Игорь Крошкин, Red Hat
Архитектор
ikroshki@redhat.com

Игорь Малкин, МОНТ
Инженер по продуктам Red Hat
imalkin@mont.com

Управление доступом с помощью Red Hat Identity Manager

Программа

- Что такое Identity Management?
- Обзор продукта Red Hat Identity Manager
- Архитектура решения
- Сценарии использования
- Дополнительные возможности IdM
- Интеграция с другими продуктами Red Hat
- Установка и регистрация клиентов

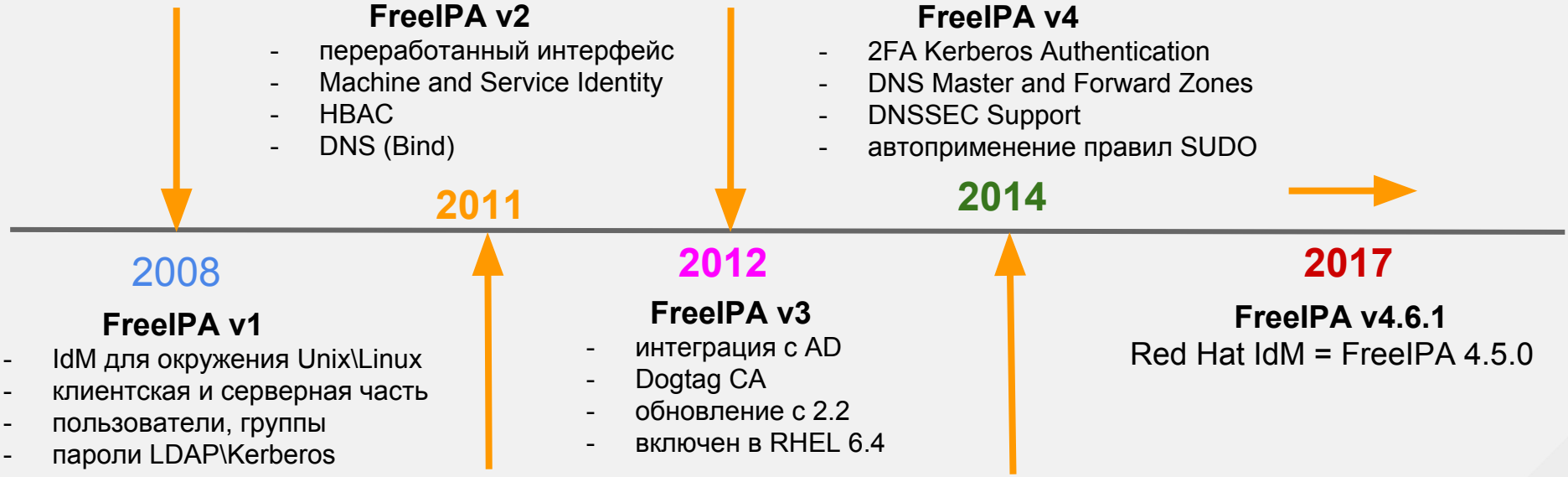
Что такое Red Hat Identity Manager?

Определение (продукт)

- Создание домена на основе и под контролем Red Hat Enterprise Linux
  - Клиентские машины только на базе ОС Linux и Unix
  - Не требует дополнительной подписки (включен в состав подписки на RHEL)
- Обеспечение централизованного хранения идентификационной информации и политик (аналог Active Directory)
- Единый набор инструментов, связывающий существующие протоколы и приложения в среде ОС Linux

Что такое Red Hat Identity Manager?

История развития



freeIPA identity | policy | audit - **Upstream-проект (https://www.freeipa.org/page/Downloads)**

MCNT GROUP OF COMPANIES redhat.

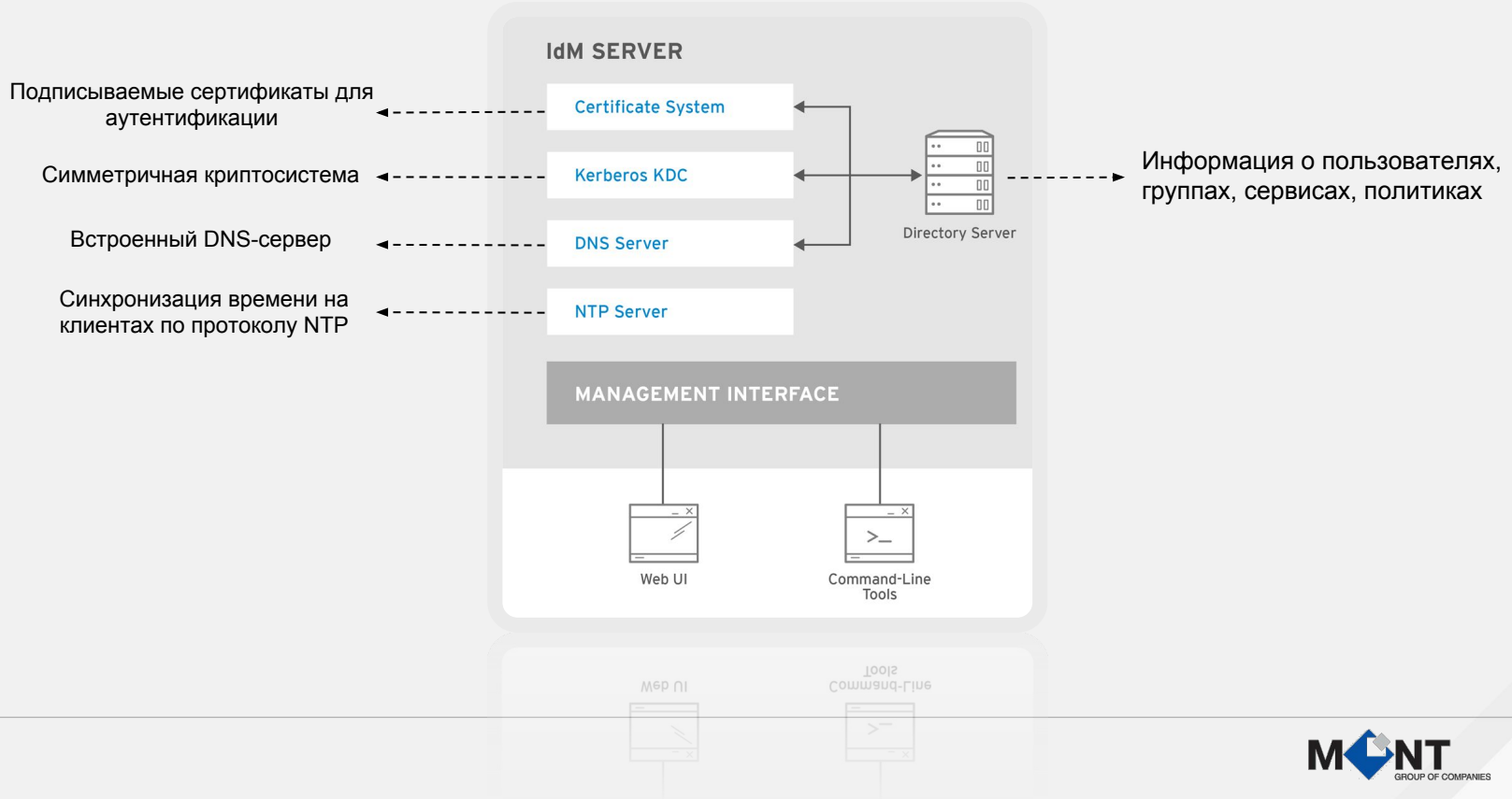
Что такое Red Hat Identity Manager?

Основные возможности

- Создание единого пользовательского пространства
- Single-Sign-On (SSO) авторизация внутри домена
- Создание пользовательских групп для разделения уровня доступа
- Управление политиками SUDO
- Назначение политик для паролей
- Возможность смены пароля пользователями без помощи администратора
- Аутентификация с использованием OTP токенов
- Отказоустойчивость: поддержка репликации
- Интеграция с Microsoft Active Directory

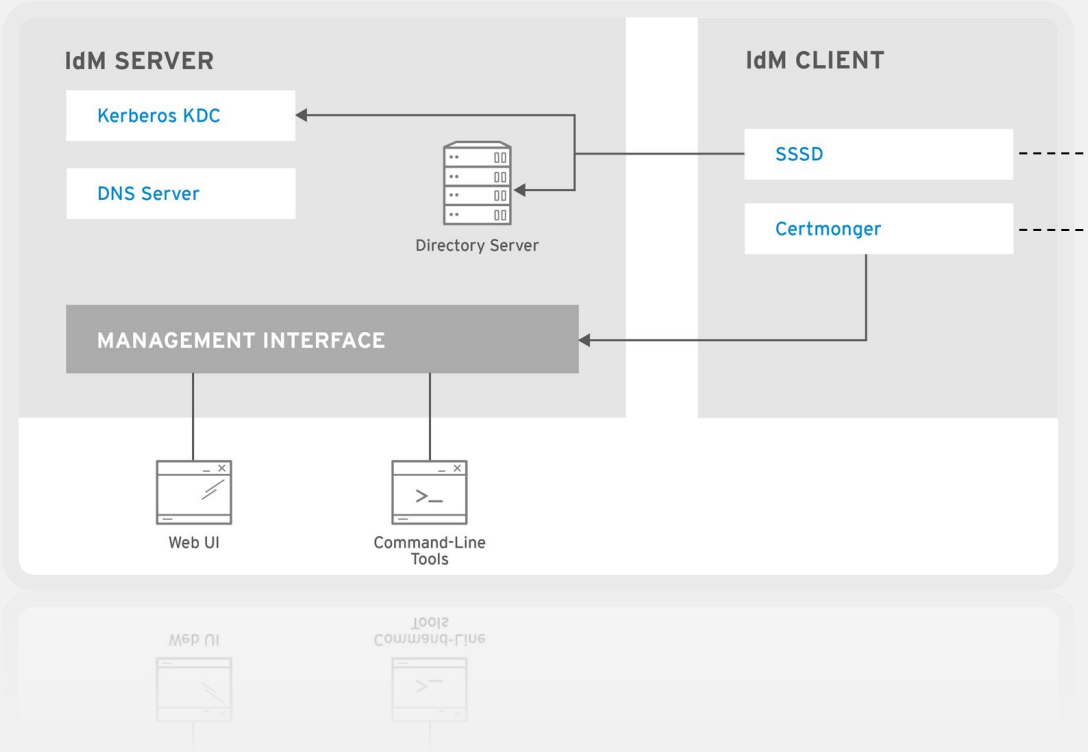
Архитектура Red Hat Identity Manager

Основные компоненты (серверная часть)



Архитектура Red Hat Identity Manager

Основные компоненты (клиентская часть)



Сценарии использования Identity Manager

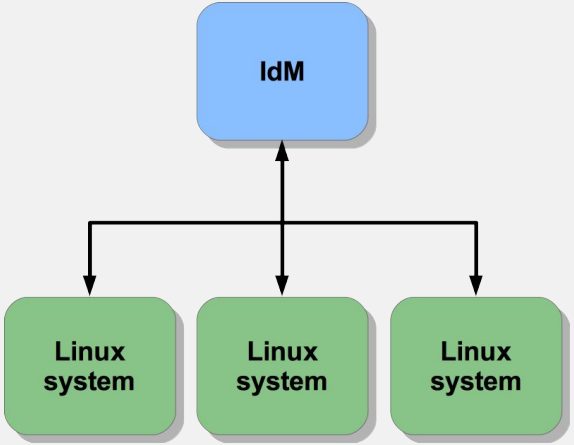
Основные задачи

- **Организация централизованной системы аутентификации**
- Проблема взаимодействия с Active Directory
- Контроль доступа, политики SUDO, ключи SSH, automount и т.п.
- Двухфакторная аутентификация

