

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 политиками



Gupdate, WEB GUI

gupdate для применения и
grui для редактирования
политик

АРХИТЕКТУРА РЕШЕНИЯ



Расширение схемы LDAP

Хранения объектов групповых политик и их атрибутов.



WEB, CLI интерфейсы

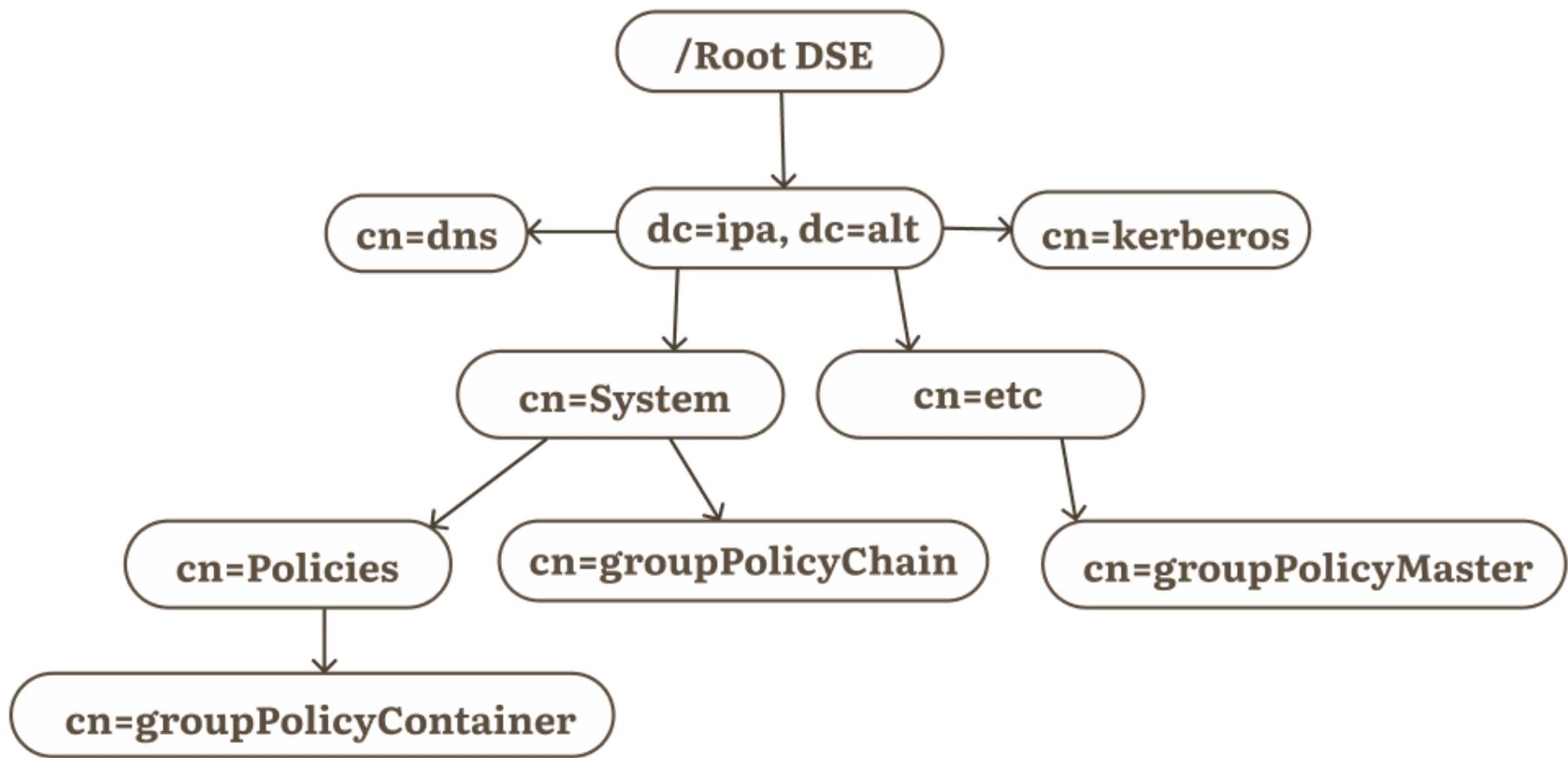
Полный цикл управления групповыми политиками



Gupdate, WEB GUI

gupdate для применения и
grui для редактирования политик

CXEMA LDAP



АРХИТЕКТУРА РЕШЕНИЯ



Расширение схемы LDAP

Хранения объектов групповых политик и их атрибутов.



