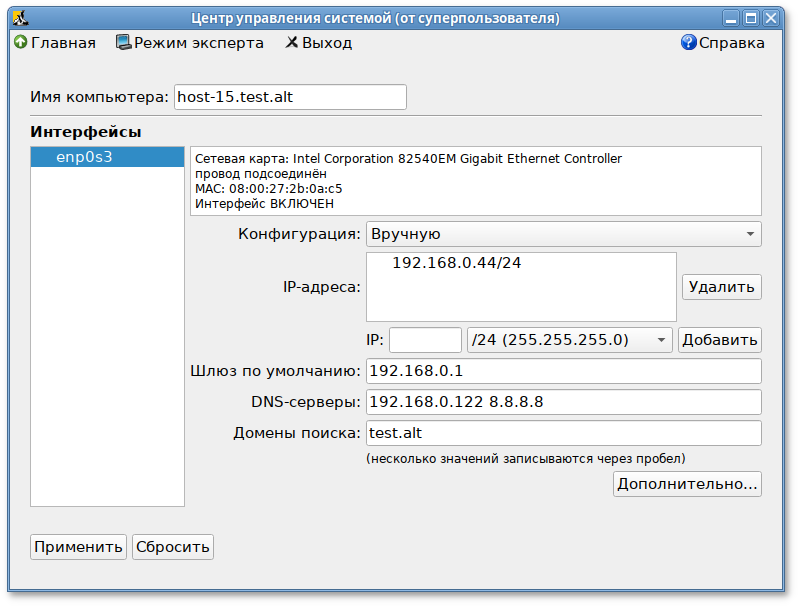
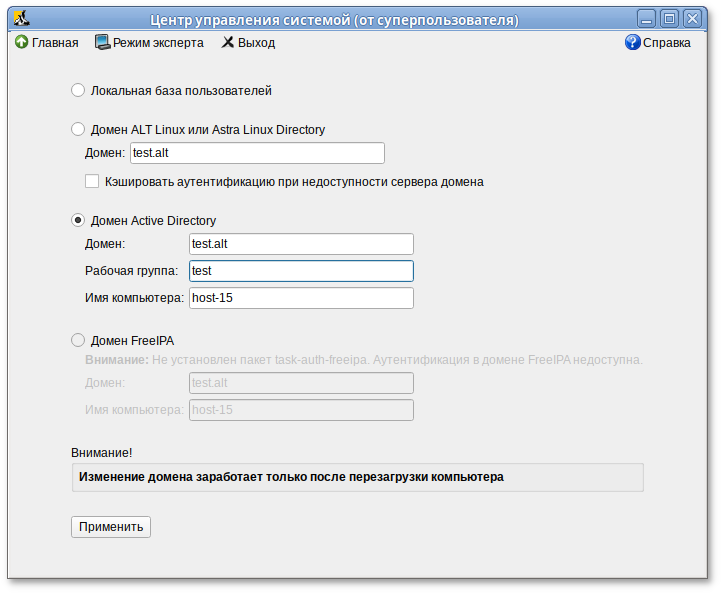
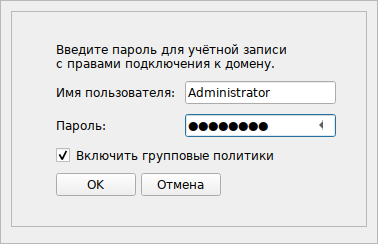
# Ввод рабочей станции в домен Active Directory



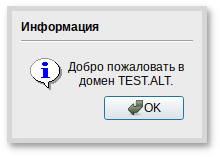


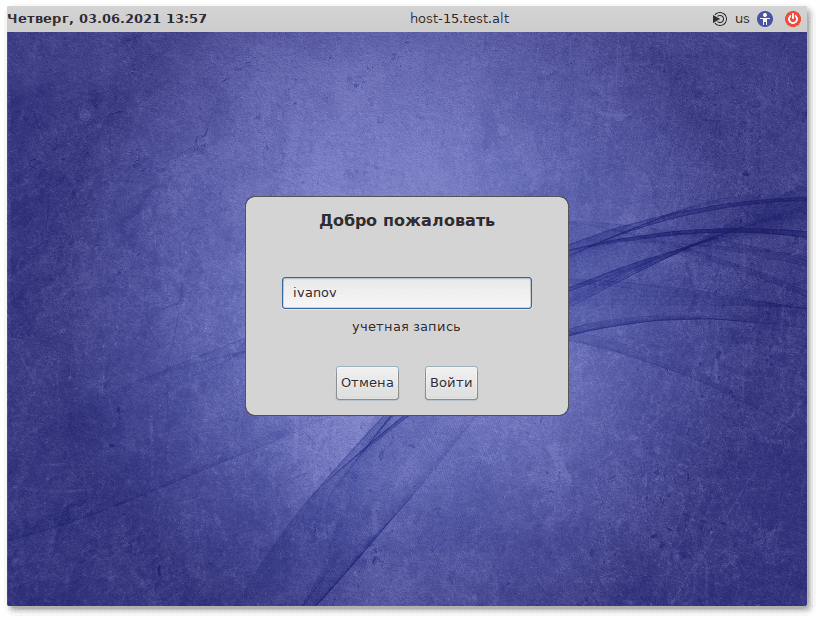


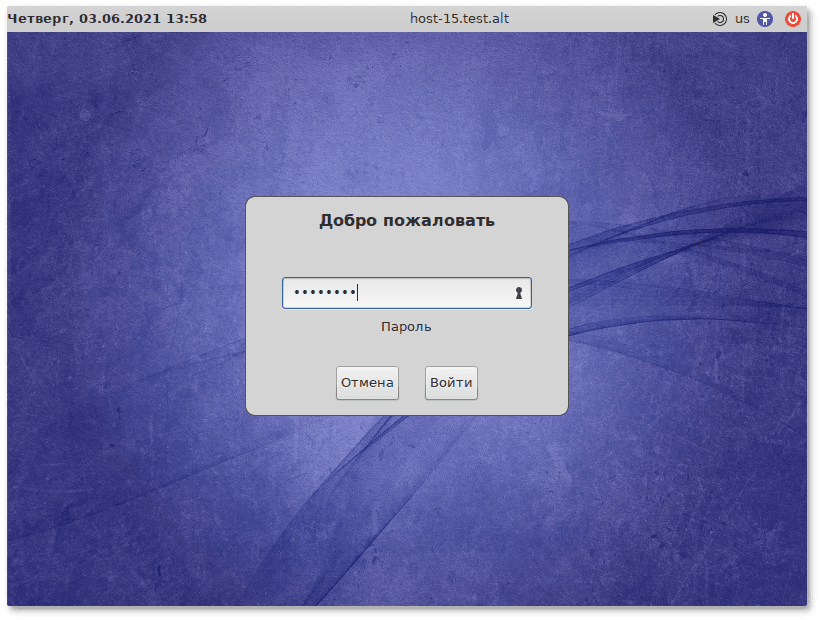












## ⁠43.5. Отображение глобальных групп на локальные

Установить, если еще не установлен, модуль ролей:

# **apt-get install libnss-role**

Настроить роли и привилегии. Для этого добавить роль локальных администраторов:

# **groupadd -r localadmins**

## ⁠43.6. Подключение файловых ресурсов

Рассматриваемые способы позволяют подключать файловые ресурсы (file shares) для доменного пользователя без повторного ввода пароля (SSO, Single Sign-On).

**⁠43.6.1. Подключение с использованием gio**

Недостаток такого способа — необходимо открыть ресурс в файловом менеджере (**Caja**, **Pcmanfm**). Однако можно открывать любые ресурсы на любых серверах, входящие в домен **Active Directory**.

* Установить необходимые пакеты:

# **apt-get install fuse-gvfs gvfs-backend-smb libgio**

* Включить пользователя в группу fuse:

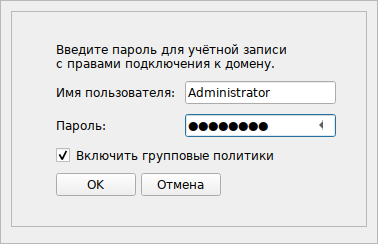
# **gpasswd -a <пользователь> fuse**

* Разрешить для всех доступ к fuse под root:

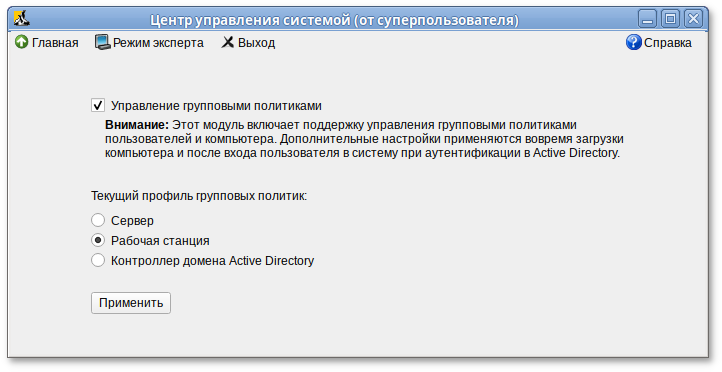
# **control fusermount public**

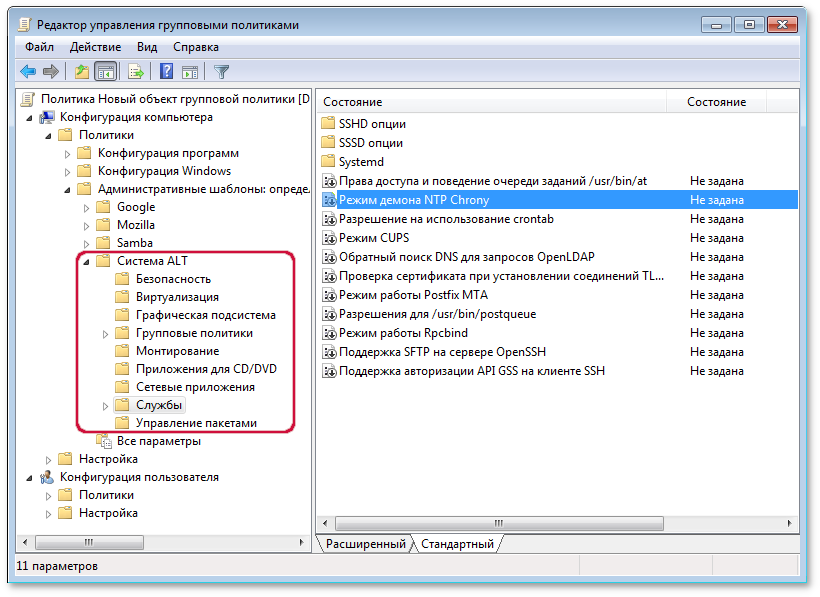


## ⁠Глава 44. Групповые политики









## Инструмент ADMC

**ADMC** — инструмент для работы с доменом Active Directory и групповыми политиками.

**Примечание**

Должен быть установлен пакет admc:

# **apt-get install admc**

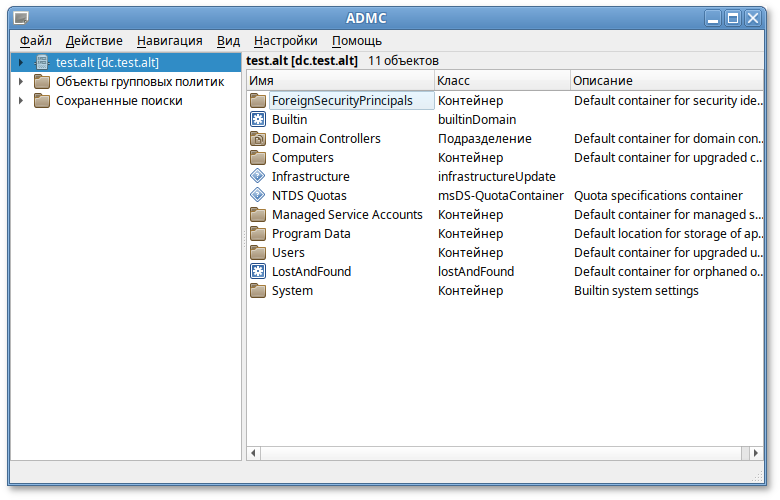
Для использования программы следует сначала получить ключ Kerberos для администратора домена:

$ **kinit administrator**

Password for administrator@TEST.ALT:

Далее запустить ADMC из меню (**Меню MATE** → **Системные** → **ADMC**) или командой **admc**:

$ **admc**

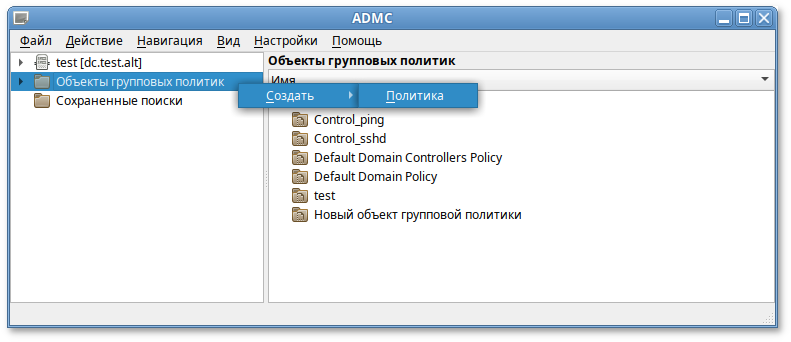


Добавление доменных устройств в группу членства GPO:

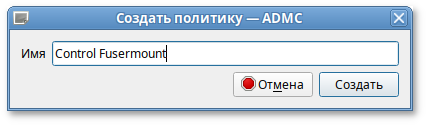
1. Создать новое подразделение:
   * в контекстном меню домена выбрать пункт **Создать** → **Организация**:
   * в открывшемся окне ввести название подразделения (например, OU) и нажать кнопку **Создать**:
2. Переместить компьютеры и пользователей домена в созданное подразделение:
   * в контекстном меню пользователя/компьютера выбрать пункт **Переместить…**;
   * в открывшемся диалоговом окне **Выберите контейнер – ADMC** выбрать контейнер, в который следует переместить учетную запись пользователя.

Cоздание политики для подразделения:

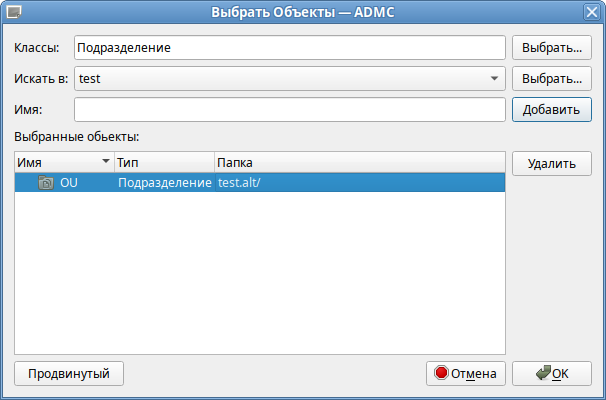
1. В контекстном меню папки «Объекты групповых политик»: **Создать** → **Политика**:



В открывшемся окне ввести название политики и нажать кнопку **Создать**: **Создать** → **Политика**:



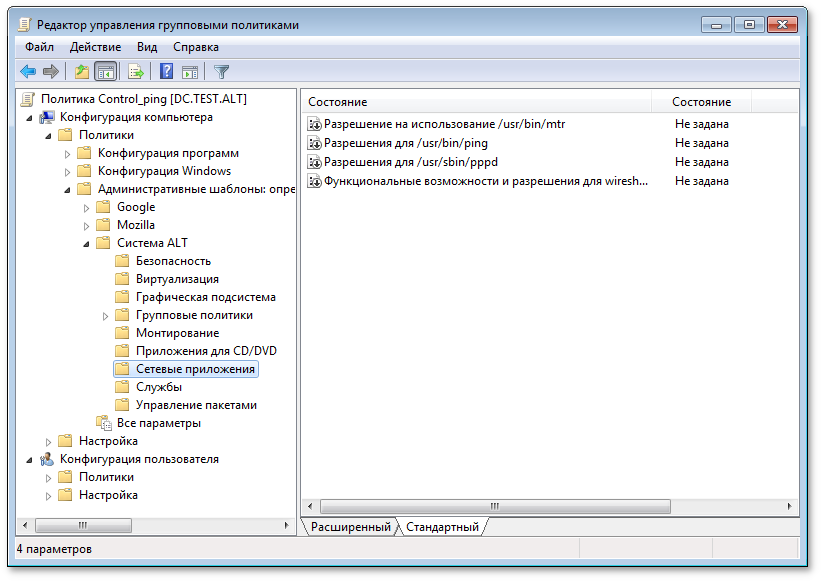
1. В контекстном меню политики выбрать пункт **Добавить линк...**;
2. Выбрать объекты, которые необходимо связать с политикой: **Создать** → **Политика**:



## ⁠Пример создания групповой политики

В качестве примера, создадим политику, разрешающую запускать команду **ping** только суперпользователю (root). Для создания новой политики, необходимо выполнить следующие действия:

1. На машине с установленным RSAT открыть оснастку **Управление групповыми политиками** (gpmc.msc).
2. В контекстном меню объектf групповой политики (GPO), выбрать пункт **Редактировать**. Откроется редактор GPO.
3. Перейти в **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Система ALT**. Здесь есть несколько разделов, соответствующих категориям control. Выбрать раздел **Сетевые приложения**, в правом окне редактора отобразится список политик:



1. Дважды щелкнуть левой кнопкой мыши на политике **Разрешения для /usr/bin/ping**. Откроется диалоговое окно настройки политики. Выбрать параметр **Включить**, в выпадающем списке **Кому разрешено выполнять** выбрать пункт **Только root** и нажать кнопку **Применить**:

