



**Механизмы применения групповых  
политик в решениях на базе  
дистрибутивов ALT**

**base  
alt**



## План доклада

- Смысл реализации групповых политик
- Групповые политики, как управление конфигурациями компьютеров и пользователей
- Задачи конфигурирования
- Компромиссы реализации (политики и механизмы, политики механизмов)



# Смысл групповых политик

- Цель — интеграция с Microsoft Windows
  - Управленческое решение, как состояние
- Терминология:
  - GPO (объект политик)
  - GPT (шаблон политики)
- Ограничения применимости
  - GPLink (привязка), свойства предпочтений



# Групповые политики, как как управление конфигурациями

- Цели для конфигурирования
  - Компьютер (Machine)
  - Пользователь (User)
- Типы конфигураций (Client-Side Extensions)
  - Политики
    - Registry.pol, gpntmpl.inf, ...
  - Предпочтения



# Конфигурации компьютеров

- Настройки безопасности
- Установка доп. ПО
- Скрипты (Startup, Shutdown)
- Ограничения ПО
- Реестр
- Межсетевой экран
- Групповые политики предпочтений...



# Конфигурации пользователей

- Установка доп. ПО
- Скрипты (Logon, Logoff)
- Пользовательские каталоги
- Групповые политики предпочтений
  - Общие каталоги
  - Принтеры
  - Ярлычки ...



# Групповые политики для Linux-решений

- Уровень декларативных объявлений
  - ADMX (административные шаблоны)
  - Собственный формат CSE-расширений
- Уровень интерпретации
  - Локальный шаблон политики
- Уровень реализации политик
- Уровень применения
  - Systemd services, PAM-modules



# ADMX для политики: Execution of program */bin/su*

```
[root@xpi ~]# control su  
wheelonly  
[root@xpi ~]# control su help  
public: Any user can execute /bin/su  
wheel: Any user can execute /bin/su, but only "wheel" group  
wheelonly: Only "wheel" group members can execute /bin/su  
restricted: Only root can execute /bin/su
```

The screenshot shows the Group Policy Management Editor interface. The left pane displays the tree structure under 'Computer Configuration' > 'Administrative Templates: Policy definitions' > 'BaseALT' > 'Security policies'. The right pane shows the configuration for the 'Execution of program /bin/su' policy. The policy is set to 'Enabled' and 'Supported on' is 'ALT Sisyphus'. A dropdown menu is open, showing the following options: 'Only "wheel" group members', 'Any user', 'Any user, but only "wheel" group members can switch to superuser' (which is selected), 'Only "wheel" group members', and 'Only root'. The 'Options' and 'Help' sections are also visible.

```
#####  
# control su  
#####
```





# Local Group Policy Object utility

```
[sin@xpi Калура-2019]$ wine LGPO.exe
LGPO.exe v2.2 - Local Group Policy Object utility
Файл Правка Вид Переход Закладки Сервис Настройка Справка
LGPO.exe has four modes:
* Import and apply policy settings;
* Export local policy to a GPO backup;
* Parse a registry.pol file to "LGPO text" format;
* Build a registry.pol file from "LGPO text".

To apply policy settings:
LGPO.exe command [...]

where "command" is one or more of the following (each of which can be repeated):

/g path import settings from one or more GPO backups under "path"
/m path\registry.pol import settings from registry.pol into machine config
/u path\registry.pol import settings from registry.pol into user config
/ua path\registry.pol import settings from registry.pol into user config for Administrators
/un path\registry.pol import settings from registry.pol into user config for Non-Administrators
/u:username path\registry.pol import settings from registry.pol into user config for Local user
specified by "username"
/s path\GptTmpl.inf apply security template
/a[c] path\Audit.csv apply advanced auditing settings; /ac to clear policy first
/t path\lgpo.txt apply registry commands from LGPO text
/e <name>|<guid> enable GP extension for local policy processing; specify a
GUID, or one of these names:
* "zone" for IE zone mapping extension
* "mitigation" for mitigation options, including font blocking
* "audit" for advanced audit policy configuration
* "LAPS" for Local Administrator Password Solution
* "DGVBVS" for Device Guard virtualization-based security
* "DGCI" for Device Guard code integrity policy
/boot reboot after applying policies
/V verbose output
/q /s path\gpttmpl.inf Apply the specified security template
/a[c] path\audit.csv Apply an Advanced Auditing backup file, as well as the
clear existing

LGPO.exe v2.2 - Local Gr
is a command-line utility
for Local Group Policy Objects
Advanced Auditing backup files, as
support the cor
be edited, and can build a Registry
described later in this document.)
Multiple Local Group Policy Objects
file and outputting "LGPO" text; for
put is written to LGPO.exe's
error. Both can be re
support batch file use, LGPO.exe's c
```

-----

\$ LGPO.exe

-----

\$ hreg

-----



# Групповые политики в Linux - вопросы и ответы

- Два основных вопроса:
  - «Где их хранить и как их получить на клиенте?»
  - «Как применить те или иные политики?»
- Два основных ответа:
  - «Реализация средств управления GPT»
  - «Шаблонизация дистрибутивов»



# Задачи конфигурирования дистрибутивных решений

- Шаблоны настроек
  - Локальная политика
  - Политика в домене, по умолчанию
  - Политики, имеющие смысл
- Практика применения
  - Инструменты управления (GPO, GPT, GPLink)
  - Механизмы вычисления
  - Шаблоны для применения



# Пользовательские групповые политики под Linux

- Политики применяемые при входе пользователя - в РАМ на этапе *аутентификации*, смены пароля, создания сессии и назначении групп;
- Пользовательские политики, требующие административных привилегий (подключение сетевых каталогов, настройка печати CUPS и других сервисов);
- Политики, требующие контекст графической сессии, выполняемые с пользовательскими привилегиями (настройка фона рабочего стола, дополнительные ярлыки на рабочем столе и т.п.).



## Заклучение

Group Policy for ALT Distributions:

<http://git.altlinux.org/people/sin/packages/oddjob.git>

<https://github.com/altlinuxteam/admx-basealt>

<https://github.com/altlinuxteam/hreg>

<https://github.com/altlinuxteam/gpupdate>

And also Samba with existing staff like

[samba-tool](#) and [samba-gpupdate](#)