ГРУППОВЫЕ ПОЛИТИКИ В FREEIPA

Данила Скачедубов, Базальт СПО

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

В доменной инфраструктуре важно централизованно управлять настройками рабочих станций и пользователей. В Windows это делают **Active Directory** и групповые политики, в Linux — **Samba AD**. **FreeIPA** является свободной альтернативой AD, но без встроенного механизма политик, поэтому администраторам приходится полагаться на скрипты и ручную настройку.

АРХИТЕКТУРА РЕШЕНИЯ

Расширение схемы LDAP

Хранение объектов групповых политик и их атрибутов

WEB, CLI интерфейсы

Полный цикл управления групповыми политикам

Gpupdate, WEB GPUI

gpupdate для применения и gpui для редактирования политик

АРХИТЕКТУРА РЕШЕНИЯ

Расширение схемы LDAP

Хранения объектов групповых политик и их атрибутов.

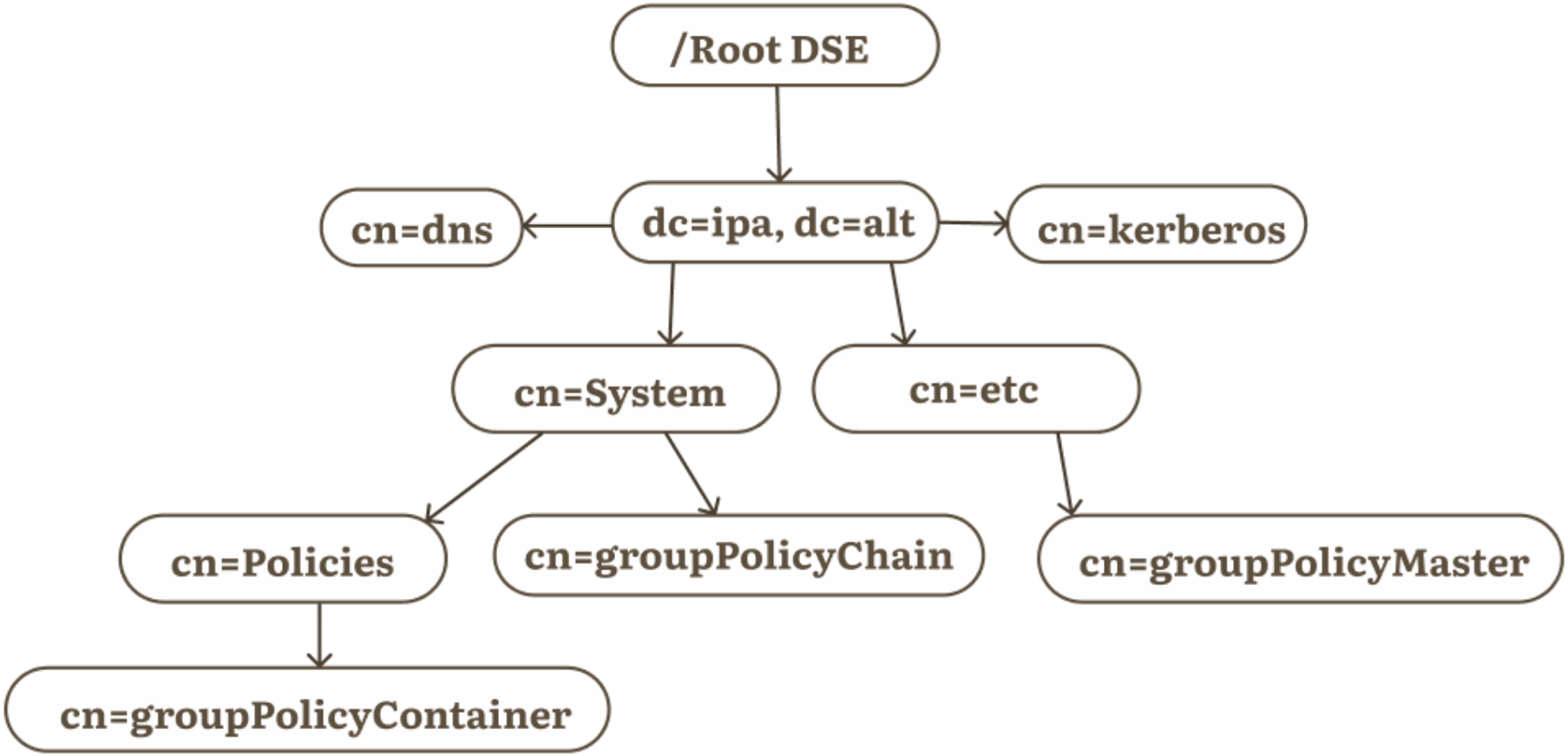
WEB, CLI интерфейсы

Полный цикл управления групповыми политикам

Gpupdate, WEB GPUI

gpupdate для применения и gpui для редактирования политик

Схема LDAP


/Root DSE
cn=dns
dc=ipa, dc=alt
cn=kerberos
cn=System
cn=etc
cn=Policies
cn=groupPolicyChain
cn=groupPolicyMaster
cn=groupPolicyContainer

АРХИТЕКТУРА РЕШЕНИЯ

Расширение схемы LDAP

Хранения объектов групповых политик и их атрибутов.

WEB, CLI интерфейсы

Полный цикл управления групповыми политикам

Gpupdate, WEB GPUI

gpupdate для применения и gpui для редактирования политик

ПРОЦЕСС РАЗВЕРТЫВАНИЯ СИСТЕМЫ

Инструмент **ipa-gpo-install** выполняет комплексное развёртывание инфраструктуры групповых политик.

01

Проверка прав доступа проверяет наличие Kerberos-тикета и административных привилегий у пользователя

02

Проверка сервисов IPA
Проверяет, что все необходимые сервисы FreeIPA запущены

03

Проверка схемы LDAP
проверяет наличие требуемых объектных классов перед расширением

04

Настройка SYSVOL
Создание структуры каталогов и настройка Samba-ресурса с Kerberos-аутентификацией

05

Активация плагина
Запуск ipa-server-upgrade для применения расширений схемы LDAP и активации плагина GPO.

CLI ИНТЕРФЕЙС

01

 # ipa gpmaster

Topic commands:
gpmaster-mod Modify Group Policy Master.
gpmaster-show Display information about Group Policy Master.

02

 # ipa chain

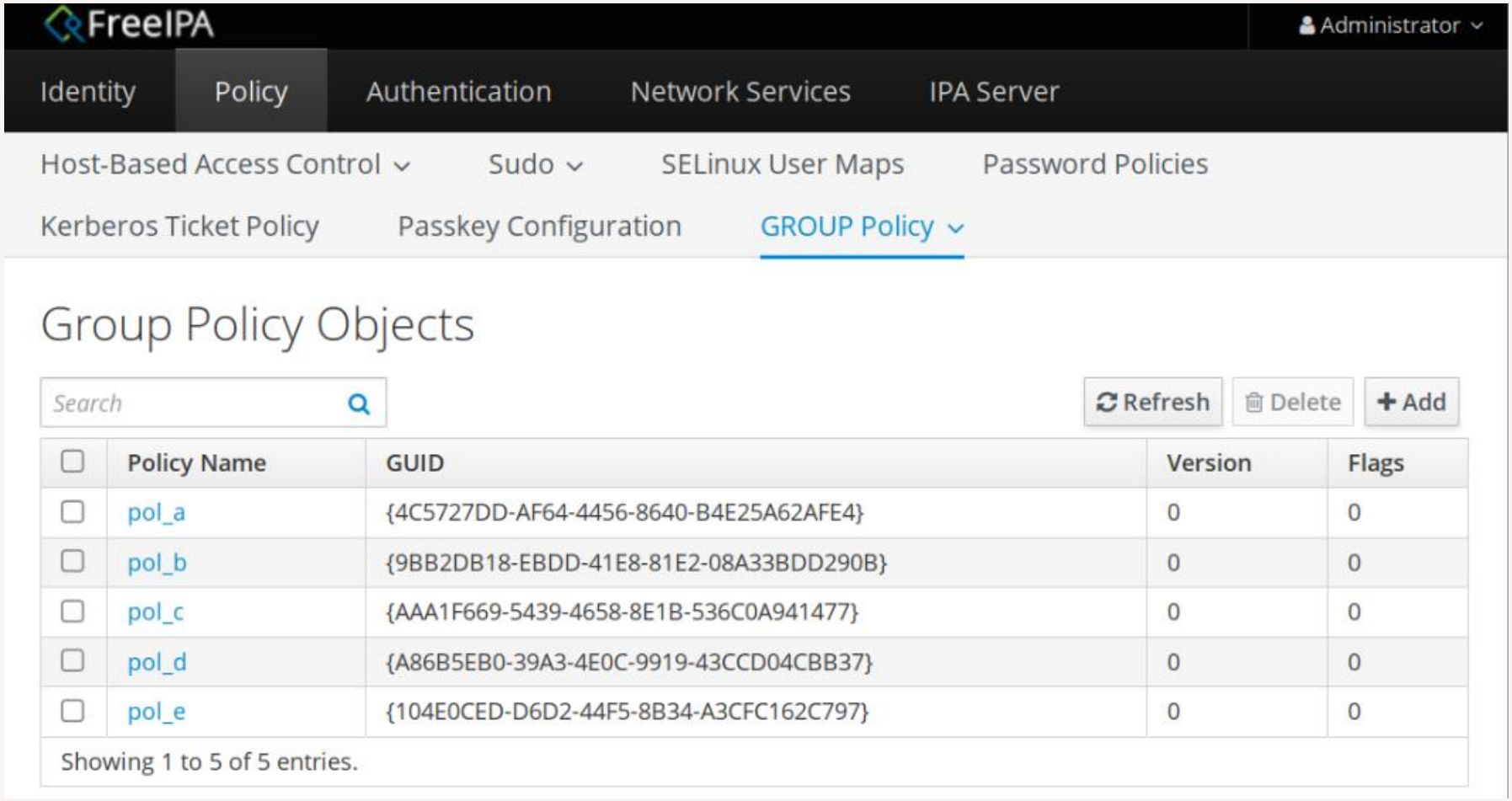
Topic commands:
chain-add Create a new Group Policy Chain.
chain-add-gpo Add Group Policy Objects to a chain.
chain-del Delete a Group Policy Chain.
chain-disable Disable a Group Policy Chain.
chain-enable Enable a Group Policy Chain.
chain-find Search for Group Policy Chains.
chain-mod Modify a Group Policy Chain.
chain-remove-gpo Remove Group Policy Objects from a chain.
chain-resolve-for-host Get applicable policies for host with essential attributes.
chain-resolve-for-user Get applicable policies for user with essential attributes.
chain-show Display information about a Group Policy Chain.

03

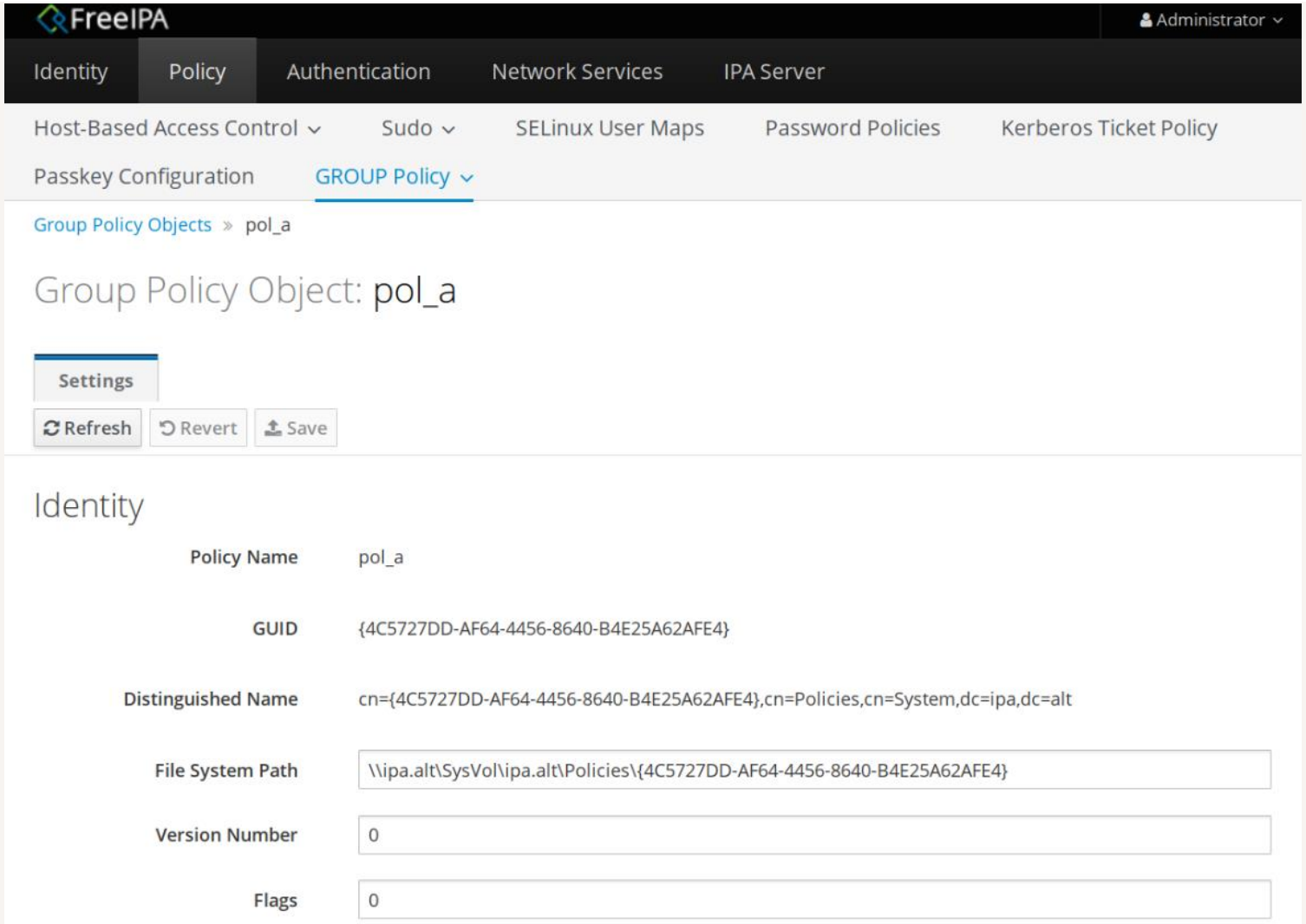
 # ipa gpo

Topic commands:
gpo-add Create a new Group Policy Object.
gpo-del Delete a Group Policy Object.
gpo-find Search for Group Policy Objects.
gpo-mod Modify a Group Policy Object.
gpo-show Display information about a Group Policy Object.

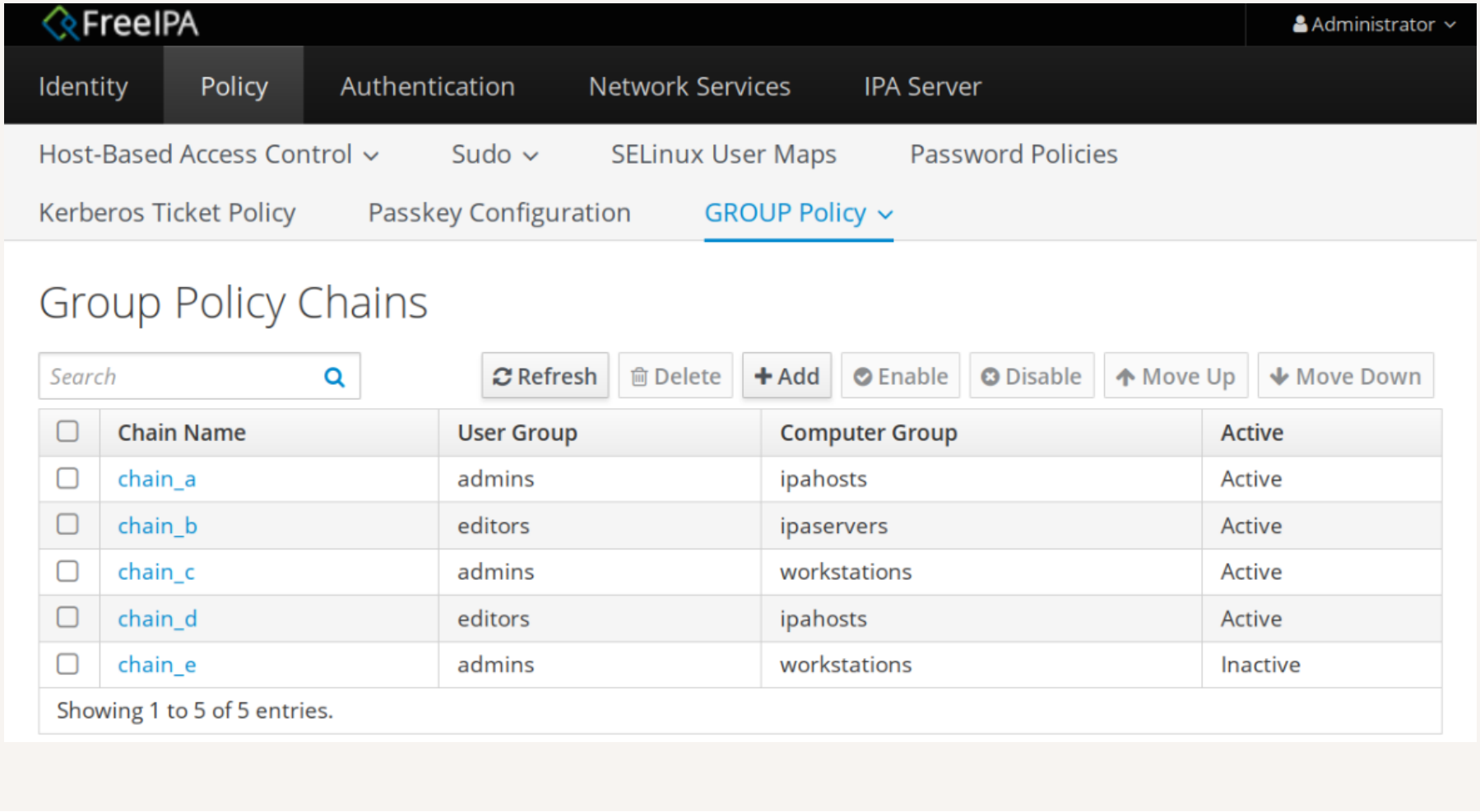
WEB ИНТЕРФЕЙС



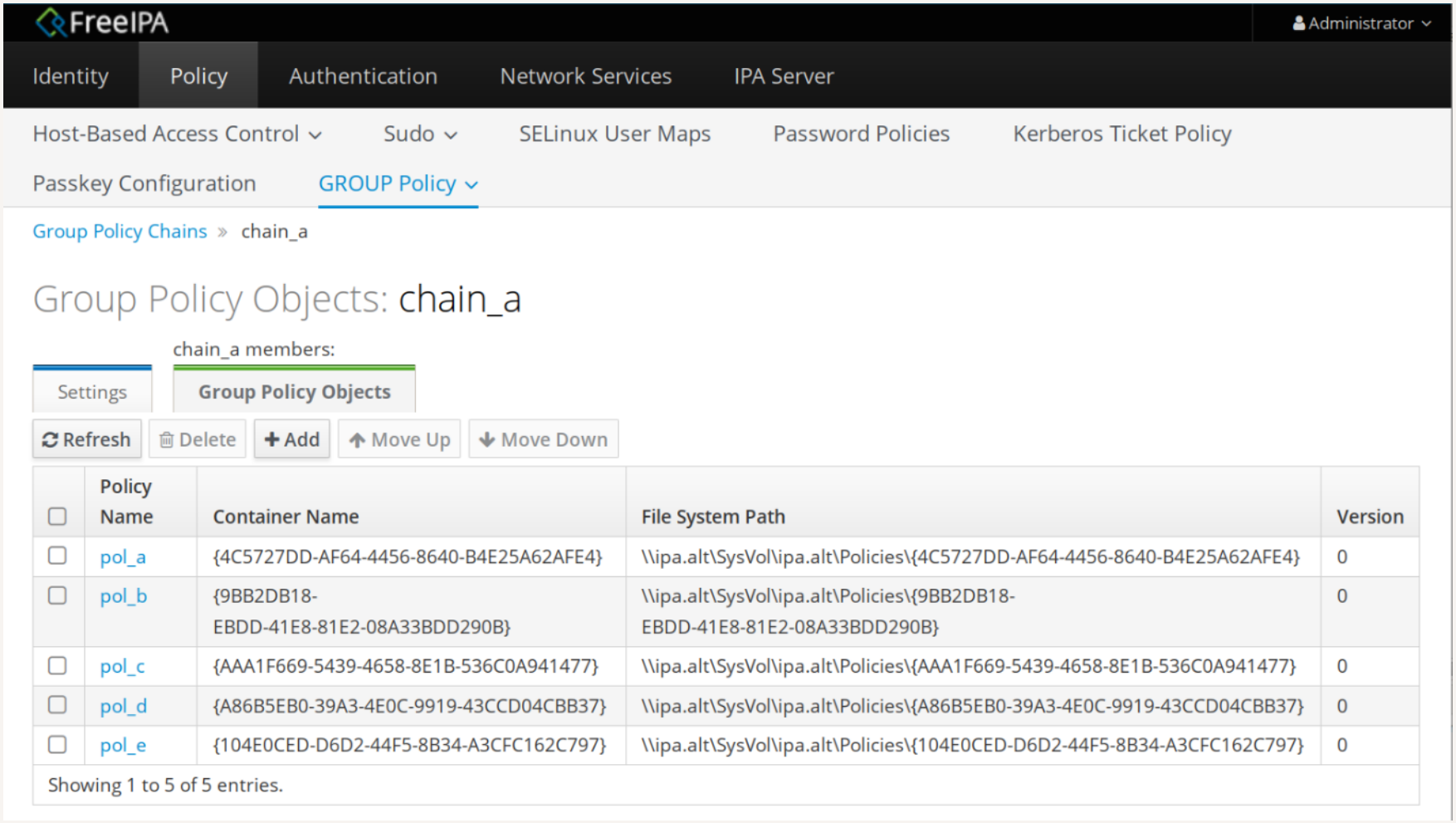
WEB ИНТЕРФЕЙС



WEB ИНТЕРФЕЙС



WEB ИНТЕРФЕЙС



АРХИТЕКТУРА РЕШЕНИЯ

Расширение схемы LDAP

Хранения объектов групповых политик и их атрибутов.

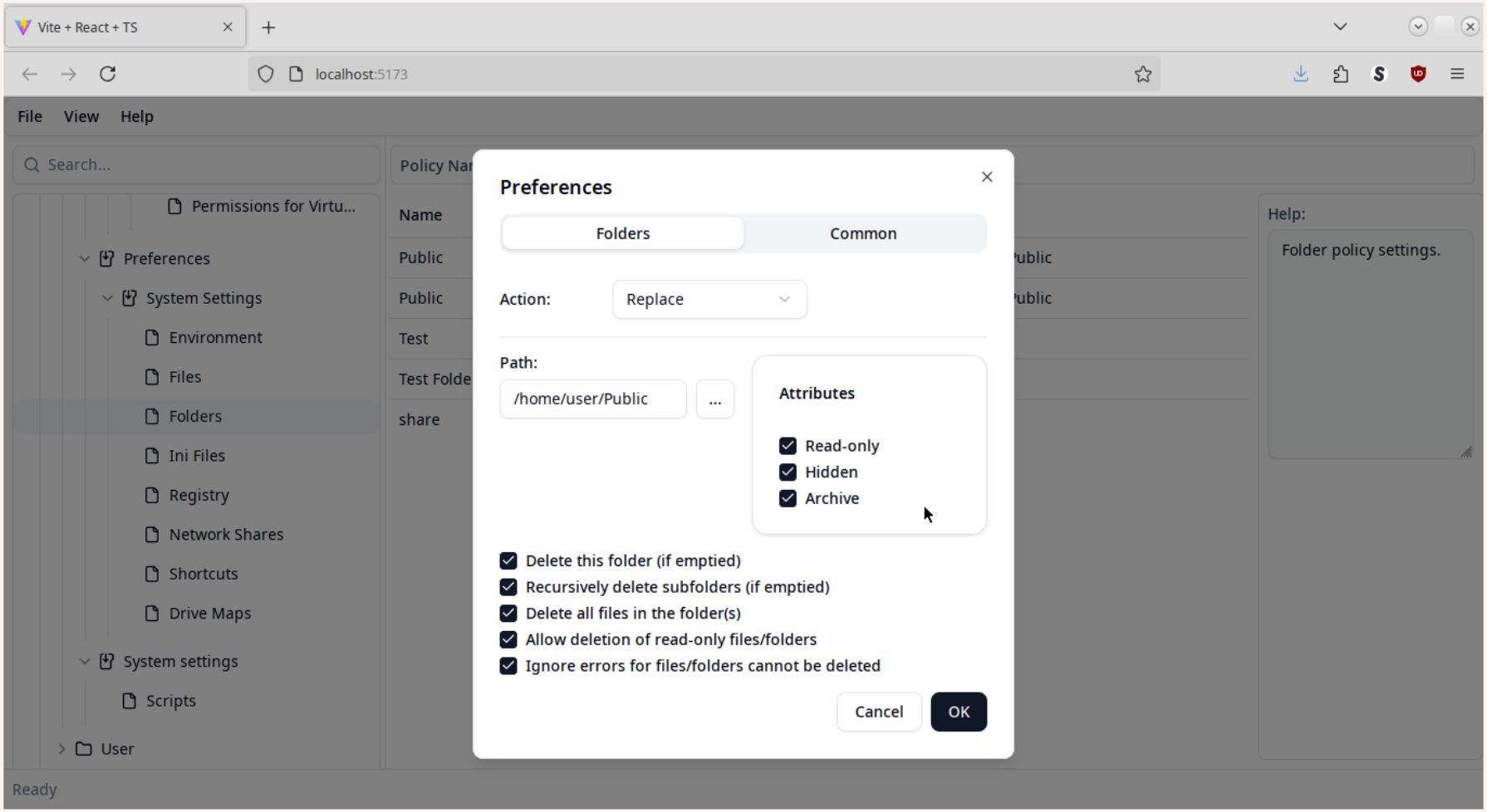
WEB, CLI интерфейсы

Полный цикл управления групповыми политикам

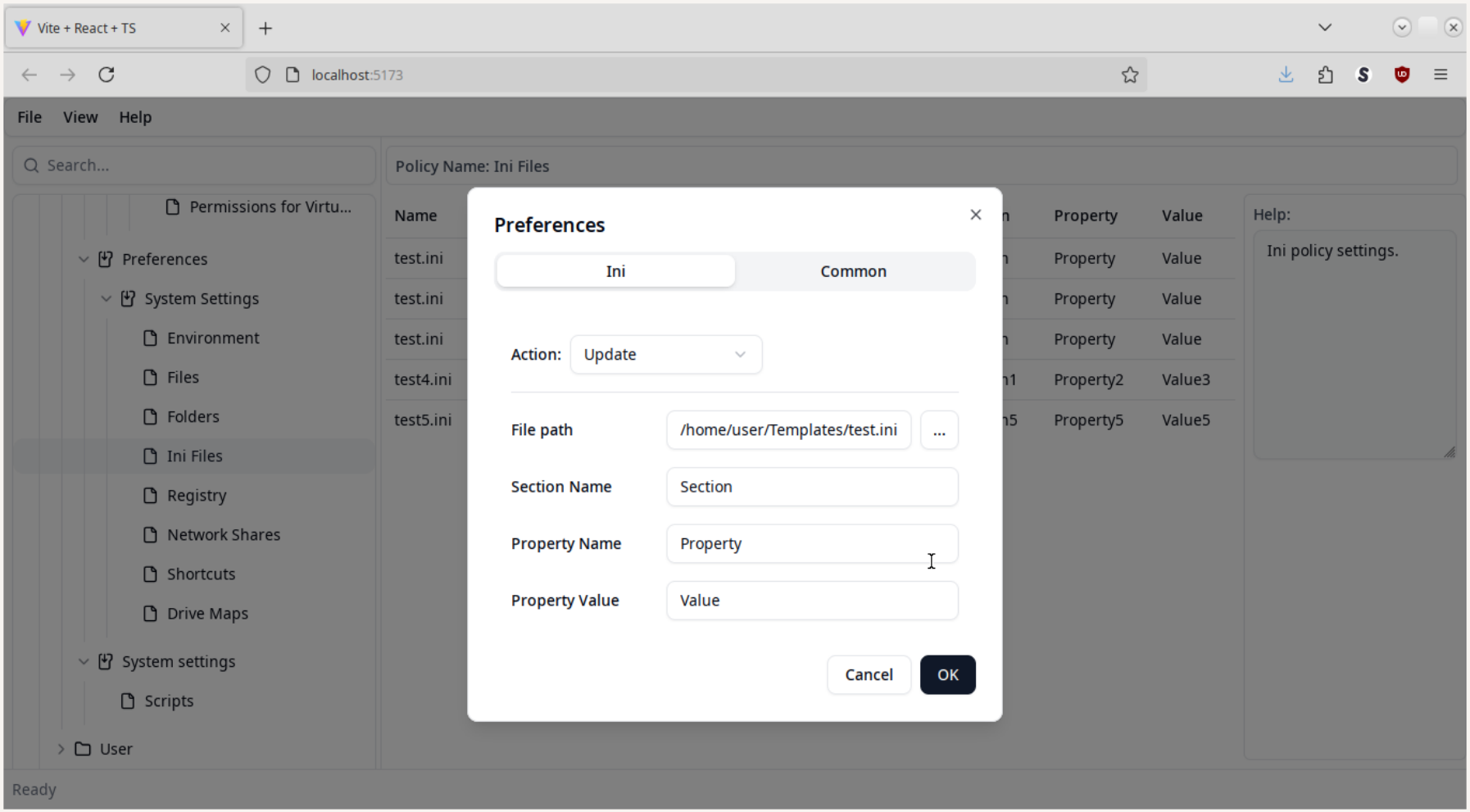
Gpupdate, WEB GPUI

gpupdate для применения и gpui для редактирования политик

WEB GPUI


Vite + React + TS
localhost:5173
File
View
Help
Search...
Permissions for Virtu...
Preferences
System Settings
Environment
Files
Folders
Ini Files
Registry
Network Shares
Shortcuts
Drive Maps
System settings
Scripts
User
Policy Na
Name
Public
Public
Test
Test Folde
share
Preferences
Folders
Common
Action:
Replace
Path:
/home/user/Public
...
Attributes
Read-only
Hidden
Archive
Delete this folder (if emptied)
Recursively delete subfolders (if emptied)
Delete all files in the folder(s)
Allow deletion of read-only files/folders
Ignore errors for files/folders cannot be deleted
Cancel
OK
Help:
Folder policy settings.
Ready

WEB GPUI


Vite + React + TS
localhost:5173
File
View
Help
Search...
Permissions for Virtu...
Preferences
System Settings
Environment
Files
Folders
Ini Files
Registry
Network Shares
Shortcuts
Drive Maps
System settings
Scripts
User
Policy Name: Ini Files
Name
Property
Value
test.ini
Property
Value
test.ini
Property
Value
test.ini
Property
Value
test4.ini
Property2
Value3
test5.ini
Property5
Value5
Help:
Ini policy settings.
Preferences
Ini
Common
Action:
Update
File path
/home/user/Templates/test.ini
...
Section Name
Section
Property Name
Property
Property Value
Value
Cancel
OK
Ready

pc.ipa.alt

gpupdate

gpresult

Group Policy Administrators

WEB, CLI

dc.ipa.alt

freeipa-server-gpo

ipa-gpo-install

Sysvol

Пользователь:
- John

Группы:
- developers
- office-user

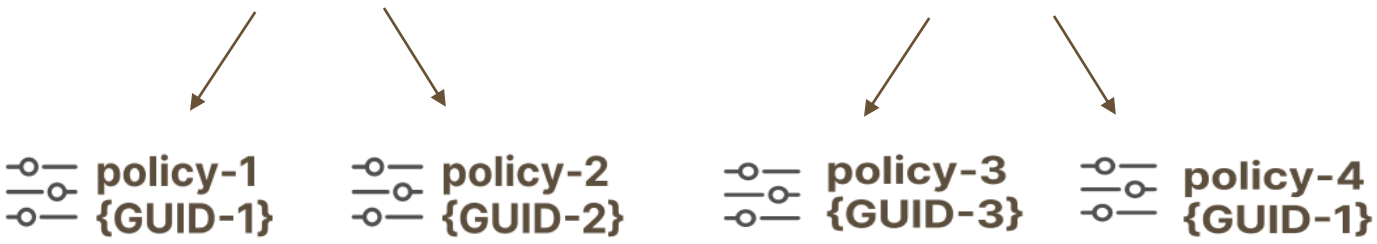
Компьютер:
- ws001

Группы:
- dev-workstations
- office-computers

Group Policy Master:
chainList
- dev-chain
- office-chain

dev-chain:
- **userGroup:** developers
- **computerGroup:** dev-workstation
- **gpLink:**
  - policy-1
  - policy-2

office-chain:
- **userGroup:** office-user
- **computerGroup:** office-computers
- **gpLink:**
  - policy-3
  - policy-4



ТЕКУЩЕЕ СОСТОЯНИЕ И ПЛАНЫ РАЗВИТИЯ

Тестирование
Ведется тестирование полного цикла работы механизма групповых политик.

1

Документация
Подготовка англоязычной документации (руководства по установке, настройке и использованию).

2

Представление сообществу
Планируется представление решения в международное сообщество FreeIPA.

3

ЗАКЛЮЧЕНИЕ

https://github.com/danila-Skachedubov/freeipa-server-gpo

Mail: skachedubovda@basealt.ru

Tg: @danila_skachedubov