We are CloudLinux™

Построение корпоративной системы управления идентификационной информацией

Леонид Кантер

lkanter@cloudlinux.com

Состояние компании на середину 2016 года

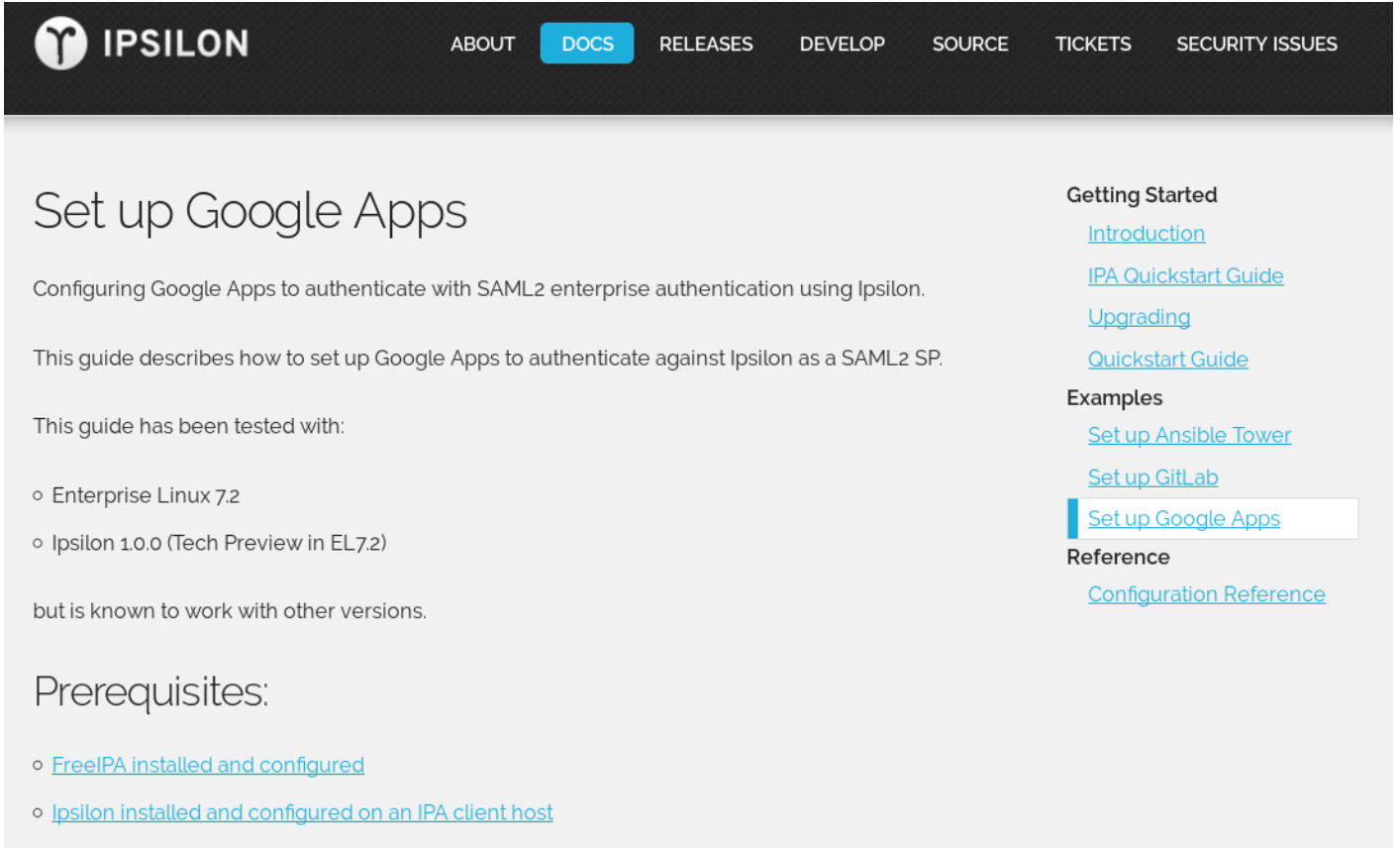
We are CloudLinux

Начало 2014 года:

- Один продукт: CloudLinux
- 40 сотрудников
- Из них 25 в Донецком офисе
- 4 сервера PCS 6 в Донецке
- Google Apps

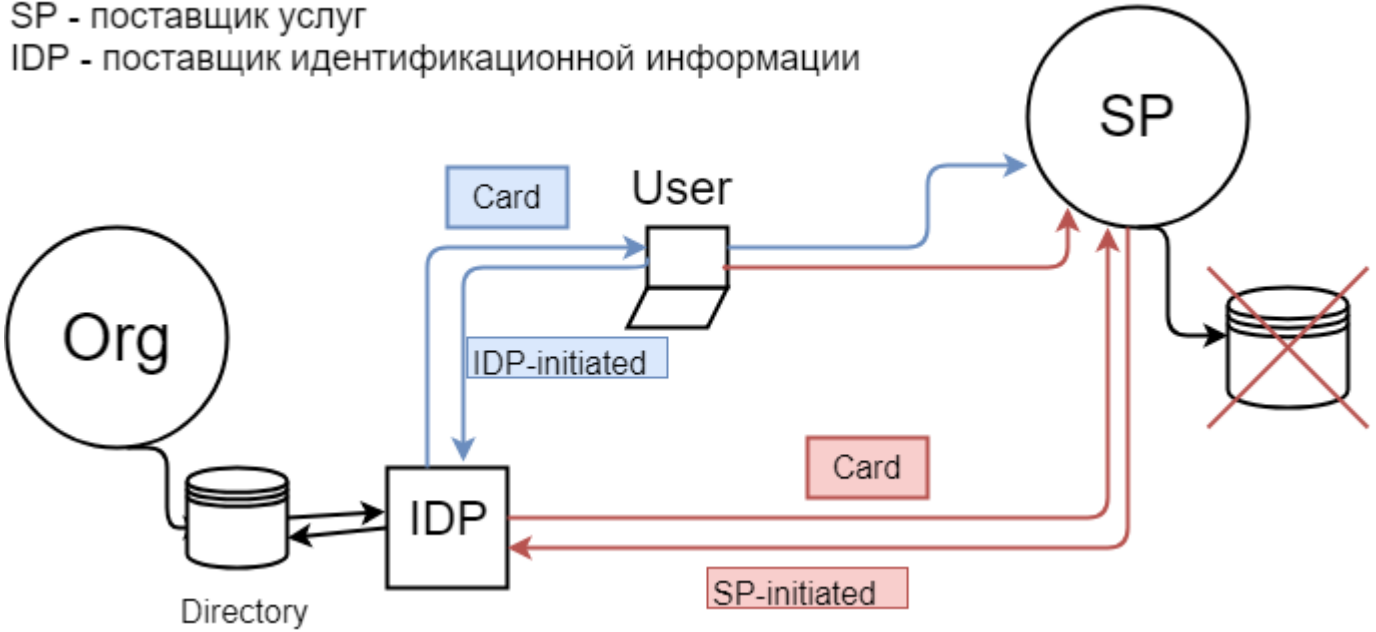
Август 2016 года:

- Три продукта
- Более 100 сотрудников
- Удаленная работа: Украина, Россия, США, Казахстан
- Два корпоративных облака виртуальных машин OpenNebula
- Google Apps

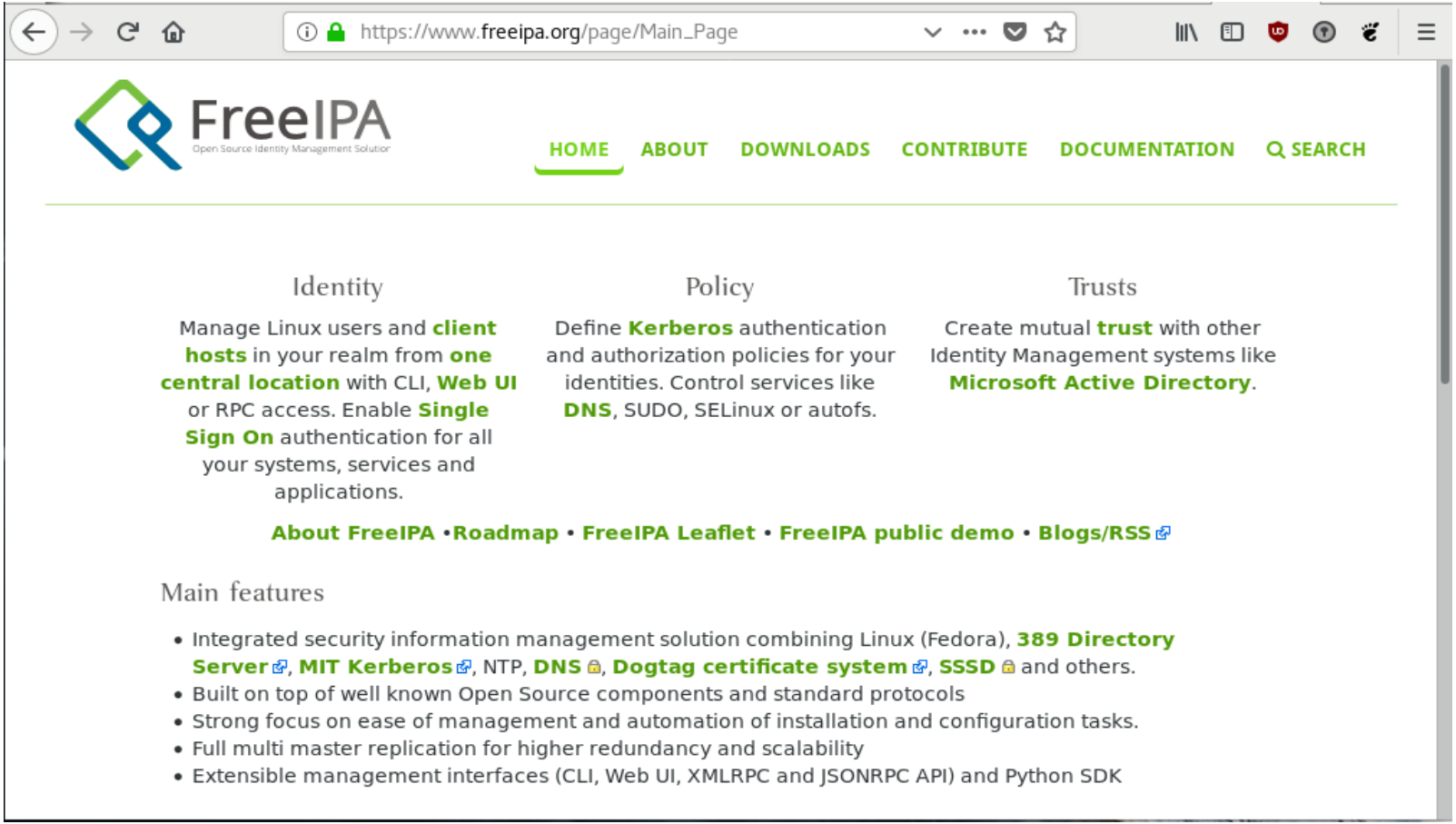

IPSILON
ABOUT
DOCS
RELEASES
DEVELOP
SOURCE
TICKETS
SECURITY ISSUES
Set up Google Apps
Configuring Google Apps to authenticate with SAML2 enterprise authentication using Ipsilon.
This guide describes how to set up Google Apps to authenticate against Ipsilon as a SAML2 SP.
This guide has been tested with:
Enterprise Linux 7.2
Ipsilon 1.0.0 (Tech Preview in EL7.2)
but is known to work with other versions.
Prerequisites:
FreeIPA installed and configured
Ipsilon installed and configured on an IPA client host
Getting Started
Introduction
IPA Quickstart Guide
Upgrading
Quickstart Guide
Examples
Set up Ansible Tower
Set up GitLab
Set up Google Apps
Reference
Configuration Reference

Введение в SAML

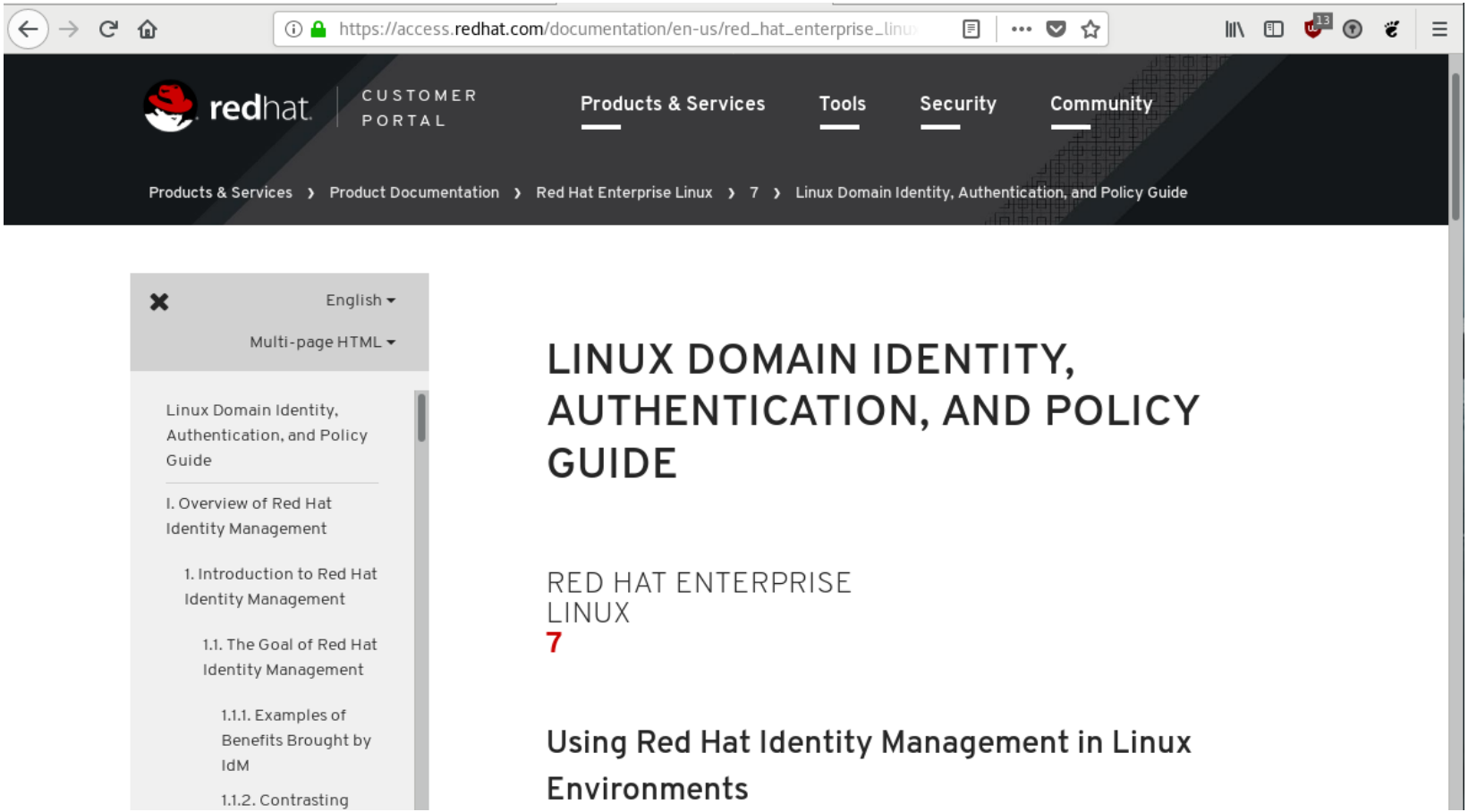
Org - организация
SP - поставщик услуг
IDP - поставщик идентификационной информации