Сценарии использования Identity Manager

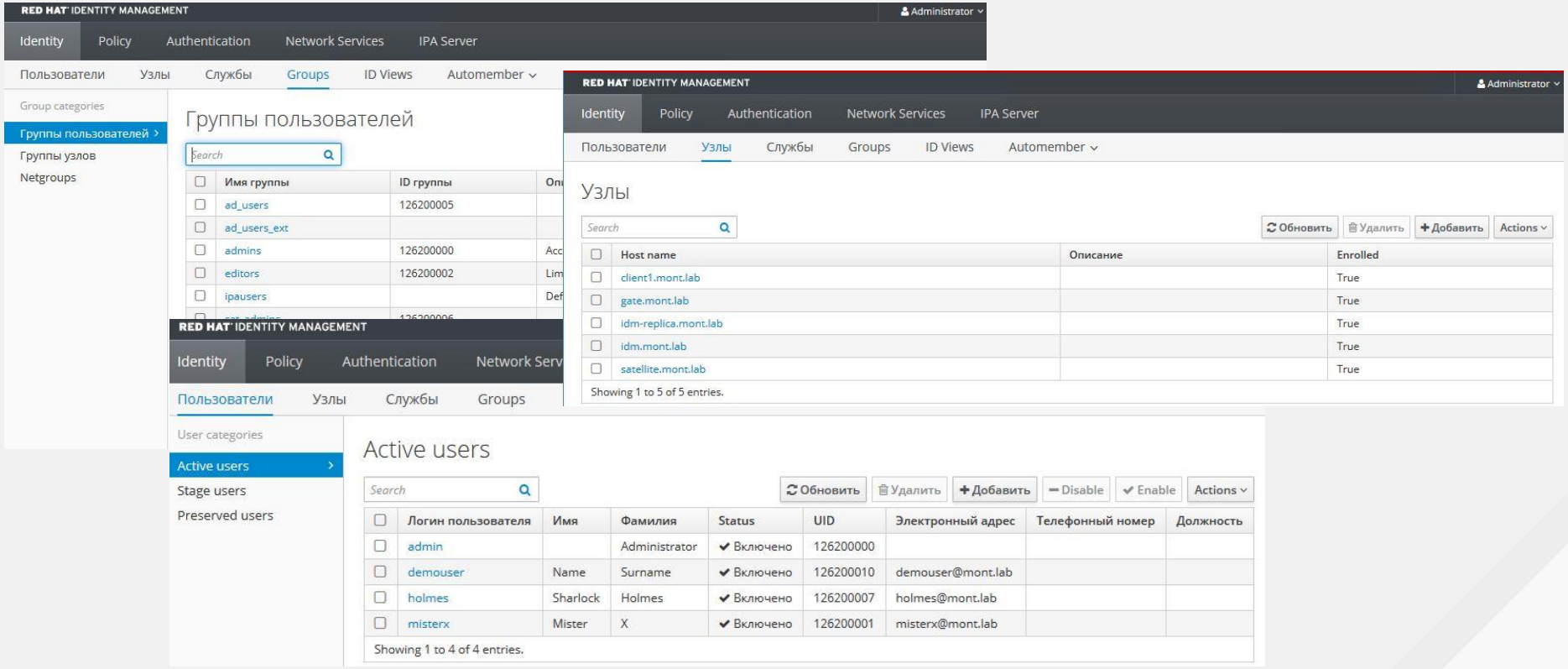
Организация централизованной системы аутентификации

- Консолидация пользовательских учетных данных
- Различные методы аутентификации: Kerberos, LDAP, SSH-ключи, OTP
- SSO для приложений через Kerberos
- SELinux для управления политиками безопасности



Сценарии использования Identity Manager

Организация централизованной системы аутентификации



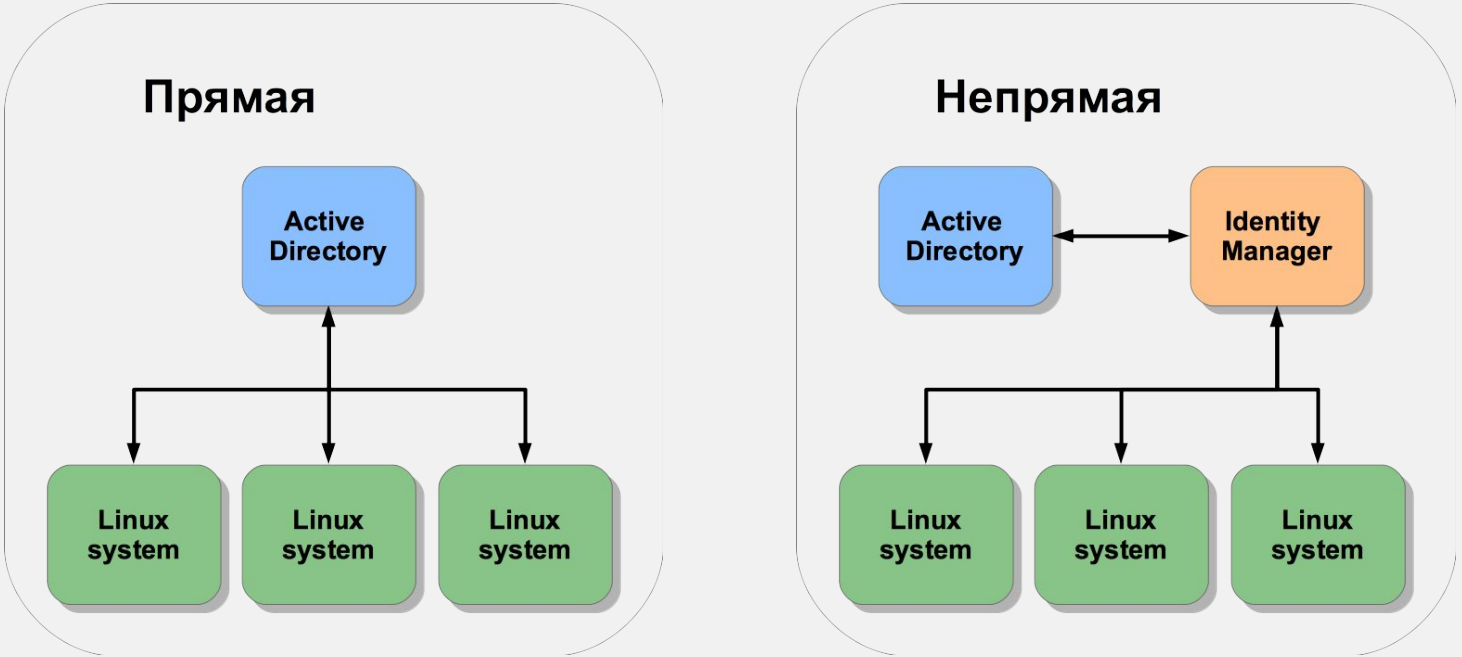
Сценарии использования Identity Manager

Основные задачи

- Организация централизованной системы аутентификации
- **Проблема взаимодействия с Active Directory**
- Контроль доступа, политики SUDO, ключи SSH, automount и т.п.
- Двухфакторная аутентификация

Сценарии использования Identity Manager

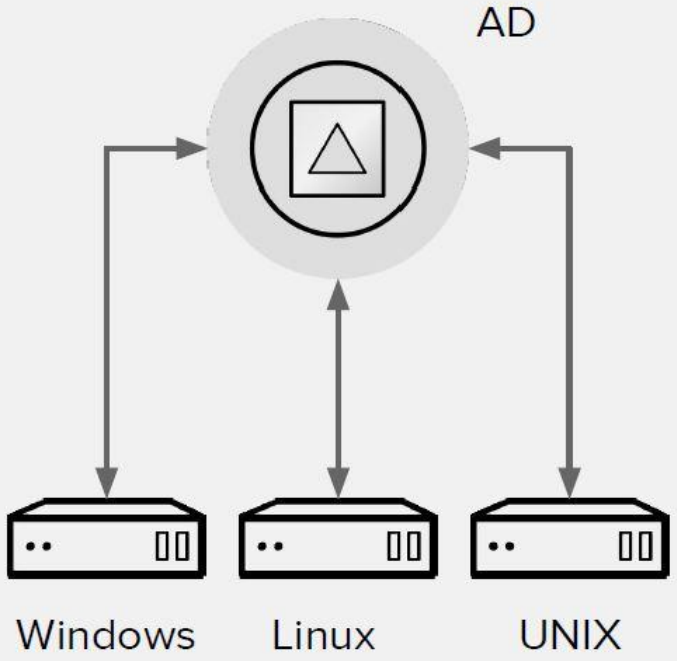
Интеграция с Active Directory



Сценарии использования Identity Manager

Прямая интеграция с Active Directory

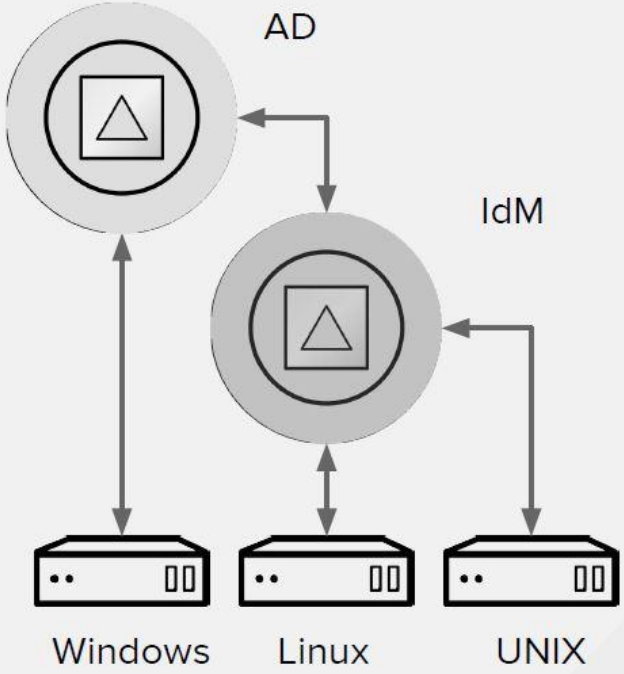
- Учетная запись в AD
- Управление базовыми правилами sudo и automount
- Соответствие AD SID и атрибутов POSIX
- Поддержка GPO для HBAC реализована в RHEL 7.1
- Управление политиками через конфигурационные файлы либо Satellite/Puppet



