



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

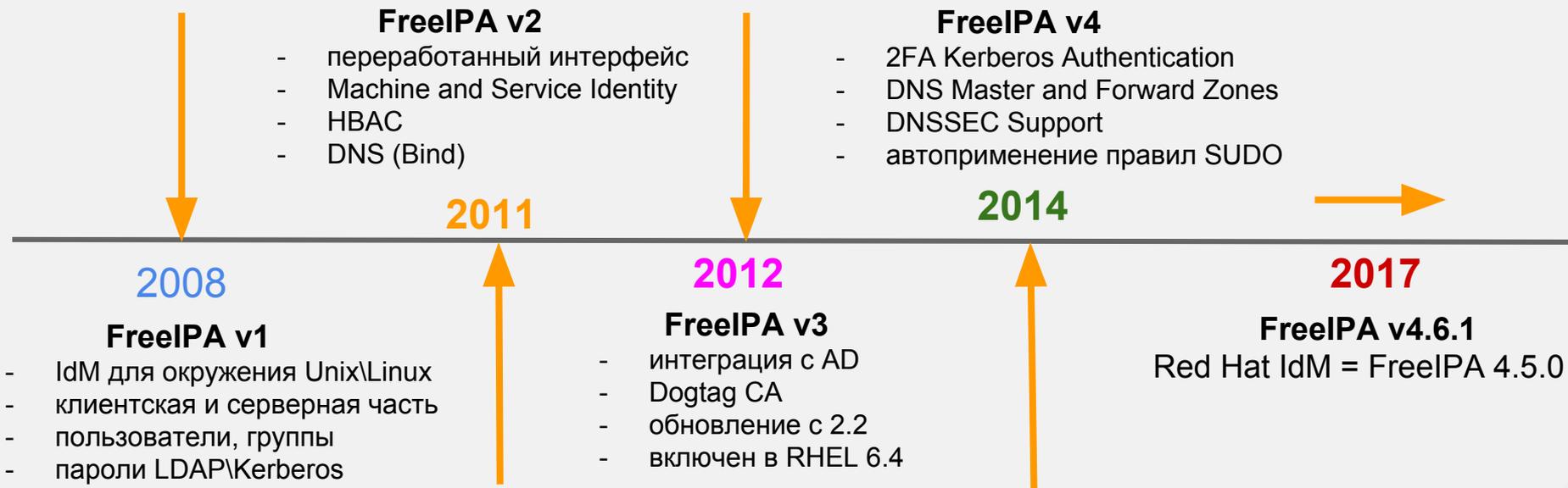
Что такое Red Hat Identity Manager?

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



Upstream-проект (<https://www.freeipa.org/page/Downloads>)

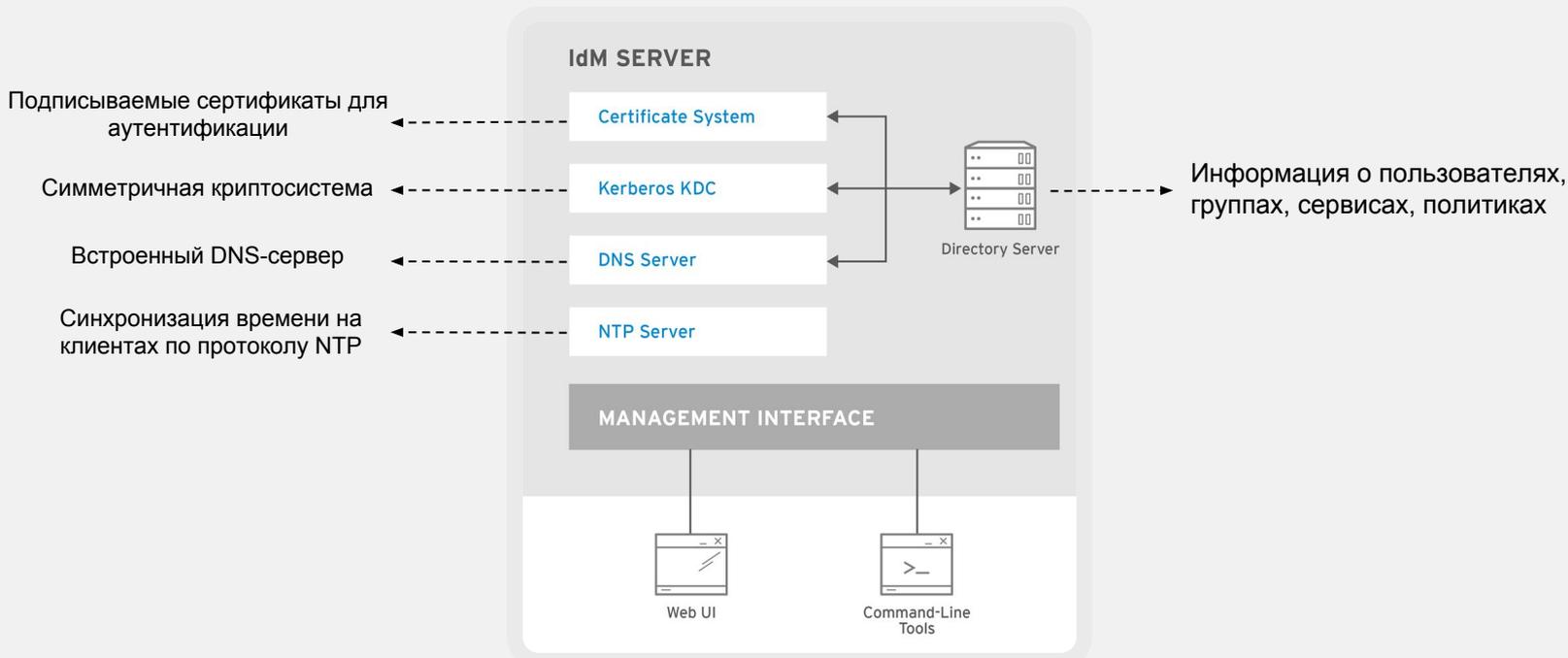
Что такое Red Hat Identity Manager?