WEB, CLI интерфейсы

Полный цикл управления групповыми политиками



Gupdate, WEB GUI

gupdate для применения и
grui 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

FreeIPA

Administrator

Identity Policy Authentication Network Services IPA Server

Host-Based Access Control ▾ Sudo ▾ SELinux User Maps Password Policies

Kerberos Ticket Policy Passkey Configuration GROUP Policy ▾

Group Policy Objects

Search		Refresh	Delete	Add
<input type="checkbox"/>	Policy Name	GUID	Version	Flags
<input type="checkbox"/>	pol_a	{4C5727DD-AF64-4456-8640-B4E25A62AFE4}	0	0
<input type="checkbox"/>	pol_b	{9BB2DB18-EBDD-41E8-81E2-08A33BDD290B}	0	0
<input type="checkbox"/>	pol_c	{AAA1F669-5439-4658-8E1B-536C0A941477}	0	0
<input type="checkbox"/>	pol_d	{A86B5EB0-39A3-4E0C-9919-43CCD04CBB37}	0	0
<input type="checkbox"/>	pol_e	{104E0CED-D6D2-44F5-8B34-A3CFC162C797}	0	0

Showing 1 to 5 of 5 entries.

WEB ИНТЕРФЕЙС

FreeIPA

Administrator

Identity Policy Authentication Network Services IPA Server

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

Passkey Configuration GROUP Policy ▾

Group Policy Objects » pol_a

Group Policy Object: pol_a

Settings

Refresh Revert Save

Identity

Policy Name pol_a

GUID {4C5727DD-AF64-4456-8640-B4E25A62AFE4}

Distinguished Name cn={4C5727DD-AF64-4456-8640-B4E25A62AFE4},cn=Policies,cn=System,dc=ipa,dc=alt

File System Path \\ipa.alt\SysVol\ipa.alt\Policies\{4C5727DD-AF64-4456-8640-B4E25A62AFE4}

Version Number 0

Flags 0

WEB ИНТЕРФЕЙС

FreeIPA

Administrator

Identity Policy Authentication Network Services IPA Server

Host-Based Access Control ▾ Sudo ▾ SELinux User Maps Password Policies

Kerberos Ticket Policy Passkey Configuration GROUP Policy ▾

Group Policy Chains

Search		Refresh	Delete	Add	Enable	Disable	Move Up	Move Down
<input type="checkbox"/>	Chain Name	User Group	Computer Group	Active				
<input type="checkbox"/>	chain_a	admins	ipahosts	Active				
<input type="checkbox"/>	chain_b	editors	ipaservers	Active				
<input type="checkbox"/>	chain_c	admins	workstations	Active				
<input type="checkbox"/>	chain_d	editors	ipahosts	Active				
<input type="checkbox"/>	chain_e	admins	workstations	Inactive				

Showing 1 to 5 of 5 entries.

WEB ИНТЕРФЕЙС

FreeIPA

Administrator

Identity Policy Authentication Network Services IPA Server

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

Passkey Configuration GROUP Policy ▾

Group Policy Chains » chain_a

Group Policy Objects: chain_a

chain_a members:

	Policy Name	Container Name	File System Path	Version
<input type="checkbox"/>	pol_a	{4C5727DD-AF64-4456-8640-B4E25A62AFE4}	\ipa.alt\SysVol\ipa.alt\Policies\{4C5727DD-AF64-4456-8640-B4E25A62AFE4}	0
<input type="checkbox"/>	pol_b	{9BB2DB18-EBDD-41E8-81E2-08A33BDD290B}	\ipa.alt\SysVol\ipa.alt\Policies\{9BB2DB18-EBDD-41E8-81E2-08A33BDD290B}	0
<input type="checkbox"/>	pol_c	{AAA1F669-5439-4658-8E1B-536C0A941477}	\ipa.alt\SysVol\ipa.alt\Policies\{AAA1F669-5439-4658-8E1B-536C0A941477}	0
<input type="checkbox"/>	pol_d	{A86B5EB0-39A3-4E0C-9919-43CCD04CBB37}	\ipa.alt\SysVol\ipa.alt\Policies\{A86B5EB0-39A3-4E0C-9919-43CCD04CBB37}	0
<input type="checkbox"/>	pol_e	{104E0CED-D6D2-44F5-8B34-A3CFC162C797}	\ipa.alt\SysVol\ipa.alt\Policies\{104E0CED-D6D2-44F5-8B34-A3CFC162C797}	0

Showing 1 to 5 of 5 entries.

АРХИТЕКТУРА РЕШЕНИЯ



Расширение схемы LDAP

Хранения объектов групповых политик и их атрибутов.



WEB, CLI интерфейсы

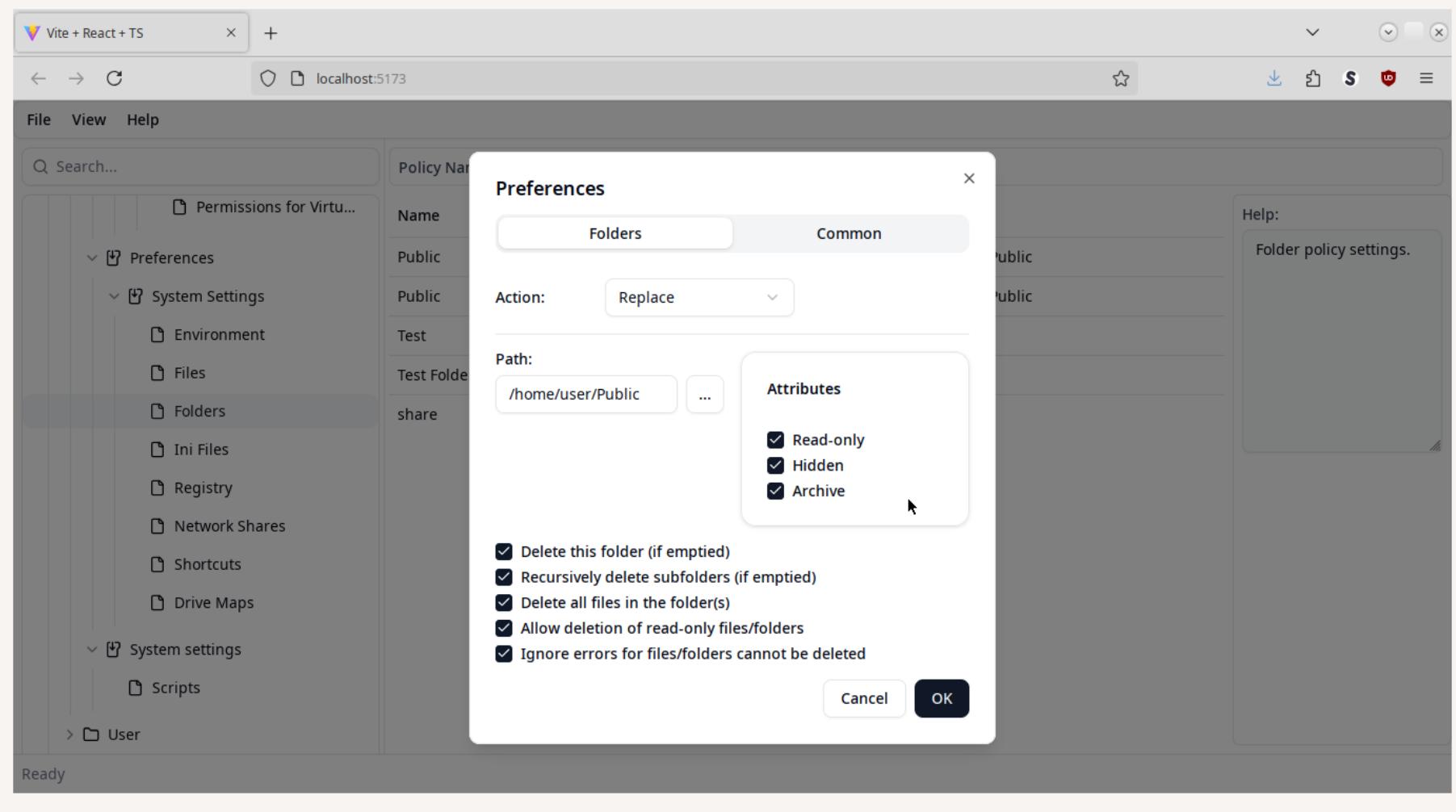
Полный цикл управления групповыми политиками



Gupdate, WEB GUI

gupdate для применения и ggui для редактирования политик

WEB GUI



WEB GUI

The screenshot shows a web-based graphical user interface (WEB GUI) running on a local host at port 5173. The application has a sidebar navigation menu and a main content area with a modal dialog.

Sidebar Navigation:

- Vite + React + TS
- + (New tab)
- File
- View
- Help
- Search bar
- Permissions for Virtu...
- Preferences (selected)
- System Settings
- Environment
- Files
- Folders
- Ini Files (selected)
- Registry
- Network Shares
- Shortcuts
- Drive Maps
- System settings
- Scripts
- User

Main Content Area:

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

Modal Dialog (Preferences):

INI Tab (Selected)

Common Tab

Action: Update

File path: /home/user/Templates/test.ini

Section Name: Section

Property Name: Property

Property Value: Value

Cancel OK

Help: Ini policy settings.



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



 **policy-1**
 {GUID-1}



 **policy-2**
 {GUID-2}



 **policy-3**
 {GUID-3}



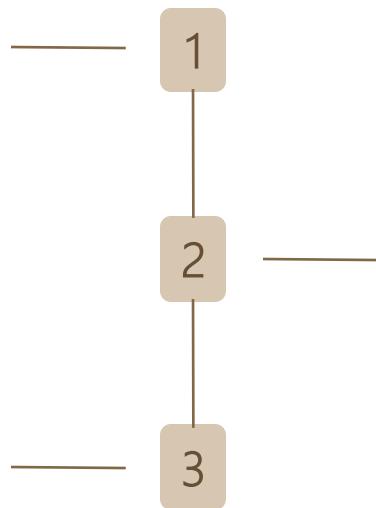
 **policy-4**
 {GUID-1}

ТЕКУЩЕЕ СОСТОЯНИЕ И ПЛАНЫ РАЗВИТИЯ

Тестирование

Ведется тестирование полного цикла работы механизма групповых политик.

Представление сообществу
Планируется представление решения в международное сообщество FreeIPA.



Документация

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

ЗАКЛЮЧЕНИЕ



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



Mail: skachedubovda@basealt.ru



Tg: @danila_skachedubov