Сценарии использования Identity Manager

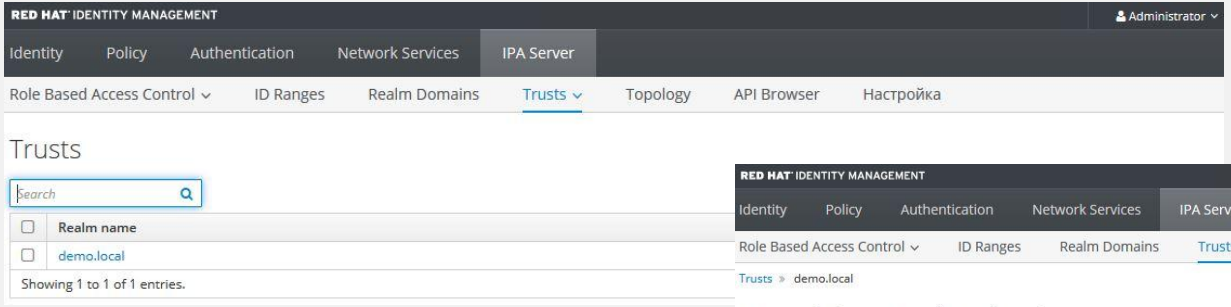
Непрямая интеграция с Active Directory

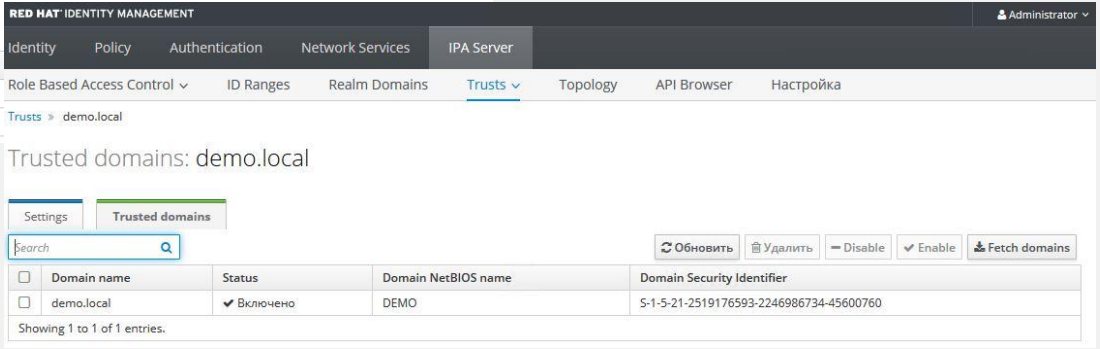
- Рекомендуемый вариант
- Доступ для пользователей AD к сервисам IdM
- Доверительные отношения на уровне доменов через Kerberos
- Зона DNS из AD может быть делегирована IdM либо дочерней
- Управление политиками через IdM

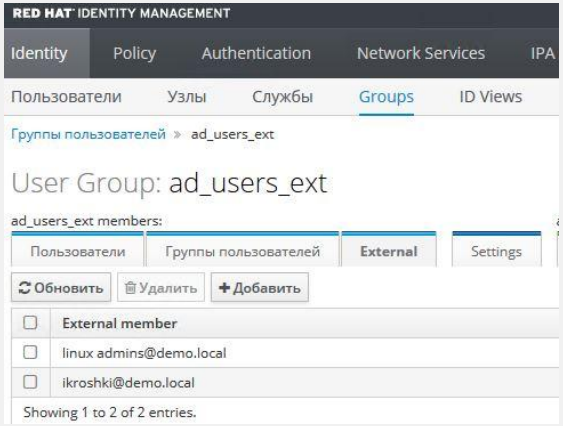


Сценарии использования Identity Manager

Интеграция с Active Directory







Сценарии использования Identity Manager

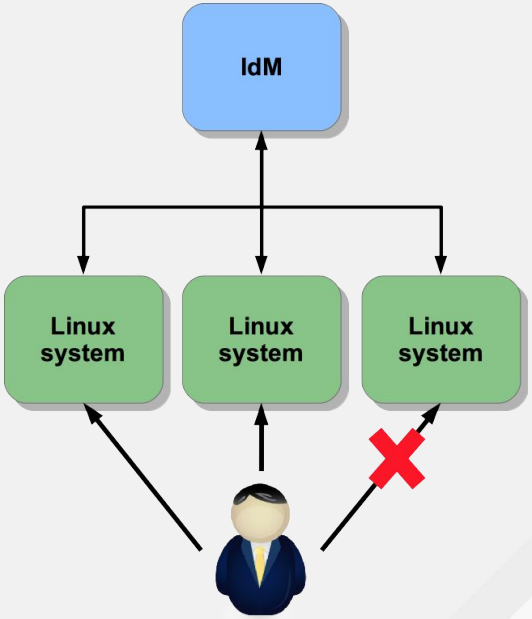
Основные задачи

- Организация централизованной системы аутентификации
- Проблема взаимодействия с Active Directory
- **Контроль доступа, политики SUDO, ключи SSH, automount и т.п.**
- Двухфакторная аутентификация

Сценарии использования Identity Manager

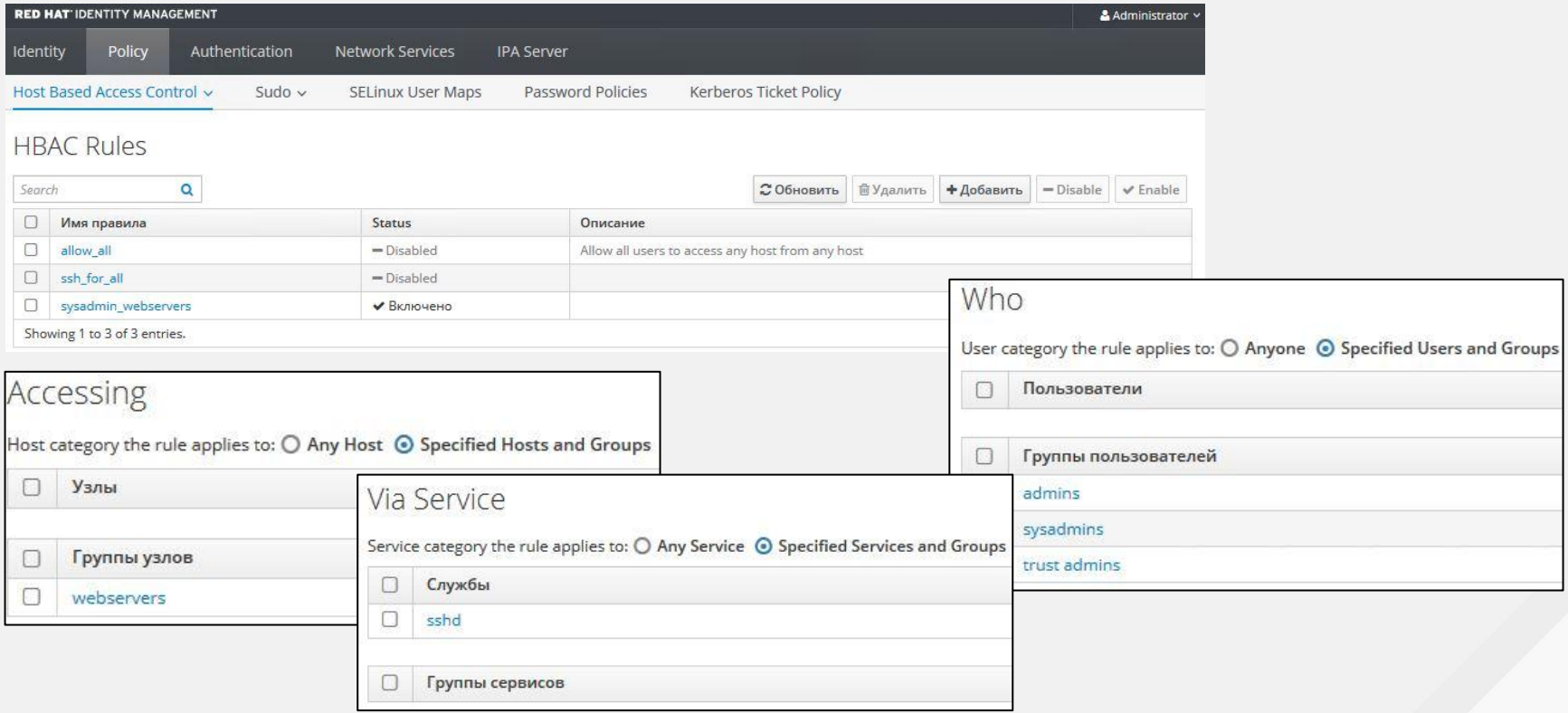
Управление доступом (Host Based Access Control)

- Какие пользователи и группы
- Какие хосты или группы хостов
- Способы доступа: консоль, ssh, sudo, ftp, sftp, и т.д.
- Правила применяются на клиенте и кэшируются (SSSD)
- Правила применимы к пользователям AD (в случае непрямой интеграции)



Сценарии использования Identity Manager

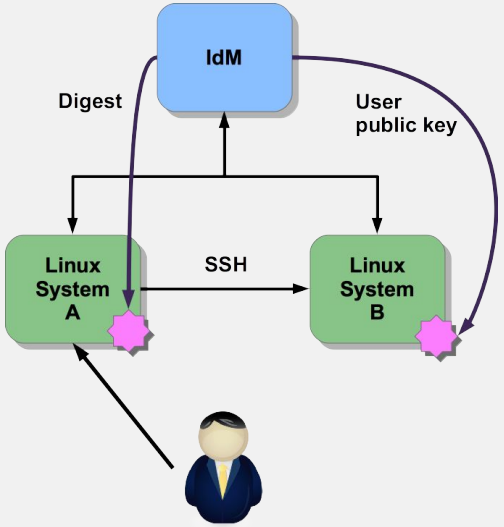
Управление доступом (Host Based Access Control)



Сценарии использования Identity Manager

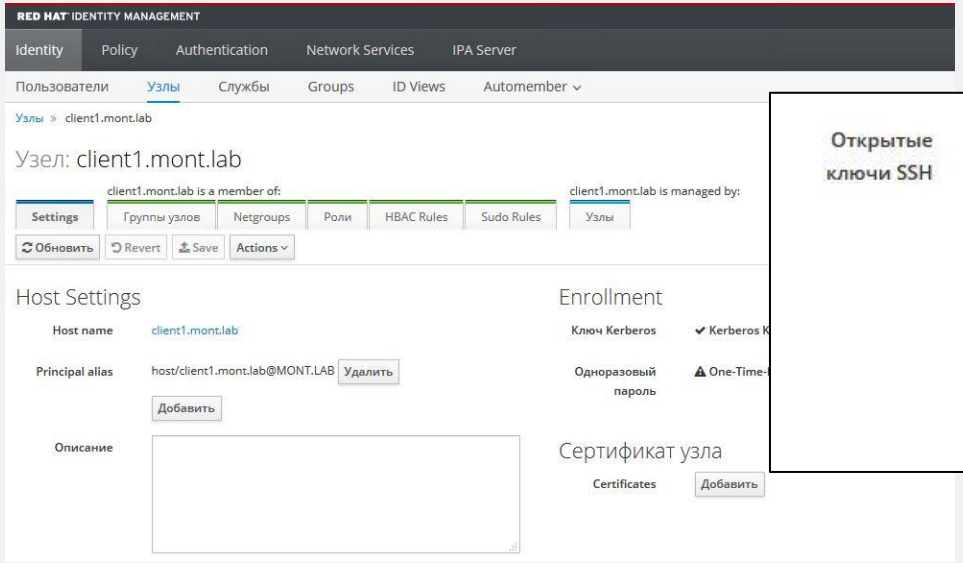
Управление SSH-ключами

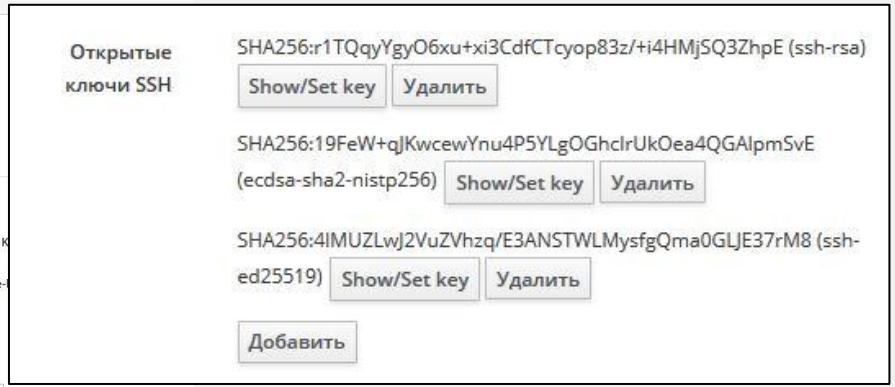
- Открытый ключ хоста загружается при установке клиента
- Пользователь также может загрузить свой открытый ключ на IdM вручную
- Правила применимы к пользователям AD (в случае непрямой интеграции)