Проект FreeIPA



Основной источник информаци



Цели и задачи FreeIPA

FreeIPA позволяет администратору:

- Управлять идентификационной информацией в одном месте — на сервере FreeIPA
- Единообразно применять политики к большому количеству машин
- Устанавливать для пользователя различные уровни доступа при помощи правил доступа на уровне хостов, делегирования, и других правил
- Централизованно управлять правилами эскалации полномочий (sudo)
- Определять, как монтируются домашние каталоги

Единый корпоративный вход в систему, или Single Sing-ON (SSO)

- Улучшает удобство использования
- Снижает риск ненадежного хранения пароля
- Повышает продуктивность пользователя

Установка сервера FreeIPA

We are CloudLinux

Подготовка у установке для домена corp.example.com

1. Настроить прямую и обратную зону для IP-адреса сервера. Команда

dig +short auth.corp.example.org A

должна возвращать IP-адрес сервера

2. Установить bind, разрешить рекурсивные запросы только для внутренних сетей

3. Настроить firewall, оставив открытыми только следующие порты:

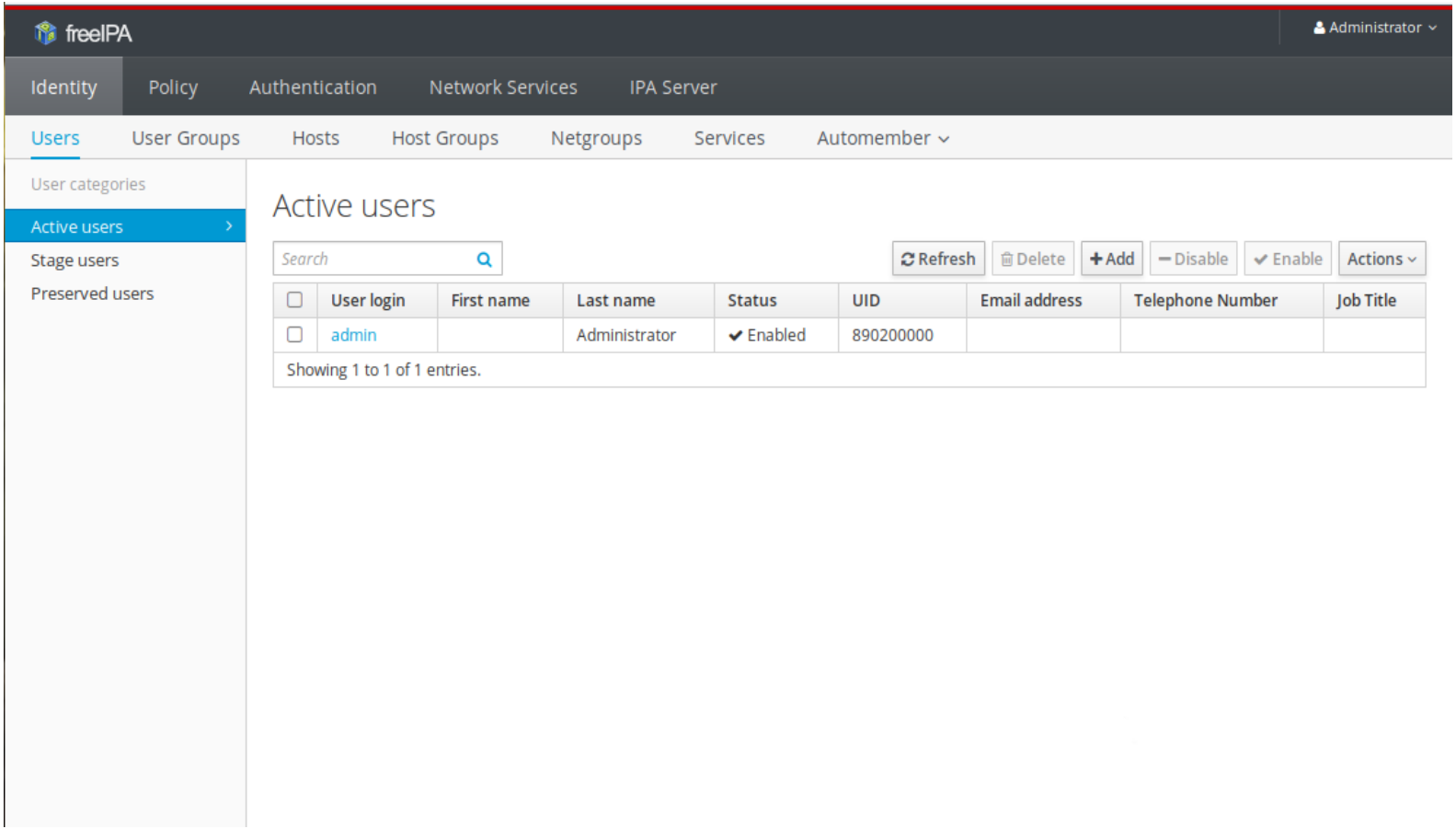
```
# firewall-cmd --permanent --add-
port={80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,464/tcp,53/tcp,88/udp,464/udp,53/udp,123/
udp}
```

После этого выполнить следующие команды:

```
# yum install freeipa server
# ipa-server-install --domain=corp.example.com --realm=CORP.EXAMPLE.COM --setup-dns
--no-forwarders --mkhomedir --idstart=10000 --dirsrv-cert-file auth.crt --http-cert-
file auth.crt --dirsrv-cert-file intermediate.crt --http-cert-file intermediate.crt
--ca-cert-file ca.crt
```