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

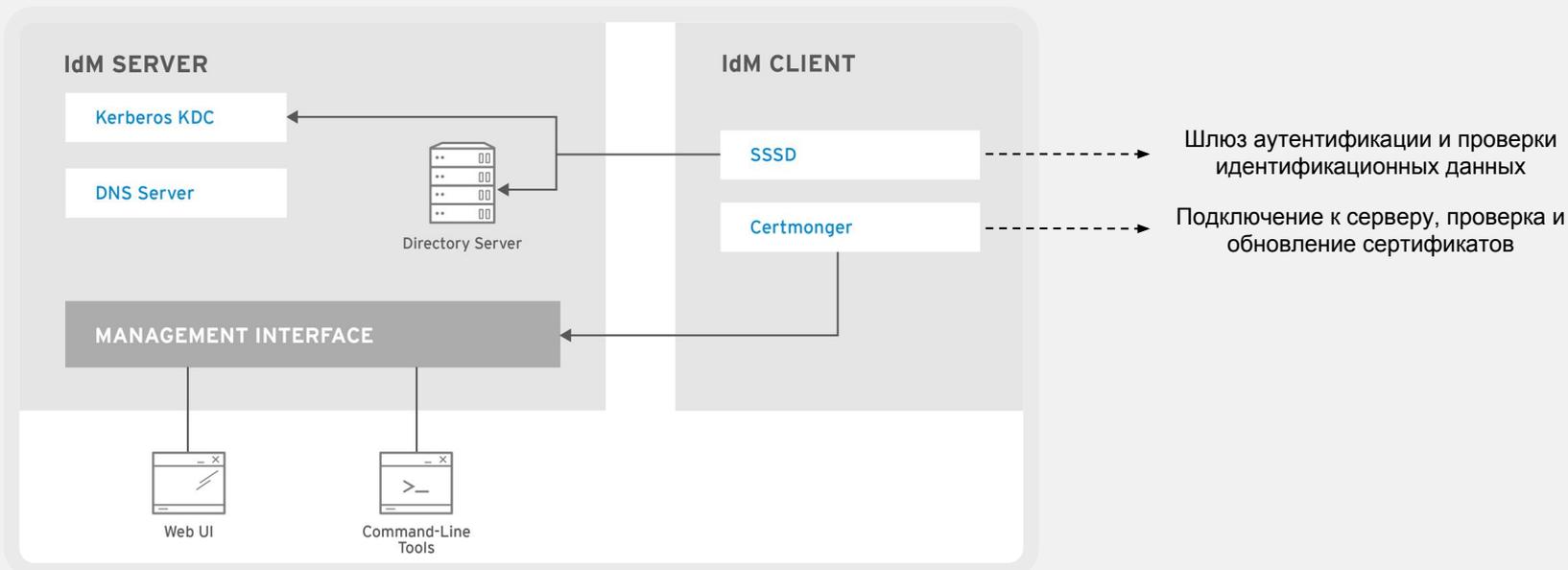
Архитектура Red Hat Identity Manager

Основные компоненты (серверная часть)



Архитектура Red Hat Identity Manager

Основные компоненты (клиентская часть)



Сценарии использования Identity Manager

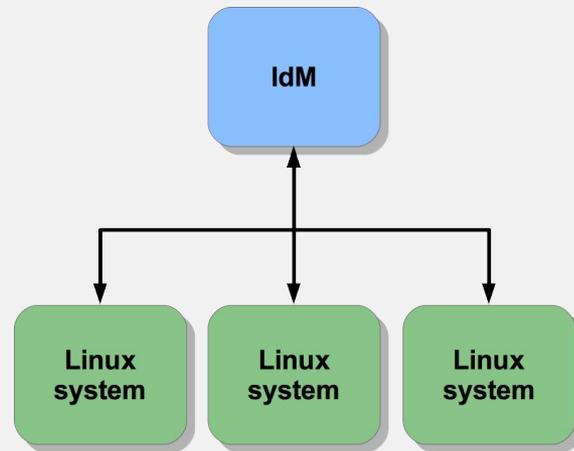
Основные задачи

- **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

The screenshot displays the Red Hat Identity Manager web interface. The top navigation bar includes 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. The main content area is divided into two sections: 'Группы пользователей' (User Groups) and 'Active users'.

Группы пользователей (User Groups):

Имя группы	ID группы	On
<input type="checkbox"/> ad_users	126200005	
<input type="checkbox"/> ad_users_ext		
<input type="checkbox"/> admins	126200000	Acc
<input type="checkbox"/> editors	126200002	Lim
<input type="checkbox"/> ipausers	126200006	Def

Узлы (Nodes):

Host name	Описание	Enrolled
<input type="checkbox"/> client1.mont.lab		True
<input type="checkbox"/> gate.mont.lab		True
<input type="checkbox"/> idm-replica.mont.lab		True
<input type="checkbox"/> idm.mont.lab		True
<input type="checkbox"/> satellite.mont.lab		True

Active users:

Логин пользователя	Имя	Фамилия	Status	UID	Электронный адрес	Телефонный номер	Должность
<input type="checkbox"/> admin		Administrator	✓ Включено	126200000			
<input type="checkbox"/> demouser	Name	Surname	✓ Включено	126200010	demouser@mont.lab		
<input type="checkbox"/> holmes	Sharlock	Holmes	✓ Включено	126200007	holmes@mont.lab		
<input type="checkbox"/> misterx	Mister	X	✓ Включено	126200001	misterx@mont.lab		