Сценарии использования Identity Manager

Управление SSH-ключами



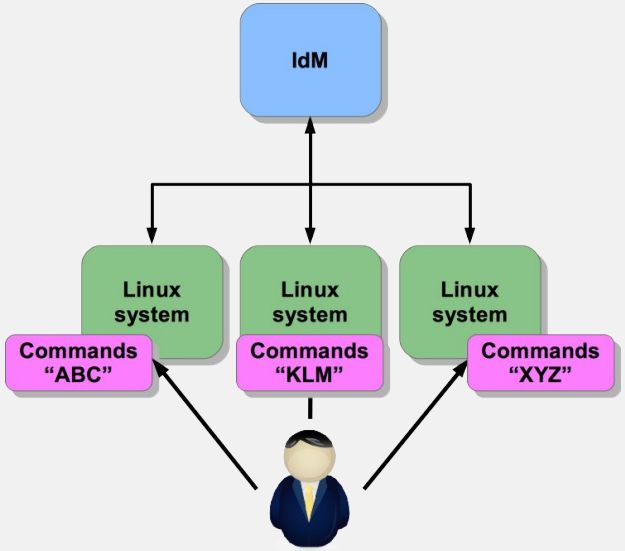


Сценарии использования Identity Manager

Управление правами SUDO

- Какие пользователи
- Какие команды или группы команд
- На каких хостах или группах хостов могут выполнять
- Правила применяются на клиенте и кэшируются (SSSD)
- Правила применимы к пользователям AD (в случае непрямой интеграции)

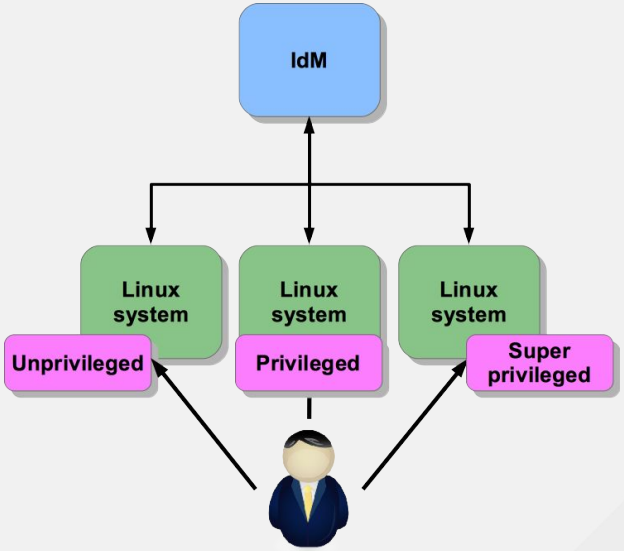
	Full refresh	Smart refresh	Rules refresh
When (default)	every 6 hours or when a rule is deleted from the cache	every 15 minutes	when user runs SUDO, rules expire after 90 minutes
Why	keep the cache consistent	store new rules	do not grant user more privilege
Operations	insert, delete	insert, modify	modify, delete
Expected traffic	large	small	small
Configuration option	ldap_sudo_full_ refresh_interval	ldap_sudo_smart_ refresh_interval	entry_cache_sudo_ timeout



Сценарии использования Identity Manager

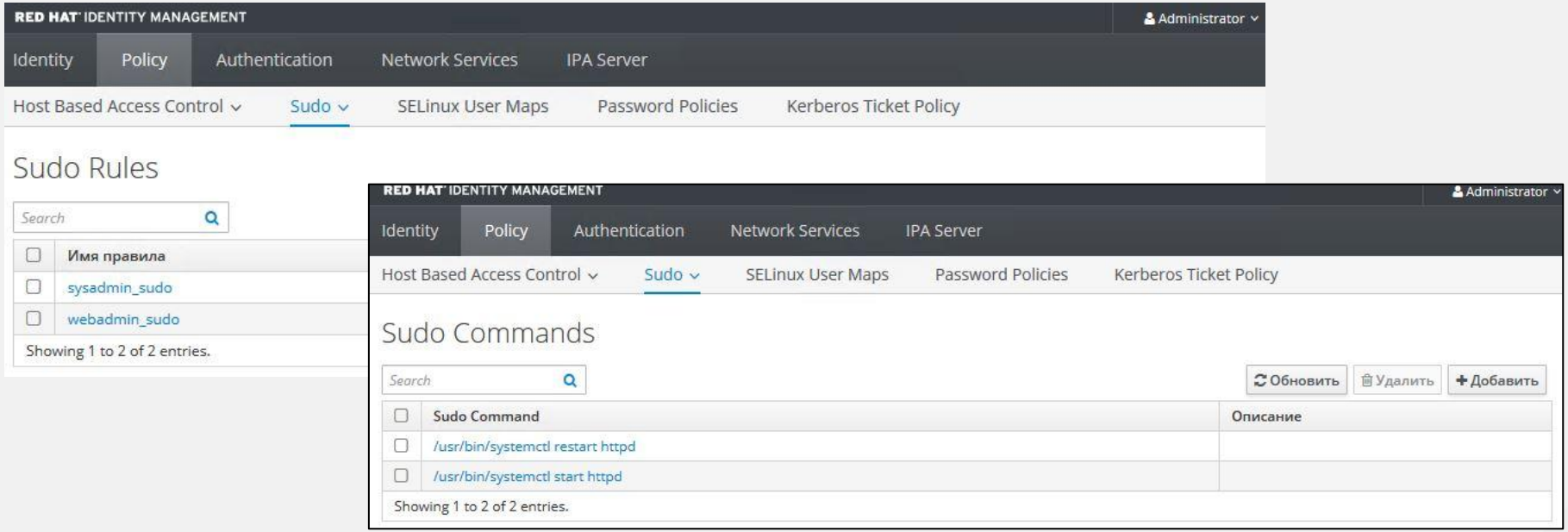
SELinux соответствие пользователей

- Позволяют пользователям на разных хостах иметь разный контекст SELinux
- Правила применяются на клиенте и кэшируются (SSSD)
- Правила применимы к пользователям AD (в случае непрямой интеграции)



Сценарии использования Identity Manager

Управление правами SUDO



Сценарии использования Identity Manager

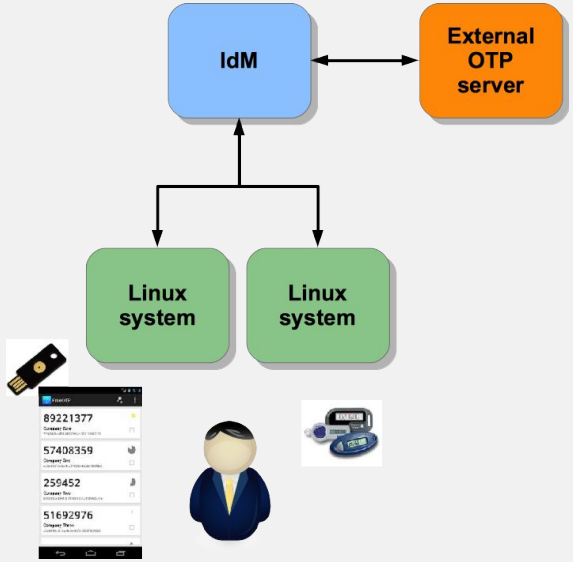
Основные задачи

- Организация централизованной системы аутентификации
- Проблема взаимодействия с Active Directory
- Контроль доступа, политики SUDO, ключи SSH, automount и т.п.
- **Двухфакторная аутентификация**

Сценарии использования Identity Manager

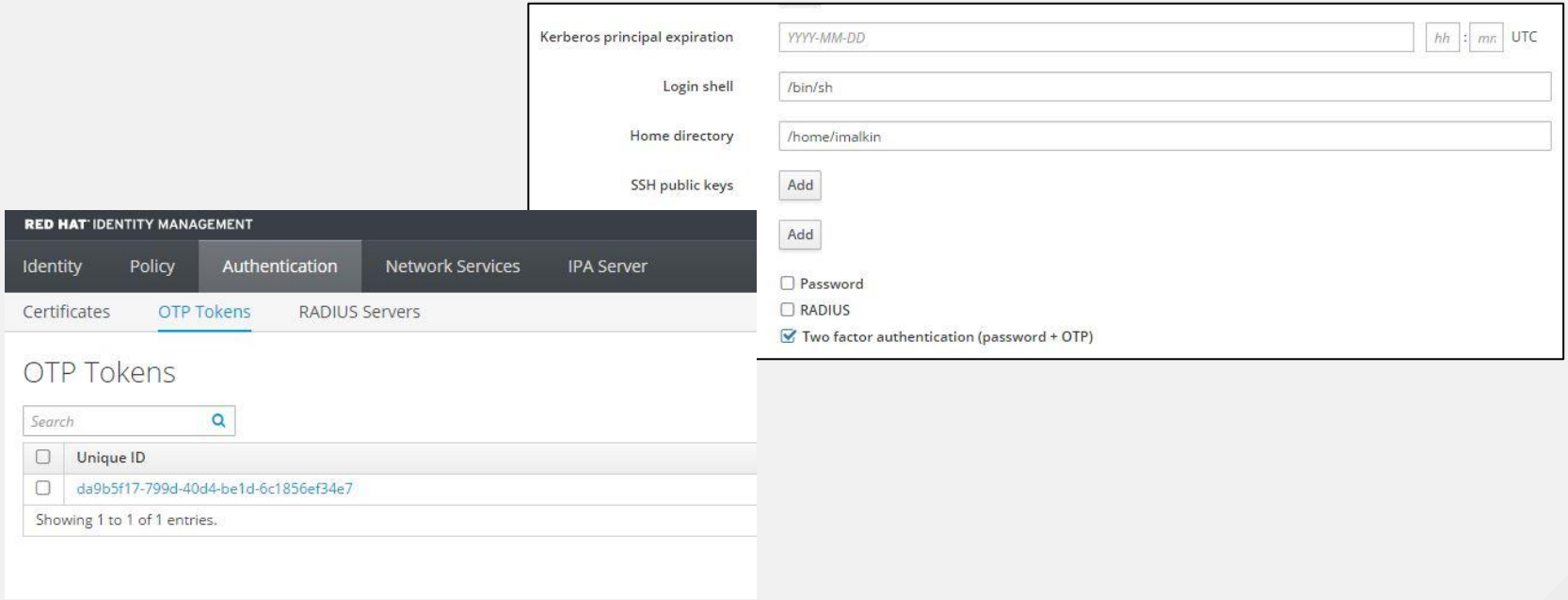
Двухфакторная аутентификация с использованием OTP