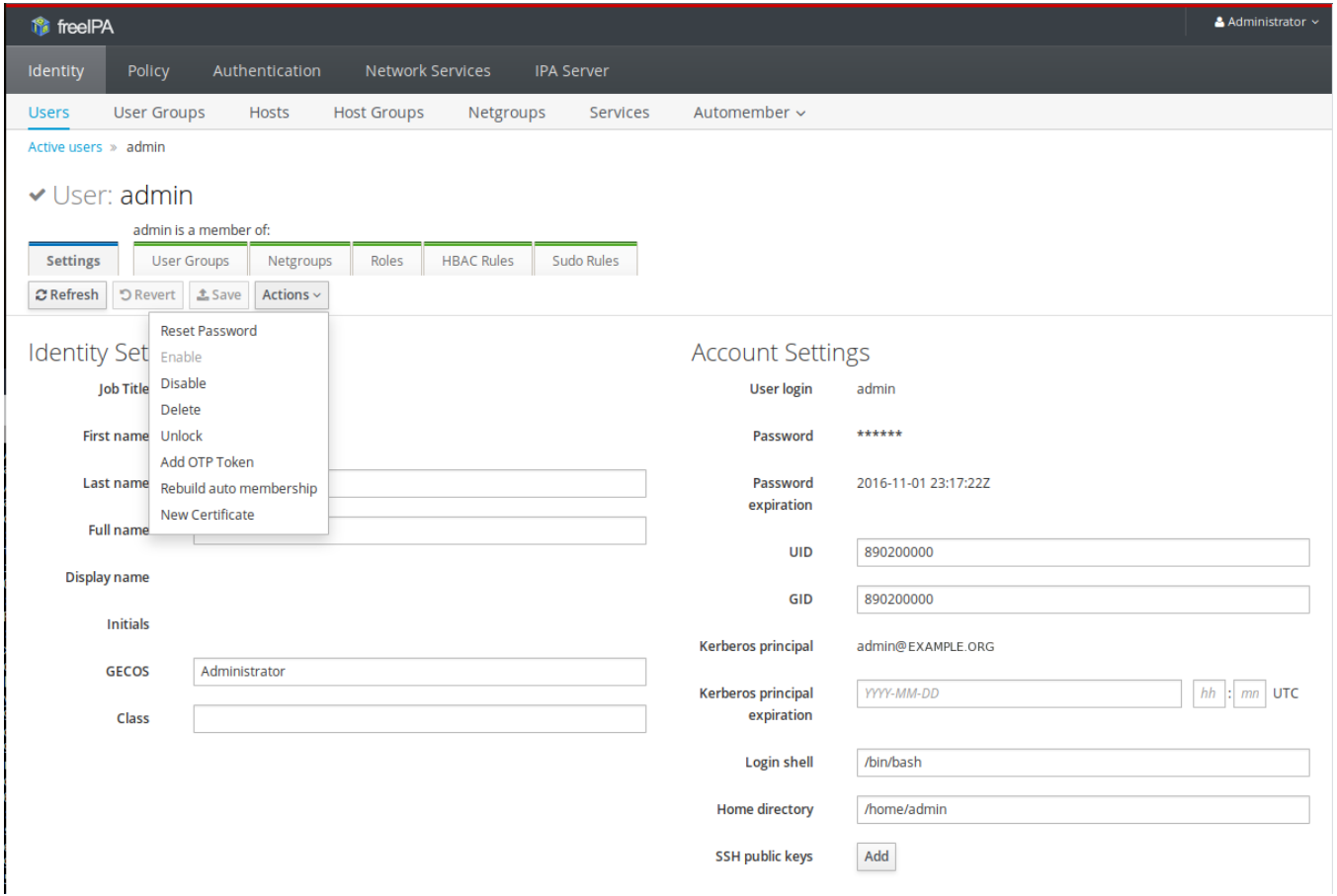
Веб-интерфейс FreeIPA

We are CloudLinux



Экран администрирования пользователя

We are CloudLinux



Интерфейс командной строки

We are CloudLinux

```
[root@auth ~]# kinit admin
Password for admin@CORP.EXAMPLE.COM:

[root@auth ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@CORP.EXAMPLE.COM

Valid starting       Expires              Service principal
09/29/2018 09:53:40  09/30/2018 09:53:30  krbtgt/CORP.EXAMPLE.COM@CORP.EXAMPLE.COM

[root@auth ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@CORP.CLOUDLINUX.COM
  UID: 10000
  GID: 10000
  Account disabled: False
  Password: True
  Member of groups: admins, infrastructure, trust admins
  Kerberos keys available: True
```