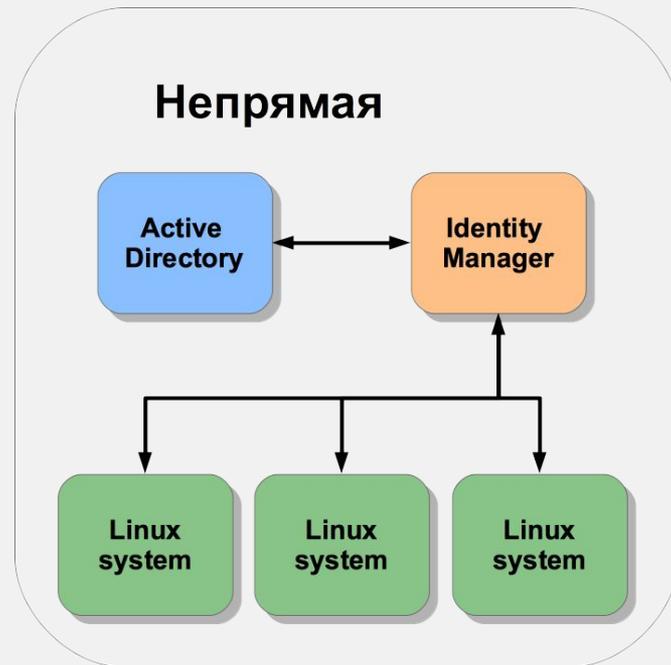
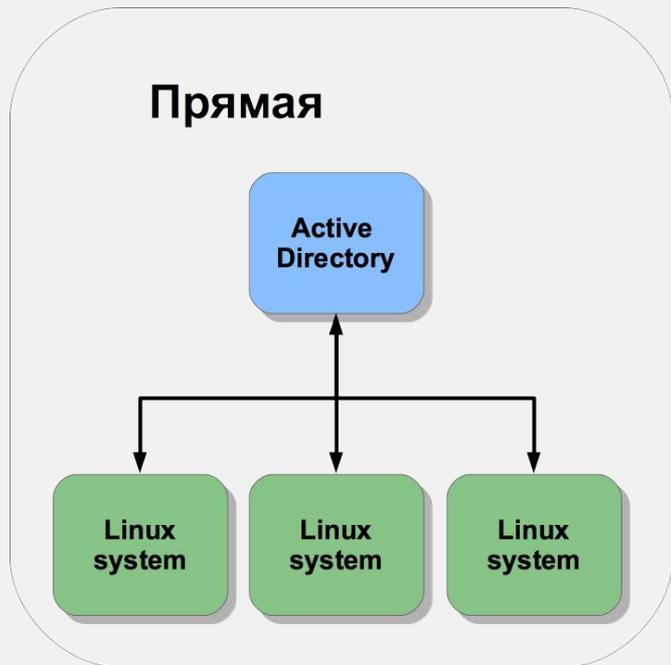
Сценарии использования Identity Manager

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

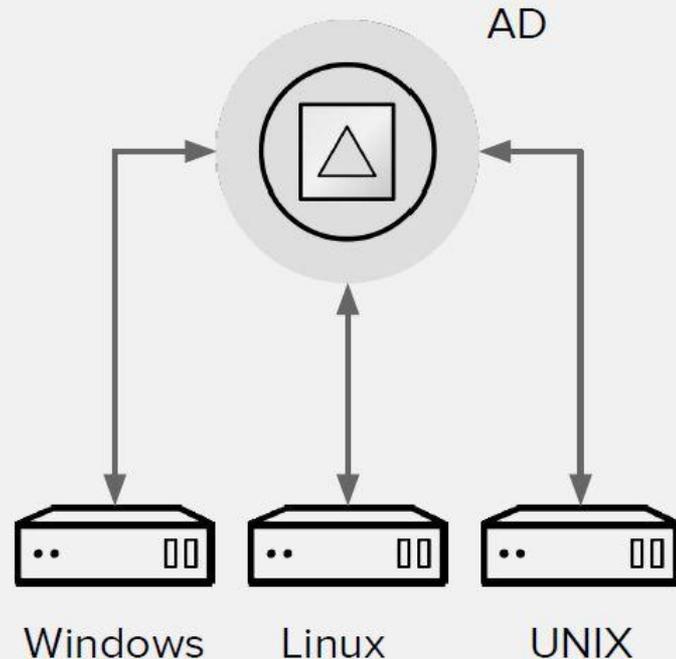
Интеграция с Active Directory



Сценарии использования Identity Manager

Прямая интеграция с Active Directory

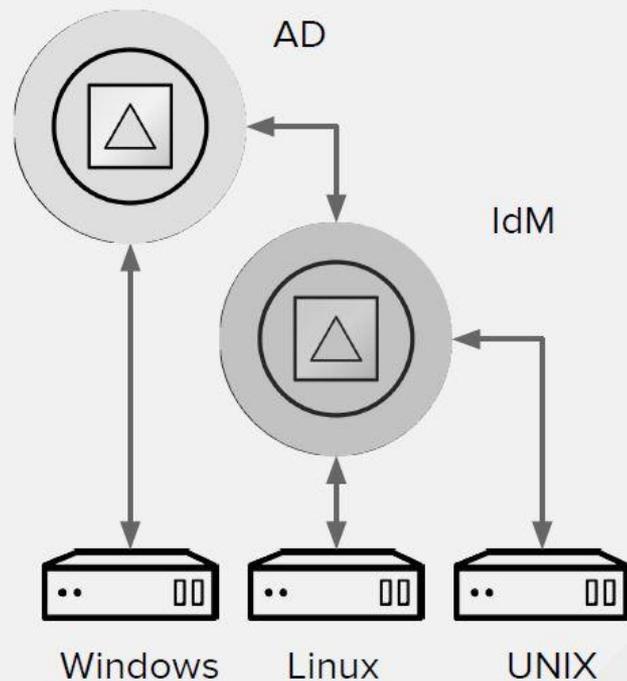
- Учетная запись в AD
- Управление базовыми правилами sudo и automount
- Соответствие AD SID и атрибутов POSIX
- Поддержка GPO для HBAC реализована в RHEL 7.1
- Управление политиками через конфигурационные файлы либо Satellite/Puppet



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

RED HAT IDENTITY MANAGEMENT Administrator

Identity Policy Authentication Network Services **IPA Server**

Role Based Access Control ID Ranges Realm Domains **Trusts** Topology API Browser Настройка

Trusts

Search

Realm name

demo.local

Showing 1 to 1 of 1 entries.

RED HAT IDENTITY MANAGEMENT

Identity Policy Authentication Network Services **IPA**

Пользователи Узлы Службы **Groups** ID Views

Группы пользователей > ad_users_ext

User Group: ad_users_ext

ad_users_ext members:

Пользователи Группы пользователей **External** Settings

Обновить Удалить +Добавить

<input type="checkbox"/>	External member
<input type="checkbox"/>	linux admins@demo.local
<input type="checkbox"/>	ikroshki@demo.local

Showing 1 to 2 of 2 entries.

RED HAT IDENTITY MANAGEMENT Administrator

Identity Policy Authentication Network Services **IPA Server**

Role Based Access Control ID Ranges Realm Domains **Trusts** Topology API Browser Настройка

Trusts > demo.local

Trusted domains: demo.local

Settings Trusted domains

Search Обновить Удалить Disable Enable Fetch domains

<input type="checkbox"/>	Domain name	Status	Domain NetBIOS name	Domain Security Identifier
<input type="checkbox"/>	demo.local	Включено	DEMO	S-1-5-21-2519176593-2246986734-45600760

Showing 1 to 1 of 1 entries.

