Catalog'a. Есть ограничения функционала, которые можно обойти, иногда.
- Опирается на Samba в родных для Windows протоколах. Требуется её установка.



Установка step by step

- 1. Настроить разрешение локального имени. (/etc/hosts)
`echo '172.25.0.10 ipa.example.com ipa' >> /etc/hosts`
- 2. Ставим пакеты сервера
`yum install bind bind-utils bind-dyndb-ldap ipa-server ipa-server-dns`
- 3. Настраиваем домен (открыть tcp udp порты)
`ipa-server-install`
- 4. Подключаем GNU/Linux машины к IPA домену
`ipa-client-install`
- 5. Настройка разрешения имён чужого dns домена в обеих сторонах (DNS Forward)
- 6. Настройка синхронизация времени (ntpd или chrony)
- 7. Подготовка IPA к доверительным отношениям с AD и создание их
`ipa-adtrust-install` (открыть tcp udp порты)
`ipa trust-add`

Доступ AD пользователей к ресурсам IPA домена

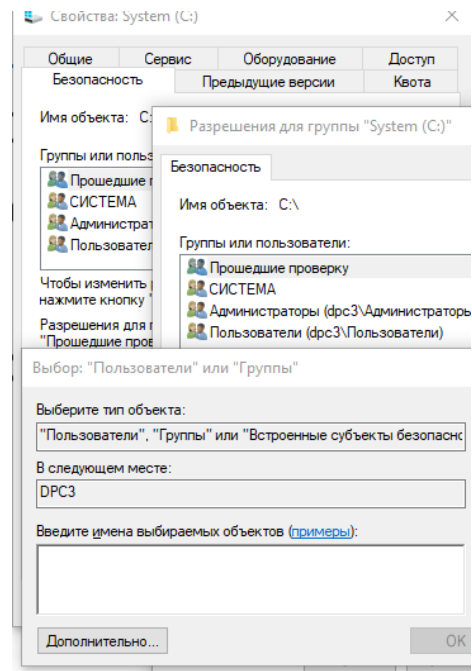
- Создайте внешнюю группу для AD пользователей
`ipa group-add --external ext_group`
- Добавьте во внешнюю группу участников
`ipa group-add-member --external 'AD_DOMAIN_NAME\AD_user' ext_group`
- Включите внешнюю группу в локальную IPA (POSIX) группу
`ipa group-add-member --groups=ext_group local_group`

Таким образом «AD» пользователи станут участниками внутренней локальной и/или IPA (POSIX) группы.

Во FreeIPA нет Global Catalog'a. Пока.

Чем это грозит:

- FreeIPA пользователи не могут получить доступ к ресурсам AD
- Закладка «Security» в свойствах файла или папки преобразовывает SID в имя
- Windows делает это с помощью сервиса Global Catalog
- У FreeIPA нет GC, который нужен для этого преобразования.
- FreeIPA пользователи не могут получить доступ к ресурсам
- Нет возможности управлять участием в группах и редактировать разрешения в общих папках Samba из Windows



Какой у разработчиков план

- 1. В первую очередь позволить AD пользователям соединяться с сервисами FreeIPA каталога, например:
 - Доступ AD пользователя с Windows машины к OpenSSH серверу, или к общей папке на Samba - используя Single-Sign-On
- 2. Потом позволить IPA пользователям входить интерактивно на машины AD и открывать все ресурсы AD.
 - Нужен GC на стороне FreeIPA
 - Пока его нет. Запросу [#3125](#) уже 5 лет

Как проверить, что всё работает?

- 1. Тестировать вручную
- 2. Проверить тестами
- Windows Protocol Test Suites

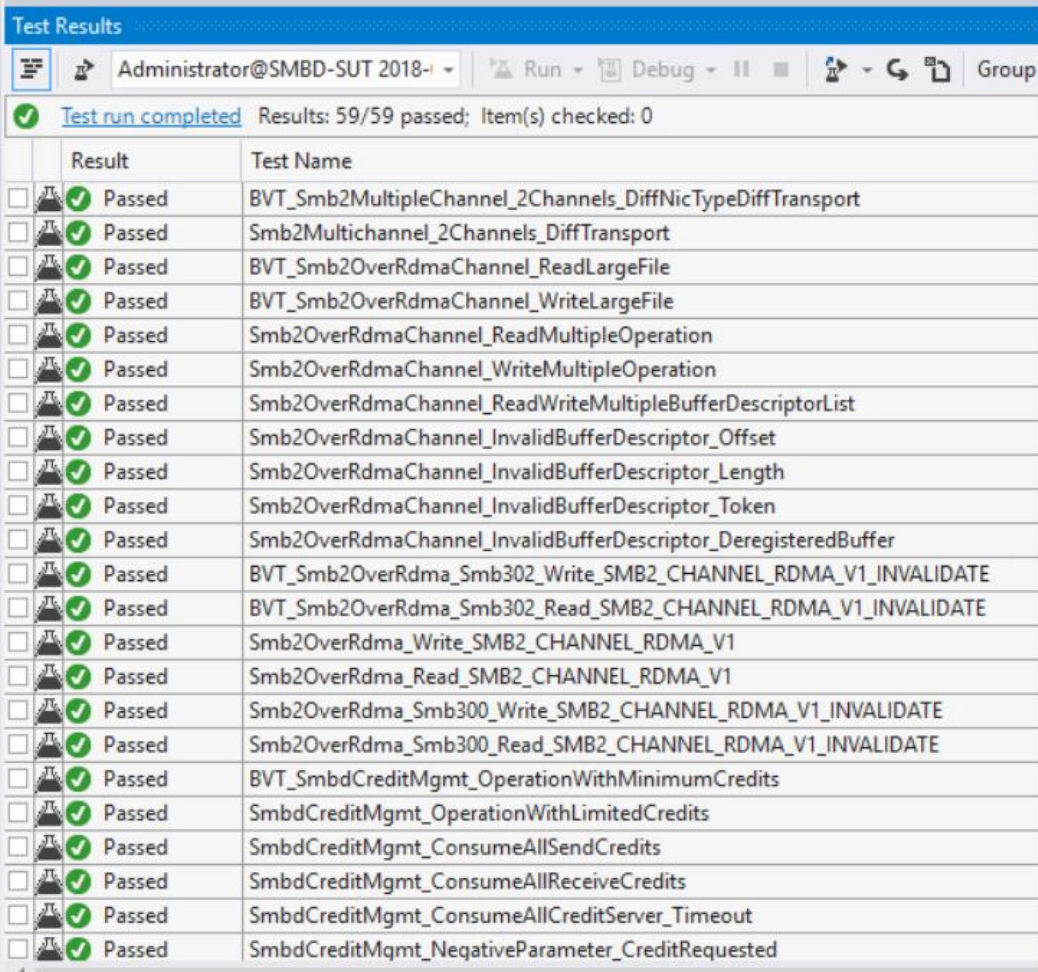
<https://github.com/Microsoft/WindowsProtocolTestSuites>

SMB1 Server Test Suite

File Server Family Test Suite.

Kerberos Server Test Suite

SMBD Server Test Suite.



	Result	Test Name
<input type="checkbox"/>	Passed	BVT_Smb2MultipleChannel_2Channels_DiffNicTypeDiffTransport
<input type="checkbox"/>	Passed	Smb2Multichannel_2Channels_DiffTransport
<input type="checkbox"/>	Passed	BVT_Smb2OverRdmaChannel_ReadLargeFile
<input type="checkbox"/>	Passed	BVT_Smb2OverRdmaChannel_WriteLargeFile
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_ReadMultipleOperation
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_WriteMultipleOperation
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_ReadWriteMultipleBufferDescriptorList
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_InvalidBufferDescriptor_Offset
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_InvalidBufferDescriptor_Length
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_InvalidBufferDescriptor_Token
<input type="checkbox"/>	Passed	Smb2OverRdmaChannel_InvalidBufferDescriptor_DeregisteredBuffer
<input type="checkbox"/>	Passed	BVT_Smb2OverRdma_Smb302_Write_SMB2_CHANNEL_RDMA_V1_INVALIDATE
<input type="checkbox"/>	Passed	BVT_Smb2OverRdma_Smb302_Read_SMB2_CHANNEL_RDMA_V1_INVALIDATE
<input type="checkbox"/>	Passed	Smb2OverRdma_Write_SMB2_CHANNEL_RDMA_V1
<input type="checkbox"/>	Passed	Smb2OverRdma_Read_SMB2_CHANNEL_RDMA_V1
<input type="checkbox"/>	Passed	Smb2OverRdma_Smb300_Write_SMB2_CHANNEL_RDMA_V1_INVALIDATE
<input type="checkbox"/>	Passed	Smb2OverRdma_Smb300_Read_SMB2_CHANNEL_RDMA_V1_INVALIDATE
<input type="checkbox"/>	Passed	BVT_SmbdCreditMgmt_OperationWithMinimumCredits
<input type="checkbox"/>	Passed	SmbdCreditMgmt_OperationWithLimitedCredits
<input type="checkbox"/>	Passed	SmbdCreditMgmt_ConsumeAllSendCredits
<input type="checkbox"/>	Passed	SmbdCreditMgmt_ConsumeAllReceiveCredits
<input type="checkbox"/>	Passed	SmbdCreditMgmt_ConsumeAllCreditServer_Timeout
<input type="checkbox"/>	Passed	SmbdCreditMgmt_NegativeParameter_CreditRequested

Люди, которые работают над IPA

<https://github.com/freeipa/freeipa/graphs/contributors>

88 человек только на Github

Вы можете стать одним из них



Simo Sorce



Dmitry Pal



Alexander
Bokovoy

- <https://www.freeipa.org/page/Documentation>
- [Linux Domain Identity, Authentication, and Policy Guide](#)
- [Windows Integration Guide](#)
- [System-Level Authentication Guide](#)

Интеграция GNU/Linux FreeIPA с Microsoft Active Directory

- Упражнение 1: Установка и настройка FreeIPA сервера и домена
- Упражнение 2: Создание пользователей, настройка парольных политик. Двухфакторная аутентификация
- Упражнение 3: Подключение серверов и рабочих станций к FreeIPA домену
- Упражнение 4: Управление группами пользователей и хостов
- Упражнение 5: Интеграция IPA домена с Active Directory

Учетные записи:

login	password
root	redhat
student	student
DOMAIN\vagrant	vagrant

Виртуальные машины:

CentOS 7	Windows
ipa.example.com	dc.domain.com
srv.example.com	wincl.domain.com
cl.example.com	

<https://github.com/dmi3mis/ipa-lab/Instructions>

Время: 1 час 45 минут