- Нативная поддержка
  - Yubikey, FreeOTP, Google authenticator
  - Совместимость с HOTP/TOTP
  - Через LDAP или Kerberos
- Прокси через RADIUS
  - Любое решение с поддержкой RADIUS
  - Работает только через Kerberos



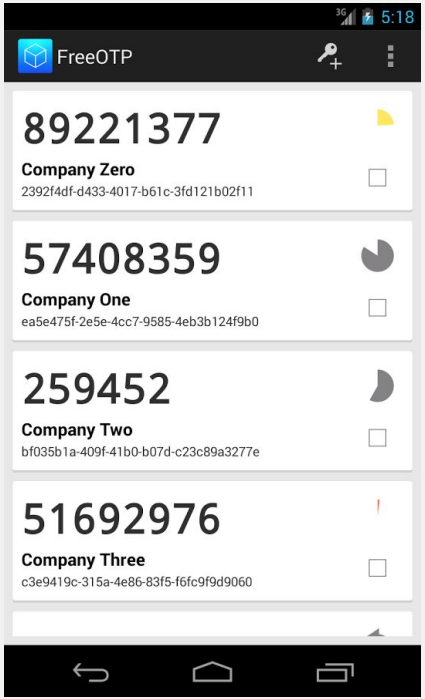
Сценарии использования Identity Manager

Двухфакторная аутентификация с использованием OTP

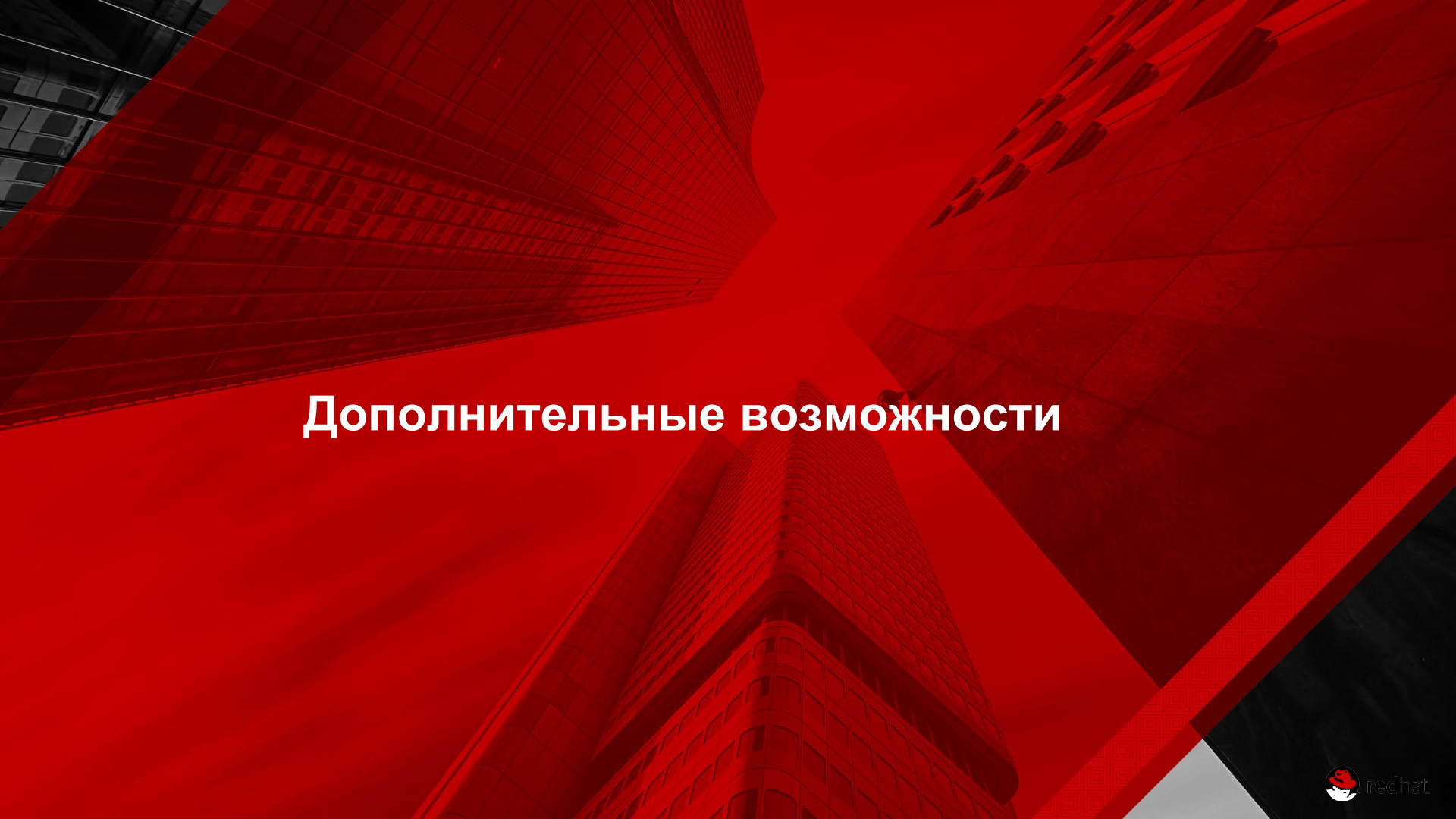


Сценарии использования Identity Manager

Двухфакторная аутентификация с использованием OTP

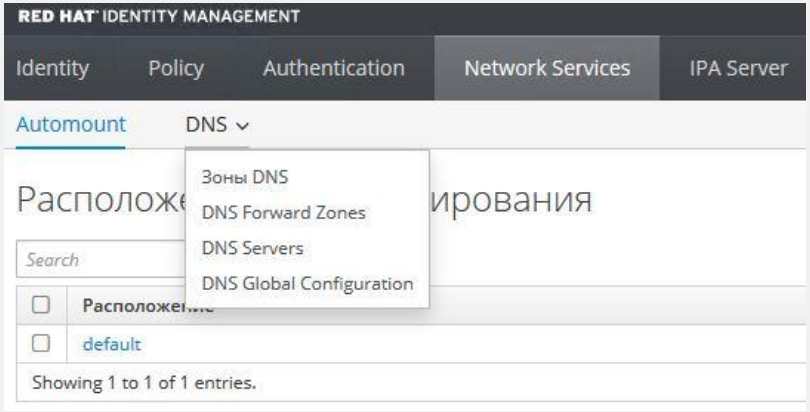


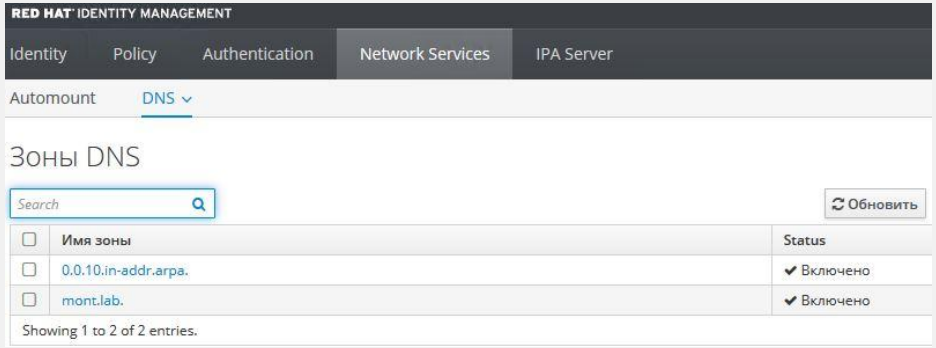
Дополнительные возможности

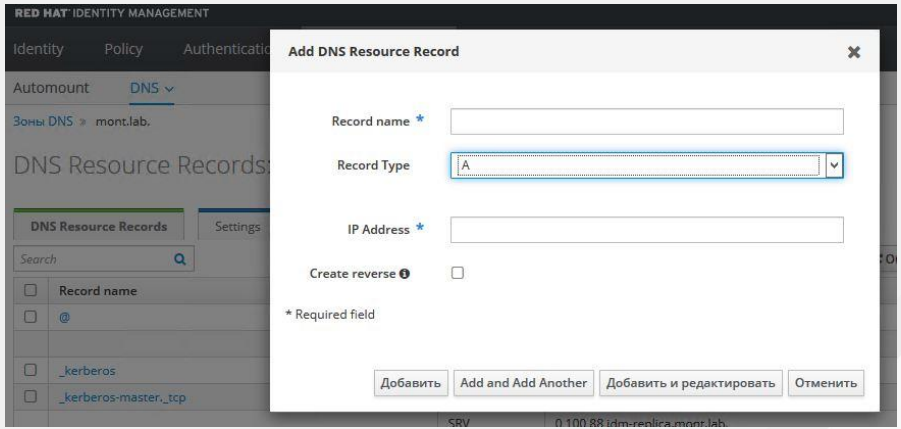


Возможности Red Hat Identity Manager

Встроенный DNS-сервер

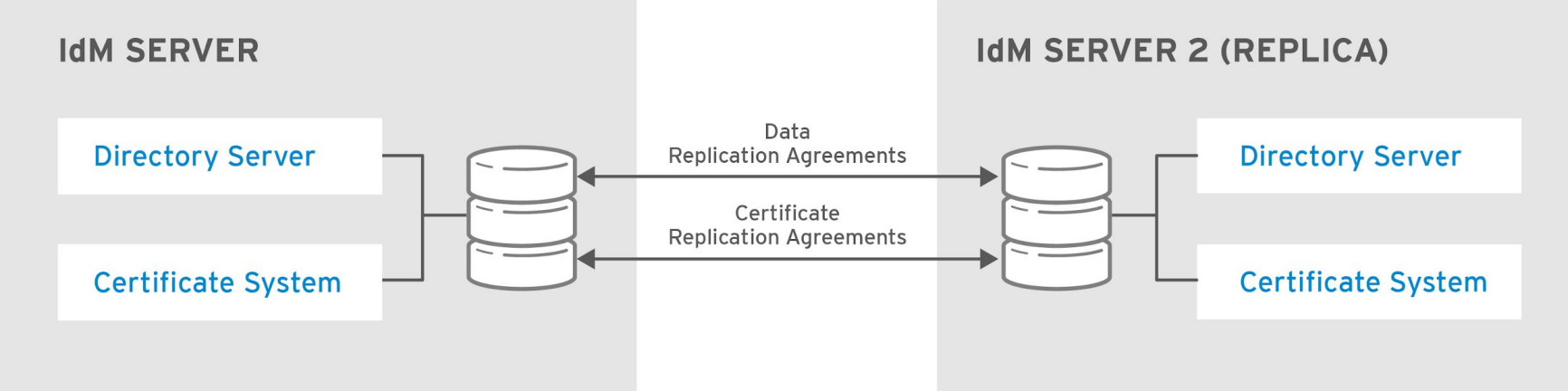






Возможности Red Hat Identity Manager

Поддержка репликации

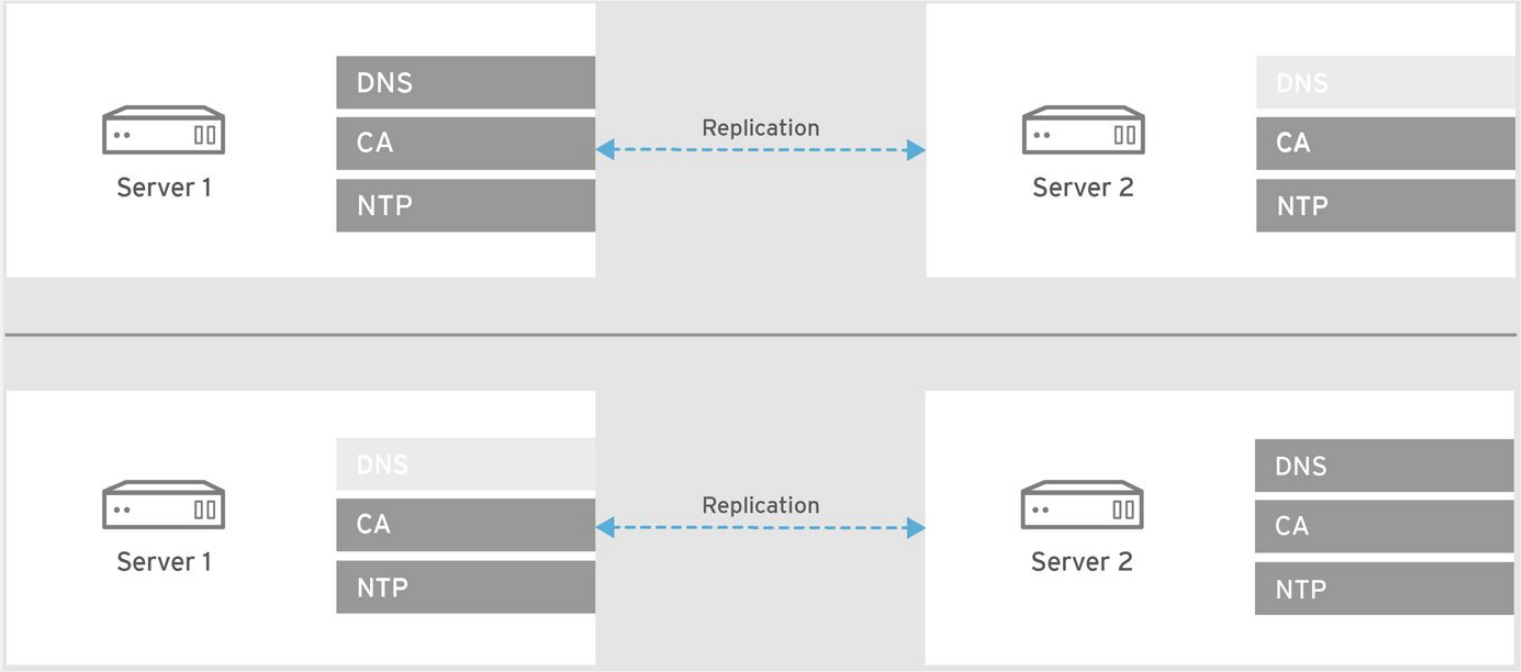


- Не более 60 реплик для одного IdM-домена
- Не менее двух, но не более четырех соглашений репликации на IdM-сервер

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/replica-considerations.html