Сценарии использования Identity Manager

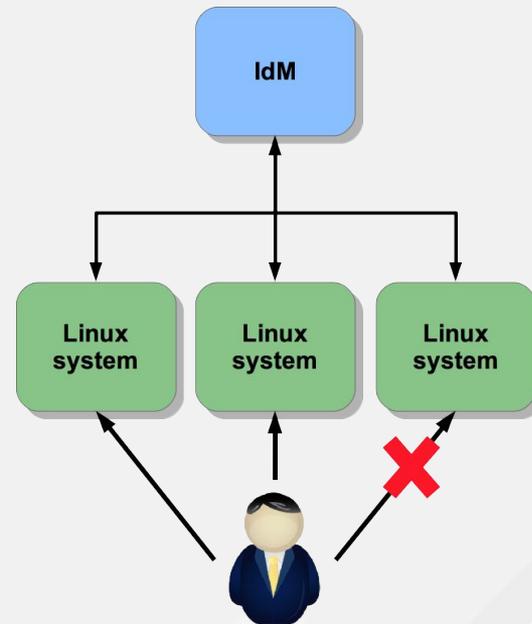
Основные задачи

- 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 не прямой интеграции)



Сценарии использования Identity Manager

Управление доступом (Host Based Access Control)

RED HAT IDENTITY MANAGEMENT Administrator

Identity Policy Authentication Network Services IPA Server

Host Based Access Control Sudo SELinux User Maps Password Policies Kerberos Ticket Policy

HBAC Rules

Search Обновить Удалить Добавить Disable Enable

<input type="checkbox"/>	Имя правила	Status	Описание
<input type="checkbox"/>	allow_all	— Disabled	Allow all users to access any host from any host
<input type="checkbox"/>	ssh_for_all	— Disabled	
<input type="checkbox"/>	sysadmin_webservers	✓ Включено	

Showing 1 to 3 of 3 entries.

Accessing

Host category the rule applies to: Any Host Specified Hosts and Groups

- Узлы
- Группы узлов
- webservers

Via Service

Service category the rule applies to: Any Service Specified Services and Groups

- Службы
- sshd
- Группы сервисов

Who

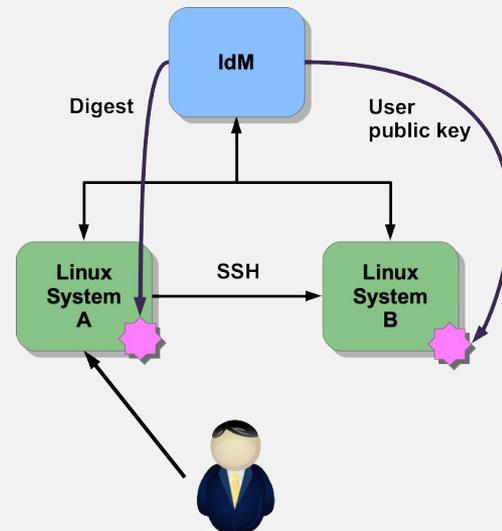
User category the rule applies to: Anyone Specified Users and Groups

- Пользователи
- Группы пользователей
- admins
- sysadmins
- trust admins

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 не прямой интеграции)



Сценарии использования Identity Manager

Управление SSH-ключами

The screenshot shows the Red Hat Identity Management web interface. The top navigation bar includes 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. The main menu has 'Пользователи', 'Узлы', 'Службы', 'Groups', 'ID Views', and 'Automember'. The current page is 'Узлы > client1.mont.lab'. Below the breadcrumb, it says 'Узел: client1.mont.lab'. There are tabs for 'client1.mont.lab is a member of:' (Settings, Группы узлов, Netgroups, Роли, HBAC Rules, Sudo Rules) and 'client1.mont.lab is managed by:' (Узлы). Below these are buttons for 'Обновить', 'Revert', 'Save', and 'Actions'. The 'Host Settings' section shows 'Host name' as 'client1.mont.lab', 'Principal alias' as 'host/client1.mont.lab@MONT.LAB' with a 'Удалить' button, and an 'Описание' field with a 'Добавить' button. The 'Enrollment' section shows 'Ключ Kerberos' with a checked 'Kerberos K' option and 'Одноразовый пароль' with a 'One-Time-' option. The 'Сертификат узла' section has a 'Certificates' field with a 'Добавить' button.

The screenshot shows the 'Открытые ключи SSH' (Open SSH Keys) section. It lists three SSH keys with their algorithms and public keys, each with 'Show/Set key' and 'Удалить' (Delete) buttons. At the bottom, there is a 'Добавить' (Add) button.

Algorithm	Public Key	Buttons
ssh-rsa	SHA256:r1TQqyYgyO6xu+xi3CdfCTcyop83z/+i4HMjSQ3ZhpE	Show/Set key, Удалить
ecdsa-sha2-nistp256	SHA256:19FeW+qJKwcewYnu4P5YLgOGhclrUkOea4QGAlpmSvE	Show/Set key, Удалить
ssh-ed25519	SHA256:4IMUZLwJ2VuZVhzq/E3ANSTWLMysfgQma0GJJE37rM8	Show/Set key, Удалить

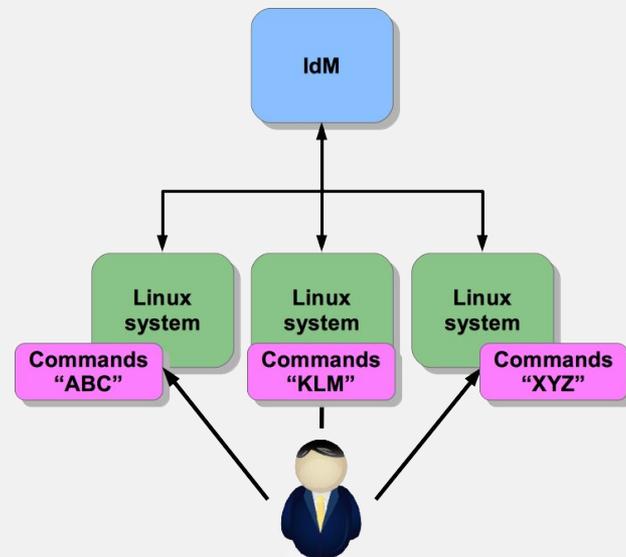
Добавить

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 не прямой интеграции)

