



Построение корпоративной системы управления идентификационной информацией

Леонид Кантер

likanter@cloudlinux.com

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



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](#)

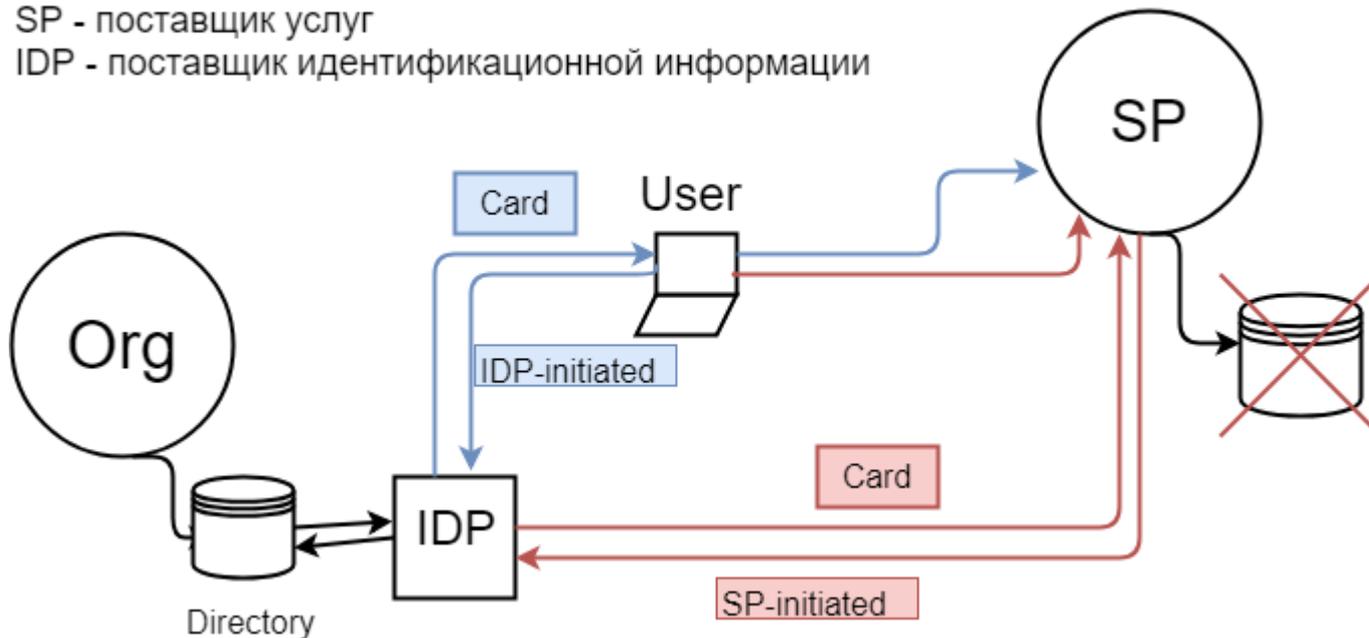
[Set up GitLab](#)

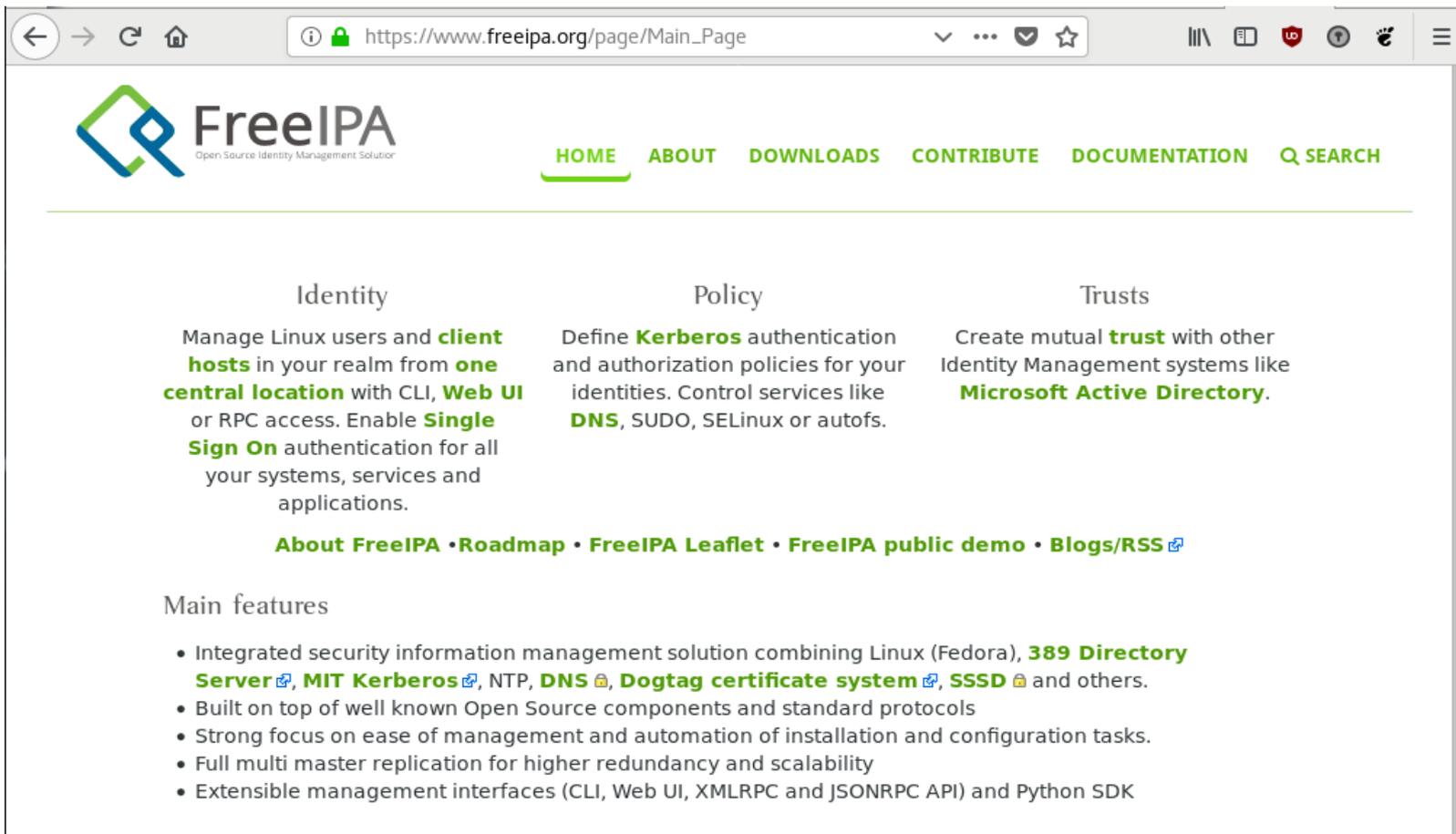
[Set up Google Apps](#)

Reference

[Configuration Reference](#)

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





The screenshot shows the main page of the FreeIPA website. At the top, there is a navigation menu with links for HOME, ABOUT, DOWNLOADS, CONTRIBUTE, DOCUMENTATION, and SEARCH. Below the navigation, the page is divided into three columns: Identity, Policy, and Trusts. Each column contains a brief description of its respective area. At the bottom, there is a section for 'Main features' with a list of key capabilities.

FreeIPA
Open Source Identity Management Solution

[HOME](#) [ABOUT](#) [DOWNLOADS](#) [CONTRIBUTE](#) [DOCUMENTATION](#) [SEARCH](#)

Identity

Manage Linux users and **client hosts** in your realm from **one central location** with CLI, **Web UI** or RPC access. Enable **Single Sign On** authentication for all your systems, services and applications.

Policy

Define **Kerberos** authentication and authorization policies for your identities. Control services like **DNS**, SUDO, SELinux or autofs.

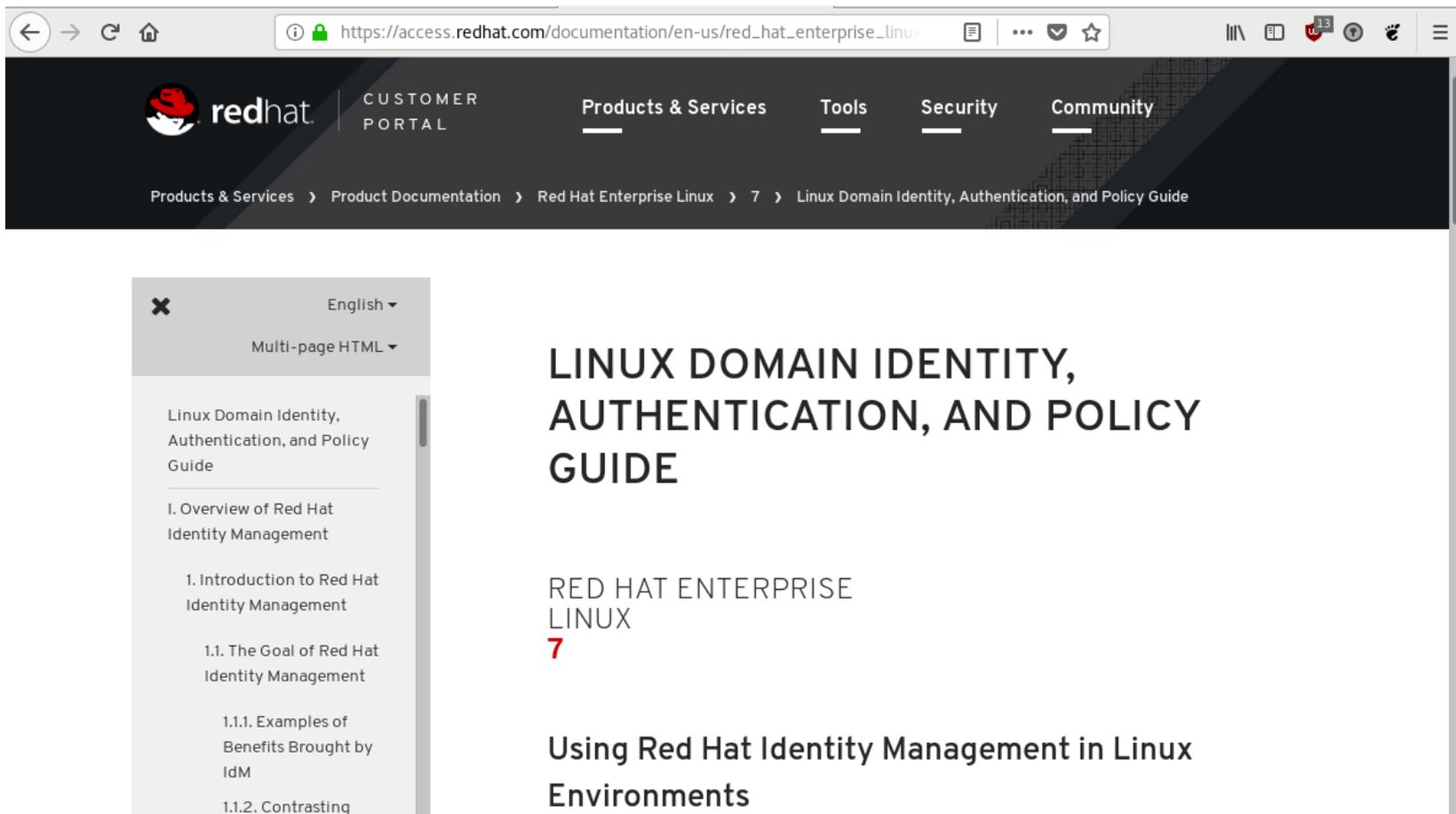
Trusts

Create mutual **trust** with other Identity Management systems like **Microsoft Active Directory**.

[About FreeIPA](#) • [Roadmap](#) • [FreeIPA Leaflet](#) • [FreeIPA public demo](#) • [Blogs/RSS](#)

Main features

- Integrated security information management solution combining Linux (Fedora), **389 Directory Server**, **MIT Kerberos**, NTP, **DNS**, **Dogtag certificate system**, **SSSD** and others.
- Built on top of well known Open Source components and standard protocols
- Strong focus on ease of management and automation of installation and configuration tasks.
- Full multi master replication for higher redundancy and scalability
- Extensible management interfaces (CLI, Web UI, XMLRPC and JSONRPC API) and Python SDK



The screenshot shows a web browser window displaying the Red Hat Customer Portal. The address bar shows the URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux. The page header includes the Red Hat logo and navigation links for 'CUSTOMER PORTAL', 'Products & Services', 'Tools', 'Security', and 'Community'. The breadcrumb trail indicates the current page is 'Linux Domain Identity, Authentication, and Policy Guide'. A left sidebar contains a table of contents with the following items:

- Linux Domain Identity, Authentication, and Policy Guide
- I. Overview of Red Hat Identity Management
 - 1. Introduction to Red Hat Identity Management
 - 1.1. The Goal of Red Hat Identity Management
 - 1.1.1. Examples of Benefits Brought by IdM
 - 1.1.2. Contrasting

The main content area features the title 'LINUX DOMAIN IDENTITY, AUTHENTICATION, AND POLICY GUIDE' in large, bold, black letters. Below the title, it reads 'RED HAT ENTERPRISE LINUX' followed by a large red number '7'. At the bottom of the main content area, the text 'Using Red Hat Identity Management in Linux Environments' is displayed in a smaller, bold, black font.

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 Sign-ON (SSO)**

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

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
```

freelPA Administrator ▾

Identity Policy Authentication Network Services IPA Server

Users User Groups Hosts Host Groups Netgroups Services Automember ▾

User categories

Active users >

Stage users

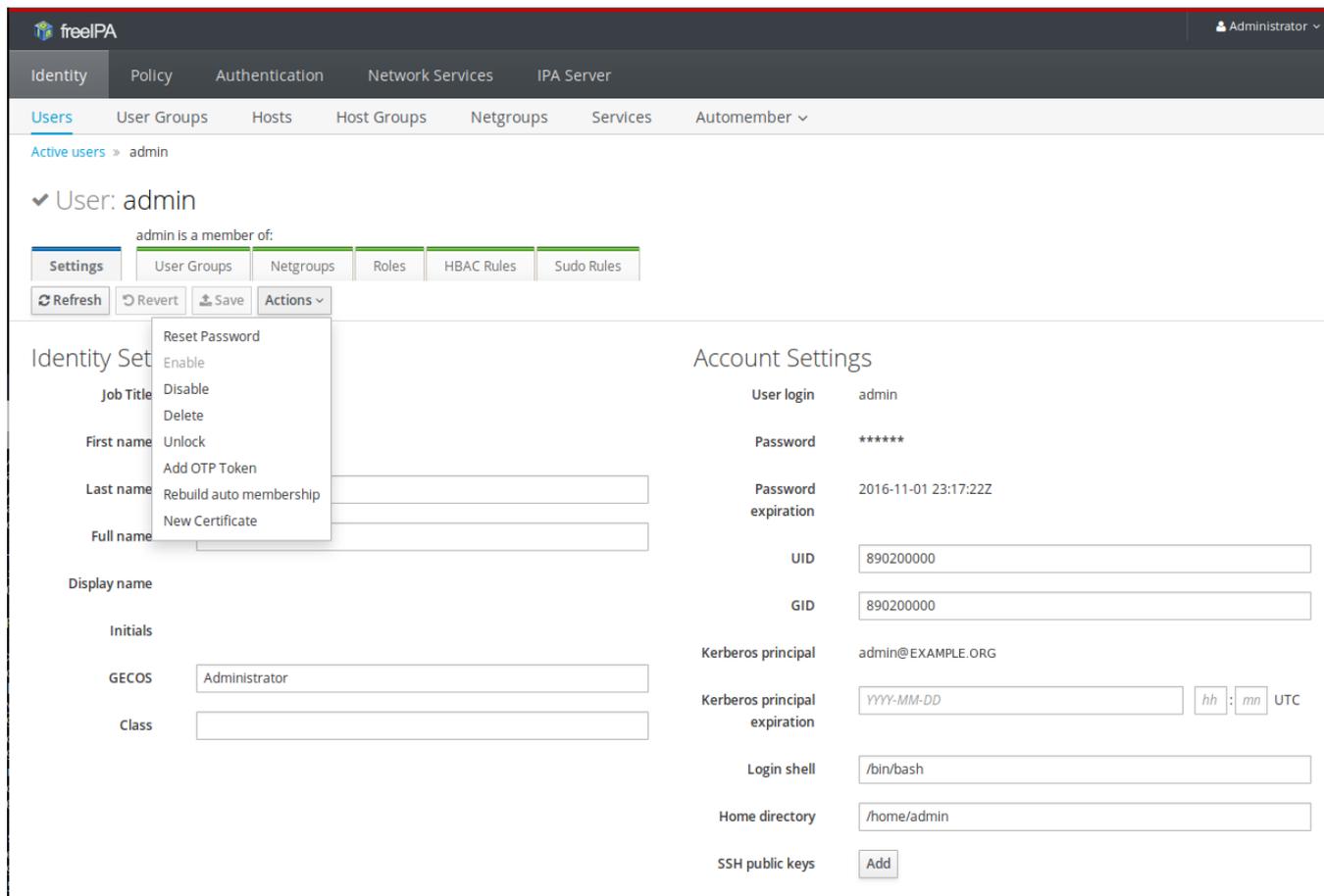
Preserved users

Active users

Search

<input type="checkbox"/>	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>	admin		Administrator	✔ Enabled	890200000			

Showing 1 to 1 of 1 entries.



The screenshot shows the freelPA web interface for managing a user. The top navigation bar includes 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. The main navigation menu has 'Users', 'User Groups', 'Hosts', 'Host Groups', 'Netgroups', 'Services', and 'Automember'. The current page is 'Active users > admin'. The user 'admin' is selected, and the 'Settings' tab is active. A dropdown menu is open over the 'Actions' button, listing options: 'Reset Password', 'Enable', 'Disable', 'Delete', 'Unlock', 'Add OTP Token', 'Rebuild auto membership', and 'New Certificate'. The 'Identity Settings' section on the left includes fields for 'Job Title', 'First name', 'Last name', 'Full name', 'Display name', 'Initials', 'GECOS' (containing 'Administrator'), and 'Class'. The 'Account Settings' section on the right includes 'User login' (admin), 'Password' (masked), 'Password expiration' (2016-11-01 23:17:22Z), 'UID' (89020000), 'GID' (89020000), 'Kerberos principal' (admin@EXAMPLE.ORG), 'Kerberos principal expiration' (YYYY-MM-DD format with hh and mn fields), 'Login shell' (/bin/bash), 'Home directory' (/home/admin), and 'SSH public keys' (Add button).

```
[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

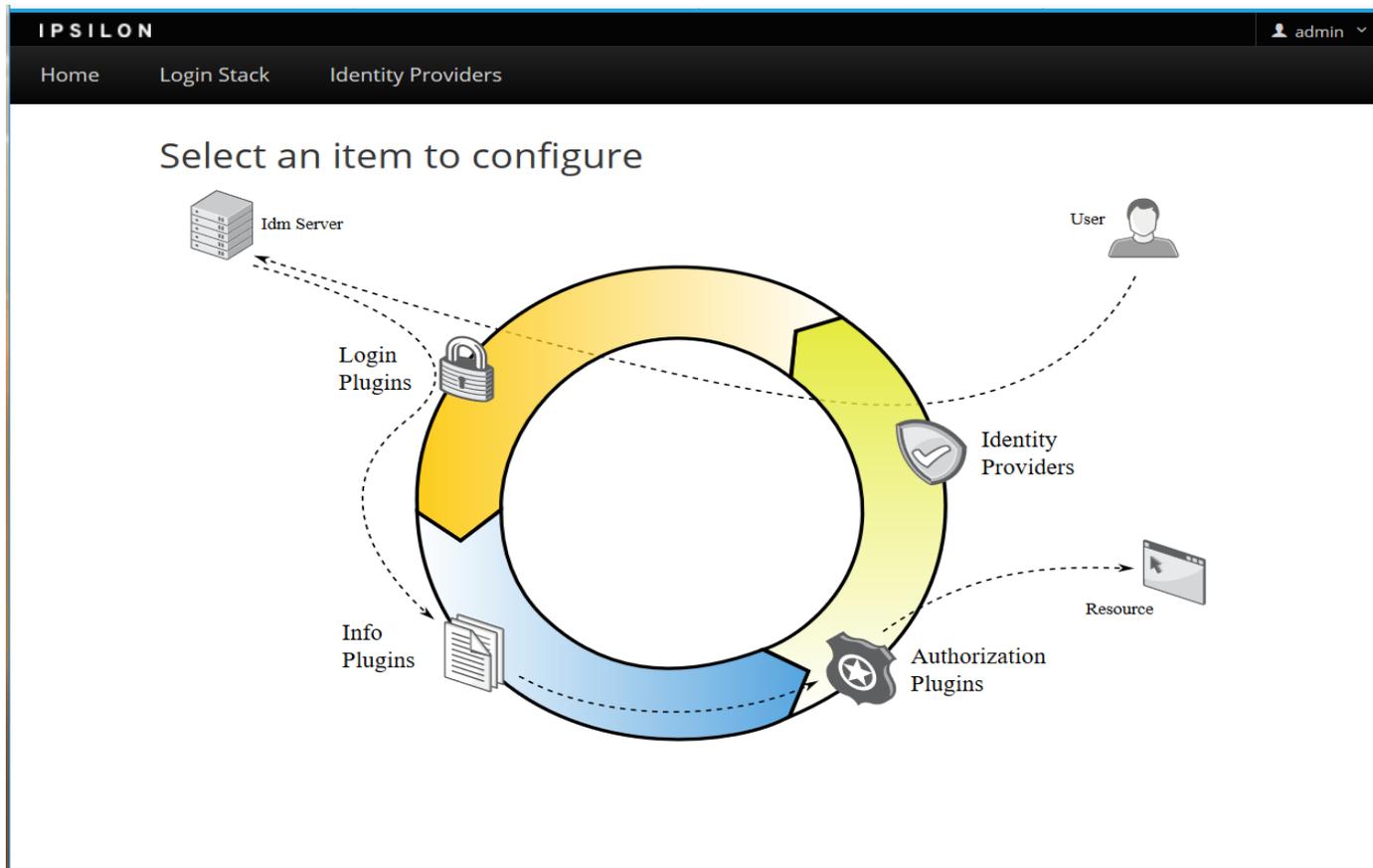
Valid starting          Expires                Service principal
09/29/2018 09:53:40    09/30/2018 09:53:30  krbtgt/CORP.EXAMPLE.COM@CORP.EXAMPLE.COM

[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
```

```
# 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
```

```
[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
```



The screenshot displays the Ipsilon administrative console interface. At the top, the header includes the text "IPSILO N" on the left and a user profile "admin" on the right. Below the header is a navigation menu with three items: "Home", "Login Stack", and "Identity Providers". The main content area features the heading "Select an item to configure" and a central circular diagram. This diagram is divided into four colored segments: a yellow segment for "Login Plugins" (with a padlock icon), a light green segment for "Identity Providers" (with a shield icon), a blue segment for "Authorization Plugins" (with a star icon), and a light blue segment for "Info Plugins" (with a document icon). Dashed arrows connect these segments to external components: "Login Plugins" to an "Idm Server" (server rack icon), "Identity Providers" to a "User" (person icon), "Authorization Plugins" to a "Resource" (document icon), and "Info Plugins" to a document icon.

Добавление поставщика услуг G Suite

New Service Provider

Name:

Description:

Visible in IdP Portal:

Portal image:
 No file selected.

Link to Service Provider:

Metadata file:
 No file selected.

- OR -
Metadata url:

- OR -
Metadata text:

```
<EntityDescriptor entityID="google.com/a/example.com" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified/>NameIDFormat
    <AssertionConsumerService index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://www.google.com/a/example.com/acs" />
    </SPSSODescriptor>
  </EntityDescriptor>
```

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. [?](#)

Sign-in page URL

URL for signing in to your system and G Suite

Sign-out page URL

URL for redirecting users to when they sign out

Change password URL

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

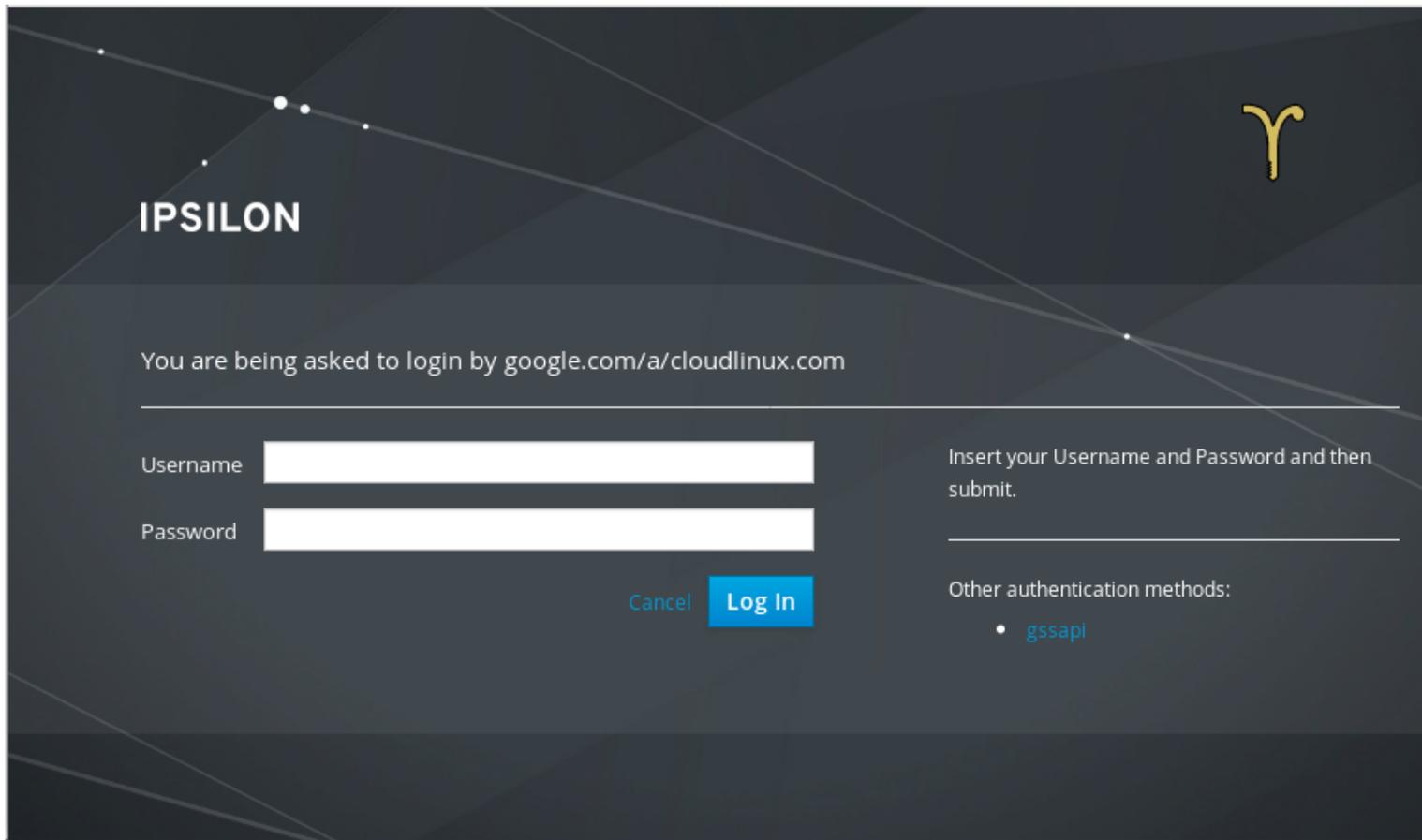
Verification certificate A certificate file has been uploaded. [Replace certificate](#)

The certificate file must contain the public key for Google to verify sign-in requests. [?](#)

Use a domain specific issuer [?](#)

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. [?](#)



The image shows a login page for Ipsilon. The background is dark with a geometric pattern of lines and dots. The word "IPSILO" is written in large white letters on the left. In the top right corner, there is a yellow Greek letter gamma symbol. Below the title, a message states "You are being asked to login by google.com/a/cloudlinux.com". There are two input fields: "Username" and "Password". To the right of these fields, there is a text prompt: "Insert your Username and Password and then submit." Below the input fields, there are two buttons: "Cancel" and "Log In". At the bottom right, there is a section for "Other authentication methods:" with a single bullet point: "gssapi".

IPSILO

You are being asked to login by google.com/a/cloudlinux.com

Username

Password

Cancel

Insert your Username and Password and then submit.

Other authentication methods:

- gssapi

Доступ на любой сайт под управлением веб-сервера Apache можно ограничить при помощи пакета `ippsilon-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 файлов, 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`.

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 Rhodocode to authenticate users against FreeIPA**
- **Setting up The Bug Genie to authenticate users against FreeIPA**

Kerberos /кэəрбəрэс/ — 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)

```
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).
```

```
[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 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.

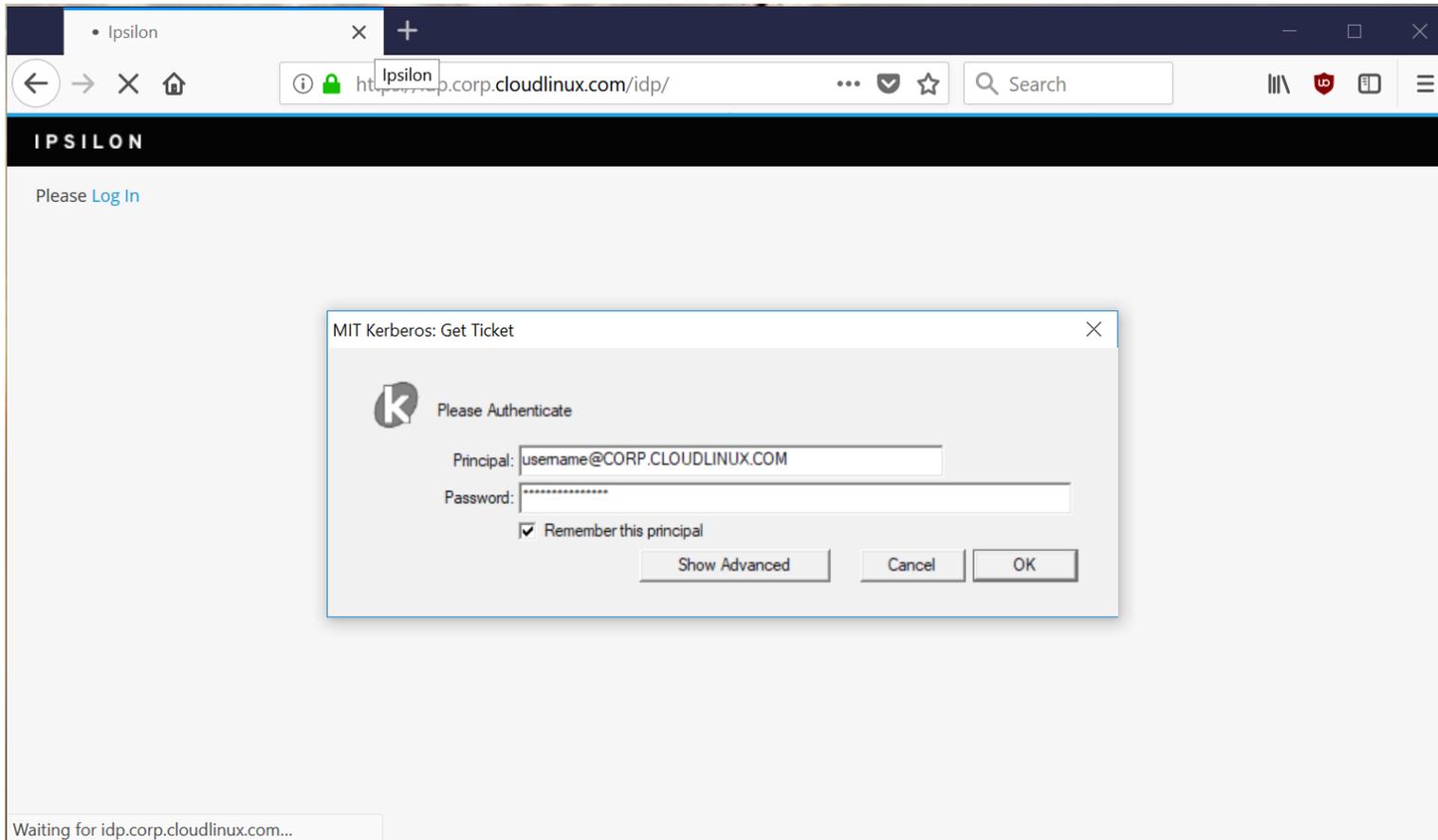
2. В поле "Фильтр" введите `negotiate` для ограничения списка параметров.

3. Дважды щелкните строку `network.negotiate-auth.trusted-uris` для отображения формы ввода параметра.

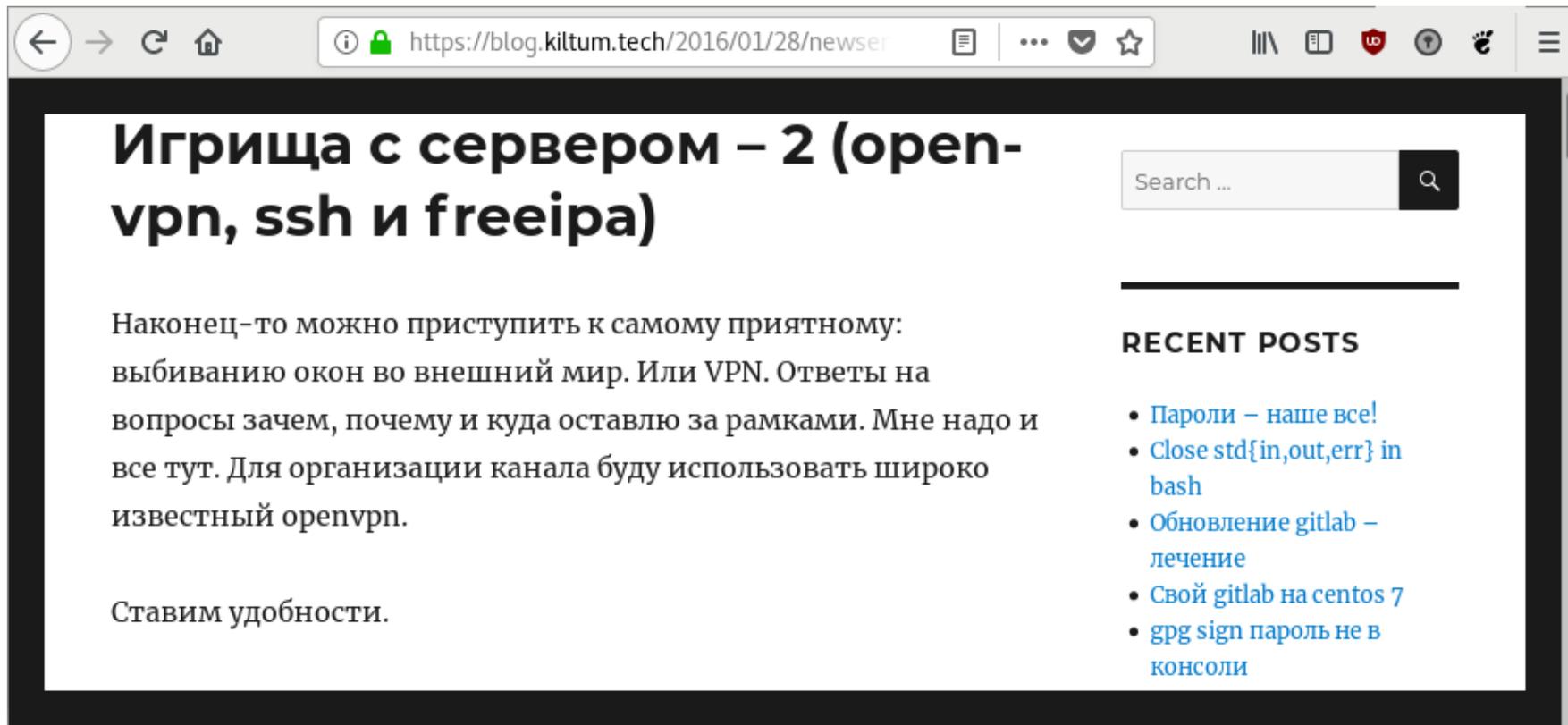
4. Введите имя домена, в котором необходимо авторизоваться. Точка впереди обязательна. `.corp.cloudlinux.com`

Настройка браузера 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"



The screenshot shows a Firefox browser window with a single tab titled "Ipsilon". The address bar displays the URL `https://idp.corp.cloudlinux.com/idp/`. The page content includes the "Ipsilon" logo and the text "Please Log In" with a blue link. A modal dialog box titled "MIT Kerberos: Get Ticket" is open, featuring a "k" icon and the text "Please Authenticate". The dialog contains two input fields: "Principal" with the value `username@CORP.CLOUDLINUX.COM` and "Password" with masked characters. A checked checkbox labeled "Remember this principal" is present. At the bottom of the dialog are three buttons: "Show Advanced", "Cancel", and "OK". A status bar at the bottom left of the browser window shows the text "Waiting for idp.corp.cloudlinux.com..."



The screenshot shows a web browser window with the address bar displaying `https://blog.kiltum.tech/2016/01/28/newser`. The main content area features a large heading and a paragraph of text. On the right side, there is a search bar and a list of recent posts.

Игрища с сервером – 2 (openvpn, ssh и freeipa)

Наконец-то можно приступить к самому приятному: выбиванию окон во внешний мир. Или VPN. Ответы на вопросы зачем, почему и куда оставляю за рамками. Мне надо и все тут. Для организации канала буду использовать широко известный openvpn.

Ставим удобства.

RECENT POSTS

- [Пароли – наше все!](#)
- [Close std{in,out,err} in bash](#)
- [Обновление gitlab – лечение](#)
- [Свой gitlab на centos 7](#)
- [gpg sign пароль не в консоли](#)

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