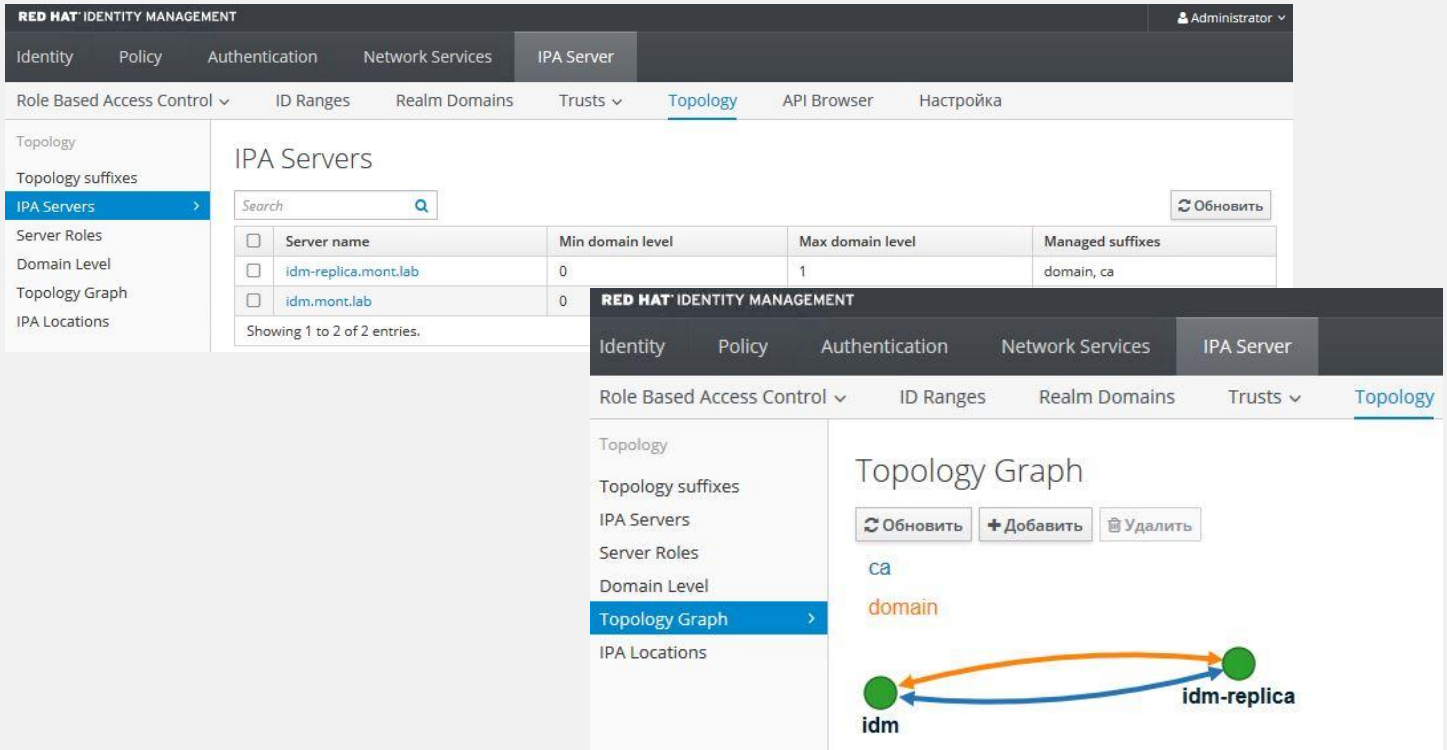
Возможности Red Hat Identity Manager

Поддержка репликации



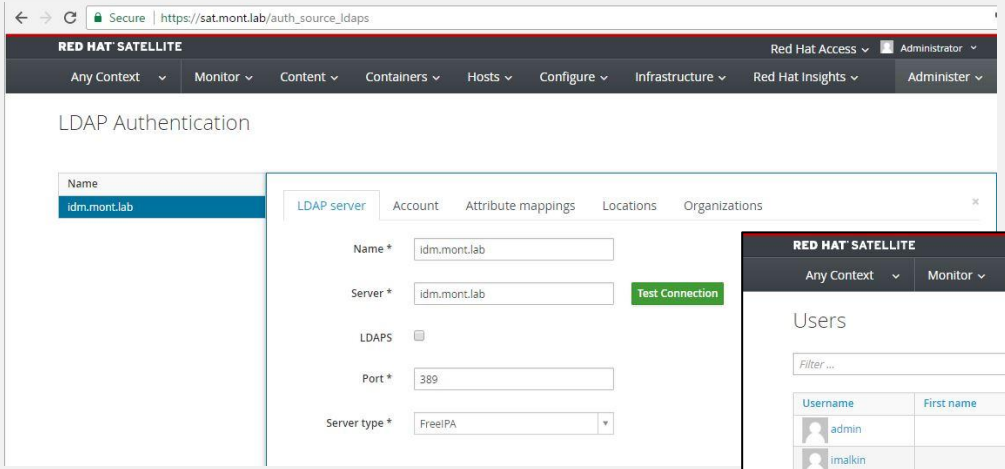
Возможности Red Hat Identity Manager

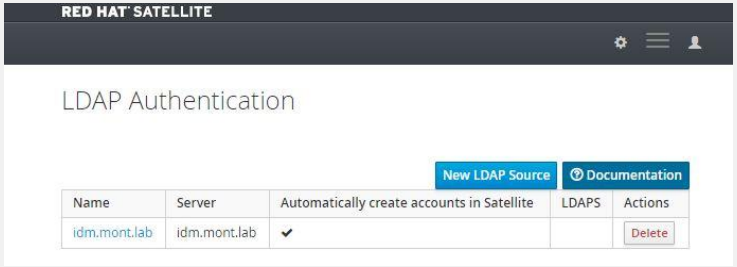
Поддержка репликации

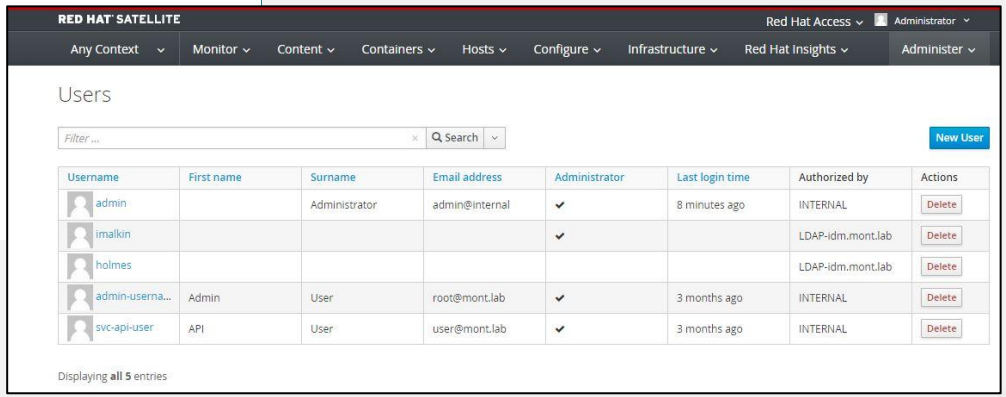


Возможности Red Hat Identity Manager

Интеграция с Red Hat Satellite

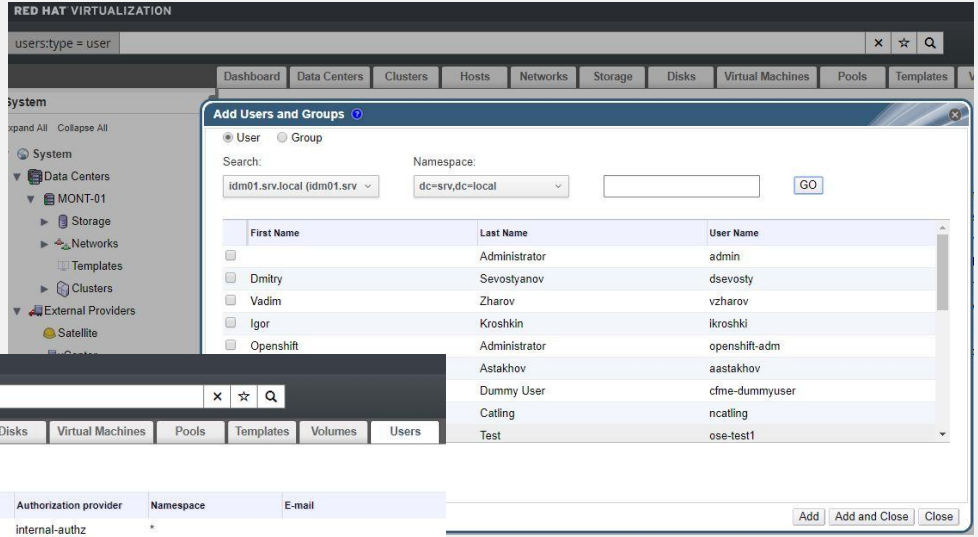


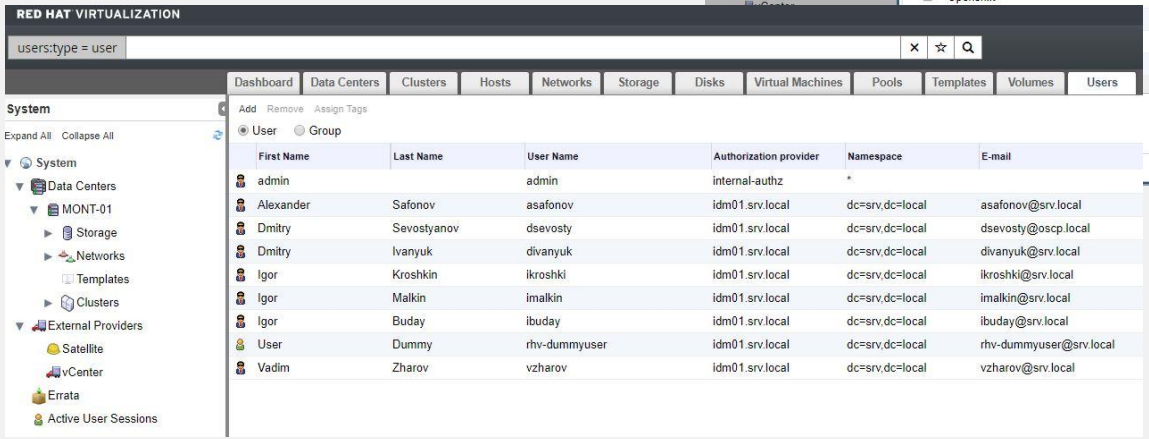




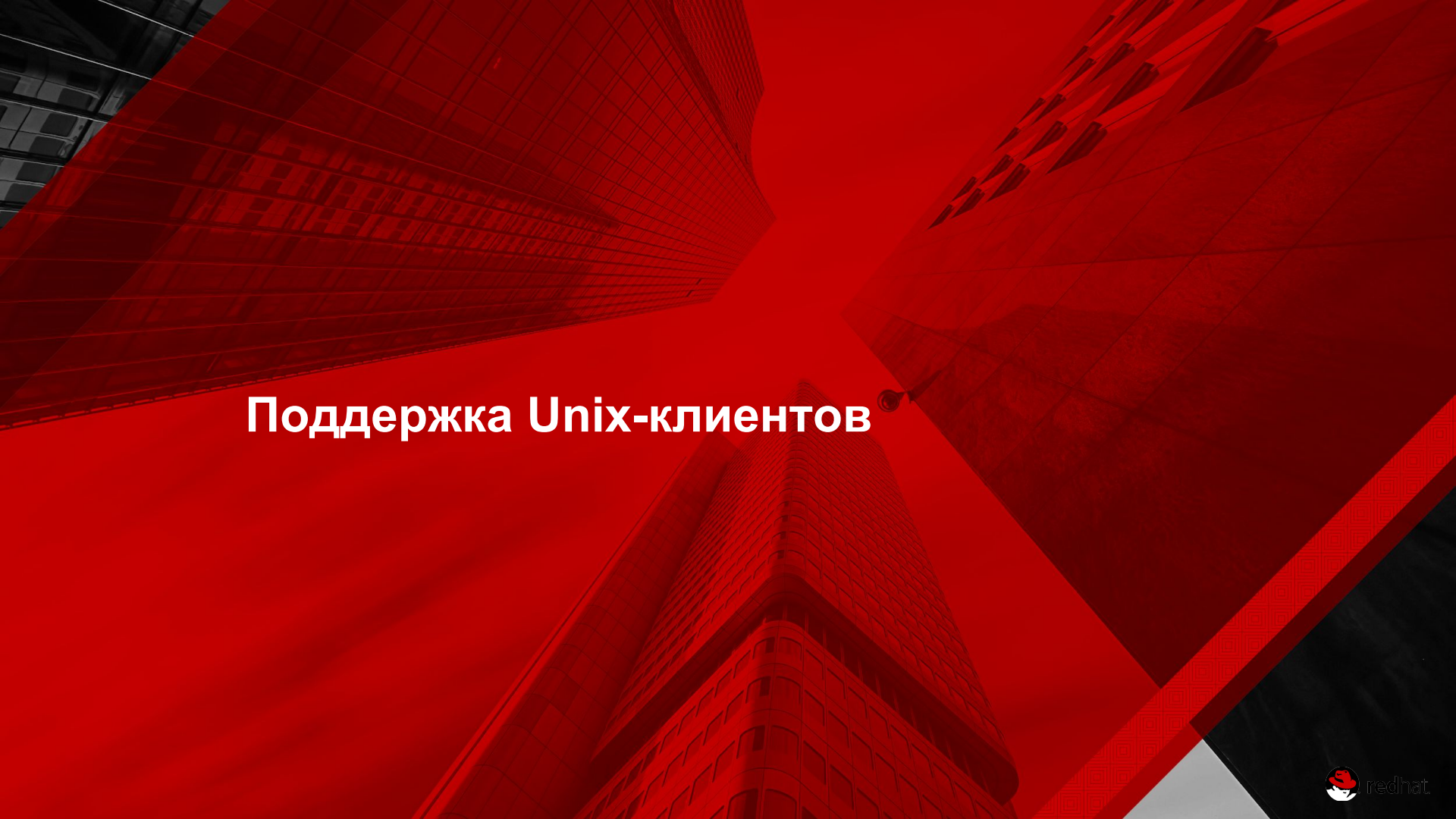
Возможности Red Hat Identity Manager

Интеграция с Red Hat Virtualization





Поддержка Unix-клиентов

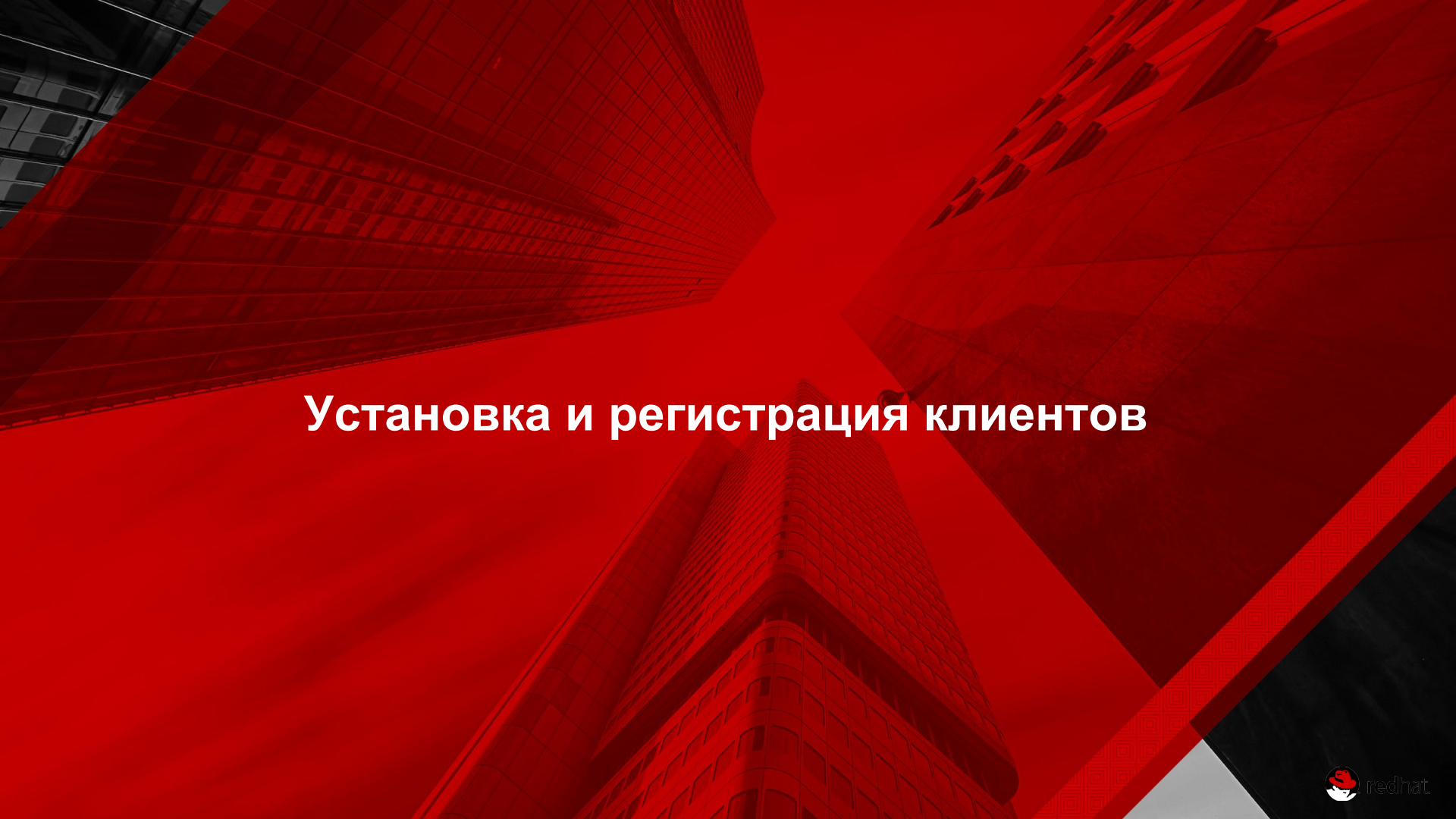


Поддержка UNIX-клиентов

- Solaris 6/7/8/9/10
- HP-UX 11.0
- HP-UX 11i v.1 and 2
- AIX 5.1
- AIX 5.2
- AIX 5.3

https://www.freeipa.org/page/HowTos
https://www.freeipa.org/page/ConfiguringUnixClients

Установка и регистрация клиентов



Установка Red Hat Identity Manager

Системные требования

- ОС Red Hat Enterprise Linux 6.2 и выше для версии IdM 3.0
- ОС Red Hat Enterprise Linux 7 для версии IdM 4.x
- 2ГБ ОЗУ и 1ГБ swap - не более 10 000 пользователей и 100 групп
- 16ГБ ОЗУ и 4ГБ swap - не более 100 000 пользователей и 50 000 групп
- Существующая DNS-запись на сервере (либо /etc/hosts)