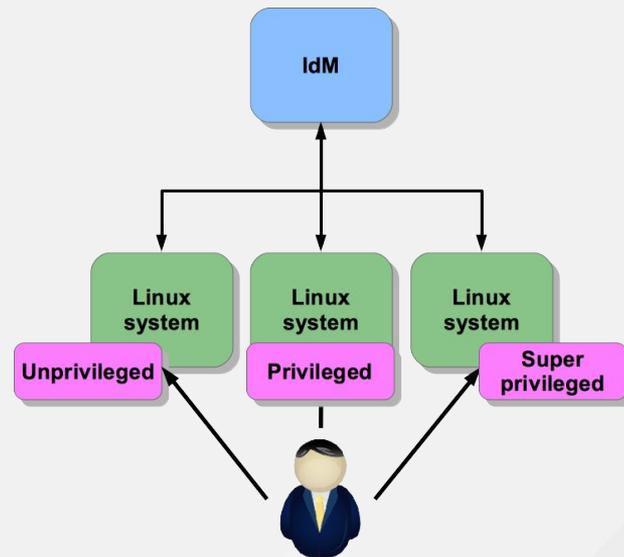
	Full refresh	Smart refresh	Rules refresh
When (default)	every 6 hours or when a rule is deleted from the cache	every 15 minutes	when user runs SUDO, rules expire after 90 minutes
Why	keep the cache consistent	store new rules	do not grant user more privilege
Operations	insert, delete	insert, modify	modify, 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 не прямой интеграции)



Сценарии использования Identity Manager

Управление правами SUDO

RED HAT IDENTITY MANAGEMENT Administrator

Identity Policy Authentication Network Services IPA Server

Host Based Access Control **Sudo** SELinux User Maps Password Policies Kerberos Ticket Policy

Sudo Rules

Search

- Имя правила
- sysadmin_sudo
- webadmin_sudo

Showing 1 to 2 of 2 entries.

RED HAT IDENTITY MANAGEMENT Administrator

Identity Policy Authentication Network Services IPA Server

Host Based Access Control **Sudo** SELinux User Maps Password Policies Kerberos Ticket Policy

Sudo Commands

Search

<input type="checkbox"/> Sudo Command	Описание
<input type="checkbox"/> /usr/bin/systemctl restart httpd	
<input type="checkbox"/> /usr/bin/systemctl start httpd	

Showing 1 to 2 of 2 entries.

Сценарии использования Identity Manager

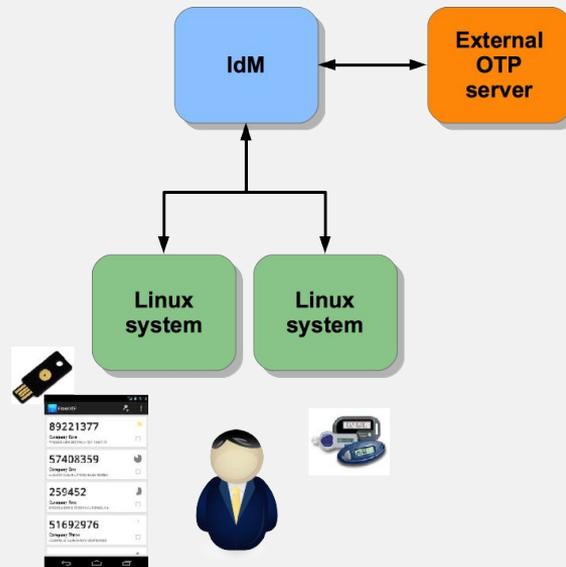
Основные задачи

- 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

The screenshot displays the Red Hat Identity Management (IdM) web interface. The top navigation bar includes 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. The 'Authentication' section is active, showing 'Certificates', 'OTP Tokens', and 'RADIUS Servers'. The 'OTP Tokens' page features a search bar and a table with one entry:

<input type="checkbox"/>	Unique ID
<input type="checkbox"/>	da9b5f17-799d-40d4-be1d-6c1856ef34e7

Showing 1 to 1 of 1 entries.

Overlaid on the right is a configuration form for a user. The fields are:

- Kerberos principal expiration: YYYY-MM-DD, hh : mm UTC
- Login shell: /bin/sh
- Home directory: /home/imalkin
- SSH public keys: Add
- Authentication options:
 - Password
 - RADIUS
 - Two factor authentication (password + OTP)

Сценарии использования Identity Manager

Двухфакторная аутентификация с использованием OTP



RED HAT® IDENTITY MANAGEMENT

Username

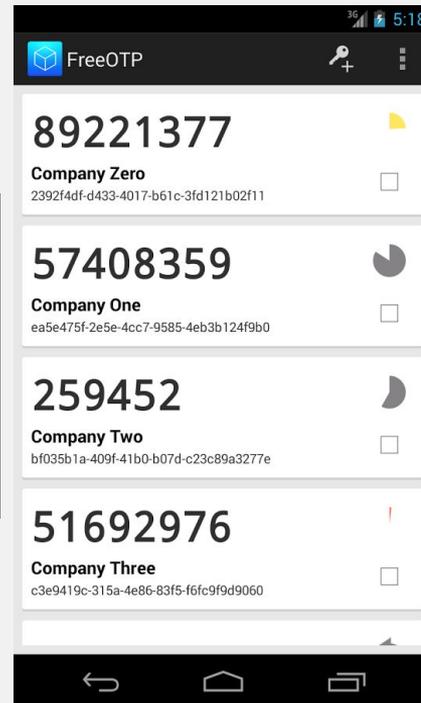
Password

First OTP

Second OTP

Token ID

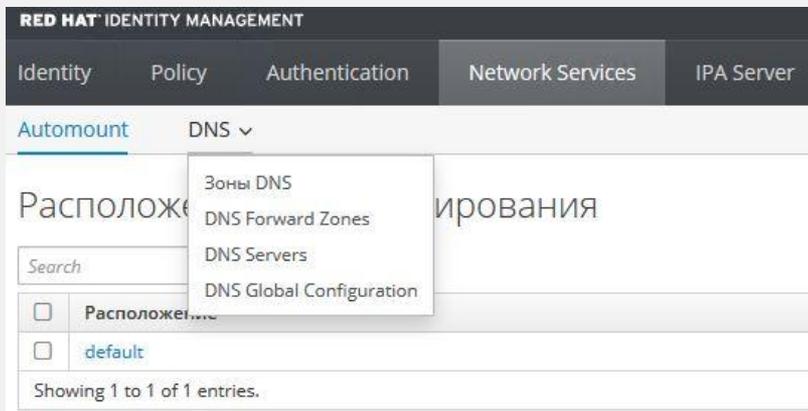
Cancel Sync OTP Token



Дополнительные возможности

Возможности Red Hat Identity Manager

Встроенный DNS-сервер



RED HAT IDENTITY MANAGEMENT

Identity Policy Authentication **Network Services** IPA Server

Automount DNS ▾

Расположение и конфигурирование

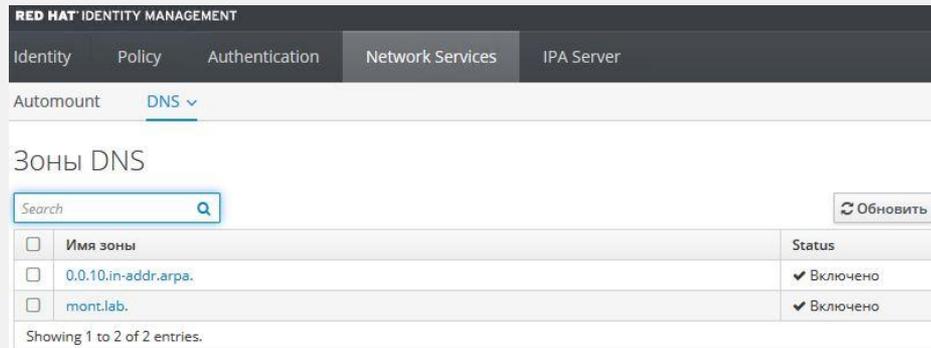
Search

- Зоны DNS
- DNS Forward Zones
- DNS Servers
- DNS Global Configuration

Расположение

default

Showing 1 to 1 of 1 entries.



RED HAT IDENTITY MANAGEMENT

Identity Policy Authentication **Network Services** IPA Server

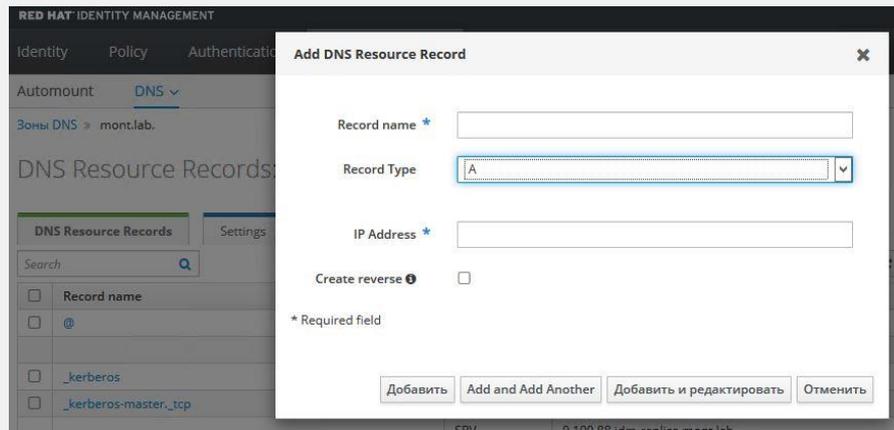
Automount **DNS** ▾

Зоны DNS

Search

<input type="checkbox"/>	Имя зоны	Status
<input type="checkbox"/>	0.0.10.in-addr.arpa.	✓ Включено
<input type="checkbox"/>	mont.lab.	✓ Включено

Showing 1 to 2 of 2 entries.



RED HAT IDENTITY MANAGEMENT

Identity Policy Authentication **Network Services** IPA Server

Automount **DNS** ▾

Зоны DNS » mont.lab.

DNS Resource Records

Search

Record name

@

_kerberos

_kerberos-master_tcp

Add DNS Resource Record

Record name *

Record Type

IP Address *

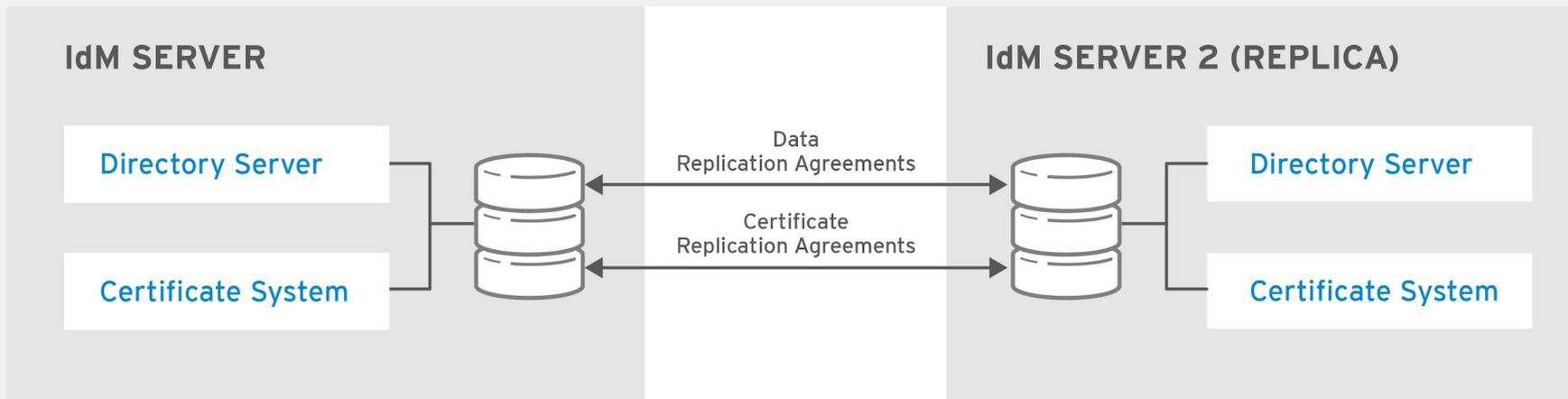
Create reverse

* Required field

SRV 0.100.88.idm-replica.mont.lab.

Возможности Red Hat Identity Manager

Поддержка репликации

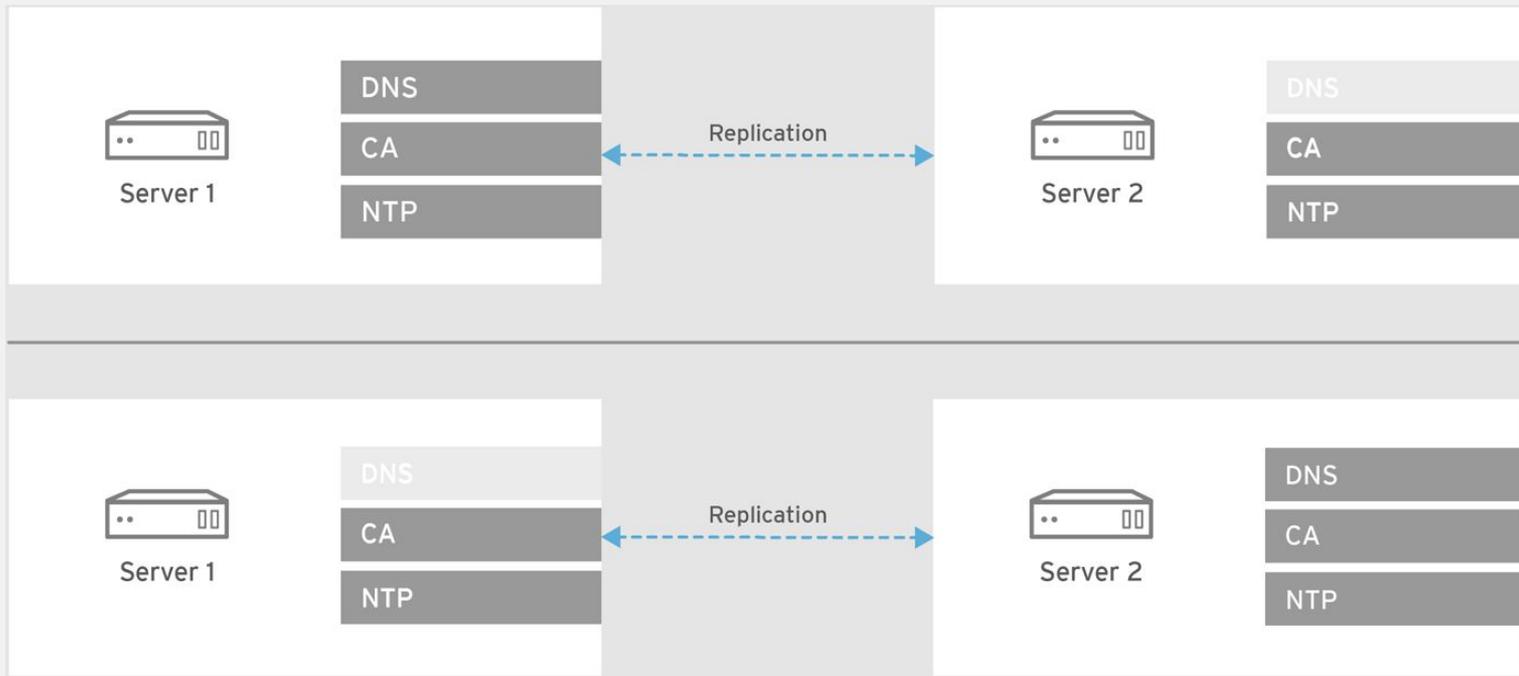


- Не более 60 реплик для одного IdM-домена
- Не менее двух, но не более четырех соглашений репликации на IdM-сервер

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

The image shows two overlapping screenshots of the Red Hat Identity Manager web interface. The top screenshot displays the 'IPA Servers' configuration page, and the bottom screenshot displays the 'Topology Graph'.

IPA Servers Screenshot:

- Navigation: Identity, Policy, Authentication, Network Services, **IPA Server**, API Browser, Настройка
- Sub-navigation: Role Based Access Control, ID Ranges, Realm Domains, Trusts, **Topology**
- Left sidebar: Topology, Topology suffixes, **IPA Servers**, Server Roles, Domain Level, Topology Graph, IPA Locations
- Search: Search [] [] [Обновить]
- Table:

<input type="checkbox"/>	Server name	Min domain level	Max domain level	Managed suffixes
<input type="checkbox"/>	idm-replica.mont.lab	0	1	domain, ca
<input type="checkbox"/>	idm.mont.lab	0		

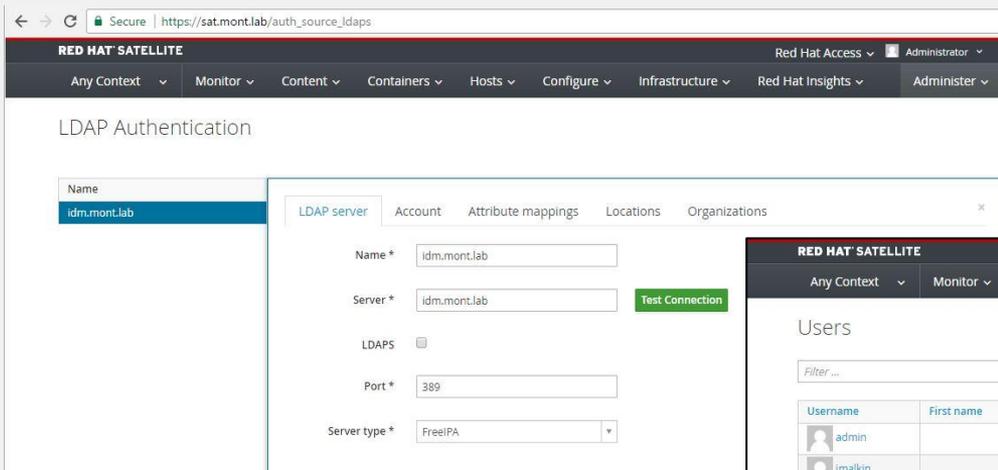
Showing 1 to 2 of 2 entries.

Topology Graph Screenshot:

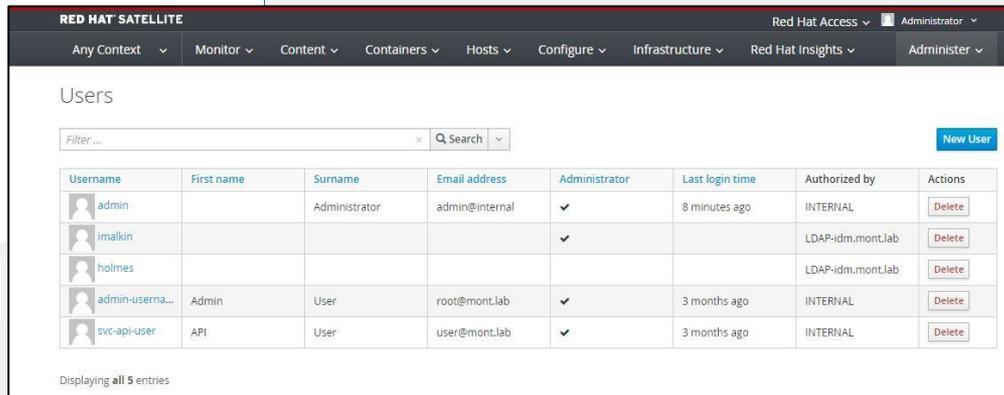
- Navigation: Identity, Policy, Authentication, Network Services, **IPA Server**, API Browser, Настройка
- Sub-navigation: Role Based Access Control, ID Ranges, Realm Domains, Trusts, **Topology**
- Left sidebar: Topology, Topology suffixes, IPA Servers, Server Roles, Domain Level, **Topology Graph**, IPA Locations
- Buttons: Обновить, + Добавить, Удалить
- Graph elements: ca, domain, idm, idm-replica
- Connections: Bidirectional arrows between idm and idm-replica (orange and blue).

Возможности Red Hat Identity Manager

Интеграция с Red Hat Satellite



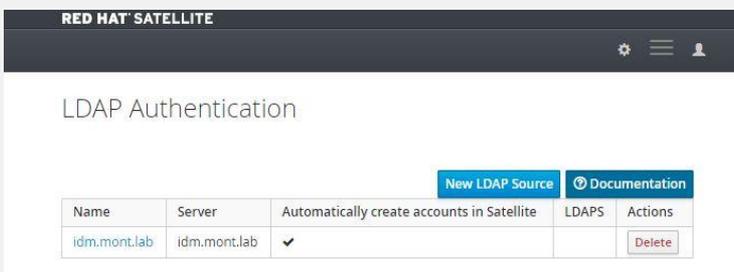
The screenshot shows the 'LDAP Authentication' configuration page in Red Hat Satellite. The browser address bar indicates the URL is https://sat.mont.lab/auth_source_ldaps. The page title is 'LDAP Authentication'. A list on the left shows the selected LDAP source 'idm.mont.lab'. The main configuration area includes fields for 'Name' (idm.mont.lab), 'Server' (idm.mont.lab), 'Port' (389), and 'Server type' (FreeIPA). A green 'Test Connection' button is visible next to the server field.



The screenshot shows the 'Users' page in Red Hat Satellite. The page title is 'Users'. A search bar is present at the top. Below it is a table listing users with columns for Username, First name, Surname, Email address, Administrator, Last login time, Authorized by, and Actions.

Username	First name	Surname	Email address	Administrator	Last login time	Authorized by	Actions
admin		Administrator	admin@internal	✓	8 minutes ago	INTERNAL	Delete
imalkin				✓		LDAP-idm.mont.lab	Delete
holmes						LDAP-idm.mont.lab	Delete
admin-userna...	Admin	User	root@mont.lab	✓	3 months ago	INTERNAL	Delete
svc-api-user	API	User	user@mont.lab	✓	3 months ago	INTERNAL	Delete

Displaying all 5 entries



The screenshot shows a table of LDAP sources in Red Hat Satellite. The table has columns for Name, Server, Automatically create accounts in Satellite, LDAPS, and Actions. A 'New LDAP Source' button and a 'Documentation' link are visible above the table.

Name	Server	Automatically create accounts in Satellite	LDAPS	Actions
idm.mont.lab	idm.mont.lab	✓		Delete

Возможности Red Hat Identity Manager

Интеграция с Red Hat Virtualization

RED HAT VIRTUALIZATION

Username:

Password:

Profile:

[Log In](#)

RED HAT VIRTUALIZATION

users:type = user

Dashboard | Data Centers | Clusters | Hosts | Networks | Storage | Disks | Virtual Machines | Pools | Templates

system

Expand All Collapse All

System

- Data Centers
 - MONT-01
 - Storage
 - Networks
 - Templates
 - Clusters
 - External Providers
 - Satellite

Add Users and Groups

User Group

Search: Namespace:

First Name	Last Name	User Name
<input type="checkbox"/>	Administrator	admin
<input type="checkbox"/>	Dmitry Sevostyanov	dsevosty
<input type="checkbox"/>	Vadim Zharov	vzharov
<input type="checkbox"/>	Igor Kroshkin	ikroshki
<input type="checkbox"/>	Openshift Administrator	openshift-admin
	Astakhov	aastakhov
	Dummy User	cfme-dummyuser
	Catling	ncatling
	Test	ose-test1

RED HAT VIRTUALIZATION

users:type = user

Dashboard | Data Centers | Clusters | Hosts | Networks | Storage | Disks | Virtual Machines | Pools | Templates | Volumes | Users

System

Add Remove Assign Tags

User Group

First Name	Last Name	User Name	Authorization provider	Namespace	E-mail
admin		admin	internal-authz	*	
Alexander	Safonov	asafonov	idm01.srv.local	dc=srv,dc=local	asafonov@srv.local
Dmitry	Sevostyanov	dsevosty	idm01.srv.local	dc=srv,dc=local	dsevosty@oscp.local
Dmitry	Ivanyuk	divanyuk	idm01.srv.local	dc=srv,dc=local	divanyuk@srv.local
Igor	Kroshkin	ikroshki	idm01.srv.local	dc=srv,dc=local	ikroshki@srv.local
Igor	Malkin	imalkin	idm01.srv.local	dc=srv,dc=local	imalkin@srv.local
Igor	Buday	ibuday	idm01.srv.local	dc=srv,dc=local	ibuday@srv.local
User	Dummy	rhv-dummyuser	idm01.srv.local	dc=srv,dc=local	rhv-dummyuser@srv.local
Vadim	Zharov	vzharov	idm01.srv.local	dc=srv,dc=local	vzharov@srv.local

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
 - `#subscription-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

The screenshot displays the Red Hat Satellite web interface for creating a job invocation. The interface is split into two panels. The left panel shows the configuration for a job, and the right panel shows the details of the job invocation.

Left Panel Configuration:

- Job category ***: Packages
- Job template ***: Package Action - SSH Default
- Bookmark**: (empty)
- Search query**: name = gate.mont.lab
- Resolves to**: 1 hosts
- action**: install (The package action: install, update, or remove)
- package**: ipa-client (The name of the package, if any)
- Schedule**: Execute now Schedule future execution Set up recurring execution

Right Panel Job Invocation Details:

- Job category ***: Commands
- Job template ***: Run Command - SSH Default
- Bookmark**: (empty)
- Search query**: name = gate.mont.lab
- Resolves to**: 1 hosts
- command ***: ipa-client-install --server server.example.com \ --domain example.com \ --enable-dns-updates
- Schedule**: Execute now Schedule future execution Set up recurring execution

Buttons: Cancel, Submit

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