Установка Ipsilon

We are CloudLinux

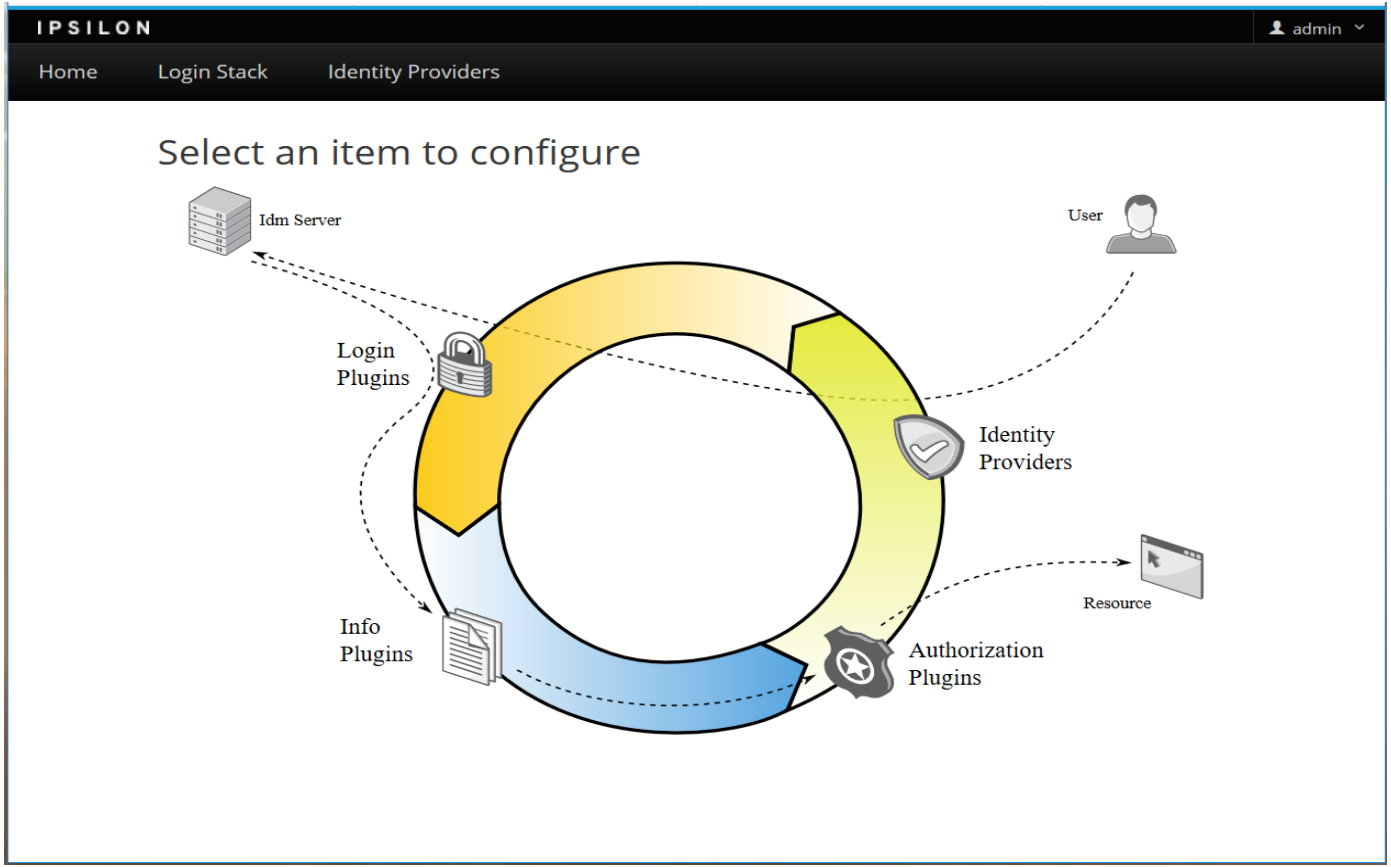
```
# yum install ipa-client
.....
# ipa-client-install --domain=corp.example.com --hostname=idp.corp.example.com \
 --no-nisdomain --mkhomedir
....
# cat /etc/yum.repos.d/ipsilon.repo
[puiterwijk-ipsilon]
name=Copr repo for ipsilon owned by puiterwijk
baseurl=https://copr-be.cloud.fedoraproject.org/results/puiterwijk/ipsilon/epel-7-$basearch/
skip_if_unavailable=True
gpgcheck=1
gpgkey=https://copr-be.cloud.fedoraproject.org/results/puiterwijk/ipsilon/pubkey.gpg
enabled=1
enabled_metadata=1

# yum install ipsilon ipsilon-authgssapi ipsilon-saml2-base ipsilon-authpam ipsilon-base \
ipsilon-tools-ipa ipsilon-saml2 ipsilon-authform ipsilon-filesystem ipsilon-infosssd
....
# kinit admin
....
# ipsilon-server-install --ipa=yes --info-sssd=yes --form=yes
....
# systemctl restart httpd
```

Дополнительные настройки безопасности

We are CloudLinux

```
[root@auth ~]# ipa hbacrule-show allow_all
  Rule name: allow_all
  Host category: all
  Service category: all
  Description: Allow all users to access any host from any host
  Enabled: TRUE
  User Groups: infrastructure
[root@auth ~]# ipa hbacrule-show allow_ipsilon
  Rule name: allow_ipsilon
  User category: all
  Enabled: TRUE
  Hosts: idp.corp.cloudlinux.com
  Services: ipsilon
```

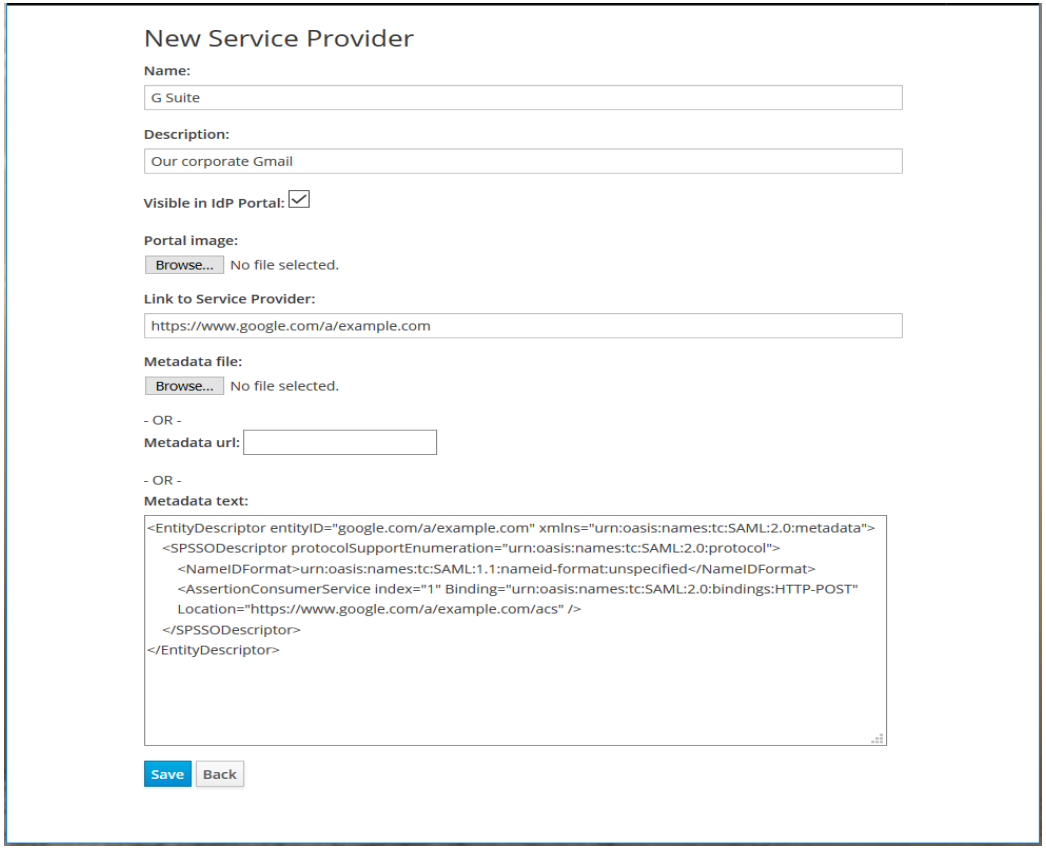
Административная консоль Ipsilon



Настройка поставщика услуг

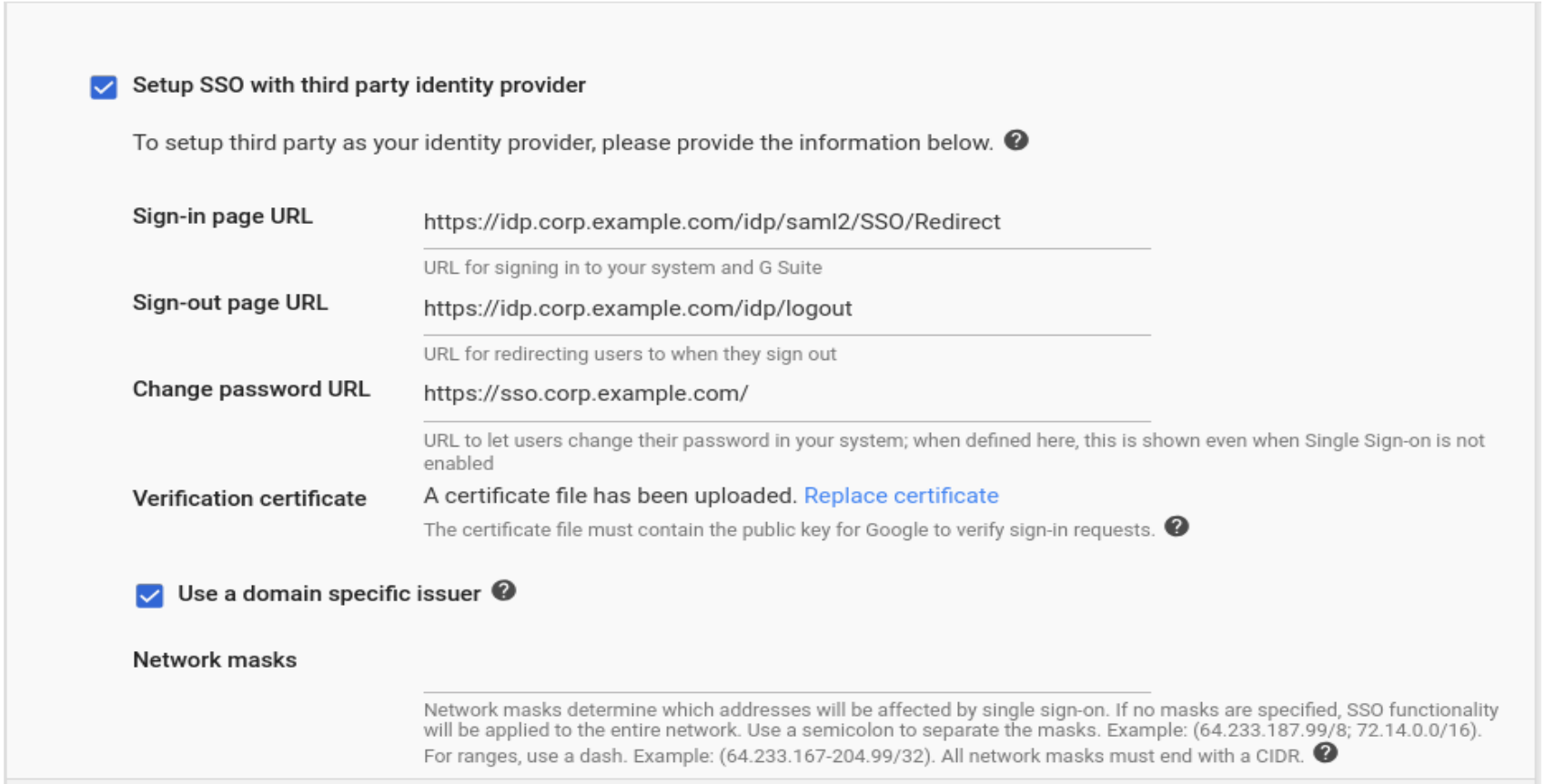
We are CloudLinux

Добавление поставщика услуг G Suite

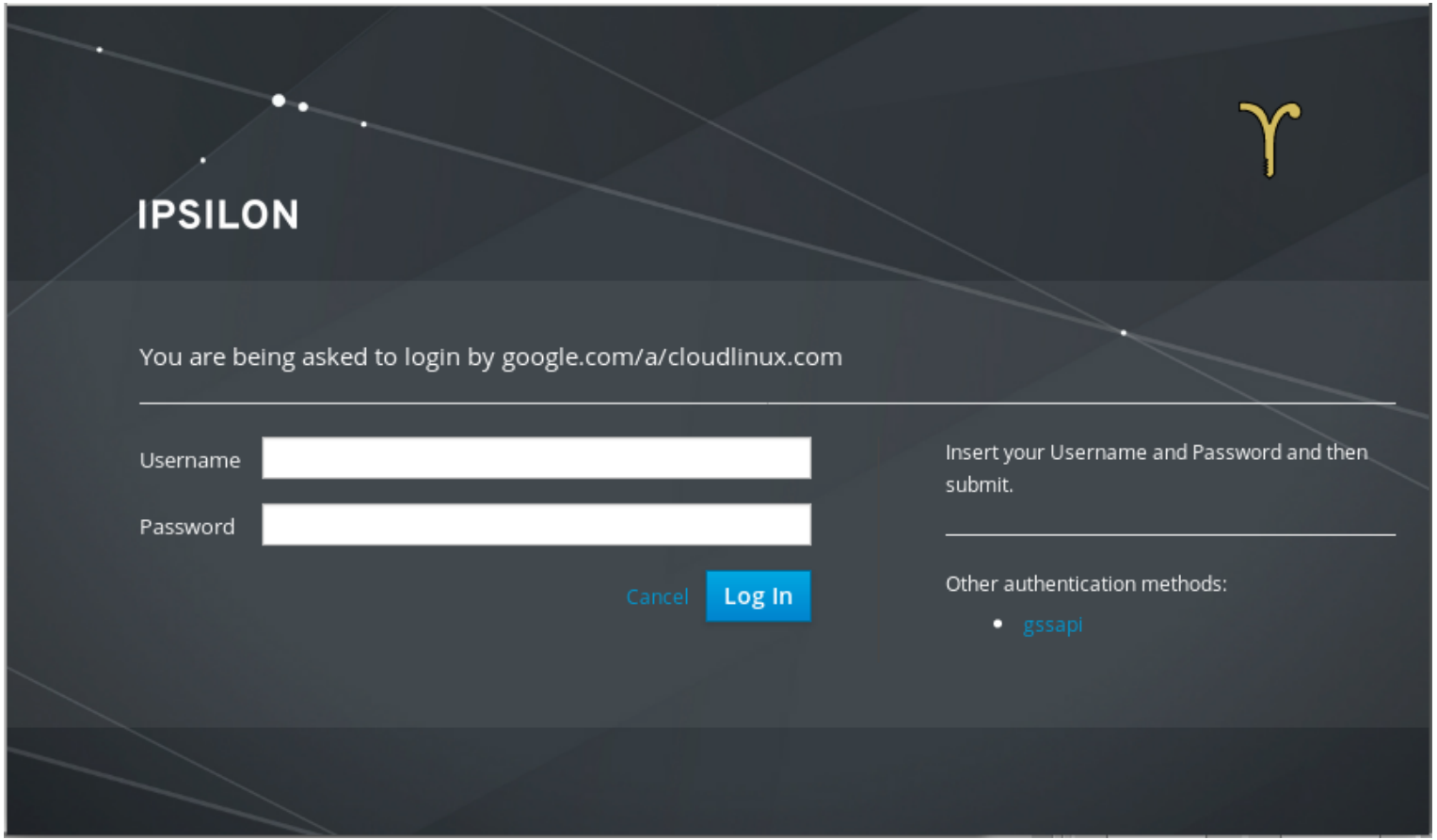


Настройка G Suite

We are CloudLinux



Результат: при попытке входа переадресация на Ipsilon



Интеграция произвольных вебсайтов

We are CloudLinux

Доступ на любой сайт под управлением веб-сервера Apache можно ограничить при помощи пакета ipsilon-client. Для установки пакета необходимо создать файл конфигурации репозитория, как описано выше, и установить пакет командой

```
# yum install ipsilon-client
```

Предположим, нужно ограничить доступ к странице `https://site.corp.example.com/site`. Для этого нужно выполнить команду:

```
# ipsilon-client-install --saml-idp-metadata https://idp.corp.example.com/idp/saml2/metadata \
--auth-location /site --hostname site.corp.example.com
```

В результате выполнения этой команды в каталоге `/etc/httpd/saml2/site.corp.example.com` будет создано несколько фалов, включая файл `metadata.xml`.

Следующим этап – настройка поставщика услуг на Ipsilon. Для этого нужно перейти на страницу добавления нового поставщика услуг, как описано выше, заполнить произвольным образом поля названия и описания ресурса, в поле перехода указать ссылку `https://site.corp.example.com/site`, а в поле ввода метаданных скопировать содержимое полученного на первом шаге файла metadata.xml.

Другие способы интеграции приложений

We are CloudLinux

Mail Services

- **Dovecot Integration**
- **Dovecot IMAPS Integration with FreeIPA using Single Sign On**
- **Postfix relaying using IPA for Kerberos Authentication**
- **Zimbra Collaboration Server 7.2 Authentication and GAL lookups against FreeIPA**
- **Kerberizing PostgreSQL with FreeIPA for Keystone** (see related **discussion**)

Web Services

- **Setting up MediaWiki to run against FreeIPA**
- **Apache and Kerberos for Django Authentication + Authorization**
- **LDAP authentication for Atlassian JIRA using FreeIPA**
- **LDAP authentication for JIRA using FreeIPA**
- **Using IPA server and sssd for web application's authentication and identity needs**
- **Setting up Redmine to authenticate users against FreeIPA**
- **Setting up Rhodecode to authenticate users against FreeIPA**
- **Setting up The Bug Genie to authenticate users against FreeIPA**

Использование Kerberos

Kerberos /kɛərbərəs/ — сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы.

После успешной первичной аутентификации центр распределения ключей (Key Distribution Center, KDC) выдает первичное удостоверение пользователя для доступа к сетевым ресурсам — Ticket Granting Ticket (TGT). В дальнейшем, при обращении к отдельным ресурсам сети, пользователь, предъявляя TGT, получает от KDC удостоверение для доступа к конкретному сетевому ресурсу — Service Ticket (TGS)

Использование Kerberos

We are CloudLinux

```
debug1: Found key in /home/lkanter/.ssh/known_hosts:881
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS received
debug1: Skipping ssh-dss key /home/lkanter/.ssh/id_dsa - not in PubkeyAcceptedKeyTypes
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<rsa-sha2-256,rsa-sha2-512>
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Next authentication method: gssapi-keyex
debug1: No valid Key exchange context
debug1: Next authentication method: gssapi-with-mic
debug1: Enabling compression at level 6.
debug1: Authentication succeeded (gssapi-with-mic).
```

Использование Kerberos

We are CloudLinux

```
[user@localhost ~]$ klist
Ticket cache: KEYRING:persistent:1000:1000
Default principal: user@CORP.CLOUDLINUX.COM

Valid starting       Expires              Service principal
09/28/2018 20:01:34  09/29/2018 19:56:18  host/idp.corp.example.com@CORP.EXAMPLE.COM
        renew until 10/05/2018 19:56:18
09/28/2018 20:01:34  09/29/2018 19:56:18  host/idp.corp.example.com@
        renew until 10/05/2018 19:56:18
09/28/2018 19:56:25  09/29/2018 19:56:18  krbtgt/CORP.EXAMPLE.COM@CORP.EXAMPLE.COM
        renew until 10/05/2018 19:56:18
```

Настройка браузеров для Linux, MacOS

We are CloudLinux

Настройка браузера Chrome (Linux, macOS), Safari (macOS)

1. Убедитесь, что в системе есть необходимый каталог, выполнив команду:

```
[root@client]# mkdir -p /etc/opt/chrome/policies/managed/
```

2. Создайте новый файл `/etc/opt/chrome/policies/managed/mydomain.json` доступный на запись только для администратора системы (пользователя root), включающий следующую строку:

```
{ "AuthServerWhitelist": "*.corp.cloudlinux.com" }
```

Это можно сделать, выполнив следующую команду:

```
[root@server]# echo '{ "AuthServerWhitelist": "*.corp.cloudlinux.com" }' > /etc/opt/chrome/policies/managed/mydomain.json
```

Настройка браузера Firefox (Linux, macOS)

1. В адресной строке Firefox введите `about:config` для отображения списка параметров настройки.
2. В поле “Фильтр” введите `negotiate` для ограничения списка параметров.
3. Дважды щелкните строку `network.negotiate-auth.trusted-uris` для отображения формы ввода параметра.
4. Введите имя домена, в котором необходимо авторизоваться. Точка впереди обязательна. `.corp.cloudlinux.com`

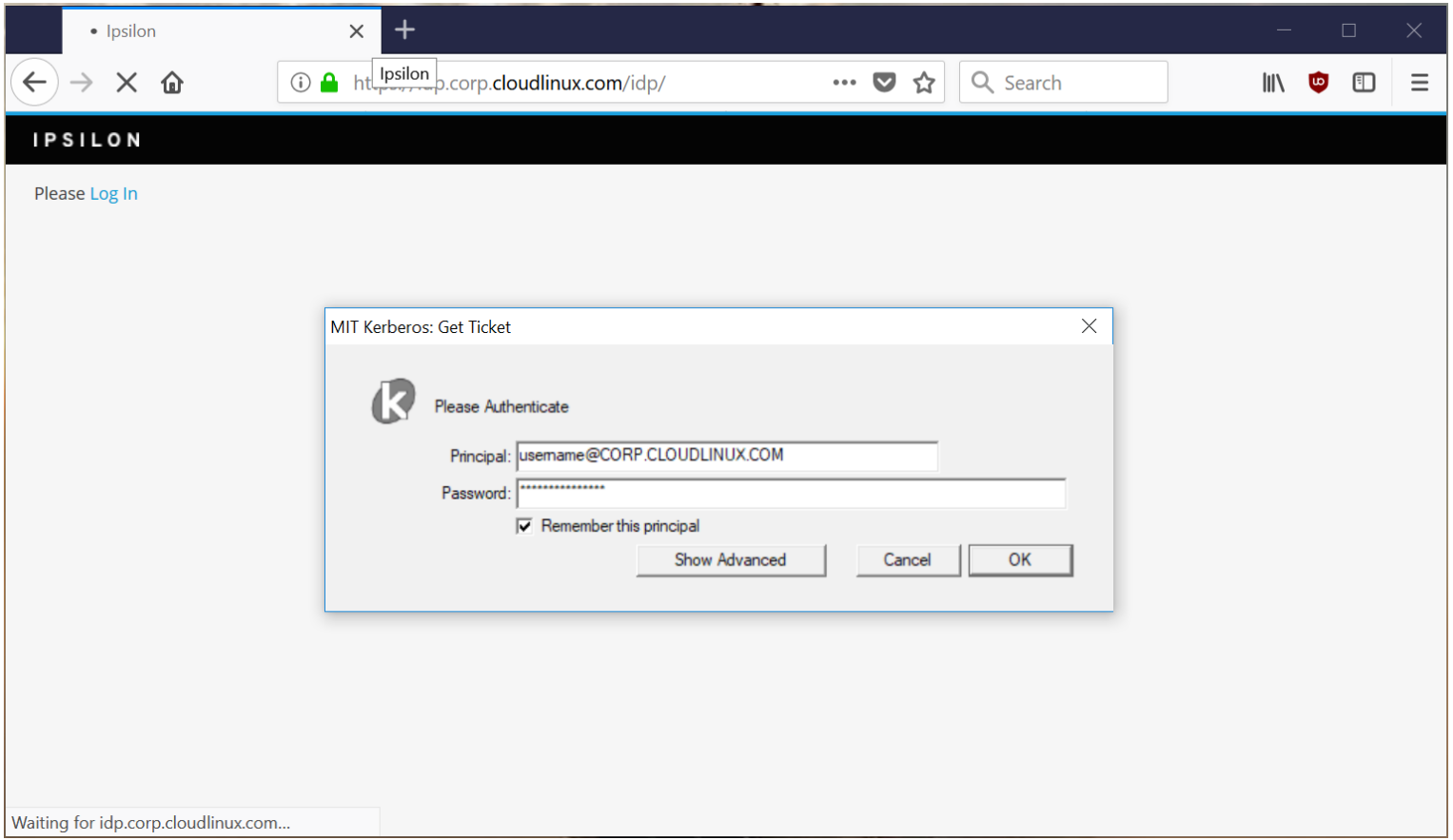
Настройка Firefox для Windows

We are CloudLinux

Настройка браузра Firefox (Windows)

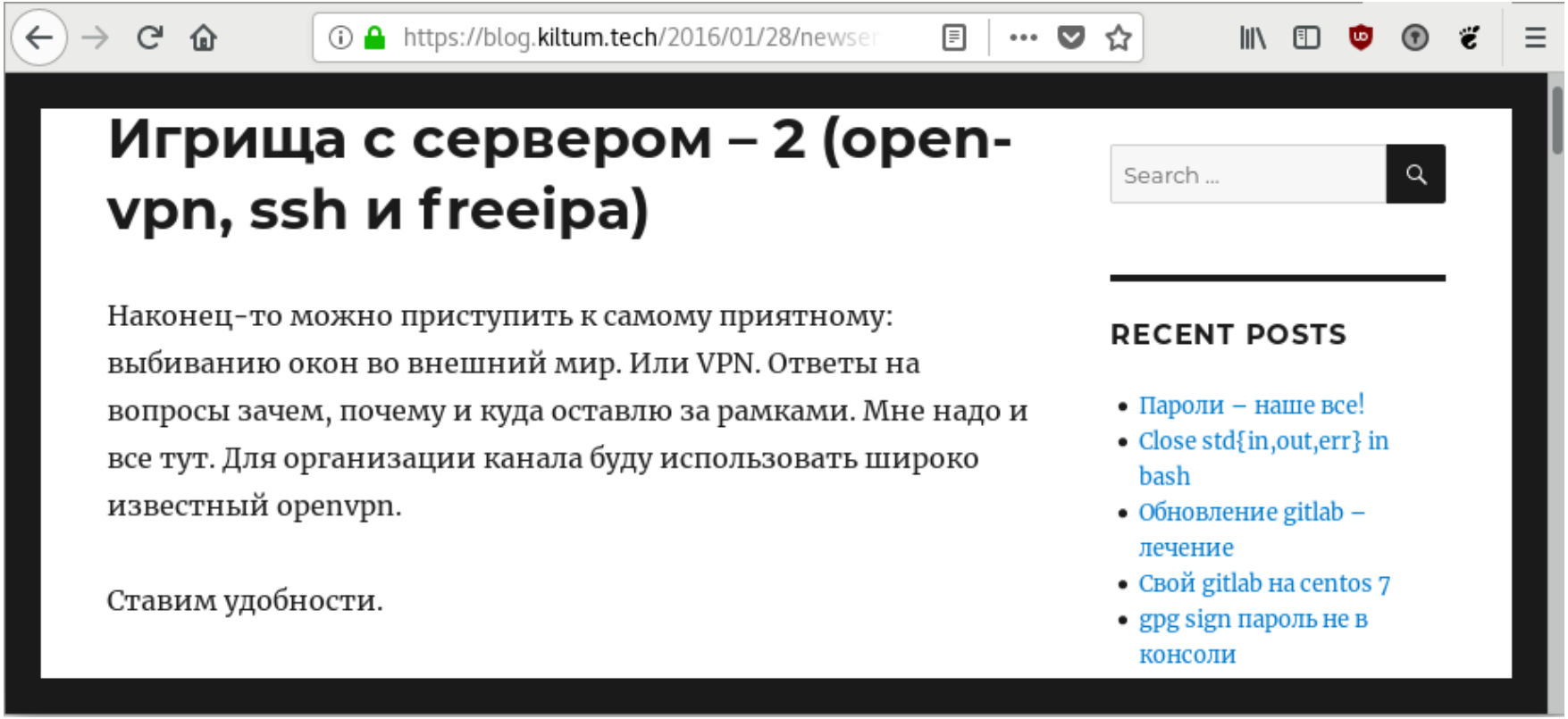
1. Скачайте и установите MIT Kerberos client for Windows 4.1 по ссылке http://web.mit.edu/kerberos/dist/index.html
2. В адресной строке Firefox введите about:config для отображения списка параметров настройки.
3. В поле “Фильтр” введите negotiate для ограничения списка параметров.
4. Дважды щелкните строку network.negotiate-auth.trusted-uris для отображения формы ввода параметра.
5. Введите имя домена, в котором необходимо авторизоваться. Точка впереди обязательна. .corp.cloudlinux.com
6. Дважды щелкните строку network.negotiate-auth.gsslib для отображения формы ввода параметра.
7. Введите значение C:\Program Files\MIT\Kerberos\bin\gssapi32.dll
8. Измените фильтр на network.auth и дважды щелкните строку network.auth.use-sspi для изменения параметра с “true” на “false”

Пример входа из Firefox for Windows



Настройка сервера OpenVPN

We are CloudLinux



Заключение

В настоящее время в нашей компании с FreeIPA интегрировано большинство внутренних и внешних сервисов и поставщиков услуг, планируется перевод с OAuth2 и локальной авторизации на SAML нескольких оставшихся.

В результате внедрения корпоративной системы управления идентификационной информацией были достигнуты следующие цели:

- Усилена информационная безопасность компании: идентификационная информация сотрудников не хранится на сторонних сайтах, установлены жесткие требования к сложности пароля, сотрудники имеют доступ только к тем ресурсам, которые им разрешены, при увольнении сотрудника достаточно заблокировать его учётную запись в одном месте.
- Благодаря системе единого входа повысилась производительность труда сотрудников
- Значительно повышена производительность труда сотрудников IT-отдела и отдела кадров