Установка Red Hat Identity Manager

Требования - [список портов]

- HTTP/HTTPS
  - tcp: 80,443
- LDAP/LDAPS
  - tcp: 389,636
- Kerberos
  - tcp/udp: 88,464
- DNS
  - tcp/udp: 53
- NTP
  - udp: 123
- Доступ к Web GUI сервера через браузер

Установка Red Hat Identity Manager

Предварительная настройка

- Настройка правил пакетной фильтрации
  - `#firewall-cmd --permanent --add-service=freeipa-ldap`
  - `#firewall-cmd --reload`
- Подключение подписки Red Hat Enterprise Linux
  - `#susbcription-manager register`
  - `#subscription-manager list --all --available`
  - `#subscription-manager attach --pool=` *`pool_id`*
  - `#subscription-manager list --consumed`
- Подключение необходимых репозиториев
  - `#subscription-manager repos --disable "*"`
  - `#subscription-manager repos --enable=rhel-7-server-rpms`

Установка Red Hat Identity Manager

Предварительная настройка

- Установка корректного hostname
  - `# hostnamectl set-hostname server.example.com`
- Проверка имени сервера
  - `# hostname`

    server.example.com
- Проверка конфигурации DNS-сервера
  - `#dig +short server.example.com A`

    192.0.2.1
  - `#cat /etc/hosts`

    192.0.2.1 server.example.com server

    127.0.0.1 localhost.localdomain localhost

Установка Red Hat Identity Manager

Процедура установки серверной части

- Установка необходимых пакетов (вариант без встроенного DNS-сервер)
  - `# yum install ipa-server`
- Установка необходимых пакетов (вариант со встроенным DNS-сервером и AD-trust)
  - `# yum install ipa-server ipa-server-dns ipa-server-trust-ad`
- Запуск установочного скрипта
  - `# ipa-server-install --setup-dns --mkhomedir`

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/install-server.html

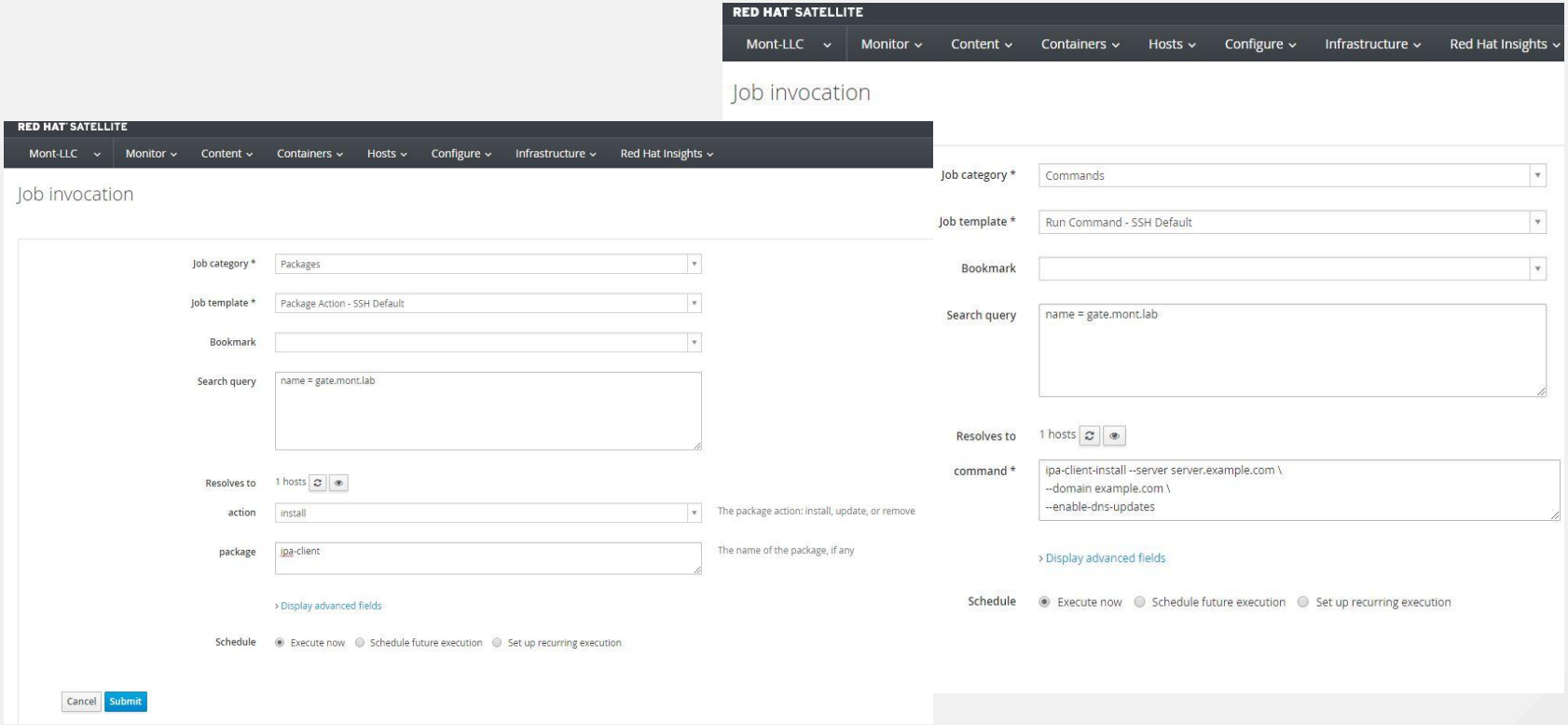
Регистрация клиентских систем

Процедура регистрации клиента

- Установка необходимых пакетов для регистрации клиента
  - `# yum install ipa-client`
- Установка пакета для управления IdM с клиентской системы
  - `# yum install ipa-admintools`
- Запуск установочного скрипта
  - ```
    # ipa-client-install --server server.example.com \
    --domain example.com \
    --enable-dns-updates
    ```
    ```

Регистрация клиентских систем

Автоматическая регистрация клиента с использованием Red Hat Satellite



Установка Red Hat Identity Manager

Проверка работоспособности (на стороне клиента)

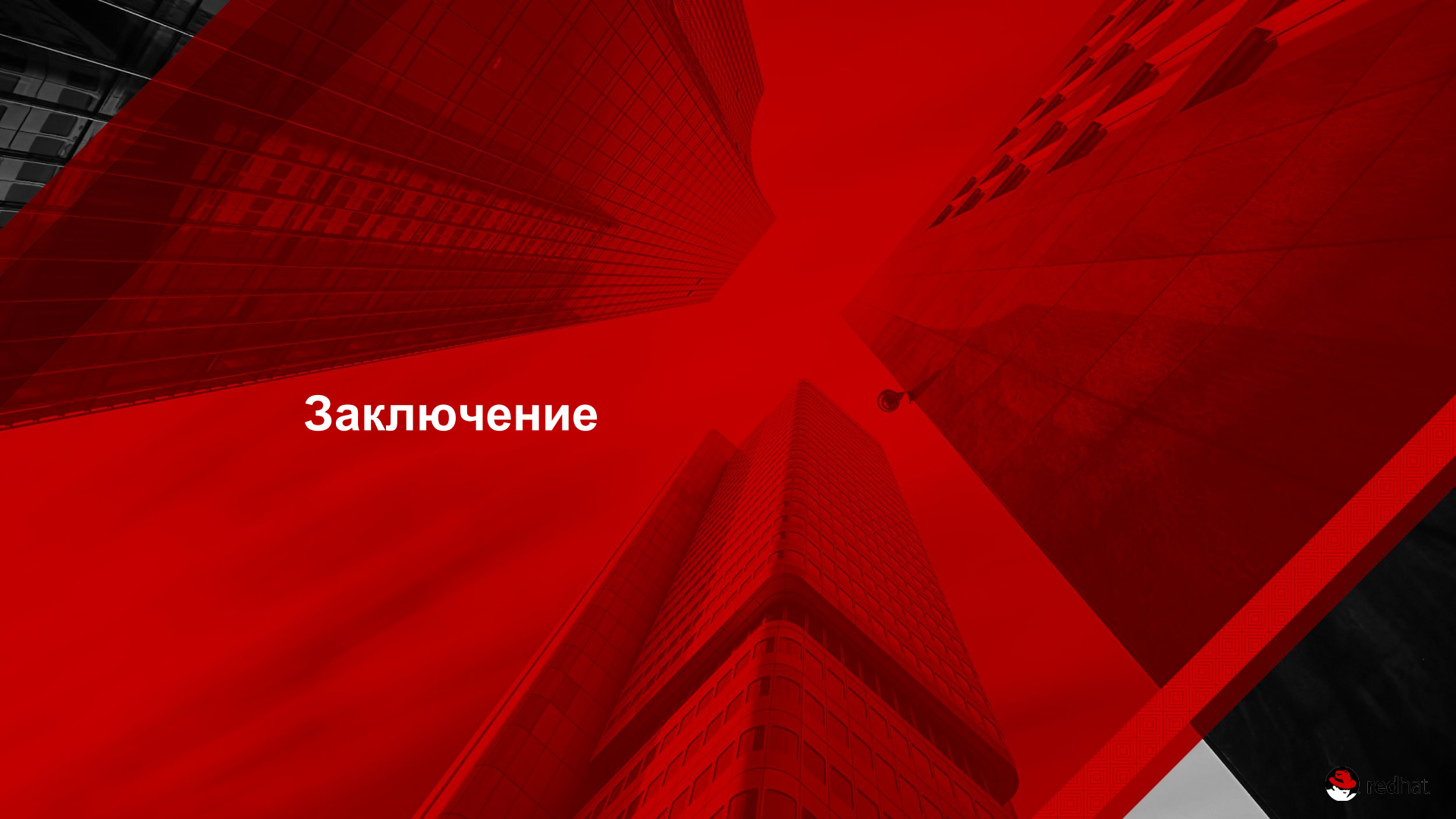
- Аутентификация учетной записи *admin* через Kerberos
  - `# kinit admin`
  - `# klist`

```
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@MONT.LAB
Valid starting       Expires              Service principal
07/18/2017 14:36:33  07/19/2017 14:36:30  krbtgt/MONT.LAB@MONT.LAB
```

- Вывод информации об аккаунте для проверки SSSD
  - `# id admin`

```
uid=574200000(admin) gid=574200000(admins) groups=574200000(admins),
574200010(rhvadmins), 574200008(satusers)
```

Заключение



Red Hat Identity Manager

Заключение

- Интегрированная аутентификация и контроль доступа для пользователей, хостов и сервисов – **без дополнительной платы с каждой подпиской на RHEL**
- Целостное и законченное IdM решение для Linux/Unix систем
- Взаимодействие с доменами Microsoft Active Directory
- Решение, основанное на стандартных, общеизвестных технологиях
- Простое и прозрачное внедрение
- Гибкие правила ограничения доступа
- До 60 серверов и реплик, неограниченное число клиентов

Документация

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/introduction.html
- http://rhelblog.redhat.com/tag/idm/
- http://www.freeipa.org/page/Main_Page
- https://access.redhat.com/products/identity-management

ВОПРОСЫ?


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos