ДОКУМЕНТАЦИЯ ALT LINUX TEAM

Альт Домен

Руководство администратора

Редакция апрель, 2025

Аннотация

«Альт Домен» — служба каталогов (доменная служба), позволяющая централизованно управлять компьютерами и пользователями в корпоративной сети с операционными системами (ОС) на ядре Linux и Windows по единым правилам из единого центра. В системе реализовано хранение данных о пользователях, компьютерах (рабочих станциях) и других объектах корпоративной сети, а также управление профилями пользователей и компьютеров с помощью групповых политик в доменах MS Active Directory / Samba DC.

Данное руководство соответствует текущему состоянию сведений, но какие-либо окончательные правки могли не попасть в него. В случае обнаружения ошибок и неточностей в руководство вносятся изменения.

I. Введение

1. Основные сведения о логической модели Альт Домен

2. Схема стенда

3. Максимальные ограничения и параметры масштабирования

II. Разворачивание домена

4. Системные требования к серверу (контроллеру домена)

5. Создание первого контроллера домена

6. Присоединение к домену в роли контроллера домена

7. Контроллер домена на чтение (RODC)

8. Редактирование существующего домена

9. Отладочная информация

10. Удаление контроллера домена

III. Репликация

11. Настройка репликации

12. Проверка статуса репликации

13. Двунаправленная репликация SysVol

IV. Клиенты Альт Домен

14. SSSD и Winbind

15. Подготовка системы к вводу в домен

16. Присоединение к домену в роли участника

17. Вход пользователя

18. Отображение глобальных групп на локальные

19. Отладочная информация

20. Удаление клиента домена

21. Повторная регистрация клиента

22. Настройка аутентификации доменных пользователей на контроллере домена

23. Настройка обновления паролей аккаунтов машин

V. Инструменты управления объектами домена и групповыми политиками

24. Групповые политики в Альт Домен

25. Установка административных шаблонов и административных инструментов

26. Включение механизма применения конфигурации на клиентских машинах

27. Модуль клиентской машины для применения конфигурации

28. Модуль удаленного управления базой данных конфигурации (ADMC)

29. Модуль редактирования настроек клиентской конфигурации (GPUI)

30. Расширение возможностей ГП

31. Решение проблем

VI. Доверительные отношения (Трасты)

32. Настройка доверия

33. Настройка DNS

34. Создание доверительного отношения

35. Управление пользователями и группами

36. Использование трастов на LINUX-клиентах

37. Удаление доверия

VII. Администрирование домена

38. Управление пользователями и группами

39. Администрирование DNS

40. Администрирование сайтов и подсетей

41. Управление парольными политиками

42. Резервное копирование и восстановление домена

43. Роли FSMO

44. Настройка Samba для привязки к определённым интерфейсам

45. Создание keytab-файла

46. Настройка DHCP-сервера для обновления DNS-записей

47. Настройка LDAP через SSL (LDAPS)

48. Аутентификация других сервисов в домене

49. Распределенная файловая система (DFS)

50. Настройка SSSD

51. Samba в режиме файлового сервера

52. Монтирование общих ресурсов samba

53. Журналирование в Samba

54. Усиление безопасности DC

55. Планирование и настройка диапазонов идентификаторов UID и GID (Winbind/IDMapping)

56. Инструменты командной строки

57. Конфигурационные файлы

VIII. Решение проблем

58. Диагностика

IX. Примечания

59. Настройка беспарольного доступа по ssh

60. Центр управления системой

Часть I. Введение

Содержание

1. Основные сведения о логической модели Альт Домен

2. Схема стенда

3. Максимальные ограничения и параметры масштабирования

Глава 1. Основные сведения о логической модели Альт Домен

Домен

Группа компьютеров, пользователей, принтеров и других объектов, совместно использующих общую БД каталога.

Дерево доменов

Иерархическая система доменов, имеющая единый корень (корневой домен).

Лес доменов

Множество деревьев доменов, находящихся в различных формах доверительных отношений.

Сервер

Компьютер, выполняющий определённые роли в домене.

Контроллер домена

Сервер, хранящий каталог и обслуживающий запросы пользователей к каталогу. Помимо хранения данных контроллер домена может выступать в качестве одной из FSMO-ролей.

Организационное подразделение (OU)

Субконтейнер в домене, который может содержать различные объекты AD: другие контейнеры, группы, аккаунты пользователей и компьютеров. OU представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователям.

Группа

Объекты, являющиеся участниками системы безопасности (security principals) и предназначенные для управления доступом к ресурсам. Каждой группе присваивается уникальный идентификатор безопасности (Security Identifier, SID), который сохраняется в течение всего срока службы.

Группы — это объекты, являющиеся участниками системы безопасности (security principals) и предназначенные для управления доступом к ресурсам. Каждой группе присваивается уникальный идентификатор безопасности (Security Identifier, SID), который сохраняется в течение всего срока службы.

Состав Альт Домен:

- контроллер домена (DC) на базе дистрибутива ОС «Альт Сервер»;
- модуль для ввода компьютера в домен;
- модуль удаленного управления базой данных конфигурации (ADMC) — управляет объектами в домене и групповыми политиками, реализован как графический инструмент;
- модуль редактирования настроек клиентской конфигурации (GPUI) — позволяет редактировать настройки групповых политик;

- шаблоны групповых политик;
- модуль для применения конфигурации на целевой Linux ОС (gpupdate).

Разворачивание домена производится в следующем порядке:

- создание первого контроллера в домене;
- присоединение сервера в роли контроллера домена к существующему домену;
- присоединение сервера или рабочей станции в роли рядового участника существующего домена.

Глава 2. Схема стенда

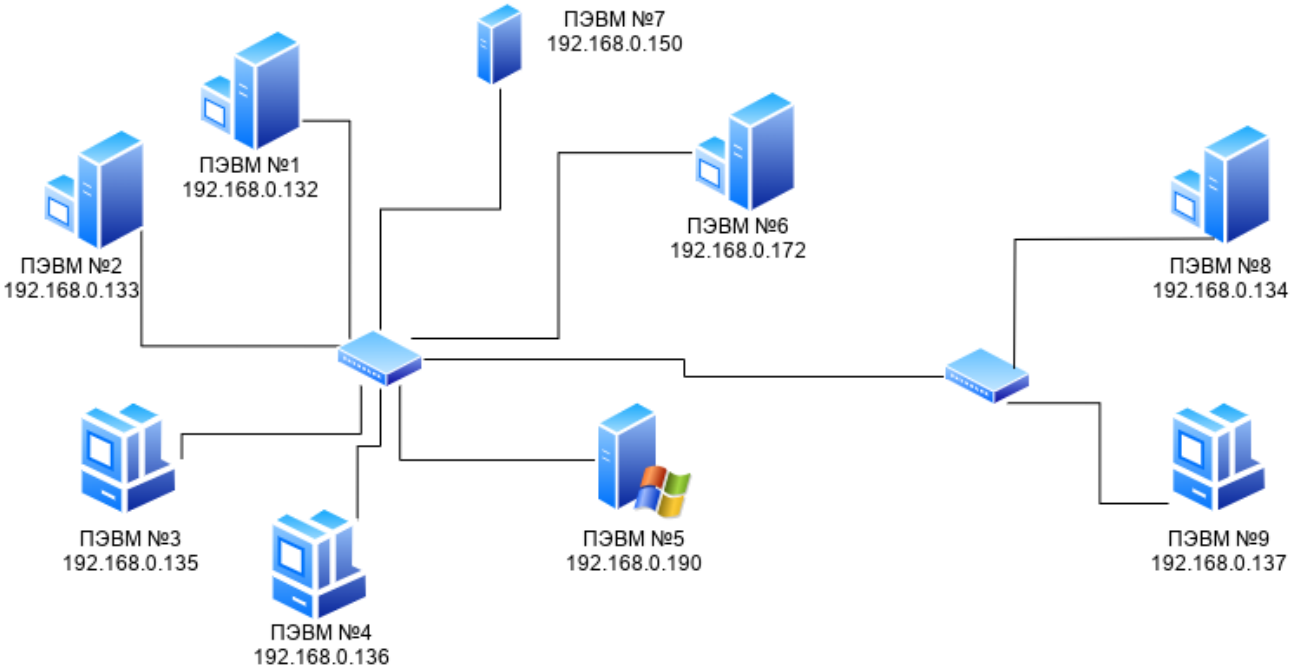


Таблица 2.1. Состав технических и программных средств стенда

№ ПЭВМ	Программная среда	Описание
1	ОС «Альт Сервер»	Контроллер домена test.alt
2	ОС «Альт Сервер»	Дополнительный контроллер домена test.alt
3	ОС Альт («Альт Рабочая станция», «Альт Рабочая станция К», «Альт Образование»)	Рабочая станция
4	ОС Альт («Альт Рабочая станция», «Альт Рабочая станция К», «Альт Образование»)	Рабочая станция
5	ОС Microsoft Windows Server 2012	Контроллер домена win.alt
6	ОС «Альт Сервер»	Контроллер домена example.alt
7	ОС «Альт Сервер»	Веб-сервер, прокси-сервер
8	ОС «Альт Сервер»	

№ ПЭВМ	Программная среда	Описание
		Контроллер домена test.alt только для чтения (RODC)
9	ОС Альт («Альт Рабочая станция», «Альт Рабочая станция K», «Альт Образование»)	Рабочая станция

Параметры домена:

- имя домена — test.alt;
- сервер (ОС ALT) — dc1.test.alt (192.168.0.132);
- дополнительный сервер (ОС ALT) — dc2.test.alt (192.168.0.133);
- RODC (ОС ALT) — rodc.test.alt (192.168.0.134);
- веб-сервер, прокси-сервер (ОС ALT) — web.test.alt (192.168.0.150);
- рабочая станция 1 (ОС ALT) — host-01.test.alt (192.168.0.135);
- рабочая станция 2 (ОС ALT) — host-02.test.alt (192.168.0.136);
- рабочая станция 3 (ОС ALT) — host-03.test.alt (192.168.0.137);
- имя пользователя-администратора — Administrator;
- пароль администратора — Pa$$word.

Дополнительные домены:

- win.alt: сервер AD (ОС Windows) — dc1.win.alt (192.168.0.190);
- example.alt: сервер (ОС ALT) — s1.example.alt (192.168.0.172).

Глава 3. Максимальные ограничения и параметры масштабирования

3.1. Общее ограничение по количеству объектов

3.2. Расчёт объема базы данных

3.3. Требования к дисковому хранилищу

3.4. Расчёт нагрузки на CPU (по сайтам)

3.1. Общее ограничение по количеству объектов

Доменная инфраструктура поддерживает хранение и обработку до 1 500 000 объектов в базе каталога. В рамках этого предела возможна работа с объектами следующих типов:

- до 700 000 пользователей;
- до 700 000 компьютеров;

- до 100 000 групп.

Важно

Один контроллер домена рекомендуется использовать для обслуживания не более 2–5 тысяч пользователей.

3.2. Расчёт объема базы данных

Оценочный размер базы данных домена можно вычислить по следующей формуле:

```
Объем (в KB) = Uc × 50KB + Cc × 10KB + Mc × 1KB
```

где:

- Uc — количество пользователей;
- Cc — количество компьютеров;
- Mc — общее количество членств пользователей в группах.

Требования к оперативной памяти масштабируются линейно в зависимости от объёма базы, начиная от 2 ГБ и заканчивая 128 ГБ (см. табл. Рекомендации по объёму оперативной памяти).

Таблица 3.1. Рекомендации по объёму оперативной памяти

Количество пользователей	Минимальный объём ОЗУ	Рекомендуемый объём ОЗУ
до 10 000	2 ГБ	8 ГБ
до 20 000	4 ГБ	16 ГБ
до 50 000	8 ГБ	16 ГБ
до 100 000	16 ГБ	32 ГБ
до 200 000	32 ГБ	32 ГБ
до 500 000	64 ГБ	64 ГБ
до 1 000 000	128 ГБ	128 ГБ

3.3. Требования к дисковому хранилищу

Расчёт требований к дисковому хранилищу аналогичен расчёту требований к оперативной памяти, но с учётом накопления логов.

Важно

Категорически не рекомендуется использовать шпиндельные HDD.

3.4. Расчёт нагрузки на CPU (по сайтам)

Примечание

Ниже приведён расчёт минимально необходимого оборудования, в реальности нужен некоторый запас.

Расчёт требований к CPU производится на основе предполагаемой пиковой нагрузки — момента, когда большинство пользователей проходит аутентификацию за короткий период времени (например, в начале рабочего дня).

Важно определить временной интервал (t), за который все пользователи проходят аутентификацию (в секундах). Для примера расчета возьмем 5 минут (300 секунд).

Следующим параметром является количество аутентификаций, обрабатываемых одним ядром CPU (r) в секунду. На основе результатов нагрузочного тестирования установлено, что при наихудшем варианте одно ядро CPU способно обрабатывать две аутентификации в секунду (принимаем r = 2).

Далее расчет распределения ядер по серверам производится из следующего правила: не менее двух серверов в сайте и не более восьми ядер в сервере. Дополнительно рекомендуется резервирование по крайней мере одного сервера на площадку — для обеспечения отказоустойчивости и возможности обслуживания без снижения доступности.

Таким образом, если, например, сайт состоит из 22 000 пользователей:

```
22000 / 300 = 74 аутентификации в секунду
74/2 = 37 ядер
```

или:

```
22000 / (2*300) = 37
```

Итоговая формула:

```
CPU_cores = Uc / (r × t)
```

Часть II. Разворачивание домена

Поддерживаются следующие базовые возможности Active Directory:

- аутентификация рабочих станций Windows и Linux и служб;
- авторизация и предоставление ресурсов;
- групповые политики (GPO);
- перемещаемые профили (Roaming Profiles);
- поддержка инструментов Microsoft для управления серверами (Remote Server Administration Tools) с компьютеров под управлением Windows;
- поддержка протоколов SMB2 и SMB3 (в том числе с поддержкой шифрования).

Содержание

4. Системные требования к серверу (контроллеру домена)

5. Создание первого контроллера домена

6. Присоединение к домену в роли контроллера домена

7. Контроллер домена на чтение (RODC)

8. Редактирование существующего домена

9. Отладочная информация

10. Удаление контроллера домена

Глава 4. Системные требования к серверу (контроллеру домена)

4.1. RAM

4.2. Размеры хранилища

4.3. CPU

4.4. DNS

4.5. Синхронизация времени

4.6. Требования к портам

В этом разделе перечислены требования для установки контроллера домена. Перед установкой необходимо убедиться, что система соответствует этим требованиям.

Примечание

В условиях реальной эксплуатации рекомендуется использовать два или более контроллера домена для обеспечения отказоустойчивости.

4.1. RAM

Для демонстрационной/тестовой системы рекомендуется 2 ГБ.

Для производственной установки рекомендуется не менее 4 ГБ ОЗУ, далее — в зависимости от размера базы (см. табл. Рекомендации по объёму оперативной памяти).

Примечание

Параметр, который оказывает наибольшее влияние на требования к памяти, — это количество одновременных открытий сеансов.

4.2. Размеры хранилища

10 ГБ достаточно для доменов с несколькими сотнями пользователей.

При планировании размера хранилища также необходимо учесть:

- уровни журналов и политику хранения журналов;
- использование изображений/аватаров для идентификации пользователей;
- количество пользователей, машин и групп;
- место под резервные копии.

4.3. CPU

Для нескольких сотен пользователей достаточно 4 vCPUs.

Некоторые процессы Samba не являются многопоточными, поэтому увеличение числа процессоров не повысит производительность.

Чтобы сбалансировать нагрузку, необходимо создать второй контроллер домена в репликации с первым и применить политику балансировки нагрузки на уровне клиента.

Необходимое количество контроллеров домена зависит от нескольких параметров:

- количество сторонних приложений LDAP, подключенных к домену;
- качество кода сторонних LDAP-приложений, подключенных к домену;
- количество запросов к файловым серверам.

4.4. DNS

Не следует использовать существующий домен, если вы не являетесь владельцем домена. Рекомендуется использовать зарезервированный домен верхнего уровня RFC2606 (**`https://tools.ietf.org/html/rfc2606`**) для частных тестовых установок, например, alt.test.

Имя домена для разворачиваемого контроллера домена (DC) должно состоять минимум из двух компонентов, разделённых точкой.

Важно

Необходимо избегать суффиксов .local. При указании домена, имеющего суффикс .local, потребуется на сервере и подключаемых компьютерах под управлением Linux отключить службу **`avahi-daemon`**.

Примечание

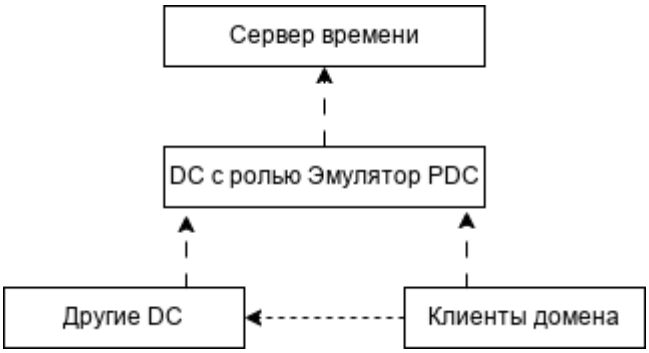
Имя как контроллера домена, так и всех ПК членов домена не должно превышать 15 символов (ограничение связано с ***sAMAccountName*** в Active Directory).

4.5. Синхронизация времени

Для аутентификации Kerberos необходима точная синхронизация времени между рабочими станциями членов домена и контроллером домена. Максимально допустимое отклонение времени по умолчанию составляет 5 минут. Если член домена или DC имеет большую разницу во времени, доступ будет запрещен. В результате пользователь не сможет получить доступ к общим папкам или выполнить запрос к каталогу.

На всех DC домена должен быть настроен сервер времени NTP.

Samba поддерживает как ntpd, так и chrony в качестве сервера NTP. Демон синхронизирует время с внешними источниками и позволяет клиентам получать время с сервера, на котором запущен демон.



Из схемы синхронизации времени видно, что только DC с ролью *Эмулятор PDC* получает свое время от внешних серверов времени, все остальные DC получают время от эмулятора PDC, все рабочие станции получают время от любого DC. Клиенты Windows в конечном итоге получают свое время от DC эмулятора PDC через DC, и если DC эмулятора PDC отключается, другие DC будут продолжать его искать, и время может смещаться. В качестве обходного пути следует установить одинаковые внешние серверы времени на всех DC. В этом случае, если эмулятор PDC отключится и его нельзя будет легко перезапустить, нужно передать или захватить роль эмулятора PDC другому DC.

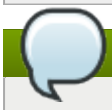
4.6. Требования к портам

Для корректной работы службы Samba на контроллере домена должны быть открыты порты, указанные в табл. Порты, используемые контроллером домена.

Таблица 4.1. Порты, используемые контроллером домена

Служба	Порт	Протокол	Примечание
DNS	53	TCP и UDP	Для DNS от контроллера домена к контроллеру домена и от клиента к контроллеру домена. Может быть предоставлен внутренним DNS-сервером Samba или DNS-сервером Bind9

Служба	Порт	Протокол	Примечание
Kerberos	88	TCP и UDP	Для аутентификации Kerberos
NTP	123	UDP (Опционально)	Если на контроллере домена настроен и работает NTP
End Point Mapper (DCE/ RPC Locator Service)	135	TCP	Для операций клиента с контроллером домена
NetBIOS Name Service	137	UDP	
NetBIOS Datagram	138	UDP	Для службы репликации файлов между контроллерами домена
NetBIOS Session	139	TCP	Для службы репликации файлов между контроллерами домена
LDAP	389	TCP и UDP	Для обработки регулярных запросов от клиентских компьютеров к контроллерам домена
SMB over TCP	445	TCP	Для службы репликации файлов
Kerberos	464	TCP и UDP	Используется **`kadmin`** для установки и смены пароля Kerberos
LDAPS	636	TCP	Если в файле **`smb.conf`** установлен параметр **`tls enabled = yes`** (по умолчанию)
Global Catalog	3268	TCP	Для глобального каталога от клиента к контроллеру домена
Global Catalog SSL	3269	TCP	Если в файле **`smb.conf`** установлен параметр **`tls enabled = yes`** (по умолчанию)
Dynamic RPC Ports	49152-65 535	TCP	Диапазон соответствует диапазону портов, используемому в Windows Server 2008 и более поздних версиях. Чтобы вручную установить диапазон портов в Samba, необходимо задать требуемый диапазон в параметре **`rpc server port`** в файле **`smb.conf`**. Подробности см. в описании данного параметра на справочной странице **`man smb.conf`**.



Примечание

В зависимости от состава используемых служб для работы Samba могут потребоваться и другие порты.

Глава 5. Создание первого контроллера домена

5.1. Выбор DNS-бэкенда

5.2. Установка имени контроллера домена

5.3. Установка пакетов

5.4. Остановка конфликтующих служб

5.5. Настройка NTP-сервера

5.6. Параметры команды разворачивания домена

5.7. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

5.8. Домен с BIND9_DLZ

5.9. Настройка Kerberos

5.10. Проверка работоспособности домена

Примечание

Для установки контроллера домена Samba AD нужны привилегии суперпользователя.

5.1. Выбор DNS-бэкенда

Служба DNS в «Альт Домен» необходима для таких функций как:

- разрешение имен;
- обнаружение служб;
- обнаружение контроллеров домена.

Для управления службой DNS Samba поддерживает работу с двумя DNS-бэкендами:

- **SAMBA_INTERNAL** — встроенный сервер имен:
  - поддерживает базовую функциональность, необходимую для работы домена;
  - используется по умолчанию при подготовке нового домена, присоединении к существующему домену;
  - прост в настройке и не требует дополнительного ПО или знаний о DNS;
  - следует использовать для простых настроек DNS;

  SAMBA_INTERNAL не поддерживает следующий функционал:
  - роль кеширующего DNS-сервера (caching resolver);
  - обработку рекурсивных запросов (но может пересылать их другому рекурсивному серверу DNS);
  - аутентификацию DNS-транзакций с использованием общих ключей (TSIG);
  - работу с зонами-заглушками (stub zones);

- передачу зон DNS (zone transfers);
- балансировку нагрузки циклического перебора между контроллерами домена (Round Robin load balancing among DC's);
- условную пересылку DNS-запросов (conditional DNS forwarding).

- **BIND9_DLZ** — использует Samba AD для хранения информации о зоне:
  - требуется BIND 9.8 или более поздняя версия, установленная и настроенная локально на контроллере домена Samba;
  - необходимы знания о DNS-сервере BIND и о том, как настроить службу;
  - следует использовать для сложных сценариев DNS, которые нельзя настроить во внутреннем DNS.

Примечание

Внутренний DNS-сервер Samba не управляет кешем, поэтому он будет отправлять запрос серверу пересылки для каждого DNS-запроса, который не соответствует его домену. Бэкенд BIND9_DLZ использует кеш Bind для рекурсивных запросов. Запросы на сам домен каждый раз передаются модулю DLZ, кеша на этом уровне у него нет.

Чтобы определить, какой вариант развертывания DNS-сервера выбрать, необходимо учесть следующие факторы:

- необходимость условной пересылки DNS-запросов. Если не требуется — можно использовать встроенный сервер имен (SAMBA_INTERNAL). Если требуется и при этом нежелательно использовать выделенный DNS-сервер — DNS-сервер на основе BIND 9;
- уже имеющаяся инфраструктура. В случае, если уже есть настроенные DNS-серверы, на которые могут быть возложены функции перенаправления, можно использовать выделенный DNS-сервер на основе BIND 9.

Важно

Бэкенд DNS **BIND9_FLATFILE** не поддерживается.

5.2. Установка имени контроллера домена

Для сервера, на котором будет разворачиваться контроллер домена, должно быть и установлено правильное имя узла и домена.

Для установки имени узла и домена следует выполнить команды:

```
# hostnamectl set-hostname <имя узла>
# domainname <имя домена>
```

Например:

```
# hostnamectl set-hostname dc1.test.alt
# domainname test.alt
```

Примечание

В системах, в которых управление сетью осуществляется через etcnet и используется SysVinit вместо systemd, полное доменное имя (FQDN) необходимо указать в файле **/etc/sysconfig/network**:

```
HOSTNAME=dc1.test.alt
```

Во все остальных случаях параметр HOSTNAME игнорируется.

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

5.3. Установка пакетов

Samba поддерживает две реализации Kerberos — Heimdal и MIT.

Для Samba DC на базе Heimdal Kerberos необходимо установить пакет *task-samba-dc*:

```
# apt-get install task-samba-dc
```

Если будет использоваться Samba DC на базе MIT Kerberos следует установить пакет *task-samba-dc-mitkrb5*:

```
# apt-get install task-samba-dc-mitkrb5
```

Примечание

Samba на базе Heimdal Kerberos использует KDC несовместимый с MIT Kerberos, поэтому на контроллере домена на базе Heimdal Kerberos из пакета *samba-dc*, для совместимости с клиентской библиотекой libkrb5, в **krb5.conf** (в блоке — libdefaults) необходимо отключить использование ядерного кеша ключей — ***KEYRING:persistent:%{uid}***:

```
# control krb5-conf-ccache default
```

5.4. Остановка конфликтующих служб

Так как Samba в режиме контроллера домена (Domain Controller, DC) использует свой сервер LDAP, свой центр распределения ключей Kerberos и свой сервер DNS (если не включен плагин BIND9_DLZ), перед установкой необходимо остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

Примечание

Выключить автозагрузку служб и отключить службы можно в ЦУС (**Система** → **Системные службы**).

5.5. Настройка NTP-сервера

Настроить сервер времени chrony в качестве NTP-сервера:

1. Установить пакет *chrony*:

   ```
   # apt-get install chrony
   ```

2. Включить доступ к серверу chrony:

   ```
   # control chrony server
   ```

3. Установить синхронизацию с российским пулом NTP:

   ```
   # sed -i -r 's/^(pool.*)/#\1\npool ru.pool.ntp.org iburst/' /etc/chrony.conf
   ```

   или указать серверы NTP в директиве server или pool в файле конфигурации NTP **/etc/chrony.conf**:

   ```
   pool ru.pool.ntp.org iburst
   ```

   Примечание

   Параметр ***iburst*** используется для ускорения начальной синхронизации.

4. Запустить и включить автоматический запуск для службы **chronyd**:

   ```
   # systemctl enable --now chronyd
   ```

5. Убедиться в нормальной работе NTP-сервера:

   ```
   # systemctl status chronyd.service
   ```

5.6. Параметры команды разворачивания домена

Команда **`samba-tool domain provision`** имеет множество опций, которые можно использовать для предоставления дополнительной информации при установке сервера. Эти опции также можно использовать в скриптах.

В табл. Основные опции для samba-tool domain provision описаны некоторые опции. Для получения более подробной информации следует обратиться к man странице **`samba-tool(8)`**.

Таблица 5.1. Основные опции для samba-tool domain provision

Опция	Описание
--interactive	Запрашивать ввод данных у пользователя (интерактивное создание домена)
--domain=DOMAIN	Имя домена NetBIOS (имя рабочей группы)
--domain-guid=GUID	Установить domainguid (иначе используется случайное значение)
--domain-sid=SID	Установить domainsid (иначе используется случайное значение)
--ntds-guid=GUID	Установить GUID объекта NTDS (иначе используется случайное значение)
--host-name=HOSTNAME	Установить имя хоста
--host-ip=IPADDRESS	Установить IPv4 IP-адрес
--host-ip6=IP6ADDRESS	Установить IPv6 IP-адрес
--adminpass=PASSWORD	Пароль основного администратора домена (иначе используется случайное значение)
--krbtgtpass=PASSWORD	Пароль krbtgtpass (иначе используется случайное значение)
--dns-backend=NAMESERVER-BACKEND	Бэкенд DNS-сервера: SAMBA_INTERNAL — встроенный сервер имен (по умолчанию), BIND9_FLATFILE — использует текстовую базу данных bind9 для хранения информации о зоне, BIND9_DLZ — использует Samba AD для хранения информации о зоне, NONE — полностью пропускает настройку DNS (не рекомендуется).
--dnspass=PASSWORD	Пароль dns (иначе используется случайное значение)
--server-role=ROLE	Позволяет указать тип серверной роли: domain controller, dc (по умолчанию), member server, member или standalone
--function-level=FOR-FUN-LEVEL	Позволяет указать уровень домена и леса: 2000, 2003, 2008, 2008_R2 (по умолчанию) или 2016
--base-schema=BASE-SCHEMA	Версия базовой схемы домена (по умолчанию 2019)
--use-rfc2307	Позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux (по умолчанию no)

Опция	Описание
--machinepass=PASSWORD	Пароль для машины (иначе используется случайное значение)
--plaintext-secrets	Сохранять конфиденциальные данные в виде обычного текста на диске (по умолчанию конфиденциальные данные шифруются)
--realm=REALM	Задаёт область Kerberos (LDAP), и DNS имя домена
--option=OPTION	Позволяет установить параметры **smb.conf** из командной строки
-s FILE, --configfile=FILE	Позволяет указать файл конфигурации
-d DEBUGLEVEL, --debuglevel=DEBUGLEVEL	Включить отладку

5.7. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Контроллер домена предоставляет внутренний DNS-сервер, который поддерживает основные функции, необходимые для Альт Домен. Он прост в настройке и не требует дополнительного программного обеспечения или знаний о DNS. Создание домена с внутренним DNS-сервером рекомендуется для простых настроек DNS.

Внутренний DNS Samba имеет следующие недостатки:

- нельзя использовать как кеширующий сервер (caching resolver);
- не поддерживает рекурсивные запросы;
- не поддерживает подпись транзакции с общим ключом (TSIG) (shared-key transaction signature);
- не поддерживает работу с зонами-заглушками (stub zones);
- не поддерживает передачу зоны DNS (zone transfers);
- не поддерживает балансировку нагрузки циклического перебора между контроллерами домена (Round Robin load balancing among DC's).

Внутренний DNS-сервер может разрешать только DNS-зоны домена. Чтобы включить рекурсивные запросы других зон, следует в параметре ***dns forwarder*** (файл **smb.conf**) указать один или несколько IP-адресов DNS-серверов, поддерживающих рекурсивное разрешение. Например:

```
dns forwarder = 192.168.0.190
```

Примечание

Samba 4.5 и более поздние версии в параметре ***dns forwarder*** поддерживают несколько IP-адресов, разделенных пробелами. Старые версии поддерживают один IP-адрес. Обращение ко второму и последующим DNS-серверам произойдёт только в том случае, если первый не вернул никакого ответа.

Примечание

Внешний DNS-сервер можно указать при создании домена.

При создании домена с внутренним DNS-сервером нужно использовать параметр ***--dns-backend=SAMBA_INTERNAL*** или не указывать этот параметр вообще.

5.7.1. Настройка файла /etc/resolvconf.conf

Для корректного распознавания всех локальных DNS-запросов в файле **/etc/resolvconf.conf** должна присутствовать строка:

```
name_servers=127.0.0.1
```

Если этой строки в файле **/etc/resolvconf.conf** нет, то в конец этого файла следует добавить строку:

```
name_servers=127.0.0.1
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

Если на сервере используется systemd-networkd, чтобы избежать конфликтов systemd-resolved с Samba DNS, следует отключить ***DNSStubListener***:

- в файле конфигурации systemd-resolved (**/etc/systemd/resolved.conf**) установить значение:

  ```
  DNSStubListener=no
  ```

- перезапустить службу systemd-resolved:

  ```
  # systemctl restart systemd-resolved
  ```

5.7.2. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Предупреждение

Перед созданием домена необходимо обязательно удалить **/etc/samba/smb.conf**:

```
# rm -f /etc/samba/smb.conf
```

5.7.3. Создание домена

5.7.3.1. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **Enter**.

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
```

При запросе *DNS forwarder IP address* можно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена:

```
DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:
8.8.8.8
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, — это одна из причин завершения развертывания домена ошибкой.

Начнется процесс конфигурации:

```
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/
kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/
samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              dc1
NetBIOS Domain:        TEST
DNS Domain:            test.alt
DOMAIN SID:            S-1-5-21-3617232745-2316959539-2936900449
```

5.7.3.2. В пакетном режиме

Для пакетной установки необходимо как минимум указать следующие параметры:

- **`--realm REALM_NAME`** — имя области Kerberos (LDAP) и DNS имя домена;
- **`--domain=DOMAIN`** — имя домена (имя рабочей группы);
- **`--adminpass=PASSWORD`** — пароль основного администратора домена;
- **`dns forwarder=forwarder_ip_address`** — внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;

- **--server-role=ROLE** — тип серверной роли;
- **--dns-backend=NAMESERVER-BACKEND** — бэкенд DNS-сервера;
- **--use-rfc2307** — позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, — это одна из причин завершения развертывания домена ошибкой.

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt --domain=test \
--adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL \
--option="dns forwarder=8.8.8.8" \
--server-role=dc --use-rfc2307
```

Если уровень не указан, то домен разворачивается на уровне 2008_R2. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt --domain=test \
--adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL \
--option="dns forwarder=8.8.8.8" --option="ad dc functional level = 2016" \
--server-role=dc --function-level=2016
```

Примечание

Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2 (см. Повышение уровня схемы, функционального уровня домена).

Примечание

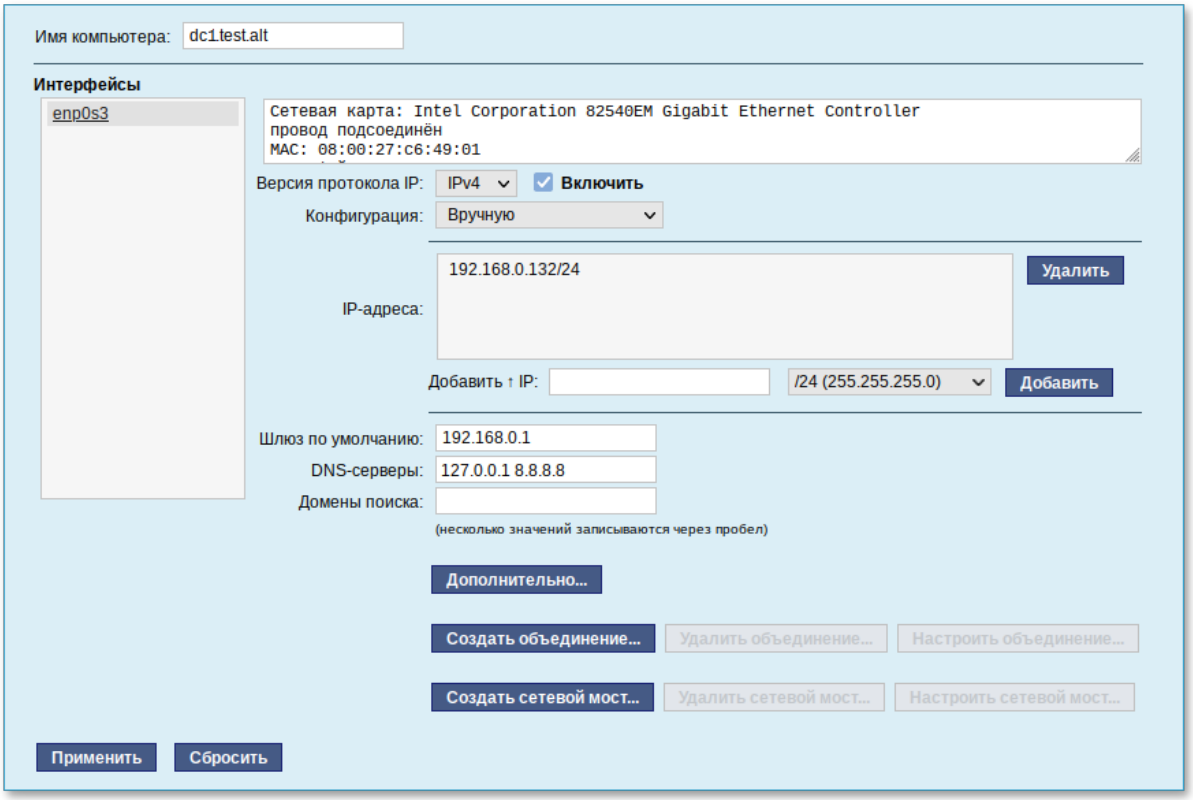
Некоторые параметры команды **samba-tool domain provision** приведены в в табл. Основные опции для samba-tool domain provision. Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

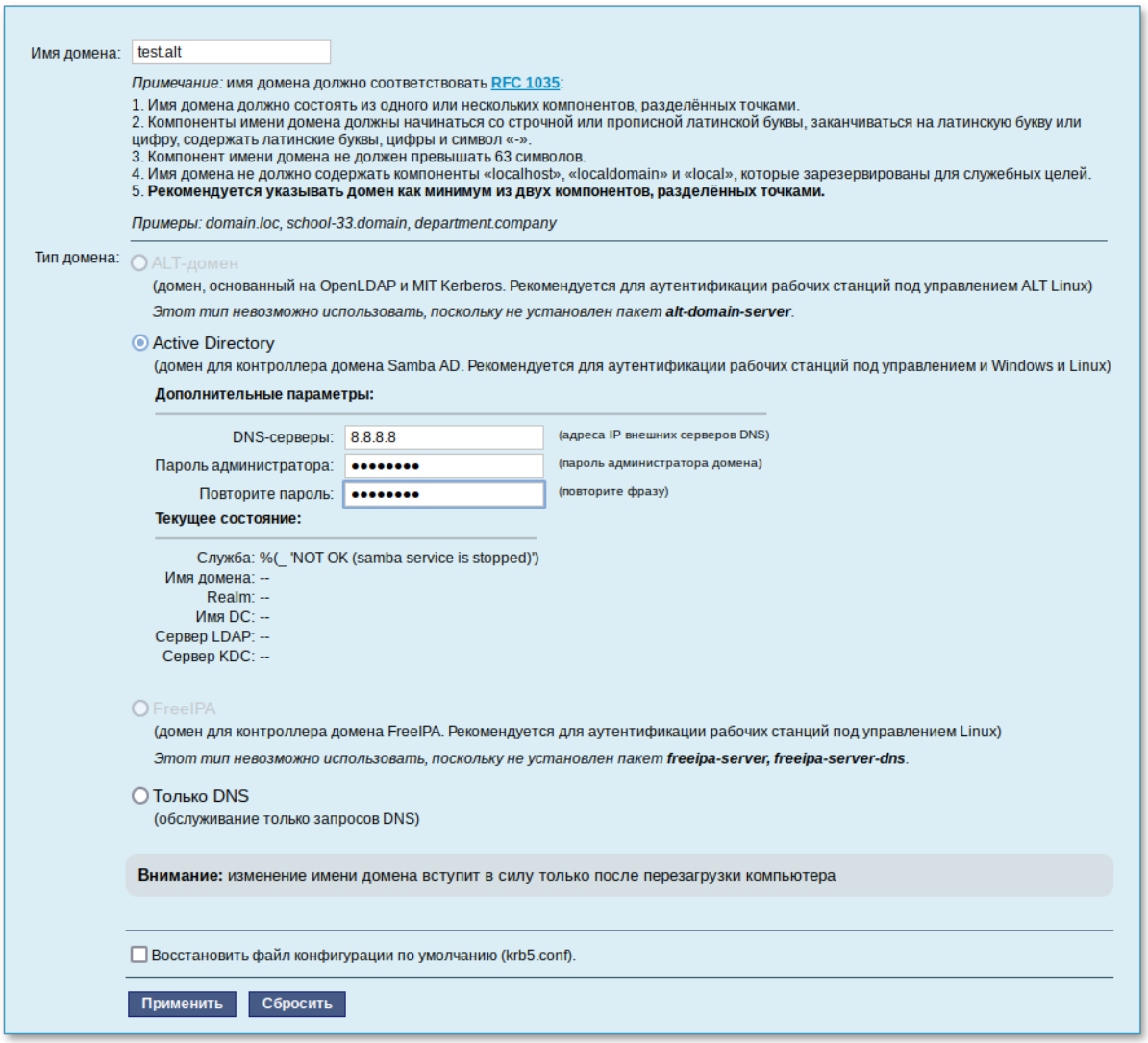
5.7.3.3. Создание домена в ЦУС

При инициализации домена в веб-интерфейсе Центра управления системой (см. ЦУС) следует выполнить следующие действия:

1. В модуле **Ethernet-интерфейсы** указать имя компьютера и DNS 127.0.0.1:



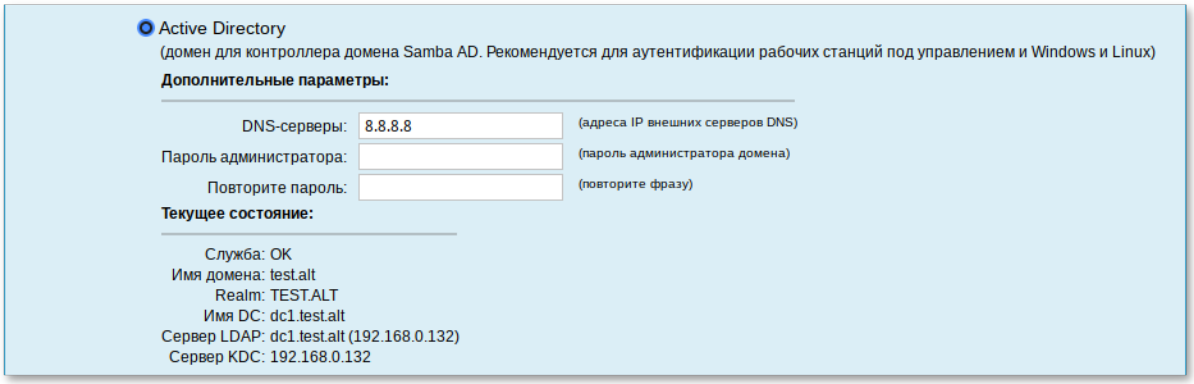
2. В модуле **Домен** указать имя домена, отметить пункт **`Active Directory`**, указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку **Применить**:



Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, — это одна из причин завершения развертывания домена ошибкой.

3. После успешного создания домена, будет выведена информация о домене:



4. Перегрузить сервер для применения изменений.

5.7.4. Запуск службы каталогов

Установить службу samba запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Примечание

Если служба после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание

Пример файла **/etc/samba/smb.conf** после создания домена с SAMBA_INTERNAL:

```
# Global parameters
[global]
        dns forwarder = 8.8.8.8
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        workgroup = TEST
        idmap_ldb:use rfc2307 = yes

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

5.8. Домен с BIND9_DLZ

В состав Samba входит модуль BIND9_DLZ, позволяющий использовать в качестве DNS-сервера решение с открытым исходным кодом BIND 9.

BIND 9 представляет собой полнофункциональную реализацию протокола DNS, включающую поддержку DNSSEC, DNS over HTTPS (DoH) и DNS over TLS (DoT).

Служба DNS может разворачиваться как на отдельном сервере, так и на контроллере домена совместно с Samba.

Работа с внешним сервером DNS осуществляется с помощью бэкенда BIND9_DLZ и используется в следующих случаях:

- сложная схема зон DNS;

- поддержка более одного сервера форвардинга (параметр ***dns forwarder*** на бэкенде SAMBA_INTERNAL работает только с одним адресом).

Если планируется настроить контроллер домена Samba AD с использованием серверной части BIND9_DLZ, необходимо сначала установить и настроить DNS-сервер BIND.

5.8.1. Настройка DNS-сервера BIND

На сервере должны быть установлены пакеты *bind* и *bind-utils*:

```
# apt-get install bind bind-utils
```

Примечание

Пакет *bind* содержит различные утилиты, связанные с DNS, например:

- **named-checkconf** — проверка синтаксиса файлов конфигурации;
- **named-checkzone** — проверка файлов зон DNS;
- **rndc** — инструмент управления службой DNS.

Пакет *bind-utils* содержит следующие утилиты:

- **dig** — многофункциональный инструмент для опроса DNS-серверов;
- **host** — позволяет получить информацию о DNS-связях между доменными именами и IP-адресами;
- **nslookup** — позволяет получить информацию DNS об удаленном сервере;
- **nsupdate** — инструмент для динамического обновления записей DNS.

Примечание

Основные файлы настройки DNS и некоторые параметры конфигурационного файла bind описаны в разделе Bind. Для получения более подробной информации следует обратиться к man странице **named.conf(5)**.

Настройка BIND9 для работы с Альт Домен:

1. Отключить chroot:

```
# control bind-chroot disabled
```

2. Отключить KRB5RCACHETYPE:

```
#
grep -q KRB5RCACHETYPE /etc/sysconfig/bind || echo 'KRB5RCACHETYPE="none"'
>> /etc/sysconfig/bind
```

3. Подключить плагин BIND_DLZ:

```
# grep -q 'bind-dns' /etc/bind/named.conf || echo 'include "/var/lib/samba/
bind-dns/named.conf";' >> /etc/bind/named.conf
```

4. Отредактировать файл **`/etc/bind/options.conf`**:

- в раздел *options* добавить строки:

```
tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
minimal-responses yes;
```

- в параметре **`forwarders`** указать сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне (если этой информации нет в файле **`/etc/bind/resolvconf-options.conf`**):

```
forward first;
forwarders { 8.8.8.8; };
```

- в параметр **`listen-on`** добавить IP-адрес DNS-сервера, на котором он будет принимать запросы;
- раскомментировать параметр **`allow-query`** и указать в нём подсети, из которых разрешено подавать запросы;
- раскомментировать параметр **`allow-recursion`** и указать в нём подсети, из которых будут обрабатываться рекурсивные запросы;
- в раздел *logging* добавить строку:

```
category lame-servers {null;};
```

Пример файла **`/etc/bind/options.conf`**:

```
options {
        version "unknown";
        directory "/etc/bind/zone";
        dump-file "/var/run/named_dump.db";
        statistics-file "/var/run/named.stats";
        recursing-file "/var/run/recursing";


        // disables the use of a PID file
        pid-file none;
        tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
        minimal-responses yes;

        listen-on { 127.0.0.1; 192.168.0.132; };
        listen-on-v6 { ::1; };

        include "/etc/bind/resolvconf-options.conf";

        allow-query { localnets; 192.168.0.0/24; };
        allow-recursion { localnets; 192.168.0.0/24; };

        //max-cache-ttl 86400;

};

logging {
        category lame-servers {null;};
};
```

5. В файле **/etc/bind/resolvconf-options.conf** в параметре **forwarders** должен быть указан DNS-сервер, на который будут перенаправляться запросы клиентов;

6. Выполнить остановку **bind**:

```
# systemctl stop bind
```

5.8.2. Восстановление к начальному состоянию Samba

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

Предупреждение

Перед созданием домена необходимо обязательно удалить **/etc/samba/smb.conf**:

```
# rm -f /etc/samba/smb.conf
```

5.8.3. Создание домена

5.8.3.1. Интерактивное создание домена

Для запуска интерактивной установки необходимо выполнить команду:

```
# samba-tool domain provision
```

В ответе на первые два вопроса нужно указать доменное имя и имя рабочей группы:

```
Realm [TEST.ALT]:
Domain [TEST]:
```

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **Enter**.

Далее нужно указать тип серверной роли и бэкенд DNS-сервера:

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
BIND9_DLZ
```

Задать пароль для администратора:

```
Administrator password:
Retype password:
```

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, — это одна из причин завершения развертывания домена ошибкой.

Начнётся процесс конфигурации:

```
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=test,DC=alt
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test,DC=alt
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
See /var/lib/samba/bind-dns/named.conf for an example configuration include file
for BIND
and /var/lib/samba/bind-dns/named.txt for further documentation required for
secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
The Kerberos KDC configuration for Samba AD is located at /var/lib/samba/private/
kdc.conf
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/
samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
```

```
Hostname:               dc1
NetBIOS Domain:         TEST
DNS Domain:             test.alt
DOMAIN SID:             S-1-5-21-3684382553-2825304832-3399765044
```

5.8.3.2. В пакетном режиме

Для пакетной установки необходимо указать следующие параметры:

- **`--realm REALM_NAME`** — имя области Kerberos (LDAP) и DNS имя домена;
- **`--domain=DOMAIN`** — имя домена (имя рабочей группы);
- **`--adminpass=PASSWORD`** — пароль основного администратора домена;
- **`--server-role=ROLE`** — тип серверной роли;
- **`--dns-backend=NAMESERVER-BACKEND`** — бэкенд DNS-сервера;
- **`--use-rfc2307`** — позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux.

Примечание

Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов. Пароль, не полностью соответствующий требованиям, — это одна из причин завершения развертывания домена ошибкой.

Так как в роли DNS-сервера Samba используется Bind, то при создании домена нужно использовать параметр ***`--dns-backend=BIND9_DLZ`***.

Пример команды создания контроллера домена test.alt в пакетном режиме:

```
# samba-tool domain provision --realm=test.alt --domain test --adminpass='Pa$
$word' --dns-backend=BIND9_DLZ --server-role=dc
```

Если уровень не указан, то домен разворачивается на уровне 2008_R2. Для разворачивания домена на другом уровне, уровень необходимо явно указать, например:

```
# samba-tool domain provision --realm=test.alt --domain=test --adminpass='Pa$
$word' --dns-backend=BIND9_DLZ --option="ad dc functional level = 2016" --server-
role=dc --function-level=2016
```

Примечание

Если необходим уровень 2012_R2, то следует сначала развернуть домен на уровне 2008_R2, а затем повысить его до 2012_R2 (см. Повышение уровня схемы, функционального уровня домена).

Примечание

Некоторые параметры команды **samba-tool domain provision** приведены в в табл. Основные опции для samba-tool domain provision. Полный список параметров можно увидеть, запустив команду:

```
# samba-tool domain provision --help
```

5.8.4. Запуск служб samba и bind

Установить службы **samba** и **bind** запускаемыми по умолчанию и запустить их:

```
# systemctl enable --now samba
# systemctl enable --now bind
```

Примечание

Если служба **samba** после установки никаким способом не запускается, необходимо перезагрузить сервер.

Примечание

Пример файла **/etc/samba/smb.conf** после создания домена с BIND9_DLZ:

```
# Global parameters
[global]
        netbios name = DC1
        realm = TEST.ALT
        server role = active directory domain controller
        server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl,
winbindd, ntp_signd, kcc, dnsupdate
        workgroup = TEST

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[netlogon]
        path = /var/lib/samba/sysvol/test.alt/scripts
        read only = No
```

5.8.5. Проверка зон

Следующие примеры запрашивают службу DNS о локальном хосте (127.0.0.1).

Проверка зоны перенаправления localhost:

```
# host -t A localhost 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
localhost has address 127.0.0.1
```

Проверка реверсивной зоны 0.0.127.in-addr.arpa.:

```
# host -t PTR 127.0.0.1 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
1.0.0.127.in-addr.arpa domain name pointer localhost.
```

5.9. Настройка Kerberos

После создания домена необходимо внести изменения в файл **/etc/krb5.conf**. В этом файле следует раскомментировать строку *default_realm* и содержимое разделов *realms* и *domain_realm* и указать название домена (следует обратить внимание на регистр символов), в строке *dns_lookup_realm* должно быть установлено значение false:

```
includedir /etc/krb5.conf.d/

[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
# admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT
# default_ccache_name = KEYRING:persistent:%{uid}

[realms]
TEST.ALT = {
default_domain = test.alt
}

[domain_realm]
dc = TEST.ALT
```

Примечание

В момент создания домена Samba конфигурирует шаблон файла **krb5.conf** для домена в каталоге **/var/lib/samba/private/**. Можно просто заменить этим файлом файл, находящийся в каталоге **/etc/**:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

5.10. Проверка работоспособности домена

Просмотр общей информации о домене:

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC1
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Просмотр предоставляемых служб:

```
# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

Sharename       Type      Comment
---------       ----      -------
sysvol          Disk
netlogon        Disk
IPC$            IPC       IPC Service (Samba 4.19.9)
SMB1 disabled -- no workgroup available
```

Создаваемые по умолчанию общие ресурсы netlogon и sysvol нужны для функционирования контроллера домена и создаются в **`smb.conf`** в процессе развертывания/модернизации.

Проверка конфигурации DNS:

- проверка наличия nameserver 127.0.0.1 в **`/etc/resolv.conf`**:

```
# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search test.alt
nameserver 127.0.0.1

# host test.alt
test.alt has address 192.168.0.132
```

- проверка имён хостов:
  - адрес **_kerberos._udp.***адрес домена с точкой:

```
# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

  - адрес **_ldap._tcp.***адрес домена с точкой:

```
# host -t SRV _ldap._tcp.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
```

- адрес **адрес хоста.***адрес домена с точкой:

```
# host -t A dc1.test.alt.
dc1.test.alt has address 192.168.0.132
```

Если имена не находятся, следует проверить выключение службы **bind** (если не включен плагин BIND9_DLZ).

Проверка Kerberos (имя домена должно быть в **верхнем регистре**):

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
Warning: Your password will expire in 15 days on Пт 12 апр 2024 11:46:29
```

Просмотр полученного билета:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
renew until 28.03.2024 14:14:32
```

Глава 6. Присоединение к домену в роли контроллера домена

6.1. Заведение дополнительного контроллера домена с бэкендом SAMBA_INTERNAL

6.2. Заведение дополнительного контроллера домена с бэкендом BIND9_DLZ

6.3. Проверка результатов присоединения

6.4. Настройка NTP-сервера

Для обеспечения отказоустойчивости и балансировки нагрузки в домен могут добавляться дополнительные контроллеры домена.

Системные требования к дополнительному DC такие же, как и для первого DC (см. Системные требования к серверу (контроллеру домена)).

Примечание

В терминологии контроллеров домена нет понятия PDC/BDC, т.е. все контроллеры равны, но один из них выступает владельцем ролей FSMO (см. Просмотр и передача ролей FSMO).

На дополнительном домене необходимо настроить NTP для работы в режиме сервер (см. Настройка NTP-сервера).

Заведение дополнительного контроллера домена выполняется путём присоединения дополнительного DC к существующему домену.

Команда присоединения к домену в роли контроллера домена:

```
# samba-tool domain join <dnsdomain> [DC|RODC|MEMBER] [options]
```

Некоторые параметры, используемые в команде **samba-tool domain join**:

- **--realm REALM_NAME** — имя области Kerberos (LDAP), и DNS имя домена;
- **--dns-backend=NAMESERVER-BACKEND** — бэкенд DNS-сервера: SAMBA_INTERNAL — встроенный сервер имен (по умолчанию), BIND9_DLZ — использует Samba AD для хранения информации о зоне, NONE — полностью пропускает настройку DNS (этот DC не будет DNS-сервером);

Примечание

На втором DC необходимо иметь DNS-бэкенд аналогичный первому DC.

Примечание

При использовании SAMBA_INTERNAL, необходимо указать значение ***dns forwarder***, чтобы на новом сервере была настроена пересылка запросов:

```
--option="dns forwarder=forwarder_ip_address"
```

Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex, например:

```
--option="dns forwarder=8.8.8.8"
```

- **--option='idmap_ldb:use rfc2307 = yes'** — если первый контроллер домена создавался с ключом **--rfc2307**, то и для текущего необходимо это учесть, указав данный параметр;
- **--site=SITE** — привязка контроллера домена к определенному сайту AD;
- **--option="interfaces= lo eth0" --option="bind interfaces only=yes"** — привязка Samba к указанным сетевым интерфейсам сервера (если их несколько); указание данной опции позволяет **samba-tool** зарегистрировать корректный IP-адрес при присоединении;
- **--option="ad dc functional level = LEVEL"** — функциональный уровень AD. Возможные значения: 2008_R2 (по умолчанию), 2012, 2012_R2.

Примечание

При присоединении к существующему домену рекомендуется указывать функциональный уровень не выше текущего уровня домена.

Примечание

Для получения дополнительной информации о параметрах команды **samba-tool domain join** можно воспользоваться командой:

```
# samba-tool domain join --help
```

Для сервера, на котором будет разворачиваться контроллер домена, должен быть назначен статический IP-адрес и установлено правильное имя узла.

В следующей таблице представлены параметры, используемые в качестве примера в данном разделе.

Таблица 6.1. Параметры контроллеров домена

	IP-адрес	Полное доменное имя (FQDN)
Существующий DC	192.168.0.132	dc1.test.alt
Добавляемый DC	192.168.0.133	dc2.test.alt

Установить имя узла можно, выполнив команду:

```
# hostnamectl set-hostname dc2.test.alt
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

6.1. Заведение дополнительного контроллера домена с бэкендом SAMBA_INTERNAL

Все действия, указанные ниже, выполняются на узле dc2.test.alt (192.168.0.133), если не указано иное.

Примечание

Для выполнения операции присоединения к домену требуется пароль администратора домена.

Этапы настройки сервера и присоединения к домену в роли контроллера домена:

1. Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2. На добавляемом DC в **/etc/resolv.conf** обязательно должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.132" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

3. Остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

4. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

5. На существующем контроллере домена завести IP-адрес для нового DC (команда выполняется на узле dc1.test.alt):

```
# samba-tool dns add 192.168.0.132 test.alt DC2 A 192.168.0.133
-Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примечание

Синтаксис команды **samba-tool dns add** см. в разделе Администрирование DNS

6. На новом контроллере домена установить следующие параметры в файле конфигурации клиента Kerberos (**/etc/krb5.conf**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

7. Запросить билет Kerberos администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Предупреждение

Имя домена должно быть указано в верхнем регистре.

Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

8. Ввести дополнительный DC в домен test.alt в качестве контроллера домена:

```
# samba-tool domain join test.alt DC -Uadministrator \
--realm=test.alt --option="dns forwarder=8.8.8.8"
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-3293631772) as a DC
```

9. Установить службу **samba** запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

6.2. Заведение дополнительного контроллера домена с бэкендом BIND9_DLZ

Все действия, указанные ниже, выполняются на узле dc2.test.alt (192.168.0.133), если не указано иное.

Примечание

Для выполнения операции присоединения к домену требуется пароль администратора домена.

Этапы настройки сервера и присоединения к домену в роли контроллера домена с бэкендом BIND9_DLZ:

1. Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2. Установить и настроить DNS-сервер BIND (см. Настройка DNS-сервера BIND);

3. На добавляемом DC в **/etc/resolv.conf** обязательно должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.132" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

4. Остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

5. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

6. На существующем контроллере домена завести IP-адрес для нового DC (команда выполняется на узле dc1.test.alt):

```
# samba-tool dns add 192.168.0.132 test.alt DC2 A 192.168.0.133
-Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примечание

Синтаксис команды **samba-tool dns add** см. в разделе Администрирование DNS

7. На новом контроллере домена установить следующие параметры в файле конфигурации клиента Kerberos (**/etc/krb5.conf**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true
```

8. Запросить билет Kerberos администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Предупреждение

Имя домена должно быть указано в верхнем регистре.

Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

9. Ввести дополнительный DC в домен test.alt в качестве контроллера домена:

```
# samba-tool domain join test.alt DC -Uadministrator \
--realm=test.alt --dns-backend=BIND9_DLZ
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-80639820-2350372464-3293631772) as a DC
```

10. Установить службы **samba** и **bind** запускаемыми по умолчанию и запустить их:

```
# systemctl enable --now samba
# systemctl enable --now bind
```

6.3. Проверка результатов присоединения

Примечание

После присоединения к домену службе синхронизации данных может понадобиться до 15 минут для автоматического формирования подключений для репликации.

Проверка корректности присоединения:

1. Проверить работу DNS:

```
# host -t A test.alt
test.alt has address 192.168.0.132
test.alt has address 192.168.0.133
```

   В списке адресов должен отображаться IP-адрес добавленного контроллера домена.

2. Проверить статус репликации между контроллерами домена. Для этого на добавленном DC выполнить команду:

```
# samba-tool drs showrepl --summary
```

   В случае успешного выполнения репликации в каждом из блоков в разделах «INBOUND NEIGHBORS» и «OUTBOUND NEIGHBORS» отображаются сообщения вида:

```
Default-First-Site-Name\DC1 via RPC
    DSA object GUID: 10e22808-960e-4cb3-8724-abd2223555cd
    Last attempt @ Sat Jun 15 10:27:21 2024 EET was successful
    0 consecutive failure(s).
    Last success @ Sat Jun 15 10:27:21 2024 EET
```

   В пункте *Last attempt* должны стоять актуальные дата и время, идентичные указанным в строке *Last success* (отображает время последней репликации). Также должно быть «0 consecutive failure(s)».

   Подробнее о настройке репликации см. в разделе Репликация.

3. На добавленном DC создать нового пользователя домена:

```
# samba-tool user add testuser --random-password
User 'testuser' added successfully
```

4. Убедиться, что учетная запись созданного пользователя доступна на первом контроллере домена:

```
# samba-tool user list | grep testuser
testuser
```

6.4. Настройка NTP-сервера

Настроить NTP для работы в режиме сервер (Настройка NTP-сервера).

Глава 7. Контроллер домена на чтение (RODC)

7.1. Установка и настройка RODC

7.2. Политики репликации и кеширования паролей на RODC

7.3. Проверка репликации пароля пользователя на сервере RODC

При присоединении к домену для контроллера может быть выбрана роль RODC (read-only domain controller).

Основная цель контроллера домена, доступного только на чтение, — возможность безопасной установки собственного контроллера домена в удаленных филиалах, в которых сложно обеспечить физическую защиту сервера. Контроллер домена RODC содержит копию базы Альт Домен, доступную только на чтение. Это означает, что никто, даже при получении физического доступа к такому контроллеру домена, не сможет изменить данные в Альт Домен (в том числе сбросить пароль администратора домена).

Основные отличия RODC от обычных контроллеров домена, доступных для записи (RWDC):

- RODC хранит копию базы Альт Домен, доступную только для чтения. Клиенты не могут вносить изменения в базу такого контроллера домена;
- RODC не реплицирует данные Альт Домен на другие контроллеры домена (RWDC) (используется односторонняя репликация);
- контроллер RODC хранит полную копию базы Альт Домен, за исключением хешей паролей объектов Альт Домен и других атрибутов, содержащих чувствительную информацию;
- при получении контроллером RODC запроса на аутентификацию от пользователя, он перенаправляет этот запрос на ближайший RWDC контроллер;
- контроллер RODC может кешировать учетные данные некоторых пользователей (это ускоряет аутентификацию и позволяет пользователям авторизоваться на контроллере домена, даже при отсутствии связи с RWDC);
- DNS служба на RODC работает только на чтение.

Требования, которые должны быть выполнены для разворачивания RODC:

- на сервере должен быть назначен статический IP-адрес;
- уровень функциональности леса и домена должен быть не ниже 2008 R2. Проверить текущие уровни можно, выполнив на контроллере домена команду:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

- в качестве DNS сервера должен быть указан ближайший RWDC контроллер.

7.1. Установка и настройка RODC

Таблица 7.1. Параметры контроллеров домена

	IP-адрес	Полное доменное имя (FQDN)
Существующий RWDC	192.168.0.132	dc1.test.alt
Добавляемый RODC	192.168.0.134	rodc.test.alt

Для сервера, на котором будет разворачиваться контроллер домена, должен быть назначен статический IP-адрес и установлено правильное имя узла.

Установить имя узла можно, выполнив команду:

```
# hostnamectl set-hostname rodc.test.alt
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

Все дальнейшие действия выполняются на узле rodc.test.alt (192.168.0.134), если не указано иное.

Этапы настройки сервера и присоединения к домену в роли RODC:

1. Установить пакет *task-samba-dc*, который установит все необходимое:

```
# apt-get install task-samba-dc
```

2. На RODC в **/etc/resolv.conf** должен быть добавлен первый DC как nameserver:

```
# echo "name_servers=192.168.0.132" >> /etc/resolvconf.conf
# echo "search_domains=test.alt" >> /etc/resolvconf.conf
# resolvconf -u
# cat /etc/resolv.conf
search test.alt
nameserver 192.168.0.132
nameserver 8.8.8.8
```

3. Остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
# for service in smb nmb krb5kdc slapd bind; do systemctl disable $service;
systemctl stop $service; done
```

4. Очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
# rm -f /etc/samba/smb.conf
# rm -rf /var/lib/samba
# rm -rf /var/cache/samba
# mkdir -p /var/lib/samba/sysvol
```

5. На существующем контроллере домена завести IP-адрес для RODC (команда выполняется на узле dc1.test.alt):

```
# samba-tool dns add 192.168.0.132 test.alt RODC A 192.168.0.134
-Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

Предупреждение

Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примечание

Синтаксис команды **samba-tool dns add** см. в разделе Администрирование DNS

6. На RODC установить следующие параметры в файле конфигурации клиента Kerberos (**/etc/krb5.conf**):

```
[libdefaults]
default_realm = TEST.ALT
dns_lookup_realm = false
dns_lookup_kdc = true

[realms]
TEST.ALT = {
kdc = rodc.test.alt
kdc = dc1.test.alt
default_domain = TEST.ALT
}
```

7. Для проверки настройки запросить билет Kerberos для администратора домена:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

Предупреждение

Имя домена должно быть указано в верхнем регистре.

8. Убедиться, что билет получен:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

9. Ввести данный DC в домен test.alt в качестве контроллера домена, доступного только для чтения (RODC):

```
# samba-tool domain join test.alt RODC -Uadministrator@TEST.ALT \
--realm=test.alt --option="dns forwarder=8.8.8.8"
```

Если всё нормально, в конце будет выведена информация о присоединении к домену:

```
Joined domain TEST (SID S-1-5-21-578923263-1107570656-1287136478) as an RODC
```

Примечание

При использовании SAMBA_INTERNAL, необходимо указать значение ***dns forwarder***, чтобы на новом сервере была настроена пересылка запросов. Форвардером может быть как вышестоящий DNS-сервер организации, так и публичные от google или yandex, например:

```
--option="dns forwarder=8.8.8.8"
```

Если первый контроллер домена создавался с ключом **--rfc2307**, то и для текущего необходимо это учесть, указав параметр:

```
--option='idmap_ldb:use rfc2307 = yes'
```

10. Сделать службу **samba** запускаемой по умолчанию и запустить её:

```
# systemctl enable --now samba
```

Примечание

Для получения дополнительной информации о параметрах команды **samba-tool domain join** можно воспользоваться командой:

```
# samba-tool domain join --help
```

7.2. Политики репликации и кеширования паролей на RODC

На RODC можно задать список пользователей, чьи хеши паролей можно или нельзя реплицировать на данный контроллер домена.

Примечание

Все пользователи в кеше RODC смогут аутентифицироваться на этом контроллере домена, даже если отсутствует связь с RWDC.

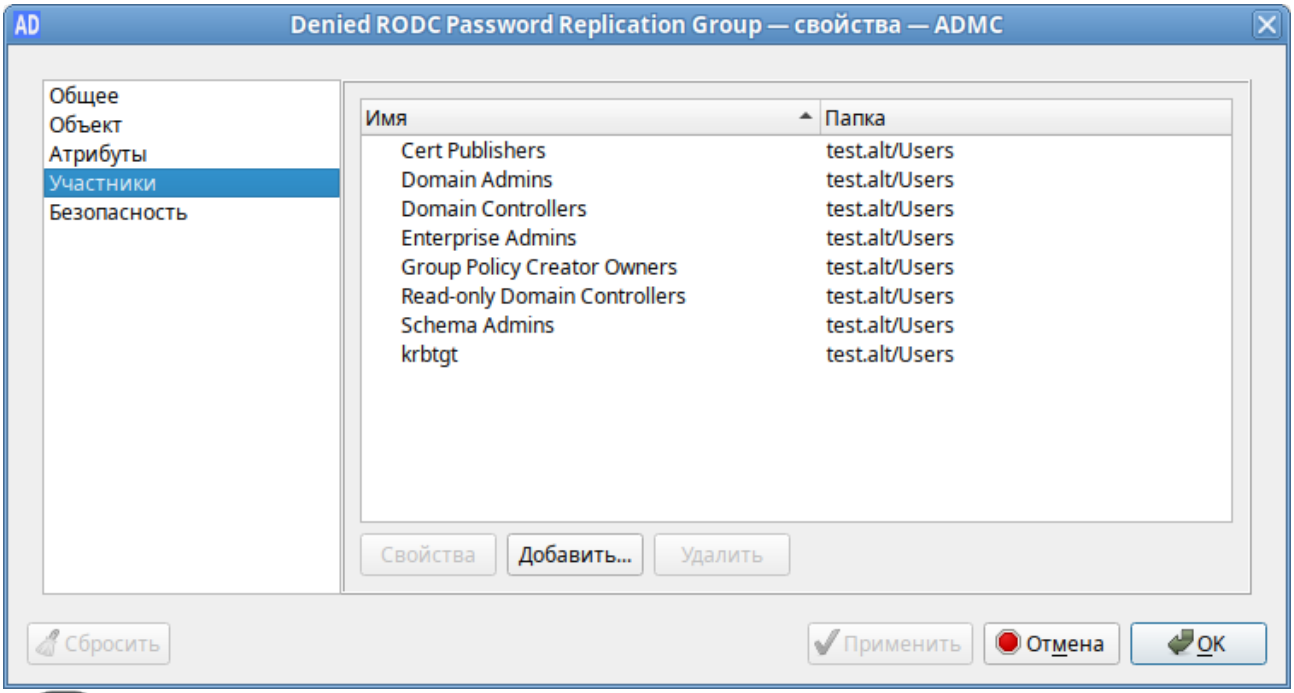
По умолчанию в домене создаются две новые глобальные группы:

- Allowed RODC Password Replication Group

- Denied RODC Password Replication Group

Первая группа по умолчанию пуста, а во второй содержатся административные группы безопасности, пароли пользователей которых нельзя реплицировать и кешировать на RODC. В группу *Denied RODC Password Replication Group* по умолчанию входят группы:

- Cert Publishers
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Group Policy Creator Owners
- Read-only Domain Controllers
- Schema Admins
- учётная запись krbtgt



Примечание

Список участников групп *Denied RODC Password Replication Group* и *Allowed RODC Password Replication Group*:

```
# samba-tool group listmembers "Denied RODC Password Replication Group"
Read-only Domain Controllers
Domain Admins
Enterprise Admins
Domain Controllers
Schema Admins
krbtgt
```

```
Group Policy Creator Owners
Cert Publishers

# samba-tool group listmembers "Allowed RODC Password Replication Group"
```

В группу *Allowed RODC Password Replication Group* обычно добавляются группы пользователей филиала, в котором находится RODC.

Для предварительной загрузки данных учетных записей на контроллере RODC используется команда:

```
# samba-tool rodc preload (<SID>|<DN>|<accountname>)+ ... [опции]
```

Возможные опции:

- **`--server`** — обычный контроллер домена, который будет выступать источником данных при репликации;
- **`--file`** — имя файла со списком реплицируемых объектов, либо «-» для ввода списка через стандартный поток ввода (stdin);
- **`--ignore-errors`** — игнорировать ошибки репликации при загрузке нескольких объектов.

Эта команда запускает процесс репликации данных указанных объектов с переданного в параметре **`--server`** контроллера домена. Для идентификации объектов могут использоваться идентификаторы безопасности (SID), DN или имена учетных записей SAM (samAccountName).

Для передачи списка объектов может использоваться:

- перечисление объектов списком через пробел;
- файл (одна строка соответствует одному объекту);
- stdin (одна строка соответствует одному объекту).

Примечание

Для получения дополнительной информации о параметрах команды **`samba-tool rodc preload`** можно воспользоваться командой:

```
# samba-tool rodc preload --help
```

7.3. Проверка репликации пароля пользователя на сервере RODC

Тестирование репликации пароля пользователя на сервере RODC:

1. На обычном контроллере домена (в примере DC1) создать пользователя и добавить его в группу *Allowed RODC Password Replication Group* (пароли пользователей/групп, входящих в группу *Allowed RODC Password Replication Group* разрешено реплицировать на RODC):

```
# samba-tool user add ivanov --given-name='Иван' \
--surname='Иванов' --mail-address='ivanov@test.alt'

New Password:
Retype Password:
User 'ivanov' added successfully

# samba-tool group addmembers "Allowed RODC Password Replication Group"
ivanov

Added members to group Allowed RODC Password Replication Group
```

2. На RODC проверить возможность загрузки кеша пароля, выполнив команду:

```
# samba-tool rodc preload ivanov --server=dc1.test.alt

Replicating DN CN=Иван Иванов,CN=Users,DC=test,DC=alt
Exop on[CN=Иван Иванов,CN=Users,DC=test,DC=alt] objects[1] linked_values[0]
```

Пример получения билета при отсутствии связи с RWDC (пользователь ivanov есть в кеше RODC, а пользователь kim — нет):

```
$ kinit ivanov
Password for ivanov@TEST.ALT:

$ kinit kim
kinit: A service is not available that is required to process the request while
getting initial credentials
```

Глава 8. Редактирование существующего домена

8.1. Повышение уровня схемы, функционального уровня домена

8.2. Включение RFC2307 после разворачивания домена

8.3. Изменение DNS бэкенда контроллера домена

8.1. Повышение уровня схемы, функционального уровня домена

Просмотреть текущий уровень домена и леса можно, выполнив команду:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Для повышения уровня домена необходимо выполнить следующие действия:

1. Указать функциональный уровень AD, который будет поддерживаться контроллером домена, в параметре ***ad dc functional level*** файла **/etc/samba/smb.conf**. Возможные значения:

   - 2008_R2 — аналог функционального уровня Windows 2008 R2 (по умолчанию);
   - 2012 — аналог функционального уровня Windows 2012;
   - 2012_R2 — аналог функционального уровня Windows 2012 R2;
   - 2016 — аналог функционального уровня Windows 2016.

2. Обновить схему домена, выполнив команду:

   ```
   # samba-tool domain schemaupgrade --schema=<SCHEMA>
   ```

   где SCHEMA — схема, до которой необходимо выполнить обновление (по умолчанию 2019).

3. Подготовить функциональный уровень домена, выполнив команду:

   ```
   # samba-tool domain functionalprep --function-level=<FUNCTION_LEVEL>
   ```

   где FUNCTION_LEVEL — функциональный уровень, к которому нужно подготовиться (по умолчанию 2016).

4. Указать функциональные уровни домена и леса, выполнив команду:

   ```
   # samba-tool domain level raise --domain-level=<DOMAIN_LEVEL> --forest-level=<FOREST_LEVEL>
   ```

   где:

   - FOREST_LEVEL — уровень работы леса. (возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016);
   - DOMAIN_LEVEL — уровень работы домена. (возможные значения: 2003, 2008, 2008_R2, 2012, 2012_R2, 2016).

Примечание

При установке значения параметра ***ad dc functional level*** в файле **/etc/samba/smb.conf** вручную, защита от несовпадения функций между контроллерами домена снижается. Поэтому на всех контроллерах домена должна использоваться одна и та же версия Samba, чтобы гарантировать, что поведение, наблюдаемое клиентом, будет одинаковым независимо от того, к какому контроллеру домена осуществляется соединение.

Пример повышения уровня домена до 2016:

- в раздел [global] файла **/etc/samba/smb.conf** добавить строку:

```
ad dc functional level = 2016
```

- перезагрузить службу samba:

```
# systemctl restart samba.service
```

- обновить схему домена:

```
# samba-tool domain schemaupgrade --schema=2019
```

- подготовить функциональный уровень домена:

```
# samba-tool domain functionalprep --function-level=2016
```

- повысить функциональные уровни домена и леса до 2016:

```
# samba-tool domain level raise --domain-level=2016 --forest-level=2016
Domain function level changed!
Forest function level changed!
All changes applied successfully!
```

- убедиться, что уровни домена и леса повышены:

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=test,DC=alt'

Forest function level: (Windows) 2016
Domain function level: (Windows) 2016
Lowest function level of a DC: (Windows) 2016
```

8.2. Включение RFC2307 после разворачивания домена

Примечание

До запуска этой процедуры следует убедиться, что она необходима.

Проверка того, что расширения NIS установлены в AD:

```
# ldbsearch -H /var/lib/samba/private/sam.ldb -s base -b
CN=ypservers,CN=ypServ30,CN=RpcServices,CN=System,DC=test,DC=alt cn

# record 1
dn: CN=ypservers,CN=ypServ30,CN=RpcServices,CN=System,DC=test,DC=alt
cn: ypservers

# returned 1 records
# 1 entries
# 0 referrals
```

Если команда **ldbsearch** возвращает одну запись (returned 1 records), расширения NIS установлены и больше ничего делать не нужно.

Предупреждение

Обновление схемы может привести к поломке домена. Прежде чем обновлять схему, необходимо убедиться в наличии рабочей резервной копии.

Для установки расширения NIS необходимо выполнить следующие действия:

1. Найти контроллер домена (DC) с ролью (FSMO) хозяина схемы:

```
# samba-tool fsmo show | grep SchemaMasterRole
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

   В выводе команды показано имя DC, которому принадлежит эта роль. Все дальнейшие дествия следует выполнять на этом DC.

2. Остановить службу **samba**:

```
# systemctl stop samba
```

3. Создать копию файла схемы **ypServ30.ldif**, например:

```
# cp /usr/share/samba/setup/ypServ30.ldif /tmp/
```

4. Заменить переменные в скопированном файле LDIF именем домена (DN), именем NetBIOS и доменом NIS вашей установки, например:

```
#
sed -i -e 's/\${DOMAINDN}/DC=test,DC=alt/g' -e 's/\${NETBIOSNAME}/DC/g' -e
's/\${NISDOMAIN}/test/g' /tmp/ypServ30.ldif
```

5. Импортировать измененный файл LDIF в локальную базу данных Samba **/var/lib/samba/private/sam.ldb**:

```
# ldbmodify -H /var/lib/samba/private/sam.ldb /tmp/ypServ30.ldif --
option="dsdb:schema update allowed"=true
```

6. В файл **/etc/samba/smb.conf** в секцию **[global]** добавить параметр:

```
idmap_ldb:use rfc2307 = yes
```

7. Запустить службу каталогов:

```
# systemctl start samba
```

AD реплицирует обновленную схему на все контроллеры домена в лесу.

8.3. Изменение DNS бэкенда контроллера домена

Samba позволяет переключаться между бэкендом SAMBA_INTERNAL и BIND9_DLZ на контроллере домена без потери данных.

8.3.1. Миграция с SAMBA_INTERNAL на BIND9_DLZ

Для переключения с SAMBA_INTERNAL на BIND9_DLZ на контроллере домена необходимо выполнить следующие шаги:

1. Установить и настроить DNS-сервер BIND (см. Настройка DNS-сервера BIND);
2. Остановить службу samba:

```
# systemctl stop samba
```

3. Выполнить миграцию:

```
# samba_upgradedns --dns-backend=BIND9_DLZ
```

4. Отключить модуль SAMBA_INTERNAL в файле **/etc/samba/smb.conf**:
   - если в файле нет параметра ***server services***, добавить в секцию ***global*** строку:

     ```
     server services = -dns
     ```

   - если в секции ***global*** есть параметр ***server services***, удалить опцию **dns**, например:

     ```
     server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl,
     winbindd, ntp_signd, kcc, dnsupdate
     ```

5. Запустить службу **bind** и сделать её запускаемой по умолчанию:

```
# systemctl enable --now bind
```

6. Запустить службу **samba**:

```
# systemctl start samba
```

8.3.2. Миграция с BIND9_DLZ на SAMBA_INTERNAL

Для переключения с BIND9_DLZ на SAMBA_INTERNAL на контроллере домена необходимо выполнить следующие шаги:

1. Остановить службу **bind** и убрать её из автозагрузки:

```
# systemctl disable --now bind
```

2. Остановить службу **samba**:

```
# systemctl stop samba
```

3. Выполнить миграцию:

```
# samba_upgradedns --dns-backend=SAMBA_INTERNAL
```

4. Отключить модуль BIND9_DLZ в файле **/etc/samba/smb.conf**:

   - если в параметре ***server services*** есть только опция **-dns**, удалить этот параметр из файла (удалить всю строку):

     ```
     server services = -dns
     ```

   - если в секции ***global*** есть параметр ***server services***, добавить в него опцию **dns**, например:

     ```
     server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl,
     winbindd, ntp_signd, kcc, dnsupdate, dns
     ```

5. Запустить службу **samba**:

   ```
   # systemctl start samba
   ```

Примечание

Так как SAMBA_INTERNAL — это одна из настроек по умолчанию для параметра ***server services***, удаление параметра ***server services*** включает все серверы по умолчанию, включая DNS-сервер.

Глава 9. Отладочная информация

9.1. Настройка уровня журналирования Samba

9.2. Управление процессами

9.3. DNS

9.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в разделе Уровни журналирования.

9.2. Управление процессами

Для проверки выполнения процессов Samba можно использовать утилиту **ps**:

```
# ps axf | grep -E "samba|smbd|winbindd"
…
3078 ?        S      0:00 /usr/sbin/samba --no-process-group
   3091 ?        S      0:00  \_ /usr/sbin/samba --no-process-group
   3092 ?        S      0:00  |   \_ /usr/sbin/samba --no-process-group
   3096 ?        S      0:00  |       \_ /usr/sbin/samba --no-process-group
   3101 ?        Ss     0:00  |           \_ /usr/sbin/smbd -D --option=server
role check:inhibit=yes --foreground
   3138 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
   3139 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
```

```
option=server role check:inhibit=yes --foreground
   3149 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
   3150 ?        S      0:00  |               \_ /usr/sbin/smbd -D --
option=server role check:inhibit=yes --foreground
…
   3127 ?        Ss     0:00  |           \_ /usr/sbin/winbindd -D --
option=server role check:inhibit=yes --foreground
   3140 ?        S      0:00  |               \_ /usr/sbin/winbindd -D --
option=server role check:inhibit=yes --foreground
…
```

Все процессы **samba**, **smbd** и **winbindd** должны быть дочерними процессами одного процесса **samba**.

Если структура процесса не отображается:

- следует проверить файлы журнала Samba. Для подробного вывода можно увеличить уровень журнала (см. раздел Уровни журналирования);
- можно запустить Samba в интерактивном режиме и посмотреть на результат:

```
# samba -i
```

9.3. DNS

9.3.1. Устранение неполадок, связанных с серверной частью DNS

9.3.1.1. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Если клиенты не могут разрешать записи из зоны DNS AD, необходимо убедиться, что на клиенте указан IP-адрес DNS-сервера, способного разрешать зону AD DNS.

Если конфигурация клиента правильная, следует убедиться, что DNS-сервер Samba работает.

Если DNS-сервер Samba не запускается, необходимо убедиться, что ни один другой процесс не использует TCP- и UDP-порт 53:

- проверить файлы журнала Samba на наличие ошибок, связанных с DNS;
- убедиться, что никакой другой процесс не прослушивает TCP- и UDP-порт 53, например:

```
# ss -tulpn | grep ":53"
```

Если порт 53 занят другим процессом, необходимо:

- остановить службу, прослушивающую порт 53, и отключить её автоматический запуск во время загрузки;
- перезапустить службу каталогов.

9.3.1.2. Samba с BIND9_DLZ

Каталог **/var/lib/samba/bind-dns** создается только в том случае, если произошло одно из следующих трёх событий:

- при создании контроллера домена использовался параметр ***--dns-backend=BIND9_DLZ***;
- при подключении к домену использовался параметр ***--dns-backend=BIND9_DLZ***;
- домен был обновлён до Bind9 с помощью команды **samba_upgradedns** и опции ***--dns-backend=BIND9_DLZ***.

Глава 10. Удаление контроллера домена

10.1. Понижение роли онлайн-контроллера домена

10.2. Понижение автономного контроллера домена

10.3. Проверка

В некоторых ситуациях необходимо навсегда удалить контроллер домена из домена. Если для обычного участника домена достаточно просто удалить соответствующую учётную запись, то чтобы удалить контроллер из домена требуется понизить его роль (demoting).

Если роль контроллера домена будет понижена неправильно, домен может стать нестабильным. Например:

- могут начаться сбои репликации;
- оставшиеся контроллеры домена могут замедлять свою работу из-за тайм-аутов и неудачных попыток репликации;
- вход в систему доменных пользователей может завершиться ошибкой или занять больше времени.

10.1. Понижение роли онлайн-контроллера домена

Если удаляемый контроллер домена всё ещё работает правильно, для понижения его роли необходимо выполнить следующие действия (в примере понижается роль DC3):

1. Авторизоваться на контроллере домена под локальным пользователем.
2. Убедиться, что контроллер не владеет никакими ролями FSMO:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

```
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Если контроллеру домена принадлежит одна или несколько ролей FSMO, передать их другому контроллеру домена (см. Просмотр и передача ролей FSMO).

3. Вывести **`objectGUID`** контроллера домена:

```
#
ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs
objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена.

4. Понизить DC:

```
# samba-tool domain demote -Uadministrator
Using dc1.test.alt as partner server for the demotion
Password for [TEST\administrator]:
Deactivating inbound replication
Asking partner server dc1.test.alt to synchronize from us
Changing userControl and container
Removing Sysvol reference: CN=DC3,CN=Enterprise,CN=Microsoft System
Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=test.alt,CN=Microsoft System
Volumes,CN=System,CN=Configuration,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Domain System Volumes (SYSVOL
share),CN=File Replication Service,CN=System,DC=test,DC=alt
Removing Sysvol reference: CN=DC3,CN=Topology,CN=Domain System
Volume,CN=DFSR-GlobalSettings,CN=System,DC=test,DC=alt
updating ForestDnsZones.test.alt keeping 2 values, removing 1 values
updating test.alt keeping 6 values, removing 1 values

…
Demote successful
```

5. Остановить службу каталогов:

```
# systemctl stop samba
```

6. Если этот контроллер работал как доменный сервер DNS:

   остановить службу DNS:

```
# systemctl stop bind
```

- убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон AD DNS.

10.2. Понижение автономного контроллера домена

В определенных ситуациях, например, при сбое оборудования, из домена необходимо удалить контроллер домена, который больше недоступен. В этом случае понизить уровень контроллера домена, можно на оставшемся работающем контроллере домена Samba.

Важно

Эта процедура должна выполняться только в том случае, если контроллер домена, который нужно понизить, больше не подключен к AD, и его нельзя понизить так, как описано в разделе Понижение роли онлайн-контроллера домена. Это гарантирует, что все изменения (например, изменения паролей) будут реплицированы на другой контроллер домена. В противном случае такие изменения будут потеряны. Список изменений можно получить с помощью Samba-инструмента ldapcmp. При описанной ниже процедуре все изменения (например, изменения паролей) не будут реплицированы на работающий DC.

Важно

Нельзя понизить статус автономного удаленного контроллера домена с контроллера домена, на котором работает *Samba* 4.4 или более ранней версии.

Для понижения статуса неработающего контроллера домена необходимо выполнить следующие действия (в примере понижается статус DC3):

1. Авторизоваться на работающем контроллере домена.

2. Убедиться, что понижаемый контроллер не владеет никакими ролями FSMO:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS
Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

Если понижаемому контроллеру домена принадлежит одна или несколько ролей FSMO, захватить их локальным контроллером домена (см. Захват роли FSMO).

3. Убедиться, что понижаемый контроллер домена отключён.

4. Вывести **objectGUID** контроллера домена:

```
#
ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' --cross-ncs
objectguid | grep -A1 DC3
dn: CN=NTDS Settings,CN=DC3,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
objectGUID: 512f03b4-7042-434d-93c0-61dd6a2ea895
```

   Для того чтобы убедиться, что все записи DNS были удалены после понижения роли контроллера домена, необходимо знать имя хоста, IP-адрес и objectGUID контроллера домена.

5. Понизить статус удалённого контроллера домена:

```
# samba-tool domain demote --remove-other-dead-server=DC3
```

6. Если пониженный контроллер работал как доменный сервер DNS, убедиться, что члены домена и контроллеры домена больше не используют этот хост для разрешения зон AD DNS.

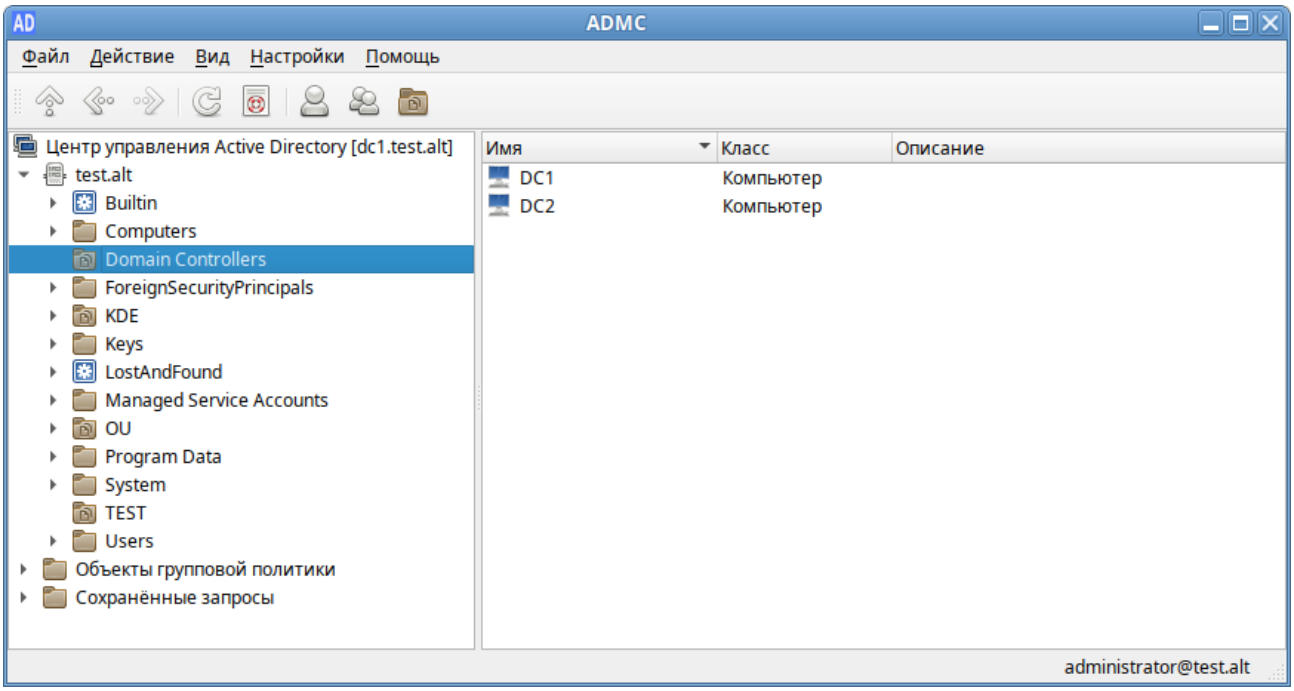
Важно

Не следует подключать к сети контроллер, выведенный по данной процедуре. Иначе домен станет несогласованным.

10.3. Проверка

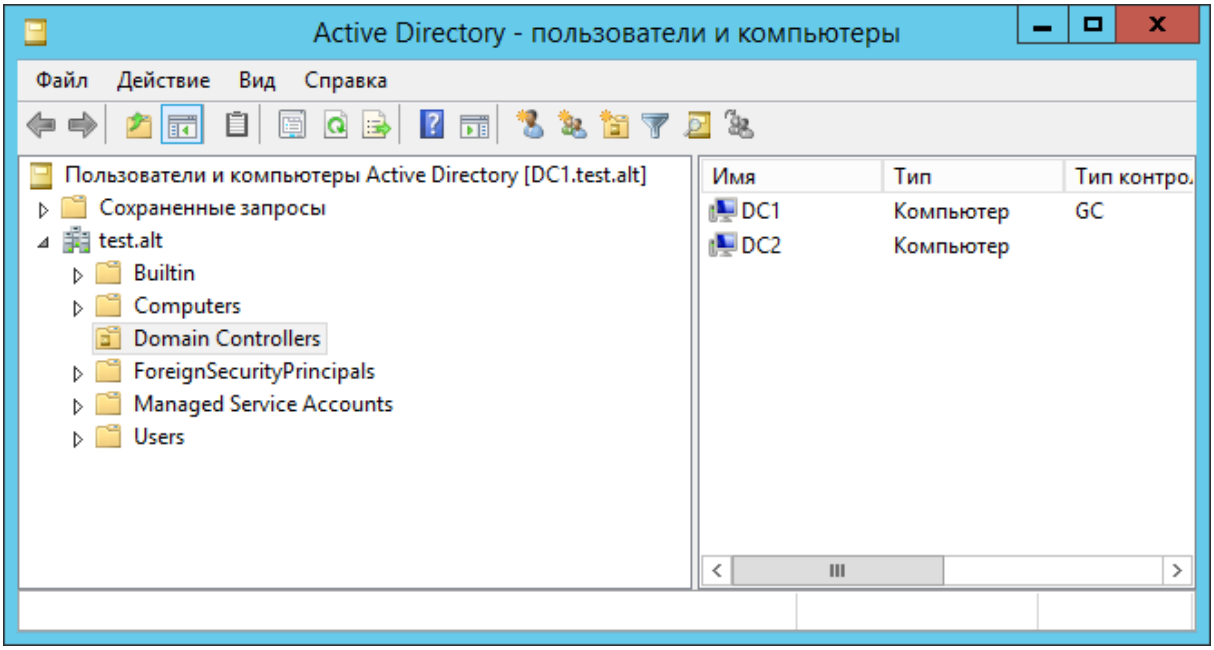
Действия, описанные в этом разделе, предназначены только для проверки и ручного удаления оставшихся записей, если процесс понижения контроллера не удался.

На машине, введённой в домен, запустить модуль удалённого управления базой данных конфигурации (ADMC) (подробнее см. Модуль удаленного управления базой данных конфигурации (ADMC)). Выбрать запись **Domain Controllers** и убедиться, что пониженный контроллер домена был удален:



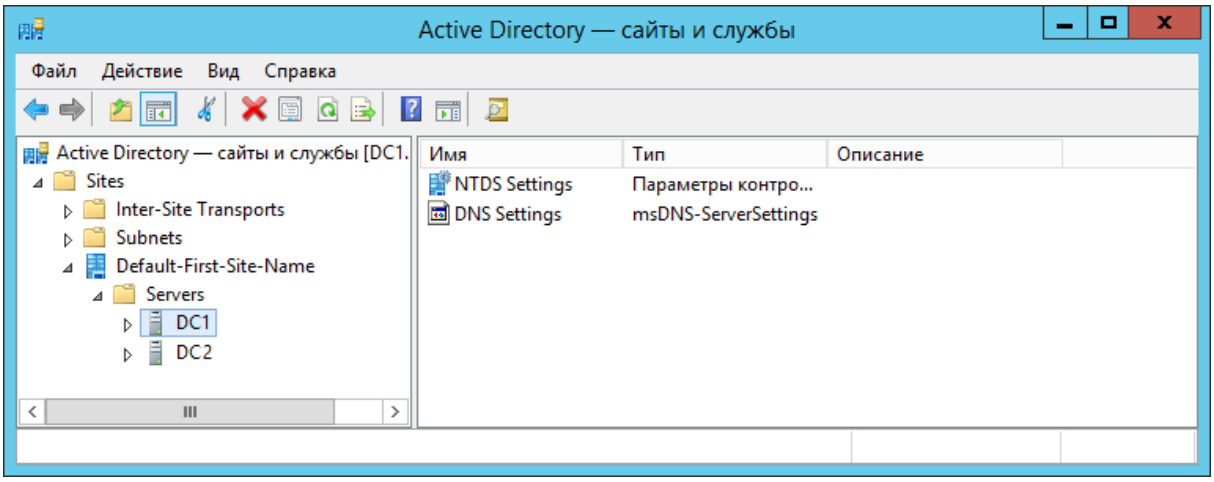
Проверить, что контроллер домена был понижен, можно также в RSAT (см. Установка административных инструментов (машина Windows)). Для этого на машине Windows введённой в домен:

1. Открыть приложение **`Пользователи и компьютеры Active Directory`**, перейти к записи **`Контроллеры домена`** и убедиться, что пониженный контроллер домена был удален:

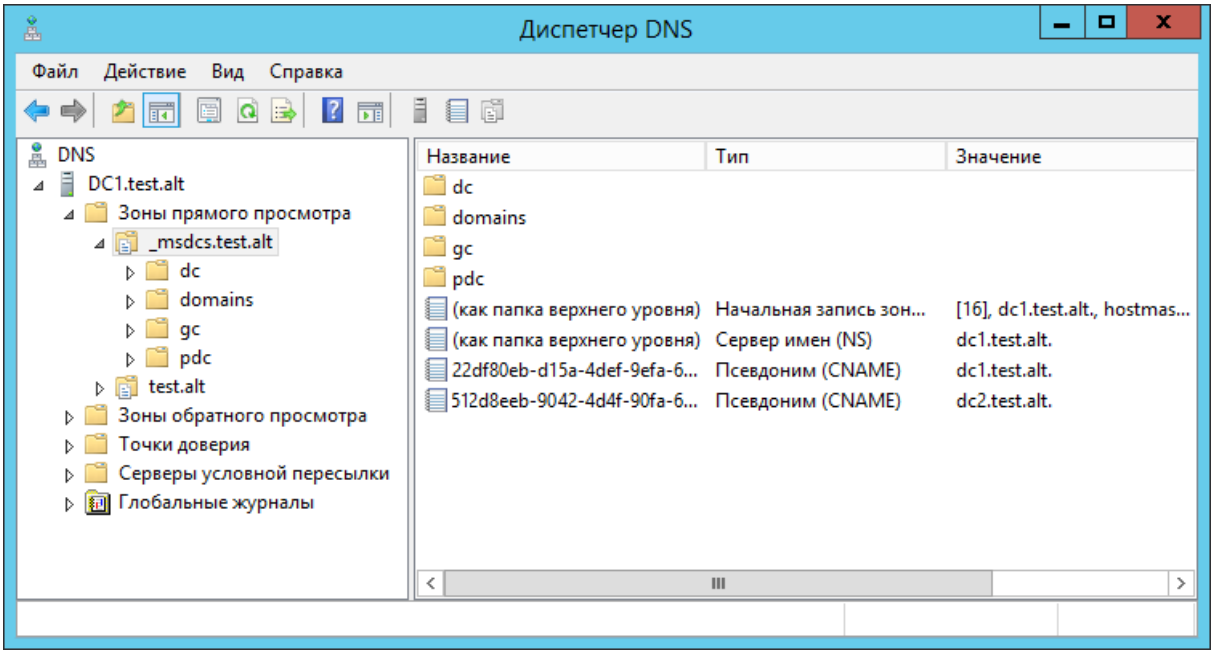
   Если запись всё ещё присутствует в списке, её можно удалить вручную, выбрав в контекстном меню записи пункт **Удалить**.

2. Открыть приложение **`Сайты и службы Active Directory`**, и убедиться, что контроллер домена с пониженным статусом больше не указан ни в одной записи сайта Active Directory:



Если запись всё ещё присутствует в списке, её можно удалить вручную, выбрав в контекстном меню записи пункт **Удалить**.

3. Открыть приложение **DNS**, и убедиться, что имя хоста, IP-адрес и objectGUID контроллера домена больше не используются ни в одной записи DNS в любой зоне AD DNS. Например:



Если записи всё ещё присутствуют в списке, их можно удалить вручную, выбрав в контекстном меню записи пункт **Удалить**.

Часть III. Репликация

Репликация Альт Домен — метод, посредством которого изменения в базе службы каталогов на одном контроллере домена передаются другим контроллерам.

В Samba всё, что хранится внутри домена, реплицируется между контроллерами домена (пользователи, группы и записи DNS).

В настоящее время Samba не поддерживает протокол репликации распределенной файловой системы (DFS-R), используемый для репликации Sysvol. Методы решения этой проблемы см. в разделе Двунаправленная репликация SysVol.

Содержание

11. Настройка репликации

12. Проверка статуса репликации

13. Двунаправленная репликация SysVol

Глава 11. Настройка репликации

Предупреждение

Без успешной двунаправленной репликации в течение 14 дней DC исключается из домена.

Начиная с версии samba 3.5, топология репликации выстраивается автоматически.

Примечание

При настройке репликации указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Команда репликации:

```
# samba-tool drs replicate <destinationDC> <sourceDC> <NC> [options]
```

Процедура двусторонней репликации:

1. Репликация с первого контроллера домена на второй:

   ```
   # samba-tool drs replicate dc2.test.alt \
   dc1.test.alt dc=test,dc=alt -Uadministrator

   Password for [TEST\administrator]:
   Replicate from dc1.test.alt to dc2.test.alt was successful.
   ```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

2. Репликация на первый контроллер домена со второго:

   ```
   # samba-tool drs replicate dc1.test.alt \
   dc2.test.alt dc=test,dc=alt -Uadministrator

   Password for [TEST\administrator]:
   Replicate from dc2.test.alt to dc1.test.alt was successful.
   ```

   Сначала указывается приемник, затем источник, после этого реплицируемая ветка в LDAP.

   Примечание

   Имя домена в именах серверов можно опустить (если они одинаковые).

3. Для просмотра статуса репликации можно запустить команду на DC (подробнее см. Проверка статуса репликации):

```
# samba-tool drs showrepl
```

Примечание

Если репликация на Windows не работает, следует добавить в Active Directory Sites and Services новое соединение Active Directory, реплицировать на DC, подождать минут 5 и попробовать реплицировать с Samba на Windows.

Глава 12. Проверка статуса репликации

12.1. Отображение статуса репликации на контроллере домена Samba

12.2. Отображение статусов репликации на контроллере домена Windows

12.1. Отображение статуса репликации на контроллере домена Samba

Команда **samba-tool drs showrepl** отображает установленные связи с другими контроллерами домена в лесу Альт Домен. Соединения отображаются с точки зрения контроллера домена, на котором запускается команда. Пример:

```
# samba-tool drs showrepl
Default-First-Site-Name\DC2
DSA Options: 0x00000001
DSA object GUID: 26a8d3d0-66b3-4f6c-8457-0def172d4af3
DSA invocationId: 83fb4bbf-9f63-44d6-acbd-c0db4e9e839a

==== INBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ Wed May 22 15:38:51 2024 EET was successful
                0 consecutive failure(s).
                Last success @ Wed May 22 15:38:51 2024 EET

CN=Configuration,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ Wed May 22 15:38:51 2024 EET was successful
                0 consecutive failure(s).
                Last success @ Wed May 22 15:38:51 2024 EET

DC=ForestDnsZones,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ Wed May 22 15:38:50 2024 EET was successful
                0 consecutive failure(s).
                Last success @ Wed May 22 15:38:50 2024 EET
```

```
DC=DomainDnsZones,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ Wed May 22 15:38:51 2024 EET was successful
                0 consecutive failure(s).
                Last success @ Wed May 22 15:38:51 2024 EET

DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ Wed May 22 15:38:51 2024 EET was successful
                0 consecutive failure(s).
                Last success @ Wed May 22 15:38:51 2024 EET

==== OUTBOUND NEIGHBORS ====

CN=Schema,CN=Configuration,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

CN=Configuration,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=DomainDnsZones,DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=test,DC=alt
        Default-First-Site-Name\DC1 via RPC
                DSA object GUID: e72594f1-4986-4ac9-8cdd-9481cff5e243
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
        Connection name: 56a02972-69f5-42fb-965a-7125f09c96d1
        Enabled        : TRUE
        Server DNS name : dc1.test.alt
        Server DN name  : CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-
```

```
Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
                TransportType: RPC
                options: 0x00000001
Warning: No NC replicated for Connection!
```

Связи отображаются в разделах ***INBOUND NEIGHBORS*** и ***OUTBOUND NEIGHBORS***. В каждом разделе должно быть по 5 пунктов:

```
CN=Schema,CN=Configuration,DC=test,DC=alt
DC=ForestDnsZones,DC=test,DC=alt
DC=test,DC=alt
DC=DomainDnsZones,DC=test,DC=alt
CN=Configuration,DC=test,DC=alt
```

В разделе ***INBOUND NEIGHBORS*** в пункте ***Last attempt*** должны стоять актуальные дата и время, идентичные указанным в строке ***Last success*** (отображает время последней репликации). Должно быть ***0 consecutive failure(s)***.

Если в разделе ***INBOUND NEIGHBORS*** есть записи:

```
Last attempt @ NTTIME(0) was successful
…
Last success @ NTTIME(0)
```

необходимо подождать (соединение устанавливается).

В разделе ***KCC CONNECTION OBJECTS*** быть приведён список всех контроллеров домена, чьи KCC установили соглашения о репликации с текущим контроллером домена. В случае когда контроллер домена только только был добавлен в домен и запущен, может пройти до 15 минут до того, как соглашения будут установлены.

Примечание

Предупреждение

```
No NC replicated for Connection!
```

можно игнорировать. Оно появляется из-за того, что при регистрации нового DC Samba неверно устанавливает некоторые флаги репликации.

Можно также проверить репликацию LDAP:

```
# samba-tool ldapcmp ldap://dc1.test.alt ldap://dc2.test.alt -Uadministrator
Password for [TEST\administrator]:

* Comparing [DOMAIN] context...

* Objects to be compared: 274

* Result for [DOMAIN]: SUCCESS

* Comparing [CONFIGURATION] context...

* Objects to be compared: 1625
```

```
* Result for [CONFIGURATION]: SUCCESS

* Comparing [SCHEMA] context...

* Objects to be compared: 1739

* Result for [SCHEMA]: SUCCESS

* Comparing [DNSDOMAIN] context...

* Objects to be compared: 41

* Result for [DNSDOMAIN]: SUCCESS

* Comparing [DNSFOREST] context...

* Objects to be compared: 18

* Result for [DNSFOREST]: SUCCESS
```

Данная команда сравнит значения атрибутов объектов всего каталога на DC1 и DC2. В ряде случаев атрибуты объектов на разных контроллерах могут отличаться, и в выводе команды это будет видно. Но не во всех случаях это будет признаком проблемы с репликацией.

12.2. Отображение статусов репликации на контроллере домена Windows

Для отображения статуса входящей репликации на контроллере домена Windows можно использовать утилиту **`repadmin`**:

```
> repadmin /showrepl
```

Windows не поддерживает отображение статусов исходящих подключений репликации. Чтобы обойти эту проблему, можно отобразить статусы входящих подключений на контроллерах домена Samba, на которые реплицируется контроллер домена Windows:

1. Найти в Альт Домен всех партнеров репликации Windows DC. Например, чтобы отобразить партнеров по репликации контроллера домена с именем WindowsDC:

   ```
   # ldbsearch -H /var/lib/samba/private/sam.ldb '(fromServer=*CN=WindowsDC*)'
   --cross-ncs dn
   # record 1
   dn: CN=a46c895e-658b-463e-9ab5-a1c237fca4b1,CN=NTDS
   Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
   Name,CN=Sites,CN=Configuration,DC=test,DC=alt

   # returned 1 records
   # 1 entries
   # 0 referrals
   ```

   В этом примере возвращается один партнер по репликации (имя хоста: DC2). Имя хоста партнера по репликации является частью возвращаемого отличительного имени (DN).

2. На каждом контроллере домена Samba, полученном на предыдущем шаге, выполнить команду **`samba-tool drs showrepl`** для отображения статуса репликации каталога.

   Необходимо убедиться, что каждый реплицируемый контейнер каталогов указан для контроллера домена Windows в разделе ***`INBOUND NEIGHBORS`*** на контроллере домена Samba, а статусы успешны.

Глава 13. Двунаправленная репликация SysVol

13.1. Настройка двунаправленной репликации SysVol на базе Rsync/Unison

13.2. Настройка двунаправленной репликации SysVol на базе Rsync/osync

13.3. Сопоставление встроенных идентификаторов пользователей и групп

Каталог **`Sysvol`** присутствует на всех контроллерах домена и используется для хранения логон скриптов и объектов групповых политик. Отсутствие репликации этого каталога приведет к неправильной работе групповых политик и сценариев входа.

Samba в своем текущем состоянии не поддерживает репликацию SysVol через DFS-R (репликация распределенной файловой системы) или более старую FRS (службу репликации файлов), используемую в Windows Server 2000/2003 для репликации SysVol. В настоящее время для репликации SysVol можно использовать один из следующих обходных путей:

- двунаправленная репликация SysVol на основе Rsync/Unison (только Samba DC);
- двунаправленная репликация SysVol на основе Rsync/osync (только Samba DC).

Важно

Следует синхронизировать **`idmap.ldb`** из контроллера домена, имеющего роль FSMO PDC_Emulator, со всеми другими контроллерами домена. Это гарантирует, что все контроллеры домена будут использовать одни и те же идентификаторы. Если файл **`idmap.ldb`** не синхронизируется, на каждом контроллере домена будут разные идентификаторы.

Синхронизировать **`idmap.ldb`** (см. раздел Сопоставление встроенных идентификаторов пользователей и групп) необходимо при первом присоединении к новому контроллеру домена, а затем периодически (для того чтобы гарантировать постоянство идентификаторов не нужно синхронизировать **`idmap.ldb`** каждый раз при синхронизации SysVol, но это следует делать периодически).

13.1. Настройка двунаправленной репликации SysVol на базе Rsync/Unison

Исходные данные:

- все команды выполняются от пользователя root;
- первый контроллер домена — DC1;

- второй контроллер домена — DC2 (уже присоединён к домену);
- **sysvol** расположен в **/var/lib/samba/** как на DC1, так и на DC2;
- **rsync** расположен в **/usr/bin/rsync**;
- **unison** расположен в **/usr/bin/unison**;
- журнал sysvolsync пишется в файл **/var/log/sysvol-sync.log**;
- настроено беспарольное взаимодействие между rootами всех контроллеров домена (см. Настройка беспарольного доступа по ssh).

На первом контроллере домена (DC1):

1. Установить пакеты *rsync* и *unison*:

```
# apt-get install rsync unison
```

2. При низких скоростях в сети, **unison** может некорректно работать. Для того чтобы при повторной работе **unison** использовал существующее SSH-соединение вместо установки нового, необходимо выполнить следующие команды:

```
# mkdir ~/.ssh/ctl
# cat << EOF > ~/.ssh/config
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
EOF
```

   Эти строки настраивают OpenSSH на использование ControlMaster для всех SSH-соединений и сохранение сокетов управления в каталоге **~/.ssh/ctl**.

3. Создать каталог **/root/.unison/**:

```
# mkdir /root/.unison
```

4. Для определения политики синхронизации создать файл конфигурации unison **/root/.unison/default.prf** со следующим содержимым:

```
# Список каталогов, которые будут синхронизированы
root = /var/lib/samba
root = ssh://root@DC2.test.alt//var/lib/samba
# Список подкаталогов, которые нужно синхронизировать
path = sysvol
# Список подкаталогов, которые нужно игнорировать
#ignore = Path
auto=true
batch=true
perms=0
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
copythreshold=0
```

```
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace
--compress
copyquoterem = true
copymax = 1
copyquoterem = false

# Сохранять журнал с результатами работы в отдельном файле
logfile = /var/log/sysvol-sync.log
```

5. Создать файл для записи журнала репликации (необходимо настроить ротацию логов для этого файла, так как размер журнала не контролируется):

```
# touch /var/log/sysvol-sync.log
```

На втором контроллере домена (DC2) установить пакеты *rsync* и *unison*:

```
# apt-get install rsync unison
```

Важно

Перед запуском команды синхронизации рекомендуется сделать резервную копию каталога **sysvol**.

Запустить команду синхронизации:

```
# /usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log \
--delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol \
root@dc2.test.alt:/var/lib/samba && /usr/bin/unison
```

В этой команде утилита **rsync** создает структуры каталогов с расширенными атрибутами, а затем утилита **unison** копирует только эти расширенные атрибуты файлов.

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * * /usr/bin/unison -silent
```

Повторная синхронизация каталога:

- отключить синхронизацию по расписанию на DC1;
- **rsync** и **unison** не должны выполняться в данный момент (можно проверить командой **ps -aux**);
- удалить хеш-файлы unison на DC1 и DC2 в каталоге **/root/.unison**;
- проверить **sysvol** и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1. Скопировать файл **/root/.unison/default.prf** в другой файл, например: **/root/.unison/sync_dc2.prf**.
2. В файле **/root/.unison/dc2.prf** изменить значение параметра ***root***.
3. Повторить шаги 1 и 2 для всех контроллеров домена.
4. Изменить задание на синхронизацию по расписанию на DC1:

```
* * * * * /usr/bin/unison sync_dc2 -silent
* * * * * /usr/bin/unison sync_dc3 -silent
…
```

13.2. Настройка двунаправленной репликации SysVol на базе Rsync/osync

Исходные данные:

- все команды выполняются от пользователя root;
- первый контроллер домена — DC1;
- второй контроллер домена — DC2 (уже присоединён к домену);
- **sysvol** расположен в **/var/lib/samba/** как на DC1, так и на DC2;
- **rsync** расположен в **/usr/bin/rsync**;
- **osync** расположен в **/usr/bin/osync**;
- журнал sysvolsync пишется в файл **/var/log/osync_*.log**;
- настроено беспарольное взаимодействие между rootами всех контроллеров домена (см. Настройка беспарольного доступа по ssh).

На первом контроллере домена (DC1):

1. Установить пакеты *rsync* и *osync*:

```
# apt-get install rsync osync
```

2. Отредактировать файл **/etc/osync/sync.conf**:

```
#!/usr/bin/env bash
INSTANCE_ID="sync_sysvol"
 # Путь до SysVol на текущем сервере
INITIATOR_SYNC_DIR="/var/lib/samba/sysvol"
 # Путь до SysVol на удалённом сервере
TARGET_SYNC_DIR="ssh://root@DC2:22//var/lib/samba/sysvol"
 # ssh ключ root
SSH_RSA_PRIVATE_KEY="/root/.ssh/id_ed25519"
 # Удалённые хосты которые osync пингует перед стартом
REMOTE_3RD_PARTY_HOSTS=""
 # Сохранять xattr
```

```
PRESERVE_ACL=yes
 # Сохранять xattr
PRESERVE_XATTR=yes
 # Сохранять резервную копию удалённых файлов
SOFT_DELETE=yes
DESTINATION_MAILS="your@test.alt"
REMOTE_RUN_AFTER_CMD="/usr/bin/samba-tool ntacl sysvolreset"
```

На втором контроллере домена (DC2) установить пакет *rsync*:

```
# apt-get install rsync
```

Важно

Перед запуском команды синхронизации рекомендуется сделать резервную копию каталога **sysvol**.

Запустить команду синхронизации:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --dry --verbose
```

Если команда выполнилась без ошибок, можно удалить параметр **--dry** и запустить команду синхронизации снова:

```
# /usr/bin/osync.sh /etc/osync/sync.conf --verbose
```

В результате **sysvol** будет синхронизирован на обоих серверах.

Примечание

Если в файле **sysvol** параметры ***SOFT_DELETE*** (сохранять резервные копии удалённых файлов) и ***CONFLICT_BACKUP*** (сохранять резервные копии файлов на целевой реплике, если они обновлены из исходной реплики) установлены в значение *yes*, то на источнике и получателе репликации необходимо создать каталоги **.osync_workdir/deleted** и **.osync_workdir/backup**:

```
# mkdir /var/lib/samba/sysvol/.osync_workdir/deleted
# mkdir /var/lib/samba/sysvol/.osync_workdir/backup
```

На DC1 включить синхронизацию по расписанию:

```
# crontab -e
*/5 * * * *  /usr/bin/osync.sh /etc/osync/sync.conf --silent
```

Если при попытке синхронизировать каталог возникают проблемы необходимо:

- отключить синхронизацию по расписанию на DC1;
- убедиться, что **rsync** и **osync** не выполняются в данный момент (можно проверить, выполнив команду **ps -aux| grep sync**);

- удалить хеш-файлы **.osync_workdir** на DC1 и DC2 в **/var/lib/samba/sysvol/**;
- проверить **sysvol** и повторить синхронизацию;
- убедиться, что синхронизация выполнена успешно;
- включить синхронизацию по расписанию на DC1.

Если контроллеров домена больше чем два, можно создать больше заданий для cron на DC1:

1. Скопировать файл **/etc/osync/sync.conf** в другой файл, например: **/etc/osync/sync_dc3.conf**.
2. В файле **/etc/osync/sync_dc3.conf** изменить значение параметра ***TARGET_SYNC_DIR***.
3. Повторить шаги 1 и 2 для всех контроллеров домена.
4. Изменить задание на синхронизацию по расписанию на DC1:

```
# crontab -e
*/5 * * * *  /usr/bin/osync.sh /etc/osync/sync.conf --silent
*/5 * * * *  /usr/bin/osync.sh /etc/osync/sync_dc3.conf --silent
…
```

13.3. Сопоставление встроенных идентификаторов пользователей и групп

По умолчанию контроллер домена Samba сохраняет идентификаторы пользователей и групп в атрибутах ***xidNumber*** в **idmap.ldb**. Из-за особенностей работы **idmap.ldb** нельзя гарантировать, что каждый контроллер домена будет использовать один и тот же идентификатор для данного пользователя или группы.

Ниже описана процедура синхронизации **idmap.ldb** с контроллера домена, на котором установлена роль FSMO *Эмулятор PDC* (см. Роли FSMO), со всеми остальными контроллерами домена. Для достижения наилучших результатов следует регулярно синхронизировать **idmap.ldb**.

На контроллере домена, имеющего роль FSMO *Эмулятор PDC*:

1. Установить пакет *ldb-tools*, если он еще не установлен:

```
# apt-get install ldb-tools
```

2. Создать резервную копию файла **/var/lib/samba/private/idmap.ldb**:

```
# rm -f /var/lib/samba/private/idmap.ldb.bak
# tdbbackup -s .bak /var/lib/samba/private/idmap.ldb
```

3. Создать ежедневное задание cron:

```
#Создание резервной копии idmap.ldb
0 3 * * * rm -f /var/lib/samba/private/idmap.ldb.bak && tdbbackup -s .bak /
var/lib/samba/private/idmap.ldb >/dev/null 2>&1
```

На контроллерах домена, которые не выполняют роль эмулятора PDC:

1. Скопировать файл резервной копии, созданный на DC с ролью *Эмулятор PDC* (в примере dc1), в каталог **/var/lib/samba/private/** с удалением суффикса .bak (заменить существующий файл):

```
# rsync -a dc1:/var/lib/samba/private/idmap.ldb.bak /var/lib/samba/private/
idmap.ldb
```

2. Запустить очистку кеша:

```
# net cache flush
```

3. Проверить разрешения ACL SysVol и при необходимости сбросить их:

```
# if ! samba-tool ntacl sysvolcheck; then samba-tool ntacl sysvolreset; fi
```

4. Если всё прошло успешно, создать ежедневное задание cron:

```
#Синхронизация idmap.ldb
15 4 * * * rsync -a  dc1:/var/lib/samba/private/idmap.ldb.bak  /var/lib/
samba/private/idmap.ldb && net cache flush && if ! samba-tool ntacl
sysvolcheck; then samba-tool ntacl sysvolreset; fi >/dev/null 2>&1
```

Важно

После синхронизации **idmap.ldb** необходим перезапуск Samba (**systemctl restart samba.service**), т.к. этот файл держится открытым процессами Samba.

Синхронизации **idmap.ldb** можно избежать, если на всех контроллерах добавить следующие параметры в **smb.conf** в секции [sysvol] (и в [netlogon]) строки:

```
acl_xattr:ignore system acls = yes
acl_xattr:default acl style = windows
```

При использовании этих параметров значения расширенных атрибутов файлов (xattr security.NTACL) на всех контроллерах будут одинаковы, независимо от uid/gid. Именно это и является проблемой при использовании **rsync**, т.к. при синхронизации **rsync** передаёт имена пользователей/групп и они разыменовываются в uid/gid уже «на месте», а xattr security.NTACL остаётся неизменным и, в конфигурации по умолчанию (без вышеуказанных параметров), зависит от значений uid/gid/facl.

Часть IV. Клиенты Альт Домен

Клиентами Альт Домен могут быть серверы и рабочие станции под управлением Windows, Linux («Альт», Astra Linux) и других операционных систем, поддерживающих стандартные протоколы LDAP, Kerberos, DNS и SMB.

Важно

> Механизмы применения групповых политик оптимизированы для семейства ОС «Альт». Аутентификация в домене рабочих станций под управлением Astra Linux и других ОС под управлением Linux, возможна, но поддержка механизмов применения групповых политик на таких машинах ограничена и требует соответствующее ПО, не входящее в комплект Альт Домен.

Содержание

14. SSSD и Winbind

15. Подготовка системы к вводу в домен

16. Присоединение к домену в роли участника

17. Вход пользователя

18. Отображение глобальных групп на локальные

19. Отладочная информация

20. Удаление клиента домена

21. Повторная регистрация клиента

22. Настройка аутентификации доменных пользователей на контроллере домена

23. Настройка обновления паролей аккаунтов машин

Глава 14. SSSD и Winbind

14.1. Аутентификация (PAM)

14.2. Авторизация (NSS)

14.3. Кеширование и управление сессией

14.4. Групповые политики

14.5. Обновление DNS

14.6. Поддержка работы с несколькими доменами и доверительные отношения

В операционных системах на базе Linux два ключевых инструмента обеспечивают взаимодействие с AD — Winbind и SSSD:

- Winbind (часть пакета Samba) — демон, обеспечивающий взаимодействие с AD и решающий проблему единого входа в систему. Winbind использует вызовы Microsoft RPC. Он поддерживает как Kerberos, так и NTLM, предоставляя системам механизмы аутентификации и авторизации, аналогичные тем, что используются в Windows;

- SSSD (System Security Services Daemon) — клиентский компонент централизованных служб каталогов (таких как FreeIPA, 389 Directory Server, Microsoft Active Directory, OpenLDAP и других). Он запрашивает и кеширует информацию, а также предоставляет услуги идентификации, аутентификации и авторизации для локальной машины.

В этом разделе описаны функции и возможности двух вариантов интеграции: решение на основе Samba Winbind и решение на базе SSSD.

Таблица 14.1. Сравнение Winbind и SSSD

Категория	Описание	Winbind	SSSD
Аутентификация	Kerberos	Да (начиная с версии 4.19.9-alt4)	Да
	NTLM	Да (используется, если Kerberos недоступен или не используется)	Нет
	LDAP	Нет	Да (не в AD-домене)
Авторизация	LDAP	Да	Да
	Вызовы Microsoft RPC	Да	Нет
Автономный вход в систему		Да	Да
Поддержка доверительных отношений	External Trust	Да	Да
	Parent-Child Trust	Да	Да
	Forest Trust	Да	Нет
Поддержка групповых политик	Групповые политики Samba	Да (не реализовано в Альт Домен)	Нет
	Групповые политики ALT Linux с помощью **`gpupdate`**	Да	Да
	GPO-Based Access Control (Централизованное управление контролем доступа на основе хоста через GPO)	Нет	Да
Сопоставление идентификаторов	Генерация UID/GID	Да	Да
	Сопоставление идентификаторов через атрибуты RFC2307	Да	Да
Обновление DNS	Встроенное	Нет	Да
	Сторонние решения	Да	Нет
Автоматическая интеграция с sudo		Нет	Да
Аутентификация с помощью электронных ключей, смарт-карт и сертификатов		Нет	Да
Производительность при обработке большого числа групп и пользователей		Высокая	Низкая

14.1. Аутентификация (PAM)

В Linux аутентификация пользователей управляется системой PAM (Pluggable Authentication Modules), которая позволяет использовать различные модули для проверки учетных данных. Winbind и SSSD реализуют собственные PAM-модули:

- Winbind: pam_winbind.so
- SSSD: pam_sss.so

Оба модуля позволяют системе проверять учетные данные пользователя через обращение к контроллеру домена:

- Winbind использует NTLM или Kerberos;
- SSSD использует Kerberos.

Конфигурация PAM обычно прописывается в файле **`/etc/pam.d/system-auth`**, где подключается преднастроенный стек:

```
system-auth-winbind-only
```

или

```
system-auth-sss-only
```

14.1.1. SSSD

В SSSD за аутентификацию отвечает параметр ***`auth_provider`***, который определяет, какой механизм используется для проверки подлинности. Поддерживаются следующие варианты:

- поставщик данных Kerberos (krb5) — аутентификация через Kerberos. Требует настройки **`auth_provider = krb5`**. Для корректной работы его необходимо использовать совместно с поставщиком данных идентификации (например, **`id_provider = ldap`**). Некоторые данные, которые требуются внутреннему серверу проверки подлинности Kerberos 5, должны предоставляться поставщиком данных идентификации (например, имя участника Kerberos пользователя (UPN));
- поставщик данных LDAP (ldap) — аутентификация через LDAP-сервер. SSSD не поддерживает аутентификацию через незащищенный канал требуется TLS/SSL или LDAPS. Даже если сервер LDAP используется только как провайдер идентификации, использование зашифрованного канала настоятельно рекомендуется;
- поставщик данных Active Directory (ad) — оптимизированная аутентификация для Active Directory (используется Kerberos + LDAP). Обмен данными с внутренним сервером выполняется по каналу с шифрованием GSSAPI. С поставщиком данных AD не следует использовать параметры SSL/TLS, поскольку использование Kerberos будет иметь приоритет над ними. Поставщик данных AD позволяет SSSD использовать поставщик данных идентификации sssd-ldap и поставщик данных проверки подлинности sssd-krb5 с оптимизацией для сред Active Directory. Поставщик данных AD принимает те же параметры, которые используются поставщиками sssd-ldap и sssd-krb5, за некоторыми исключениями;

- поставщик данных IPA (ipa) — специальный провайдер для интеграции с FreeIPA. Этот поставщик требует, чтобы компьютер был подключен к домену FreeIPA; конфигурация почти полностью определяется автоматически и получается непосредственно с сервера. Поставщик IPA позволяет SSSD использовать поставщик идентификационных данных sssd-ldap и sssd-krb5.

Для настройки аутентификации в SSSD используется файл конфигурации **`/etc/sssd/sssd.conf`**. В нём определяются параметры подключения к серверу каталога, а также параметры аутентификации.

Пример настройки аутентификации для AD:

```
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
; cache_credentials = false
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
```

14.1.2. Winbind

В Winbind за аутентификацию отвечает параметр ***`security`***, который модель безопасности Samba:

- ads — настраивает Samba как участника домена в домене AD. Для аутентификации в этом режиме используется Kerberos;
- domain — Samba выступает как член старого NT-домена (не AD) и передает учетные данные на контроллер домена Windows;
- server — устаревший вариант, при котором Samba делегирует аутентификацию другому серверу, но, если тот откажет, пробует локальную проверку;
- user — стандартный режим, когда учетные данные проверяются на самом сервере Samba, без обращения к домену.

Основными методами аутентификации являются:

- Kerberos — используется для безопасной аутентификации через Kerberos. Это основной механизм при работе с доменами AD (**`security = ads`**). Winbind автоматически получает и управляет Kerberos-билетами для пользователей;
- NTLM — в случае, если Kerberos недоступен или не используется, Winbind может прибегать к аутентификации через NTLM (NT LAN Manager), который является устаревшим, но все еще поддерживаемым методом аутентификации в Windows-средах.

Для настройки Winbind используется конфигурация в файле **`/etc/samba/smb.conf`**.

Пример настройки аутентификации Winbind для AD:

```
[global]
security = ads
workgroup = TEST
realm = TEST.ALT
idmap config * : backend = tdb
idmap config EXAMPLE : backend = rid
idmap config EXAMPLE : range = 10000-999999
winbind use default domain = yes
winbind offline logon = yes
winbind refresh tickets = yes
winbind enum users = no
winbind enum groups = no
kerberos method = secrets and keytab
log file = /var/log/samba/log.%m
log level = 3
```

14.2. Авторизация (NSS)

После успешной аутентификации системе необходимо определить, какие пользователи и группы существуют, какие у них UID/GID и какие права им назначены. Для этого используется подсистема NSS (Name Service Switch), которая позволяет системе получать информацию о пользователях и группах из различных источников.

Winbind и SSSD предоставляют свои модули для интеграции с NSS:

- Winbind: nss_winbind.so
- SSSD: nss_sss.so

Эти модули настраиваются в файле **`/etc/nsswitch.conf`**, например:

```
passwd: files winbind
shadow: tcb files winbind
group:  files winbind
```

или:

```
passwd: files sss
shadow: tcb files sss
group:  files sss
```

Здесь winbind или sss определяют, что информация о пользователях и группах запрашивается у соответствующей службы:

- Winbind — запрашивает SID пользователей и групп через RPC и LDAP и маппирует их в локальные UID/GID;
- SSSD — запрашивает данные пользователей и групп через LDAP.

14.2.1. SSSD

SSSD позволяет управлять авторизацией пользователей и групп, используя разные механизмы, которые определяются параметром ***`access_provider`***.

Доступные значения ***access_provider***:

- permit — разрешает доступ всем пользователям (по умолчанию);
- deny — блокирует доступ всем пользователям;
- ldap — проверяет доступ через LDAP-фильтр (например, членство в группе);
- ad — использует Group Policy Objects (GPO) для авторизации (при ***id_provider = ad***);
- hbac — применяет Host-Based Access Control (HBAC) (только для FreeIPA).

14.2.1.1. Механизм ID Mapping

Информацию о механизме ID Mapping в SSSD см. Настройка SSSD.

14.2.1.2. Управление правами через SUDO

Помимо контроля входа, SSSD может управлять sudo-правилами. Конфигурация sudo традиционно хранится в файле **sudoers**, который нужно вручную копировать и обновлять на каждой машине в системе (чтобы включить SSSD как источник правил sudo, необходимо добавить sss в запись sudoers в файле **nsswitch.conf**). Однако в больших инфраструктурах это может быть неудобно и трудоемко, поэтому часто для упрощения управления правами доступа используют LDAP (Lightweight Directory Access Protocol), централизованный каталог для хранения конфигураций. В этом случае локальные системы просто обращаются к центральному серверу LDAP для получения актуальной информации о правилах доступа.

На стороне SSSD достаточно расширить список служб добавлением ***sudo*** в раздел [sssd] **sssd.conf**. Чтобы ускорить поиск LDAP, также можно указать базу поиска для правил sudo с помощью параметра ***ldap_sudo_search_base***.

В следующем примере показано, как настроить SSSD на загрузку правил sudo с сервера LDAP:

```
[sssd]
config_file_version = 2
services = nss, pam, sudo
domains = TEST

[domain/TEST]
id_provider = ldap
sudo_provider = ldap
ldap_uri = ldap://test.alt
ldap_sudo_search_base = ou=sudoers,dc=test,dc=alt
```

Важно учитывать, что на платформах, где поддерживается systemd, не требуется добавлять поставщика данных «sudo» в список служб, так как он стал необязательным. Однако вместо этого следует включить sssd-sudo.socket.

14.2.2. Winbind

Winbind работает как клиент AD и получает данные учетных записей пользователей и групп через вызовы Microsoft RPC и LDAP.

14.2.2.1. Механизм ID Mapping

Информацию о механизме ID Mapping в Winbind см. Планирование и настройка диапазонов идентификаторов UID и GID (Winbind/IDMapping).

14.3. Кеширование и управление сессией

14.3.1. SSSD

По умолчанию SSSD не кеширует аутентификационные данные пользователей (пароль в виде хеша). При обработке запросов на аутентификацию SSSD всегда обращается к провайдеру идентификации (***`id_provider`***). Если провайдер недоступен, аутентификация пользователя завершается с ошибкой.

Чтобы пользователи могли входить в систему даже если провайдер идентификации недоступен, можно включить кеширование учетных данных, установив параметр ***`cache_credentials = true`*** в файле **`/etc/sssd/sssd.conf`**.

Параметр ***`cache_credentials`*** — определяет, должны ли учетные данные пользователя также сохраняться в локальном кеше LDB. Кешированные учетные данные относятся к паролям, включая первый (долгосрочный) фактор двухфакторной аутентификации, но не другие механизмы аутентификации (пароли хранятся в виде хеша SHA-512).

В SSSD информация о пользователях и группах кешируется в следующих файлах (в каталоге **`/var/lib/sss/db/`**):

- **`cache_<домен>.ldb`**
  - Тип: Авторизационный кеш
  - Функция: Основной кеш данных о пользователях и группах
- **`ccache_<домен>`**
  - Тип: Авторизационный кеш
  - Функция: Кеширование учетных данных, если используется аутентификация через Kerberos (содержит кешированные Kerberos-билеты)
- **`timestamps_<домен>.ldb`**
  - Функция: Управляет сроками действия кешированных данных

14.3.2. Winbind

Winbind использует TDB (Trivial Database) файлы, которые расположены в **`/var/lib/samba/`**:

- **`winbindd_cache.tdb`**
  - Тип: Авторизационный кеш
  - Функция: Хранит информацию об идентификации, полученной от домена AD
- **`winbindd_idmap.tdb`**
  - Тип: Авторизационный кеш

- Функция: Локальная база данных IDMAP используемая winbindd для сопоставления SID и UID/GID при бэкенде tdb

- **`gencache.tdb`**
  - Тип: Общий кеш
  - Функция: Хранит кешированную информацию о недоступных серверах и доверенных доменах.

Параметр, отвечающий за кеширование:

```
[global]
winbind offline logon = yes
```

Этот параметр включается в **`smb.conf`**, чтобы позволить Winbind использовать кешированные учетные данные для аутентификации, когда сервер AD недоступен.

Также существует ***`winbind cache time`***, который задаёт количество секунд, в течение которых демон winbindd будет кешировать информацию о пользователях и группах перед повторным запросом к серверу Windows NT. Это не относится к запросам на аутентификацию, которые всегда обрабатываются в реальном времени, если только не включена опция оффлайн-аутентификации Winbind.

14.4. Групповые политики

14.4.1. Поддержка групповых политик ALT Linux

В дистрибутивах ALT реализована поддержка групповых политик (Group Policy Objects, GPO), что позволяет централизованно управлять настройками и конфигурациями систем, аналогично средам Windows. Для применения групповых политик используется утилита **`gpupdate`**, предназначенная для работы на машинах, введённых в домен, как с помощью SSSD, так и с помощью Winbind.

При аутентификации пользователя модуль PAM system-policy-gpupdate.so запускает pam_oddjobd_gpupdate.so, который инициирует выполнение системной службы oddjob.service для выполнения привилегированных задач. oddjob.service вызывает утилиту **`gpoa`**, которая отвечает за репликацию и применение групповых политик (GPO). В зависимости от переданного параметра утилита **`gpoa`** обновляет либо настройки пользователя, если передано его имя, либо настройки всей машины, если параметр отсутствует. Этот процесс гарантирует автоматическое применение актуальных групповых политик при каждом входе пользователя в систему.

Подробнее о групповых политиках см. Групповые политики в Альт Домен.

14.4.2. Интеграция с GPO-Based Access Control для входа в систему

14.4.2.1. SSSD

Один из распространенных сценариев управления доступом к компьютерам в среде AD — использование параметров групповой политики (GPO), связанных с правами входа на машину.

Таблица 14.2. Примеры групповых политик, реализованных в SSSD

Групповая политика	Параметр конфигурации SSSD
Allow log on locally	ad_gpo_map_interactive
Allow log on through Remote Desktop Services	ad_gpo_map_remote_interactive
Log on as a batch job	ad_gpo_map_batch
Log on as a service	ad_gpo_map_service

Настройки политики GPO можно использовать для централизованной настройки нескольких наборов прав входа (Logon Rights) на клиентскую машину, каждый из которых классифицируется по способу входа (interactive, remote interactive) и состоит из белого и чёрного списка пользователей и групп, которым разрешён или запрещён доступ к компьютеру с использованием способа входа. Для этого сопоставляются имена pam-служб с определёнными правами входа. Предоставляются сопоставления по умолчанию для всех часто используемых имён pam-служб, также администратор может добавлять/удалять сопоставления по мере необходимости. Делается это с помощью параметров конфигурации вида ***gpo_map_<logon_right>*** (например, ***gpo_map_interactive***, ***gpo_map_network*** и т. д.), каждый из которых состоит из списка записей, разделённых запятыми, начинающихся либо с «+» (для добавления в набор по умолчанию), либо с «-» (для удаления из набора по умолчанию). Подробнее см. **man sssd-ad**.

Значение белого и черного списка:

- Белый список («allow»). Если этот параметр не задан, любой пользователь может войти в систему. Если он задан, только указанные пользователи и группы получают доступ. Другими словами, при включении этого параметра поведение изменяется с «доступ разрешен всем» на «доступ запрещен всем, кроме перечисленных в белом списке»;

- Черный список («deny»). Если этот параметр не задан, он не оказывает влияния. Если он определен указанные пользователи и группы не могут входить в систему. Если пользователь или группа присутствует одновременно в белом и черном списках, приоритет отдается черному списку.

Если пользователь пытается войти в систему, то:

- определяется, какое право входа (Logon Rights) связано с сервисом PAM;

- получаются соответствующие политики GPO из файла **GptTmpl.inf**, который содержит настройки политики из расширения «Security Settings». Например, для права интерактивного входа (Interactive Logon Right) используются параметры ***SeInteractiveLogonRight*** (разрешенные пользователи) и ***SeDenyInteractiveLogonRight*** (запрещенные пользователи).

Когда клиент пытается получить доступ к серверу, SSSD выполняет несколько шагов для обработки групповых политик:

- Скачивание файлов политики. Файлы **GPT.INI** и **GptTmpl.inf** скачиваются с сервера и сохраняются в кеше GPO на клиентской машине (в каталоге **/var/lib/sss/gpo_cache/**), чтобы ускорить доступ и избежать повторных запросов к серверу при каждом входе пользователя в систему;

- Анализ содержимого файлов. После того как файлы были получены и сохранены в кеше, процесс gpo_child начинает их обработку;

- Применение политики. После того как политика была загружена и ее содержание проанализировано, механизм принудительного применения GPO обеспечивает контроль доступа, проверяя политику против белого или черного списка, который может содержать разрешения или запреты для определенных групп.

Так как функция контроля доступа на основе GPO используется только провайдером AD, она включена в пакет *sssd-ad*. Исходные файлы для этой функции включены в **`libsss_ad.so`**. Эта функция не включена по умолчанию. Предоставлена конфигурационная опция ***`ad_gpo_access_control`***, которая может быть установлена в одно из следующих значений:

- disabled (не осуществляется ни проверка соответствия правилам управления доступом на основе GPO, ни их принудительное применение);
- enforcing (осуществляется проверка соответствия правилам управления доступом на основе GPO и их принудительное применение);
- permissive (осуществляется проверка соответствия правилам управления доступом на основе GPO, но не их принудительное применение. Вместо этого создаётся сообщение системного журнала, означающее, что пользователю было бы отказано в доступе, если бы в качестве значения этого параметра был задан принудительный режим).

С остальными конфигурационными параметрами, относящимися к GPO, можно ознакомиться в **`man sssd-ad`**.

14.4.2.2. Winbind

В Альт Домен поддержка групповых политик Samba не реализована, но теоретически Winbind их поддерживает.

14.5. Обновление DNS

При вводе машины в домен, в DNS-записи на DNS-сервере прописывается текущий IP-адрес машины. В случае изменения IP-адреса для взаимодействия с AD используются службы Winbind и SSSD для обновления DNS-записей.

14.5.1. SSSD

Для включения обновления IP-адресов службой sssd существует несколько способов. Подробнее см. Обновление IP-адресов службой sssd.

14.5.2. Winbind

Samba Winbind не поддерживает возможность динамического обновления DNS-записей. Для обхода этой проблемы была разработана программа, реализующая динамическое обновление адресов на DNS-сервере при использовании winbind в качестве клиента домена — **`winbind-dnsupdate`**. Подробнее см. winbind-dnsupdate.

14.6. Поддержка работы с несколькими доменами и доверительные отношения

14.6.1. SSSD

Работа с несколькими доменами

SSSD с поставщиком данных AD (***`id_provider = ad`***) может использоваться для получения данных пользователей и проверки подлинности пользователей из доверенных доменов. В настоящее время распознаются только домены, находящиеся в одном и том же лесу (Parent-Child Trust). Кроме того, контроллеры доменов из доверенных доменов всегда обнаруживаются автоматически.

Поддержка кросс-лесных доверий

SSSD не поддерживает трасты уровня леса (Forest Trusts), что ограничивает его возможности при работе с многоуровневыми лесами доменов.

14.6.2. Winbind

Работа с несколькими доменами

Winbind на клиентских машинах не распознаёт доверенные домены. Чтобы устранить эту проблему, необходимо внести изменения в конфигурационный файл **`smb.conf`** на Linux-клиентах, подключенных через Winbind. В секции [global] этого файла следует добавить соответствующую опцию:

```
winbind scan trusted domains = yes
```

Поддержка кросс-лесных доверий

Winbind поддерживает трасты уровня леса (Forest Trusts).

Глава 15. Подготовка системы к вводу в домен

15.1. Синхронизация времени

15.2. Настройка DNS

15.1. Синхронизация времени

Синхронизация времени с контроллером домена производится автоматически.

15.2. Настройка DNS

Альт Домен использует DNS для обнаружения других контроллеров домена и служб, таких как Kerberos. Поэтому, члены и серверы домена должны иметь возможность разрешать зоны DNS.

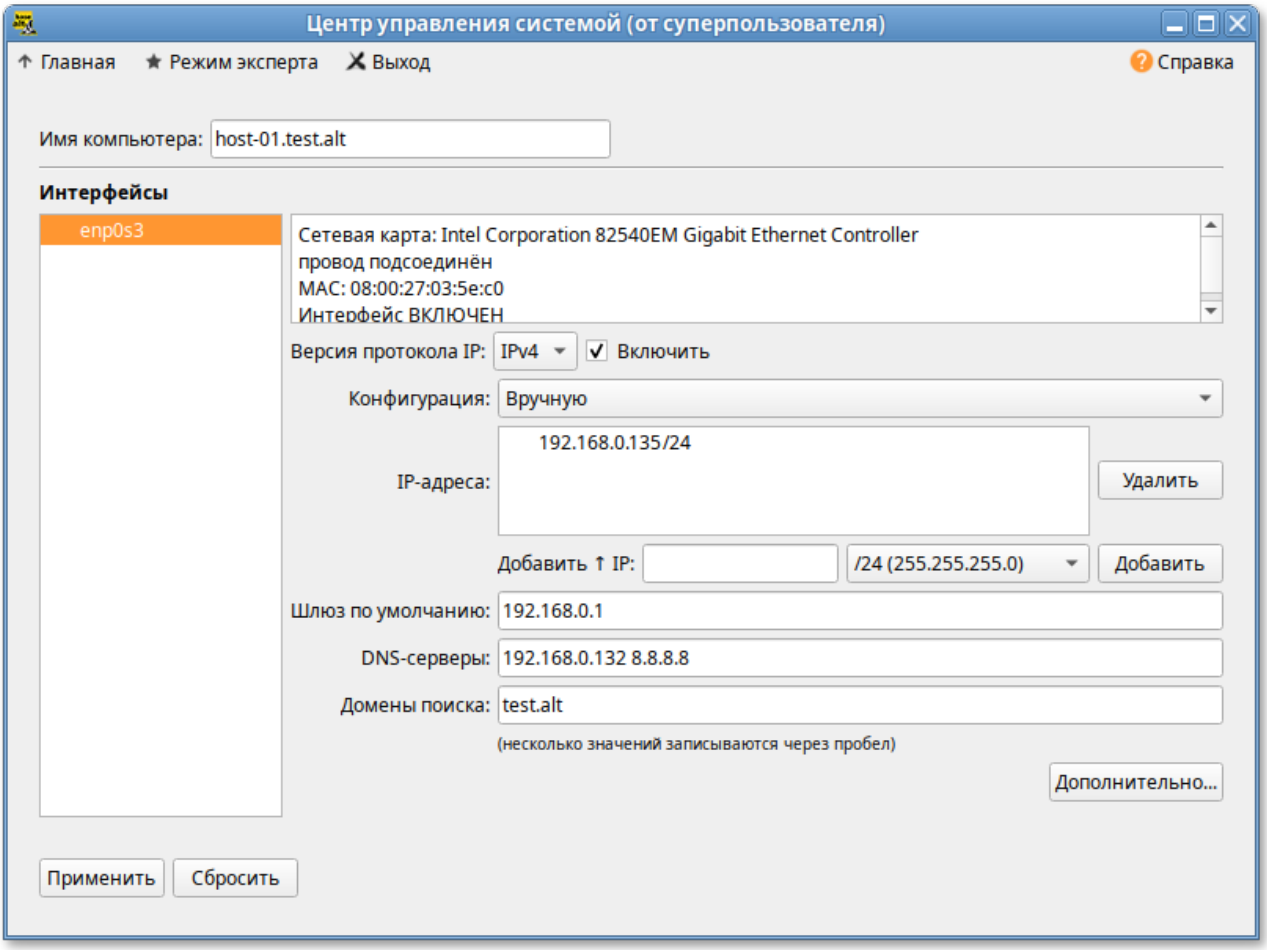
Для ввода компьютера в домен, на нём должен быть доступен сервер DNS, имеющий записи про контроллер домена. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от DHCP-сервера.

Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

15.2.1. Настройка клиентов для использования DNS-серверов вручную

Настройку сети можно выполнить как в графическом интерфейсе, так и в консоли.

В Центре управления системой **Сеть → Ethernet интерфейсы** задать имя компьютера, указать в поле **DNS-серверы** DNS-сервер домена и в поле **Домены поиска** — домен для поиска:



Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname host-01.test.alt
```

- в качестве первичного DNS должен быть указан DNS-сервер домена. Для этого необходимо создать файл **/etc/net/ifaces/enp0s3/resolv.conf** со следующим содержимым:

```
nameserver 192.168.0.132
```

где 192.168.0.132 — IP-адрес DNS-сервера домена.

- указать службе resolvconf использовать DNS контроллера домена и домен для поиска. Для этого в файле **/etc/resolvconf.conf** добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* enp0s3'
search_domains=test.alt
```

где enp0s3 — интерфейс, на котором доступен контроллер домена, test.alt — домен.

- обновить DNS адреса:

```
# resolvconf -u
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В результате выполненных действий в файле **/etc/resolv.conf** должны появиться строки:

```
search test.alt
nameserver 192.168.0.132
```

15.2.2. Проверка разрешения DNS

Для проверки того, что настройки DNS верны и машины могут разрешать IP-адреса и имена, можно использовать команды **nslookup** и **host**.

Прямой поиск:

```
# nslookup dc1.test.alt
Server:         192.168.0.132
Address:192.168.0.132#53

Name:   dc1.test.alt
Address: 192.168.0.132

# host dc1.test.alt
dc1.test.alt has address 192.168.0.132
```

Обратный поиск:

```
# nslookup 192.168.0.132
132.0.168.192.in-addr.arpa      name = dc1.alt.test.

# host 192.168.0.132
132.0.168.192.in-addr.arpa domain name pointer dc1.alt.test.
```

Следует обратить внимание, что в Samba AD обратная зона не настраивается автоматически. Чтобы настроить обратную зону, см. Администрирование DNS.

Альт Домен использует записи SRV для поиска служб, таких как Kerberos и LDAP. Проверка разрешения SRV-записей:

```
$ nslookup
> set type=SRV
> _ldap._tcp.test.alt
Server:         192.168.0.132
Address:192.168.0.132#53

_ldap._tcp.test.alt     service = 0 100 389 dc2.test.alt.
_ldap._tcp.test.alt     service = 0 100 389 dc1.test.alt.
> exit
```

или:

```
$ host -t SRV _ldap._tcp.test.alt
_ldap._tcp.test.alt has SRV record 0 100 389 dc1.test.alt.
_ldap._tcp.test.alt has SRV record 0 100 389 dc2.test.alt.
```

Глава 16. Присоединение к домену в роли участника

16.1. Команда system-auth

16.2. Подключение к домену с использованием SSSD

16.3. Подключение к домену с использованием Winbind

16.1. Команда system-auth

Для ввода клиентских машин в Альт Домен, в дистрибутивах «Альт» используется команда **system-auth**:

```
# system-auth <Действие> <Опции>
```

В таблице Параметры команды system-auth приведено описание параметров команды **system-auth**.

Таблица 16.1. Параметры команды system-auth

Параметр	Описание
Действие	
status	Показать текущую схему аутентификацию
list	Вывести список доступных схем аутентификации
write	Установить заданные параметры аутентификации
Опция	
-d	Включить отладку
--winbind	Использовать Samba Winbind для подключения системы к домену (если этот параметр не указан, будет использован SSSD)
--gpo	Включить групповые политики на машине

Параметр	Описание
--createcomputer=OU/SubOU	Субконтейнер в домене (организационная единица/подразделение), куда будет помещена машина при вводе в домен
--windows2003	Ввести станцию в домен windows 2003
--version	Вывести версию программы

Примеры использования команды **system-auth**:

- вывести текущую схему аутентификации:

```
# system-auth status
ad TEST.ALT HOST-01 TEST
```

- использовать локальную аутентификацию:

```
# system-auth write local
```

- использовать доменную аутентификацию (по умолчанию используется билет Kerberos):

```
# system-auth write ad <Домен> <Имя компьютера> <Рабочая группа> <Имя
пользователя> [<Пароль>] [--windows2003] [--createcomputer="COMPUTEROU/
SubCOMPUTEROU/SubSubCOMPUTEROU"] [--winbind] [--gpo]
```

16.2. Подключение к домену с использованием SSSD

В этом разделе описывается использование демона служб безопасности системы (SSSD) для подключения системы к Альт Домен.

SSSD используется для доступа к пользовательскому каталогу для аутентификации и авторизации через общую структуру с кешированием пользователей, чтобы разрешить автономный вход в систему. SSSD легко настраивается; он обеспечивает интеграцию подключаемых модулей аутентификации (PAM) и службы переключения имен (NSS), базу данных для хранения локальных пользователей, а также расширенных пользовательских данных, полученных с центрального сервера.

Дополнительные ресурсы:

- **man realm**
- **man sssd-ad**
- **man sssd**

16.2.1. Установка пакетов

Установить пакет *task-auth-ad-sssd*:

```
# apt-get install task-auth-ad-sssd
```

16.2.2. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-01 test 'administrator' 'Pa$$word'
Joined 'HOST-01' to dns domain 'test.alt'
```

где:

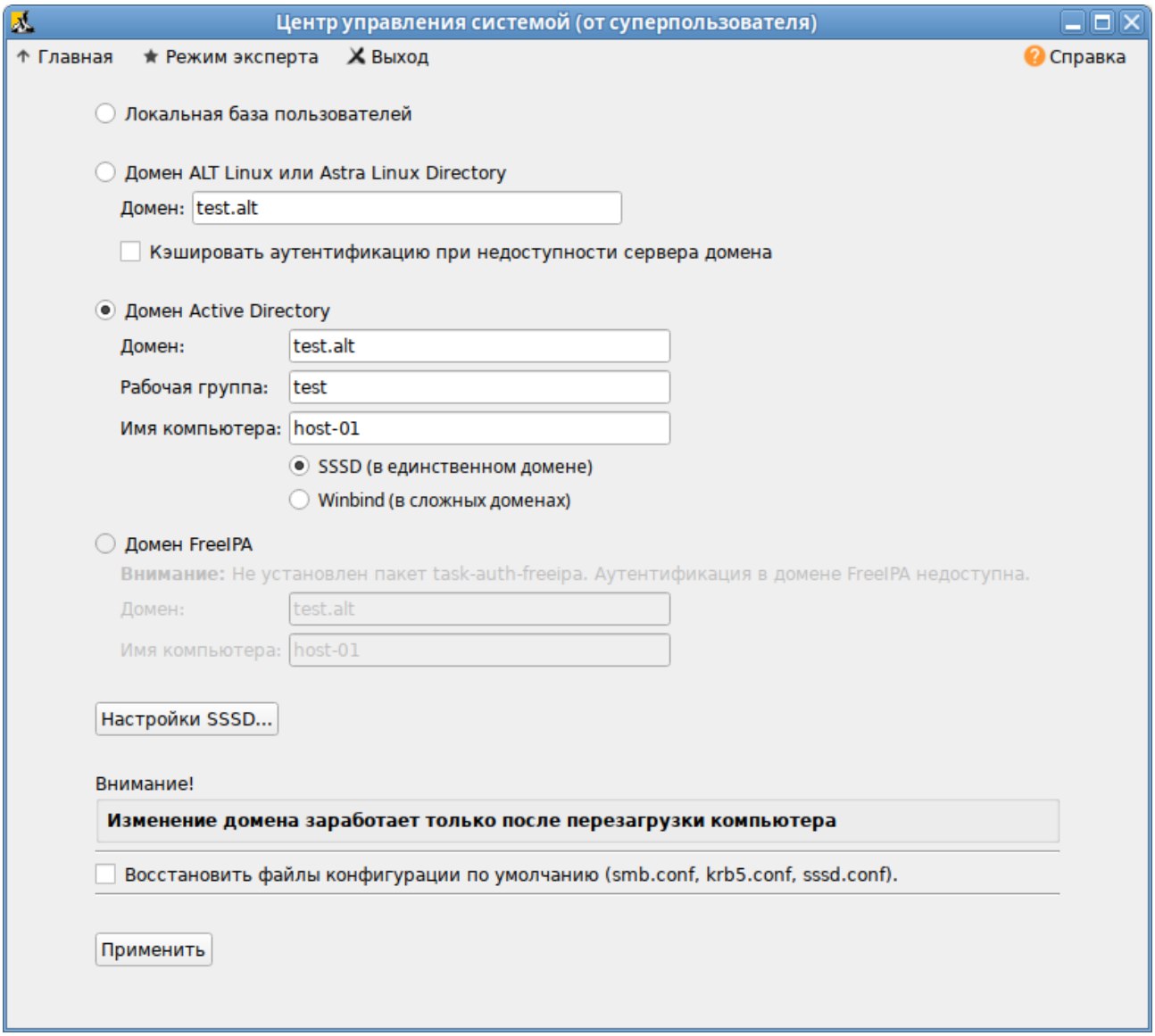
- test.alt — имя домена;
- host-01 — имя компьютера, вводимого в домен;
- test — рабочая группа;
- administrator — имя пользователя, имеющего право вводить машины в домен;
- Pa$$word — пароль пользователя, имеющего право вводить машины в домен.

Перезагрузить рабочую станцию для применения всех настроек.

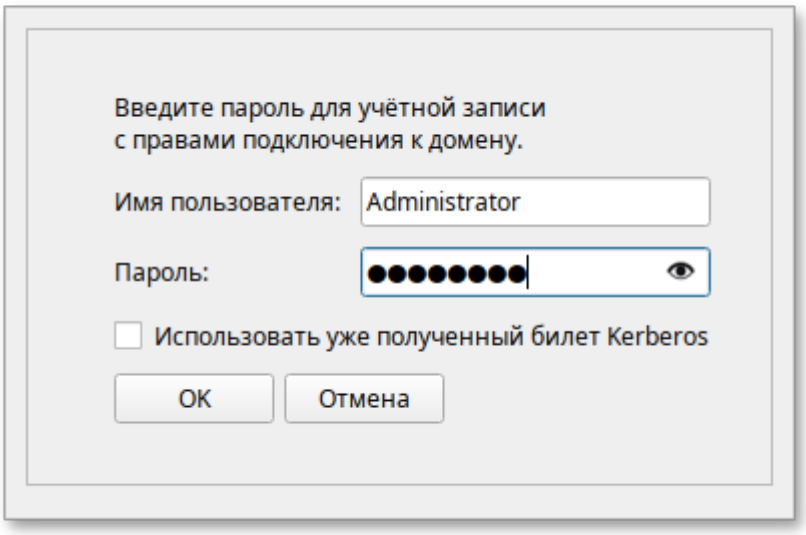
16.2.3. Ввод в домен в Центре управления системой

Для ввода компьютера в домен в **Центре управления системой** необходимо выбрать пункт **Пользователи** → **Аутентификация**.

В окне модуля **Аутентификация** следует выбрать пункт **Домен Active Directory**, заполнить поля (**Домен**, **Рабочая группа**, **Имя компьютера**), выбрать пункт **SSSD (в единственном домене)** и нажать кнопку **Применить**:

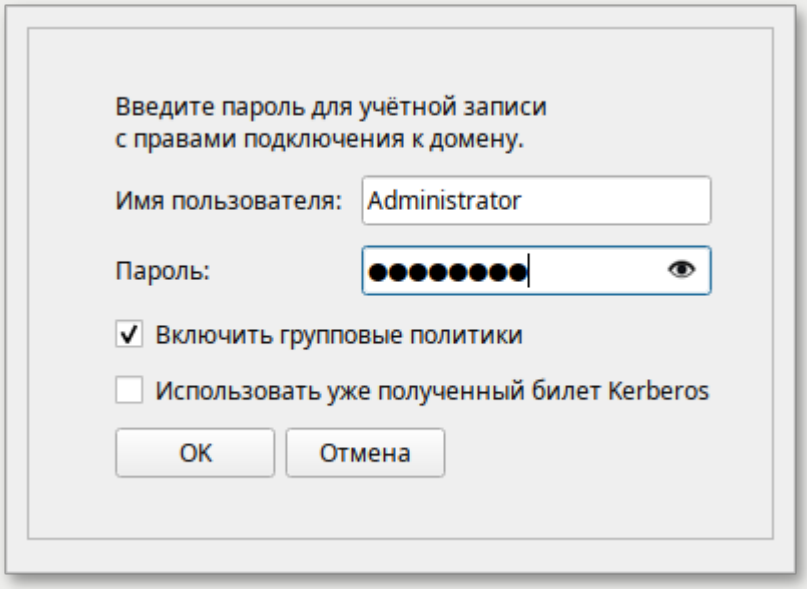


В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **OK**:

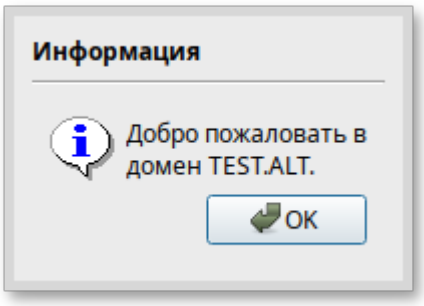


Примечание

Если на машине установлен пакет *alterator-gpupdate*, при подключении машины к домену можно включить групповые политики. Для включения групповых политик необходимо в окне ввода логина и пароля пользователя, с правами подключения к домену, отметить пункт **Включить групповые политики**:



При успешном подключении к домену отобразится соответствующая информация:



Перезагрузить рабочую станцию для применения всех настроек.

16.2.4. Проверка результатов присоединения

Проверка корректности присоединения:

1. Для проверки возможности поиска доменных пользователей отобразить сведения о пользователе домена (ivanov — пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash
```

2. Проверить возможность получения информации о домене:

```
# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
```

```
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27 EET
```

3. Проверить, действителен ли пароль учетной записи компьютера:

```
# net ads testjoin
Join is OK
```

Примечание

Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Примечание

О настройке SSSD см. Настройка SSSD и Настройки SSSD в ЦУС.

16.3. Подключение к домену с использованием Winbind

В этом разделе описывается использование Samba Winbind для подключения системы к Альт Домен.

Дополнительные ресурсы:

- **man realm**
- **man winbindd**

16.3.1. Установка пакетов

Установить пакет *task-auth-ad-winbind*:

```
# apt-get install task-auth-ad-winbind
```

16.3.2. Ввод в домен в командной строке

Для ввода компьютера в домен необходимо выполнить команду:

```
# system-auth write ad test.alt host-02 test 'administrator' 'Pa$$word' --winbind
Joined 'HOST-02' to dns domain 'test.alt'
```

где:

- test.alt — имя домена;

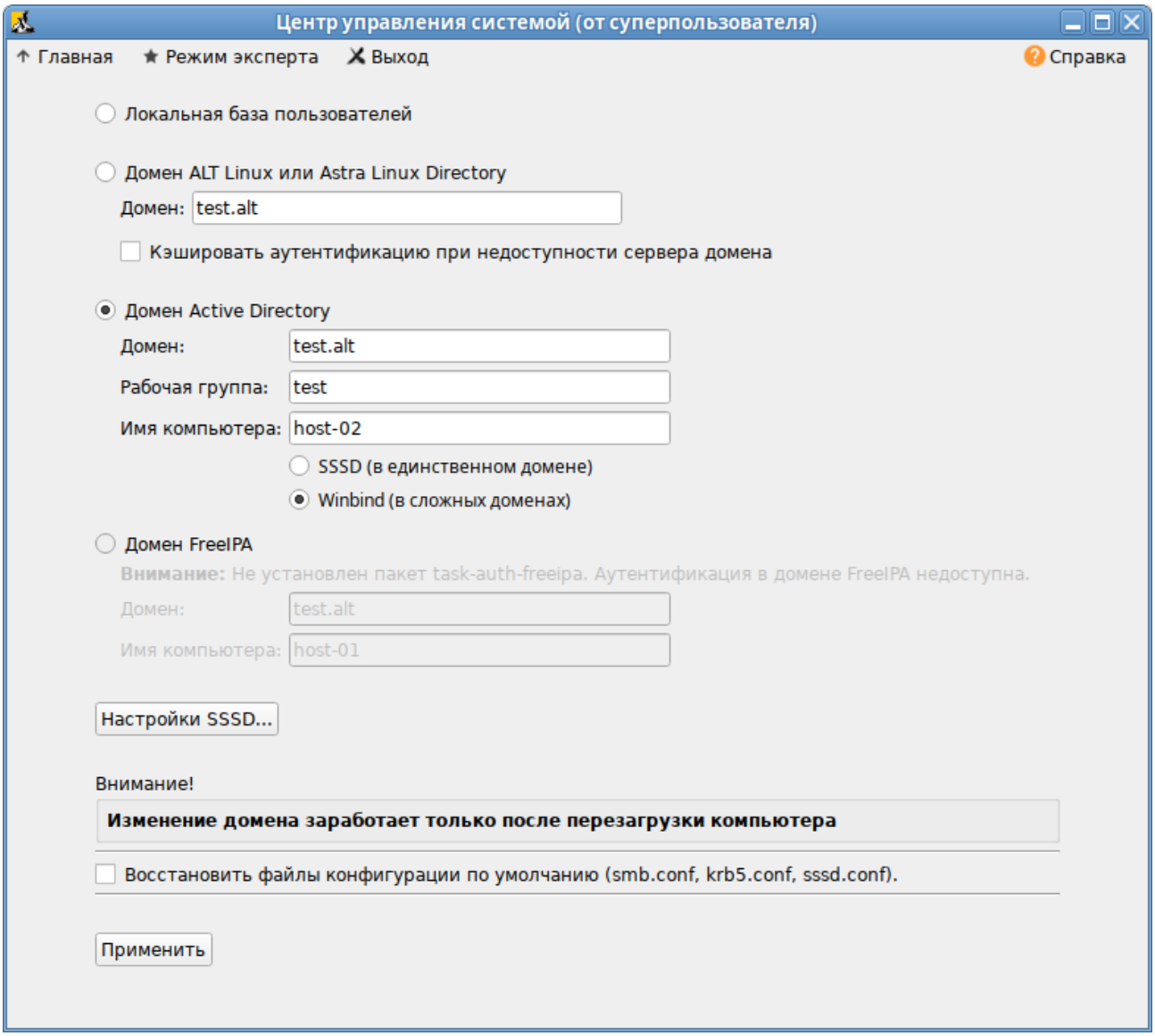
- host-02 — имя компьютера, вводимого в домен;
- test — рабочая группа;
- administrator — имя пользователя, имеющего право вводить машины в домен;
- Pa$$word — пароль пользователя, имеющего право вводить машины в домен.

Перезагрузить рабочую станцию для применения всех настроек.

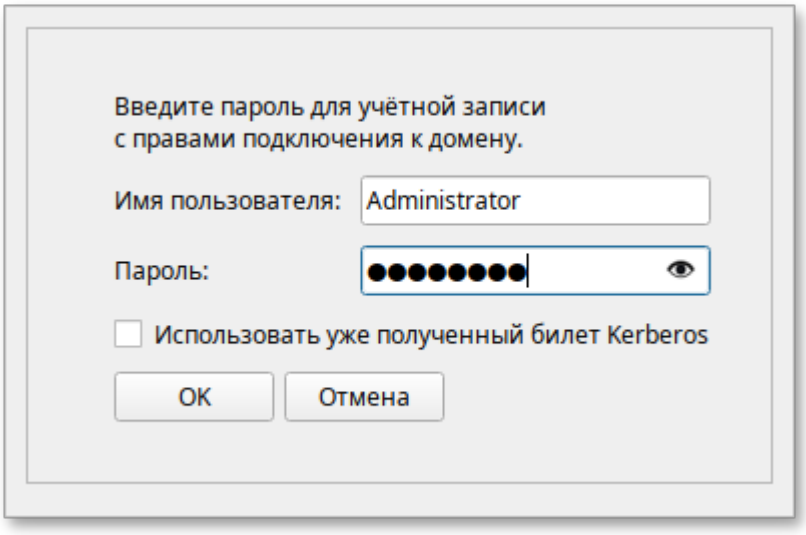
16.3.3. Ввод в домен в Центре управления системой

Для ввода компьютера в домен в Центре управления системой необходимо выбрать пункт **Пользователи** → **Аутентификация**.

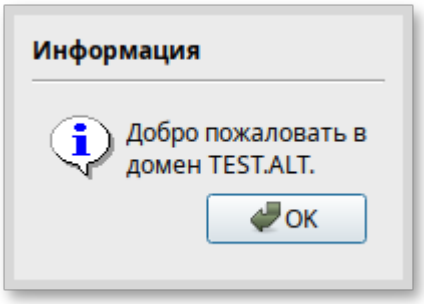
В окне модуля **Аутентификация** следует выбрать пункт **Домен Active Directory**, заполнить поля (**Домен**, **Рабочая группа**, **Имя компьютера**), выбрать пункт **Winbind (в сложных доменах)** и нажать кнопку **Применить**:



В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **OK**:



При успешном подключении к домену отобразится соответствующая информация:



Для применения всех настроек следует перезагрузить рабочую станцию.

16.3.4. Проверка результатов присоединения

Проверка корректности присоединения:

1. Для проверки возможности поиска доменных пользователей отобразить сведения о пользователе домена (ivanov — пользователь в домене):

```
# getent passwd ivanov
ivanov:*:1187401105:1187400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash
```

2. Проверить возможность получения информации о домене:

```
# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27 EET
```

3. Проверить, действителен ли пароль учетной записи компьютера:

```
# net ads testjoin
Join is OK
```

Примечание

Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Глава 17. Вход пользователя

После ввода системы в домен список локальных пользователей в окне входа в систему будет автоматически скрыт.

Примечание

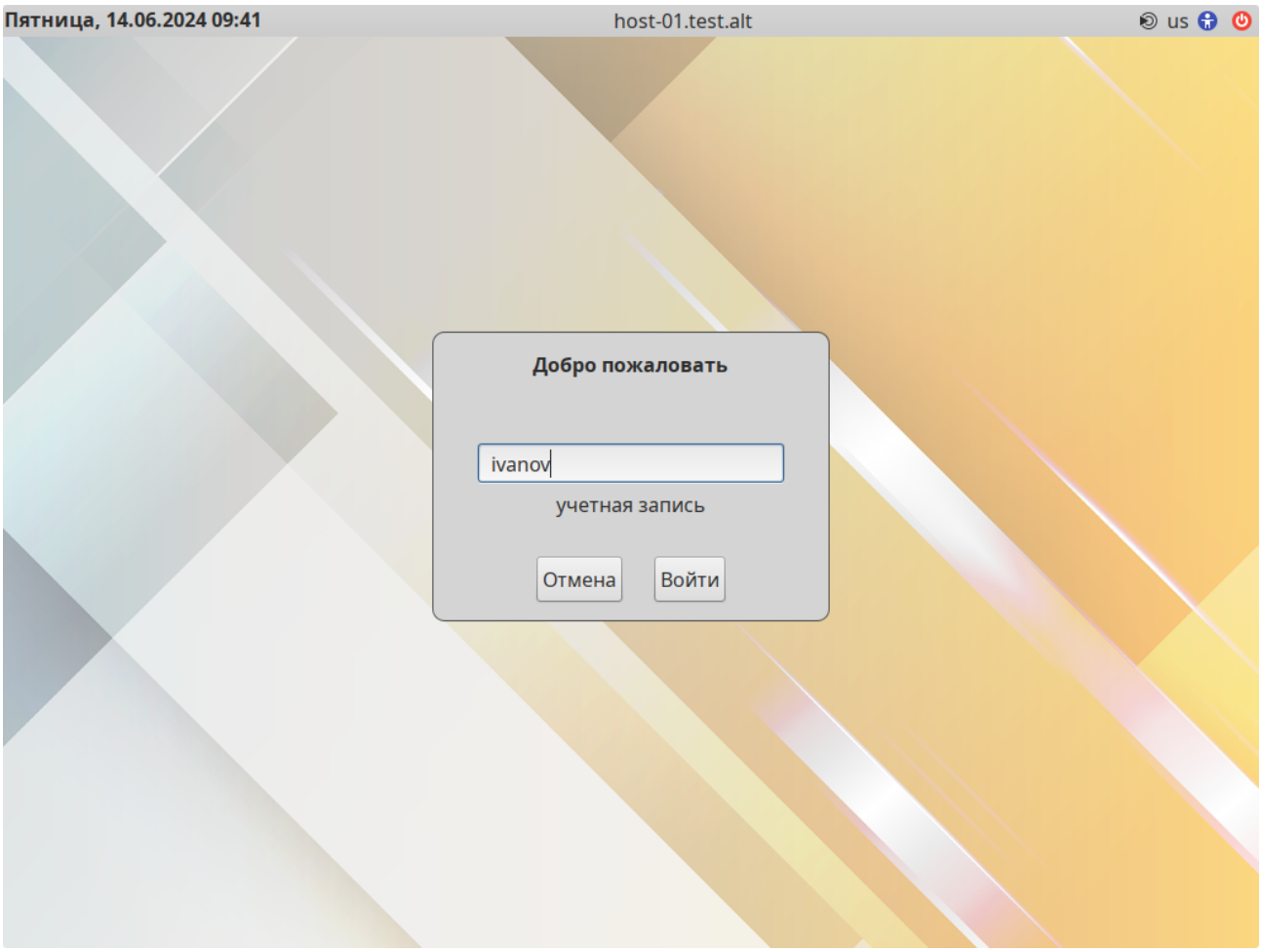
Определить будет ли показан список пользователей на экране приветствия/входа в систему LightDM можно с помощью control:

```
# control lightdm-greeter-hide-users
```

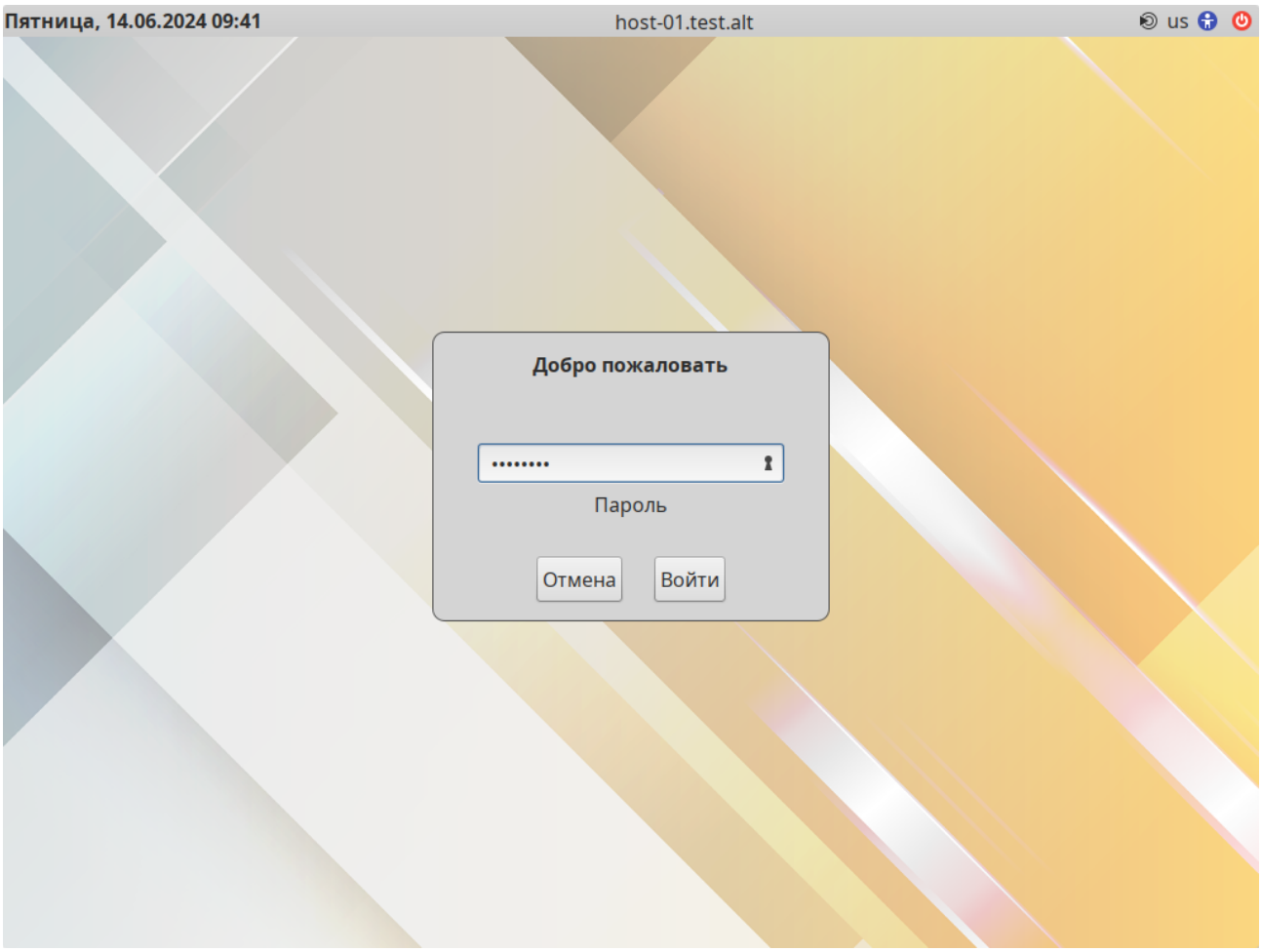
В команду можно передать следующие параметры:

- show — показать список доступных пользователей в greeter;
- hide — не перечислять пользователей в greeter.

Для регистрации в системе необходимо ввести логин учетной записи пользователя домена и нажать **Enter** или щелкнуть на кнопке **Войти**:



В открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку **Войти**:



Чтобы настроить автоматическое заполнение поля **Имя пользователя** именем последнего пользователя, входившего в систему, в файле **/etc/lightdm/lightdm-gtk-greeter.conf** (группа [greeter]), необходимо указать:

```
enter-username = true
```

Примечание

В случае использования в окне логина символов верхнего регистра (например, Irina.Soboleva вместо irina.soboleva) или лишних символов (не использующихся для стандартного имяобразования в Linux) может наблюдаться некорректное поведение системы (в частности не выставляются переменные окружения XDG_RUNTIME_DIR и DBUS_SESSION_BUS_ADDRESS).

Для возможности использовать для входа привычные способы написания логина (с доменным суффиксом, точками, символами верхнего регистра) необходимо выполнить команду (должен быть установлен пакет *pam-config-control*):

```
# control pam_canonicalize_user enabled
```

или в файле **/etc/pam.d/system-auth-common** раскомментировать строку:

```
auth required pam_canonicalize_user.so
```

Модуль PAM pam_canonicalize_user.so использует введенное имя пользователя в качестве ключа для запроса базы данных паролей и заменяет имя пользователя на возвращенное значение.

Глава 18. Отображение глобальных групп на локальные

При вводе машины в домен создаются следующие локальные роли:

- роль пользователей (users);
- роль пользователей с расширенными правами (powerusers);
- роль локальных администраторов (localadmins).

Локальные роли users и localadmins назначаются для глобальных групп в домене.

Список назначенных ролей и привилегий:

```
# rolelst
domain users:users
domain admins:localadmins
localadmins:wheel,vboxadd,vboxusers
powerusers:remote,vboxadd,vboxusers
users:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scanner,uucp,vboxu
sers,fuse,vboxadd
vboxadd:vboxsf
# id ivanov
uid=906201103(ivanov) gid=906200513(domain users) группы=906200513(domain
users),906201107(sales),
906201114(office),100(users),80(cdwriter),22(cdrom),81(audio),475(video),19(proc)
,
83(radio),444(camera),71(floppy),498(xgrp),499(scanner),14(uucp),462(vboxusers),4
64(fuse),488(vboxadd),487(vboxsf)
```

Если необходимо выдать права администраторов пользователям, которые не являются администраторами домена (Domain Admins), то нужно на контроллере домена завести новую группу в AD (например, PC Admins):

```
# samba-tool group add 'PC Admins'
Added group PC Admins
```

Добавить туда необходимых пользователей (например, пользователя ivanov):

```
# samba-tool group addmembers 'PC Admins' ivanov
Added members to group PC Admins
```

Затем на машине, введённой в домен, добавить роль для данной группы:

```
# roleadd 'PC Admins' localadmins
# rolelst
domain users:users
domain admins:localadmins
```

```
pc admins:localadmins
localadmins:wheel,vboxadd,vboxusers
powerusers:remote,vboxadd,vboxusers
users:cdwriter,cdrom,audio,video,proc,radio,camera,floppy,xgrp,scanner,uucp,vboxu
sers,fuse,vboxadd
vboxadd:vboxsf
```

После этого пользователь, входящий в группу PC Admins, сможет получать права администратора.

Глава 19. Отладочная информация

19.1. Настройка уровня журналирования Samba

19.2. Ошибка при подключении к IP-адресу 127.0.0.1

19.3. getent не показывает доменных пользователей и группы

19.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в разделе Уровни журналирования.

19.2. Ошибка при подключении к IP-адресу 127.0.0.1

Используя настройки по умолчанию, команда **net** подключается к IP-адресу 127.0.0.1. Если Samba не прослушивает петлевой интерфейс, соединение не устанавливается. Например:

```
# net rpc rights list -U administrator
Could not connect to server 127.0.0.1
Connection failed: NT_STATUS_CONNECTION_REFUSED
```

Чтобы решить эту проблему, необходимо настроить Samba для дополнительного прослушивания интерфейса loopback. Дополнительные сведения см. в разделе Настройка Samba для привязки к определённым интерфейсам.

Примечание

Чтобы временно обойти проблему, можно передать параметр ***-I <IP-адрес>*** или ***-S <Имя хоста>*** в команду **net**:

```
# net rpc rights list -U administrator -I 192.168.0.132
Password for [TEST\administrator]:
     SeMachineAccountPrivilege  Add machines to domain
      SeTakeOwnershipPrivilege  Take ownership of files or other objects
      …
```

19.3. getent не показывает доменных пользователей и группы

Используя команды **getent passwd** и **getent group** нельзя увидеть доменных пользователей и группы. Этот функционал отключен по умолчанию, для того чтобы сократить нагрузку на серверы. Поэтому для проверки необходимо указать точное имя пользователя:

```
# getent passwd <имя_пользователя>
```

Примечание

Список пользователей можно посмотреть на сервере командой:

```
# samba-tool user list
```

Если команда **getent passwd <имя_пользователя>** ничего не возвращает, следует попробовать выполнить команду:

```
# getent passwd <рабочая_группа>\<имя_пользователя>
```

Например:

```
# getent passwd "TEST\ivanov"
```

Если эта команда работает, а первая нет, то необходимо добавить следующую строку в файл **smb.conf**:

```
winbind use default domain = yes
```

Глава 20. Удаление клиента домена

Чтобы вывести систему из домена, можно воспользоваться командой **realm leave**. Эта команда удалит конфигурацию домена из SSSD и локальной системы:

```
# realm leave test.alt
```

По умолчанию удаление выполняется от имени администратора (для Альт Домен — administrator). Если для присоединения к домену использовалась учётная запись другого пользователя, может потребоваться выполнить удаление от имени этого пользователя. Чтобы указать пользователя следует использовать параметр **-U**:

```
# realm leave test.alt -U <пользователь>
```

Сначала команда пытается подключиться без использования учетных данных, но при необходимости запрашивает пароль.

Следует обратить внимание, что когда клиент удаляется из домена, учётная запись компьютера не удаляется из каталога; удаляется только конфигурация локального клиента. Если необходимо удалить учётную запись компьютера, следует запустить команду с параметром **--remove**:

```
# realm leave --remove test.alt
```

Для получения дополнительной информации см. справочную страницу **man realm** (8).

Примечание

После вывода из домена схема аутентификации пользователей в системе должна переключиться на локальную базу:

```
# control system-auth
local
```

Примечание

Для того чтобы в окне входа отображался список доступных пользователей, необходимо выполнить команду:

```
# control lightdm-greeter-hide-users show
```

или в файле **/etc/lightdm/lightdm.conf** закомментировать строку в группе ***[SeatDefaults]***:

```
#greeter-hide-users=true
```

Глава 21. Повторная регистрация клиента

В этом разделе рассмотрена процедура повторной регистрации клиента в Альт Домен с тем же именем хоста. Повторная регистрация может потребоваться, если клиентский компьютер был уничтожен и потерял связь с серверами домена, например, из-за аппаратного сбоя клиента.

Перед повторным вводом в домен необходимо убедиться в том, что машина удалена из домена. Чтобы запись в домене была автоматически удалена при выводе машины из домена, необходимо использовать команду:

```
# realm leave --remove <домен>
```

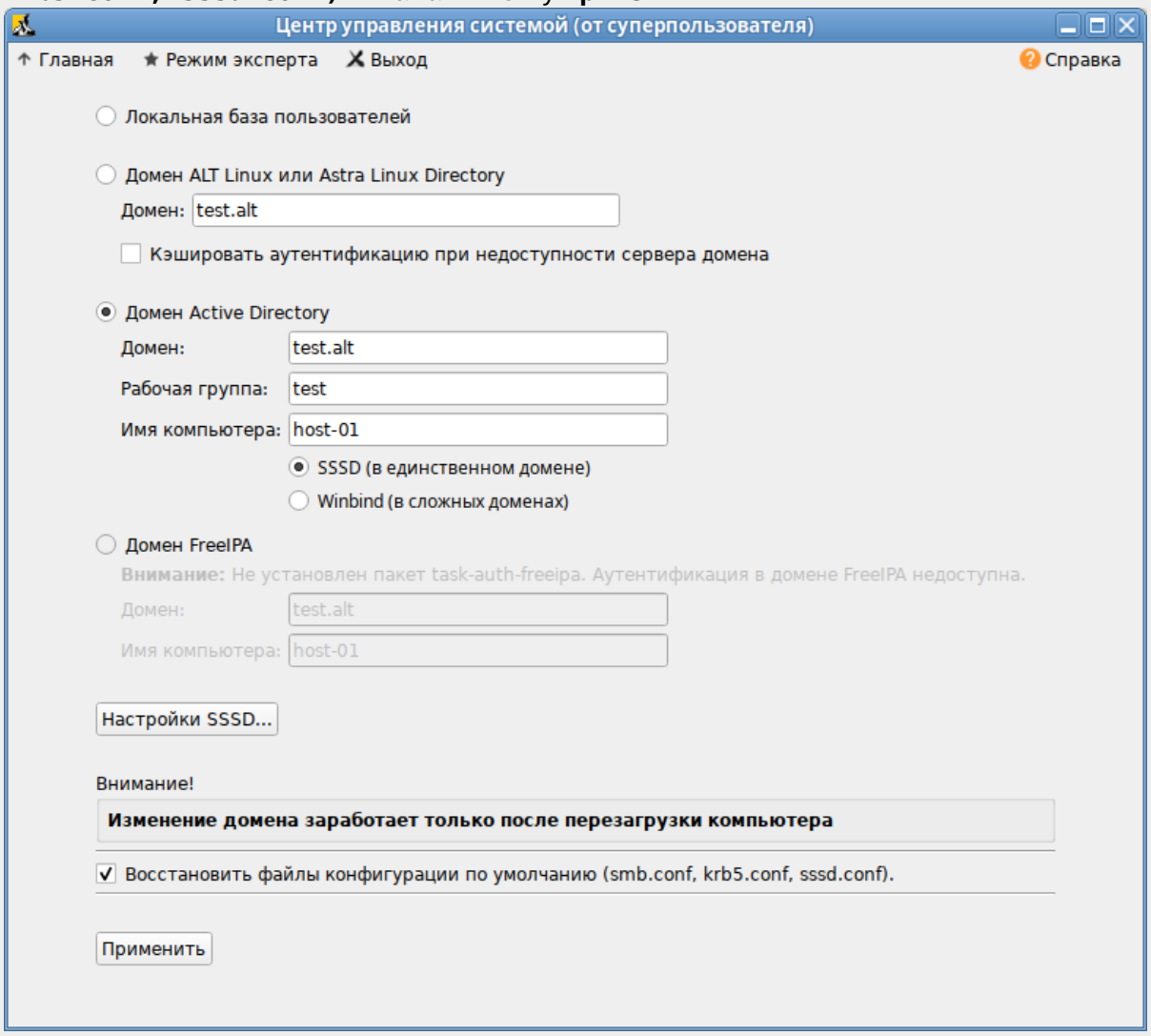
Возможно также понадобится удалить закешированные записи:

```
# sss_cache -E
```

После вывода машины из домена следует убедиться в корректности имени машины и восстановить файлы конфигурации **/etc/samba/smb.conf**, **/etc/sssd/sssd.conf** и **/etc/krb5.conf** к виду по умолчанию и повторно ввести машину в домен.

Примечание

Привести файлы **/etc/samba/smb.conf** и **/etc/krb5.conf** к виду по умолчанию можно в модуле ЦУС **Аутентификация**. В окне модуля **Аутентификация** следует установить отметку в поле **Восстановить файлы конфигурации по умолчанию (smb.conf, krb5.conf, sssd.conf)** и нажать кнопку **Применить**:



Глава 22. Настройка аутентификации доменных пользователей на контроллере домена

22.1. Установка пакетов

22.2. Изменение файлов конфигурации

22.3. Генерация keytab-файла

22.4. Службы

22.5. Настройка ролей

22.6. Групповые политики

22.7. Настройка SSH

22.8. Проверка результатов присоединения

Примечание

Настройка аутентификации доменных пользователей на контроллере домена с использованием SSSD не поддерживается.

Важно

На текущий момент (*samba 4.19.9*, *gpupdate 0.12.2*) данный метод не позволяет применять пользовательские групповые политики на контроллере домена, при этом машинные политики применяются успешно.

Важно

Для каталога **`/var/lib/samba/sysvol`** SID'ы домена сопоставляются с UID/GID по особому алгоритму, и изменить этот процесс с помощью настроек невозможно.

Важно

Winbind не поддерживает аутентификацию с использованием UPN (User Principal Name, например user@test.alt). Для входа и других операций следует использовать формат DOMAIN\user.

Контроллер домена в рамках доменной инфраструктуры является, в том числе, ещё одной машиной и имеет соответствующий машинный аккаунт. После применения настроек, описанных в этом разделе, машина с контроллером домена сможет выполнять, в том числе, и функции обычного члена домена, такие как:

- аутентификация доменными пользователями (в том числе по SSH);
- применение групповых политик;
- всё, что поддерживает обычная клиентская машина (в качестве клиента Winbind).

Важно

В качестве клиента на контроллере домена необходимо использовать Winbind.

22.1. Установка пакетов

На контроллере домена необходимо установить пакеты *task-auth-ad-winbind* и *gpupdate*:

```
# apt-get install task-auth-ad-winbind gpupdate
```

22.2. Изменение файлов конфигурации

22.2.1. Настройка Kerberos (krb5.conf)

В файле **/etc/krb5.conf** должны быть заданы следующие параметры:

- dns_lookup_realm = false
- default_realm = TEST.ALT

Пример файла **/etc/krb5.conf**:

```
[logging]

[libdefaults]
dns_lookup_kdc = true
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
default_realm = TEST.ALT

[realms]

[domain_realm]
```

22.2.2. Настройка Samba (smb.conf)

В файле **/etc/samba/smb.conf** должны быть заданы следующие параметры:

- kerberos method = dedicated keytab
- dedicated keytab file = /etc/krb5.keytab

Значения остальных параметров в файле должны соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла **/etc/samba/smb.conf**:

```
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1
    kerberos method = dedicated keytab
    dedicated keytab file = /etc/krb5.keytab
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    idmap_ldb:use rfc2307 = yes

    template shell = /bin/bash
    template homedir = /home/TEST.ALT/%U
```

```
    wins support = no
    winbind use default domain = yes
    winbind enum users = no
    winbind enum groups = no
    winbind refresh tickets = yes
    winbind offline logon = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No
```

После внесения изменений в файл **`smb.conf`** необходимо перезапустить Samba.

22.2.3. Настройка NSS (nsswitch.conf)

В файле **`/etc/nsswitch.conf`** должны быть заданы следующие параметры:

- passwd: files winbind systemd
- shadow: tcb files winbind
- group: files [SUCCESS=merge] winbind role systemd

Пример файла **`/etc/nsswitch.conf`**:

```
passwd:     files winbind systemd
shadow:     tcb files winbind
group:      files [SUCCESS=merge] winbind role systemd
gshadow:    files

hosts:      files myhostname dns

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

automount:  files
aliases:    files
```

22.2.4. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации Winbind-модуля:

```
# control system-auth winbind
```

22.3. Генерация keytab-файла

Необходимо сгенерировать системный keytab-файл для машинного аккаунта контроллера домена. Для этого следует выполнить следующую команду:

```
# net ads keytab create
```

Примечание

Сообщение об ошибке Kerberos:

```
kerberos_kinit_password TEST@TEST.ALT failed: Client not found in Kerberos
database
```

является ожидаемым в данной конфигурации и не указывает на неисправность.

Просмотреть результат:

```
# klist -ket
```

22.4. Службы

Необходимо отключить сервис **nscd**:

```
# systemctl disable --now nscd
```

22.5. Настройка ролей

Необходимо указать, какие локальные роли, каким группам домена соответствуют:

- обычные пользователи домена (*Domain Users*) соответствуют локальной роли *users*:

```
# roleadd 'domain users' users
```

- администраторы домена (*Domain Admins*) соответствуют локальной роли *localadmins*:

```
# roleadd 'domain admins' localadmins
```

Важно

В русскоязычных версиях MS Windows Server встроенные группы *Domain Users* и *Domain Admins* имеют русифицированные названия *Пользователи домена* и *Администраторы домена*.

22.6. Групповые политики

Для включения поддержки групповых политик необходимо выполнить команду:

```
# gpupdate-setup enable --local-policy ad-domain-controller
```

22.7. Настройка SSH

Разрешить удалённый доступ по SSH только *Администраторам домена*:

```
# control sshd-allow-groups enabled
# control sshd-allow-groups-list remote
```

При необходимости можно разрешить аутентификацию по Kerberos билетам:

```
# control sshd-gssapi-auth enabled
```

Примечание

Доменная учётная запись *Administrator* при использовании *winbind* получает локальный идентификатор (UID) = 0 (на контроллере домена это стандартное и неизменяемое поведение), что соответствует пользователю root в Linux. По умолчанию прямой вход по SSH под этой учётной записью запрещён из соображений безопасности.

Это поведение можно изменить, разрешив аутентификацию пользователю root:

```
# control sshd-permit-root-login enabled
```

Это снижает безопасность системы. Прямой доступ под root не рекомендуется в целях безопасности.

Для применения настроек необходимо перезапустить сервис **sshd**:

```
# systemctl restart sshd
```

Примечание

Данные настройки можно применить с помощью механизма групповых политик control. Подробнее см. Групповые политики control.

22.8. Проверка результатов присоединения

Для проверки возможности поиска доменных пользователей можно отобразить сведения о доменном пользователе (ivanov — пользователь в домене):

```
# getent passwd ivanov
TEST\ivanov:*:3000020:100::/home/TEST.ALT/ivanov:/bin/bash
```

Глава 23. Настройка обновления паролей аккаунтов машин

23.1. Локальная политика смены пароля

23.2. Включение обновления пароля

23.3. Отключение обновления пароля

23.4. Диагностика

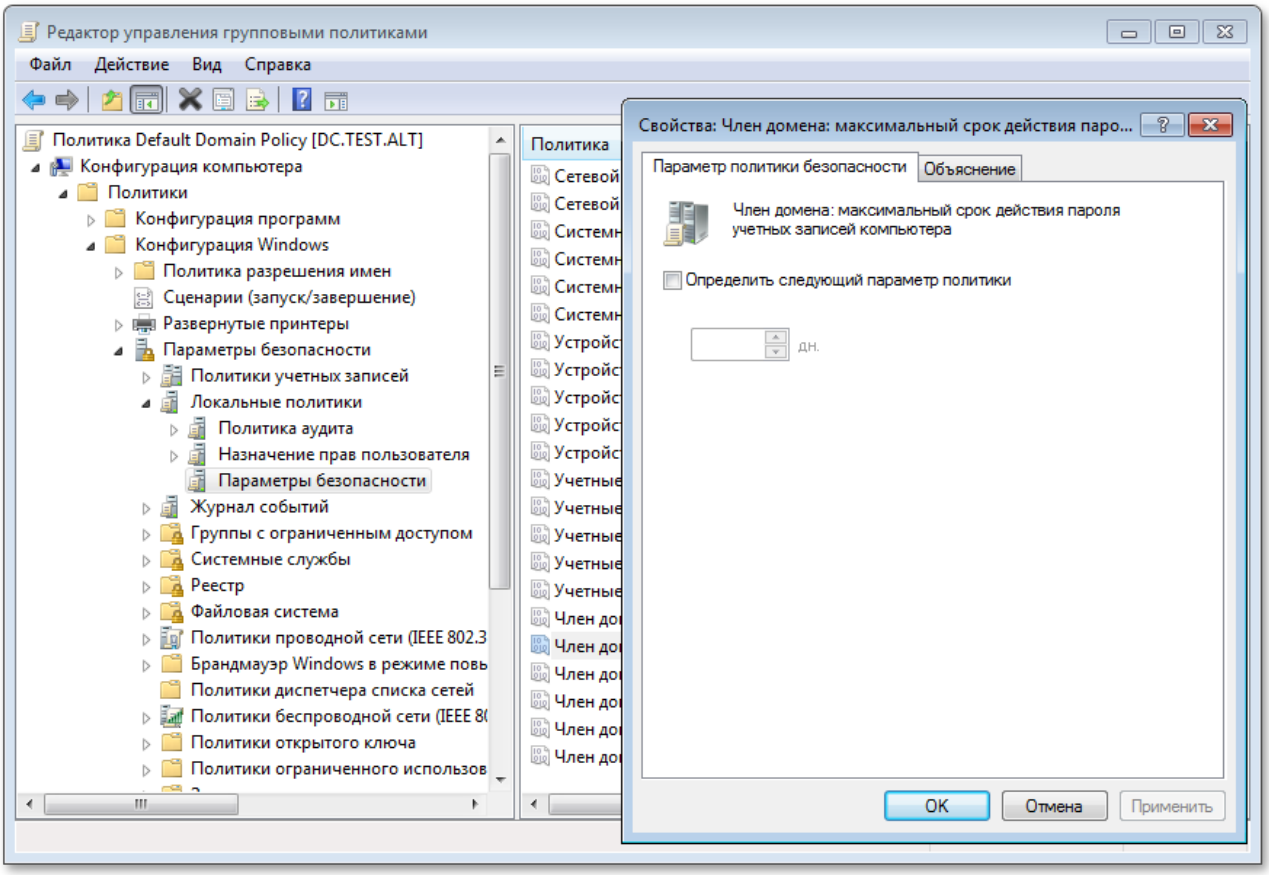
23.5. Восстановление работоспособности

После завершения процедуры ввода в домен каждая машина получает специальный аккаунт вида MACHINE01$. Такой аккаунт, ассоциированный с машиной, а не с конкретным пользователем, позволяет машине выполнять в домене действия от своего имени. Например, запрашивать информацию о пользователях, получать машинные групповые политики и т. д.

Как и у любого другого пользователя, у машинного пользователя есть свой пароль, генерируемый автоматически в процессе ввода машины в домен. В отличии от обычных пользователей, у машинных аккаунтов нет ограничения на время жизни пароля, но машина имеет возможность поменять его самостоятельно. По умолчанию машины с MS Windows 2000 и старше меняют пароль раз в 30 дней. Информация о последней смене пароля хранится в атрибуте машинного аккаунта **`pwdlastset`**.

23.1. Локальная политика смены пароля

Сменой пароля учётной записи компьютера можно управлять с помощью групповых политик. Для этого нужно отредактировать параметр политики домена по умолчанию (**`Default domain policy`**) **`Член домена: максимальный срок действия пароля учётной записи компьютера`**, который располагается в подразделе **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности** (**Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**).



Примечание

На данный момент в ADMC (*admc 0.16.3*) нет возможности настроить данные параметры групповой политики. Необходимо использовать оснастку RSAT «Управление групповыми политиками» (см. Установка административных инструментов (машина Windows)).

Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учётной записи компьютера. Значение по умолчанию: 30 дней.

С помощью параметра **`Член домена: отключить изменение пароля учётных записей компьютера`** можно отключить обновления пароля машинного аккаунта совсем, но делать этого не рекомендуется.

Важно

Выше указанные параметры корректно работают на машинах с ОС MS Windows 2000 и старше.

Важно

На машинах с ОС «Альт» (*sssd 2.9.4*) данные параметры игнорируются.

23.2. Включение обновления пароля

23.2.1. ОС Windows

Для включения периодического обновления пароля учётной записи компьютера на машинах под управлением ОС Windows 2000 и старше дополнительных действий не требуется. Периодичность обновления настраивается с помощью соответствующей групповой политики.

23.2.2. ОС «Альт»

За обновление пароля машинного аккаунта на машинах под управлением ОС «Альт» отвечают сервисы **sssd** и **winbind**.

23.2.2.1. Winbind

Winbind, на текущий момент (*samba-winbind 4.19.9*), не умеет после смены пароля учётной записи компьютера обновлять системный keytab-файл (**/etc/krb5.keytab**). Поэтому, во избежание конфликтов с sssd, следует отключить этот функционал.

Для отключения периодического обновления пароля учётной записи компьютера, необходимо в файл **/etc/samba/smb.conf** в секцию ***[global]*** добавить параметр ***machine password timeout = 0***:

```
[global]
machine password timeout = 0
```

23.2.2.2. SSSD

sssd для обновления пароля учётной записи компьютера использует утилиту **adcli**. Необходимо убедиться, что пакет *adcli* установлен в системе:

```
# apt-get install adcli
```

Периодичностью обновления пароля учётной записи компьютера можно управлять с помощью параметра ***ad_maximum_machine_account_password_age*** (секция ***[domain/<Домен>]***) в **/etc/sssd/sssd.conf**. Значение по умолчанию: 30 дней.

Для корректного функционирования обновления пароля учётной записи компьютера, **sssd** необходим доступ на запись в файл **/etc/krb5.keytab**. Для этого не достаточно привилегий пользователя _sssd, от которого обычно и запускается **sssd**. Необходимо запускать **sssd** с правами суперпользователя. Для этого следует в файле **/etc/sssd/sssd.conf** в секции ***[sssd]*** изменить значение параметра ***user*** на root:

```
[sssd]
user = root

[domain/<Домен>]
ad_update_samba_machine_account_password = true
```

Важно

При вводе компьютера в домен с помощью ЦУС следующие параметры прописываются в конфигурационные файлы по умолчанию:

- **/etc/samba/smb.conf**:

```
machine password timeout = 0
```

- **/etc/sssd/sssd.conf**:

```
ad_update_samba_machine_account_password = true
```

23.3. Отключение обновления пароля

23.3.1. ОС Windows

Для отключения периодического обновления пароля учётной записи компьютера на машинах под управлением ОС Windows 2000 и старше, достаточно включить параметр групповой политики **Default domain policy** **Член домена: отключить изменение пароля учётных записей компьютера**.

23.3.2. ОС «Альт»

Для отключения периодического обновления пароля учётной записи компьютера на машинах под управлением ОС «Альт», необходимо:

- в файле **/etc/sssd/sssd.conf** (секция ***[domain/<Домен>]***) значение параметра ***ad_maximum_machine_account_password_age*** установить равным 0:

```
[domain/<Домен>]
ad_maximum_machine_account_password_age = 0
```

- в файле **/etc/samba/smb.conf** (секция ***[global]***) значение параметра ***machine password timeout*** установить равным 0:

```
[global]
machine password timeout = 0
```

23.4. Диагностика

23.4.1. Дата последней смены пароля

Дата последней смены пароля учётной записи компьютера хранится в базе данных домена. Запросить её можно одним из следующих способов:

- на введённой в домен машине выполнить команду:

```
# net ads info
…
Last machine account password change: Ср, 20 мар 2024 12:36:35 EET
```

- если машина уже потеряла доверие в домене, то выполнить эту же команду от доменного пользователя:

```
# net ads info -U <user>
```

Дата последней смены пароля учётной записи компьютера будет показана в параметре ***Last machine account password change***.

23.4.2. Потеря доверия между машиной и доменом

Для проверки того, имеет ли машина возможность аутентифицироваться в домене, можно выполнить следующие действия:

- убедиться, что файл keytab (**/etc/krb5.keytab**) содержит корректную информацию:

```
# klist -ke
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------------
   1 host/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 host/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 host/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 host/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 host/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 host/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/WORK@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 restrictedkrbhost/WORK@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 restrictedkrbhost/work.test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 restrictedkrbhost/WORK@TEST.ALT (DEPRECATED:arcfour-hmac)
   1 WORK$@TEST.ALT (aes256-cts-hmac-sha1-96)
   1 WORK$@TEST.ALT (aes128-cts-hmac-sha1-96)
   1 WORK$@TEST.ALT (DEPRECATED:arcfour-hmac)
```

- попытаться получить билет Kerberos для учётной записи компьютера (в примере WORK$), используя файл keytab (**/etc/krb5.keytab**):

```
# kinit -k WORK\$@TEST.ALT
```

- убедиться, что билет успешно получен и удалить его:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: WORK$@TEST.ALT

Valid starting       Expires              Service principal
```

```
21.04.2023 12:25:37  21.04.2023 22:25:37  krbtgt/TEST.ALT@TEST.ALT
    renew until 28.04.2023 12:25:37

# kdestroy -p WORK\$@TEST.ALT
```

Важно

Следует убедиться, что имя машины в keytab-файле (**/etc/krb5.keytab**) соответствует реальному имени машины (см. вывод команды **hostnamectl**).

23.5. Восстановление работоспособности

Если диагностика показала, что машина потеряла доверие с доменом, то для восстановления работоспособности, необходимо выполнить следующие действия:

- обновить систему:

```
# apt-get update && apt-get dist-upgrade
```

- удалить файл **/etc/krb5.keytab**;
- повторно ввести машину в домен;
- убедиться, что конфигурационные файлы соответствуют одному из сценариев: Включение обновления пароля или Отключение обновления пароля;
- перезагрузить машину.

Часть V. Инструменты управления объектами домена и групповыми политиками

Содержание

24. Групповые политики в Альт Домен
25. Установка административных шаблонов и административных инструментов
26. Включение механизма применения конфигурации на клиентских машинах
27. Модуль клиентской машины для применения конфигурации
28. Модуль удаленного управления базой данных конфигурации (ADMC)
29. Модуль редактирования настроек клиентской конфигурации (GPUI)
30. Расширение возможностей ГП
31. Решение проблем

Глава 24. Групповые политики в Альт Домен

Групповые политики — это набор правил и настроек для серверов и рабочих станций, реализуемых в корпоративных решениях. В соответствии с групповыми политиками производится настройка рабочей среды относительно локальных политик, действующих по умолчанию.

Групповые политики, как механизм, отличаются от стандартных инструментов управления конфигурациями (Puppet, Ansible) тремя ключевыми особенностями:

- интеграцией в инфраструктуру Active Directory;
- соответствием декларативной части настроек конфигураций конкретным дистрибутивным решениям;
- наличием не только управления конфигурациями компьютеров, но и конфигурациями пользователей.

В дистрибутивах «Альт» для применения групповых политик используется инструмент **`gpupdate`** (см. Модуль клиентской машины для применения конфигурации). Инструмент рассчитан на работу на машине, введённой в Альт Домен.

Интеграция в инфраструктуру LDAP-объектов Альт Домен позволяет осуществлять привязку настроек управляемых конфигураций объектам в дереве каталогов. Кроме глобальных настроек в рамках домена, возможна привязка к следующим группам объектов:

- подразделения (OU) — пользователи и компьютеры, хранящиеся в соответствующей части дерева объектов;
- сайты — группы компьютеров в заданной подсети в рамках одного и того же домена;
- конкретные пользователи и компьютеры.

Кроме того, в самих объектах групповых политик могут быть заданы дополнительные условия, фильтры и ограничения, на основании которых принимается решение о том, как применять данную групповую политику.

Политики подразделяются на политики для компьютеров (Machine) и политики для пользователей (User). Некоторые задачи управления конфигурациями можно решить как через пользовательские, так и через машинные параметры.

Примечание

Групповая политика для компьютеров должна быть привязана к OU с компьютерами. Групповая политика для пользователей должна быть привязана к OU с пользователями. Объект, к которому должна применяться политика, должен находиться в нужном OU с компьютерами или пользователями. Подробнее см. Область действия и статус групповой политики.

Политики для компьютеров применяются на узле в момент загрузки, а также в момент явного или регулярного запроса планировщиком (раз в час). Пользовательские политики применяются в момент входа в систему.

Система управления групповых политик в Альт Домен представлена широким набором конфигурационных настроек. В общем виде эти настройки делятся на две категории — политики и предпочтения. Основное отличие политик от предпочтений состоит в том, что политики можно отменить, поскольку они «накладываются» через реестр поверх настроек приложений так, что приложения не могут их изменить. Исключение составляют настройки перегружаемые через такие такой механизм, как GConf или dconf, а также определённые правила для PolicyKit.

Основным отличием предпочтений от политик состоит в том, что эти настройки пользователь или приложение может изменить или отменить после их применения. Регулярная перезапись таких настроек частично сглаживает эту особенность, доставляя конечному пользователю неудобство, но не ограничивая его возможности повлиять на заданную для него или его компьютера политику, точнее, предпочтение.

Одним из ключевых ограничений, не позволяющих использовать политики вместо предпочтений, состоит в том, что значения конфигурационных настроек при их задании перезаписывается, а исходное состояние теряется. В рамках дистрибутивных решений «Альт» разработан механизм локальной политики (аналогичный Local Policy под Windows), позволяющий частично преодолеть эту проблему. На текущий момент этот механизм представлен профилями, определяющими шаблон локальной политики, определяемый при включении механизма применения групповых политик (см. Локальная политика).

Далее, для терминологического упрощения, политики и предпочтения называются одним термином «Групповая политика» (ГП) с поправками на особенности их применения.

В таблице Список групповых политик представлен список ГП, которые можно настроить и применять в Альт Домен.

Таблица 24.1. Список групповых политик

Политика	Статус	Комментарий
Управление политиками control	Стабильная	ADMX-файлы ALT (пакет *admx-basealt*)
Включение или выключение различных служб (сервисов systemd)	Стабильная	ADMX-файлы ALT (пакет *admx-basealt*)
Настройка браузера Firefox	Стабильная	ADMX-файлы Mozilla Firefox (пакет *admx-firefox*)
Настройка почтового клиента Thunderbird	Стабильная	ADMX-файлы Mozilla Thunderbird (пакет *admx-thunderbird*)
Настройка браузера Chromium	Стабильная	ADMX-файлы Google Chrome (пакет *admx-chromium*)
Настройка «Яндекс.Браузера»	Стабильная	ADMX-файлы Yandex (пакет *admx-yandex-browser*)
Запрет на подключение внешних носителей данных	Стабильная	
Управление Gsettings (настройки графической среды MATE и удаленного доступа к рабочему столу VNC)	Стабильная	ADMX-файлы ALT (пакет *admx-basealt*)
	Экспериментальная	

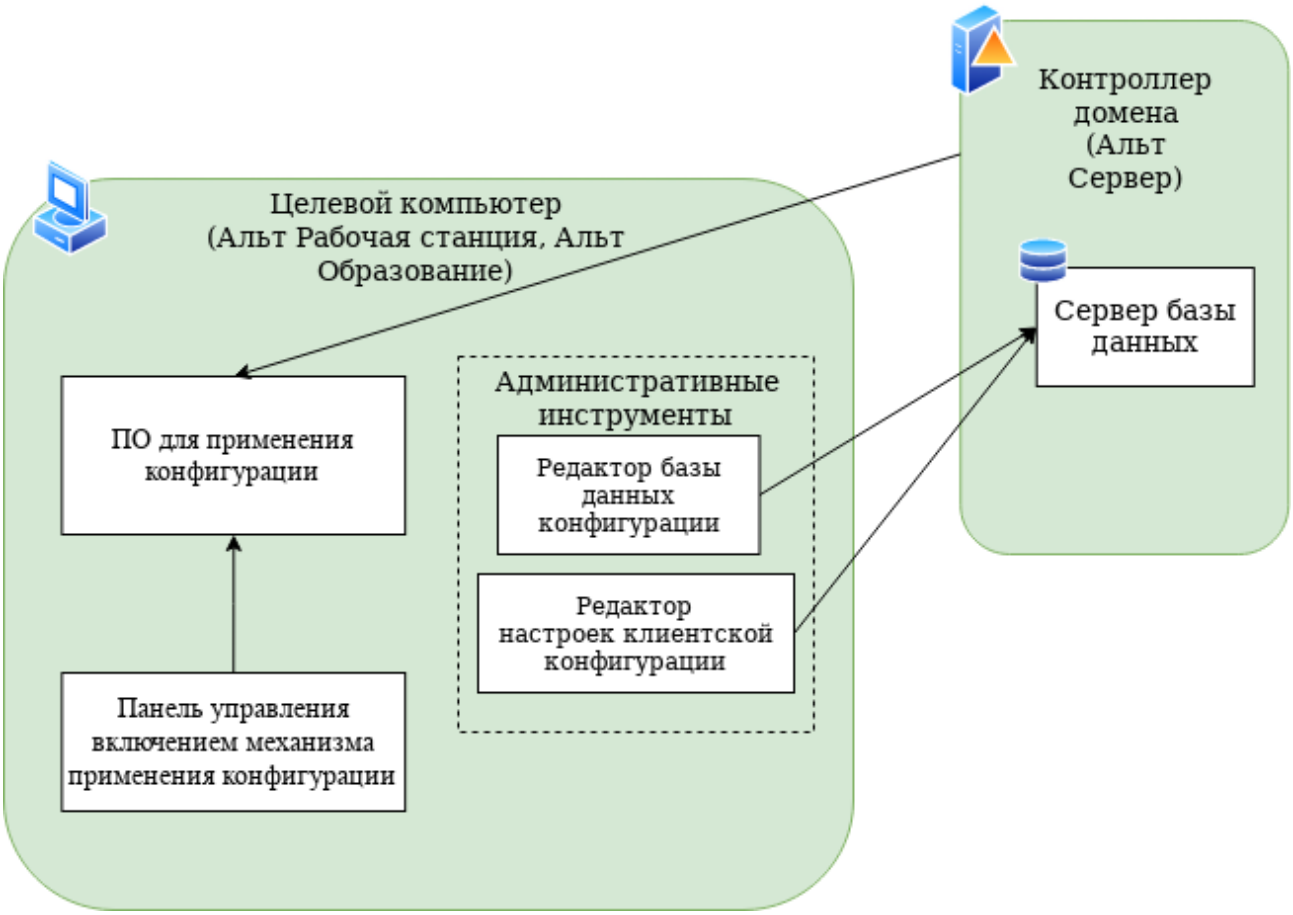
Политика	Статус	Комментарий
Настройки среды рабочего стола KDE		ADMX-файлы ALT (пакет *admx-basealt*)
Управление настройками службы Polkit	Стабильная	ADMX-файлы ALT (пакет *admx-basealt*)
Подключение сетевых дисков	Стабильная	
Управление общими каталогами	Экспериментальная	
Управление ярлыками для запуска программ	Стабильная	
Управление каталогами	Стабильная	
Управление файлами	Экспериментальная	
Управление INI-файлами	Экспериментальная	
Управление переменными среды	Экспериментальная	
Управление logon-скриптами	Экспериментальная	
Установка и удаление пакетов	Экспериментальная	
Настройка реестра Windows		

Примечание

Экспериментальными называются политики, реализация которых может в процессе разработки поменяться так, что ранее установленные политики после обновления перестанут быть установленными, поскольку настройки таких политик не утвержденны технически.

Логическая структура инструментов управления содержит следующие компоненты:

- сервер базы данных с информацией о клиентах и их конфигурации;
- клиентское ПО для репликации и применения конфигурации;
- графическая панель управления включением механизма применения конфигурации;
- графический редактор базы данных конфигурации (ADMC);
- графический редактор настроек клиентской конфигурации (GPUI).



Глава 25. Установка административных шаблонов и административных инструментов

25.1. Установка административных шаблонов

25.2. Установка административных инструментов

25.3. Установка административных инструментов (машина Windows)

25.1. Установка административных шаблонов

Для задания конфигурации необходимо на контроллере домена установить административные шаблоны (ADMX-файлы):

1. Установить пакеты политик *admx-basealt*, *admx-chromium*, *admx-firefox*, *admx-yandex-browser* и утилиту *admx-msi-setup*:

   ```
   # apt-get install admx-basealt admx-chromium admx-firefox admx-yandex-browser admx-msi-setup
   ```

   Доступны следующие пакеты политик:

   - *admx-basealt* — ADMX-файлы, специфичные для дистрибутивов «Альт»;
   - *admx-yandex-browser* — ADMX-файлы для управления настройками Яндекс.Браузера;

- *admx-firefox* — ADMX-файлы для управления настройками браузера Mozilla Firefox;
- *admx-chromium* — ADMX-файлы для управления настройками браузера Google Chrome.

2. Запустить утилиту **admx-msi-setup**, которая загрузит и установит ADMX-файлы от Microsoft:

```
# admx-msi-setup
```

3. После установки, политики будут находиться в каталоге **/usr/share/PolicyDefinitions**. Скопировать локальные ADMX-файлы в сетевой каталог sysvol (**/var/lib/samba/sysvol/<DOMAIN>/Policies/**), выполнив команду:

```
# samba-tool gpo admxload -U Administrator
```

Примечание

По умолчанию, утилита **admx-msi-setup** устанавливает последнюю версию ADMX от Microsoft (сейчас это «Microsoft Group Policy — Windows 10 October 2020 Update (20H2)»). С помощью параметров можно указать другой источник:

```
# admx-msi-setup -h
admx-msi-setup - download msi files and extract them in <destination-
directory>
default value is /usr/share/PolicyDefinitions/.
Usage: admx-msi-setup [-d  <destination-directory>] [-s  <screen>]

Removing admx-msi-setup temporary files...
```

25.2. Установка административных инструментов

Административные инструменты обычно устанавливаются на рабочей станции, введённой в домен, но могут быть установлены и на контроллере домена, если на нем установлена графическая среда.

25.2.1. ADMC

Установить пакет *admc*:

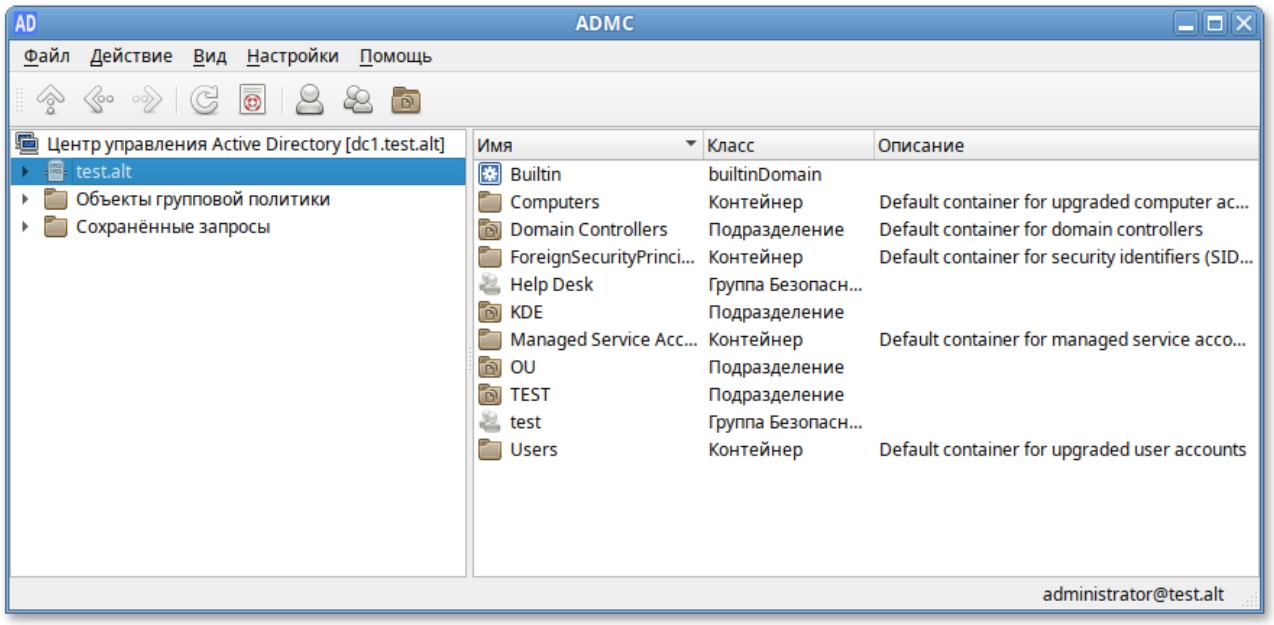
```
# apt-get install admc
```

Запуск **ADMC** осуществляется из меню запуска приложений: пункт **Системные** → **ADMC** или из командной строки (команда **admc**).

Примечание

Для использования **ADMC** необходимо предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```



Подробнее о работе с ADMC см. Модуль удаленного управления базой данных конфигурации (ADMC).

25.2.2. GPUI

Установить пакет *gpui*:

```
# apt-get install gpui
```

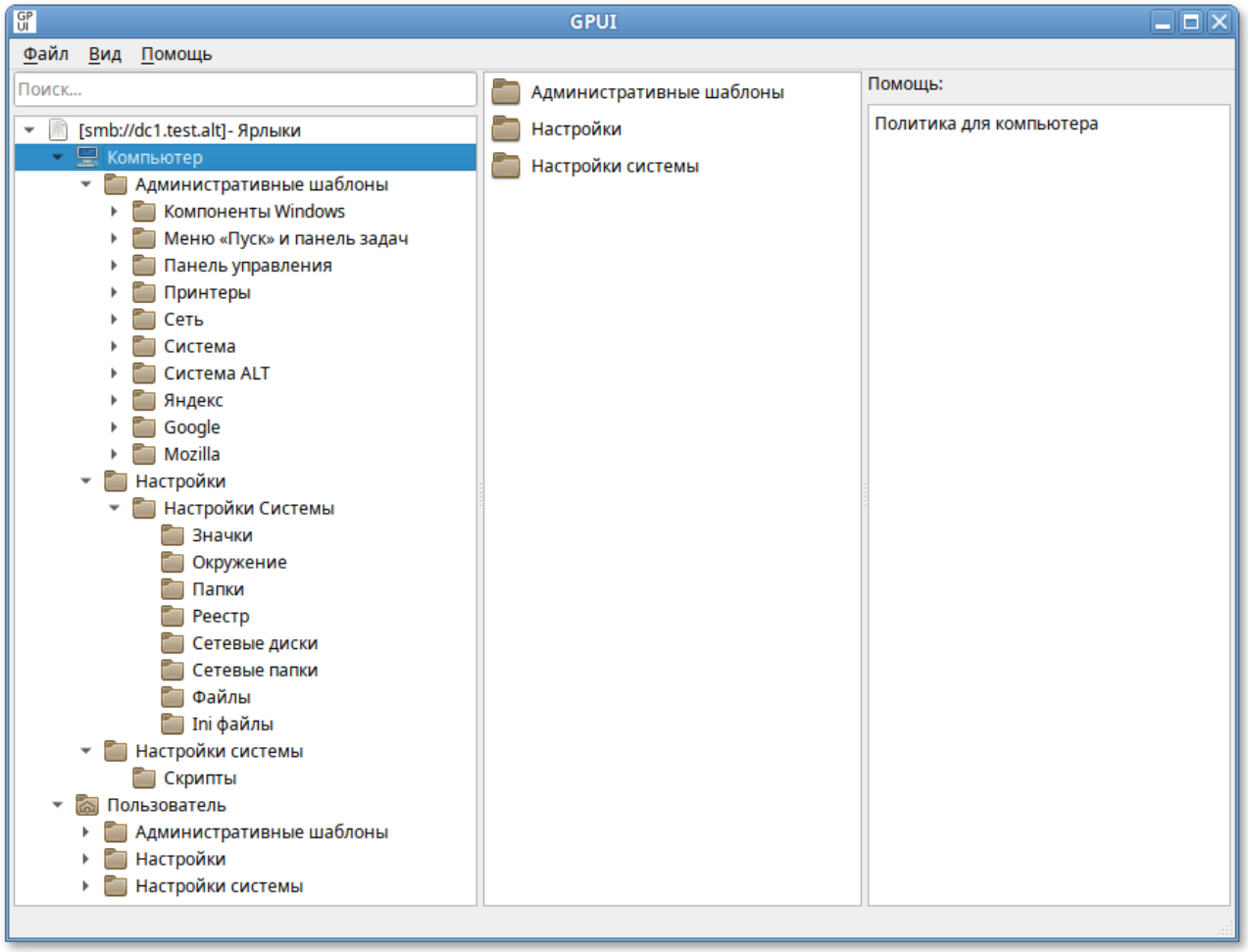
Примечание

В настоящее время **GPUI** не умеет читать файлы ADMX с контроллера домена. Для корректной работы необходимо также установить пакеты admx и файлы ADMX от Microsoft:

```
# apt-get install admx-basealt admx-chromium admx-firefox admx-yandex-
browser admx-msi-setup
# admx-msi-setup
```

Для использования **GPUI** необходимо предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```



Подробнее о работе с **GPUI** см. Модуль редактирования настроек клиентской конфигурации (GPUI).

25.3. Установка административных инструментов (машина Windows)

Для администрирования Альт Домен из Windows можно использовать средства удаленного администрирования сервера Microsoft (RSAT).

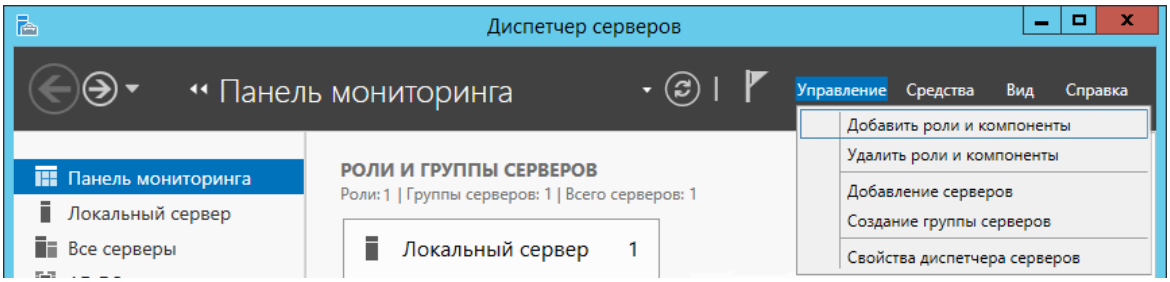
Для возможности использования административных инструментов Windows (RSAT) необходимо ввести компьютер с Windows в домен. Для выполнения этой процедуры требуется членство в группе «Администраторы» или в эквивалентной группе на локальном компьютере.

25.3.1. Windows Server

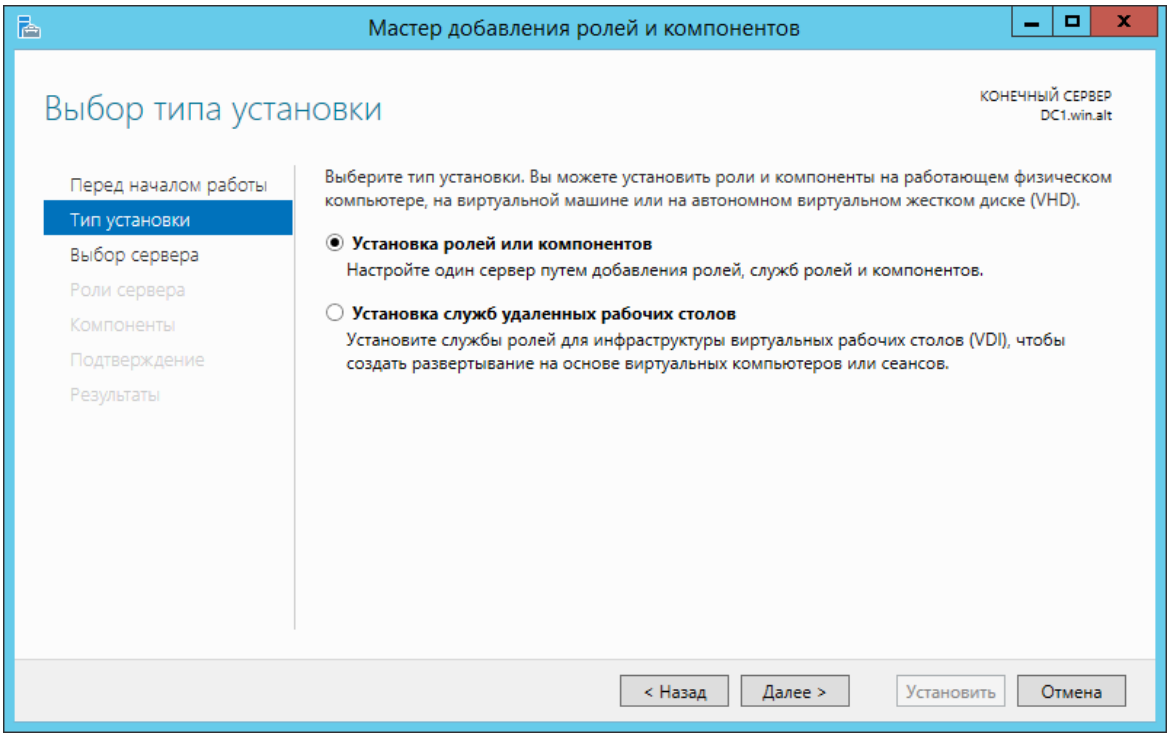
В ОС Windows Server средства удаленного администрирования сервера Microsoft (RSAT) включены по умолчанию.

Установка:

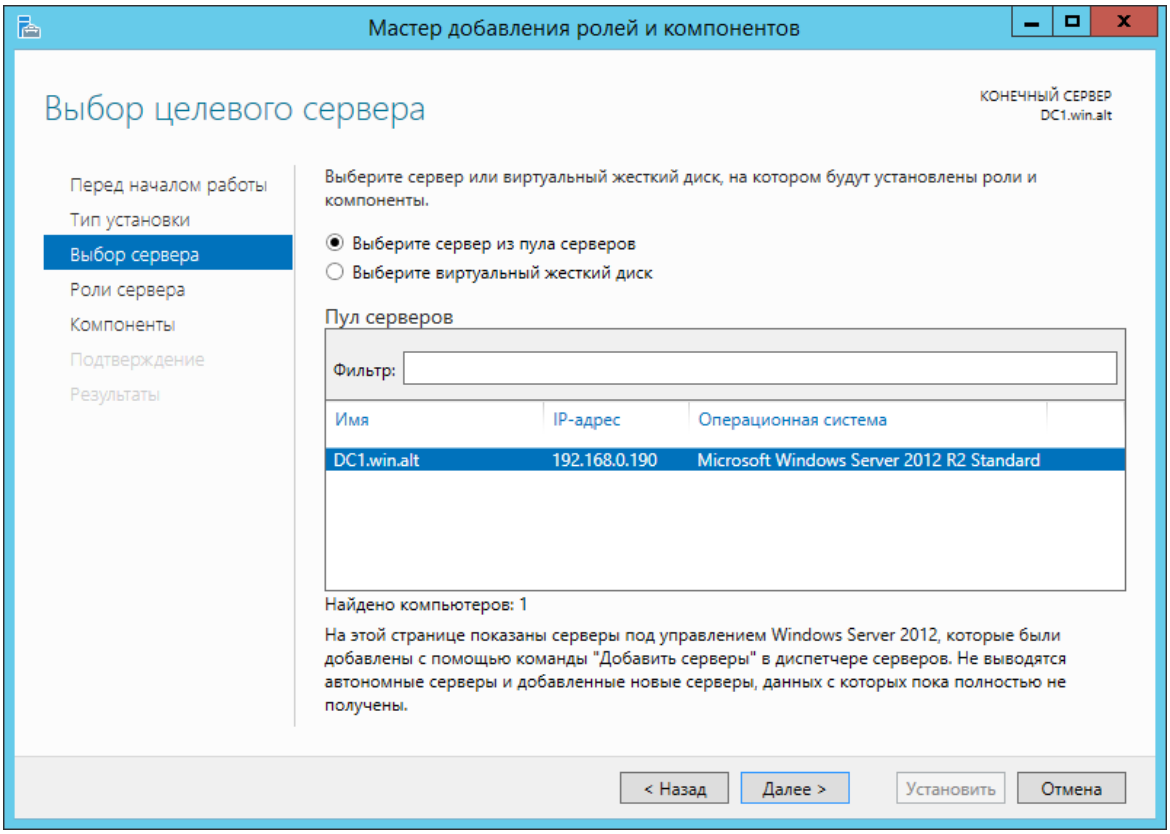
1. Запустить **`Диспетчер серверов`**.
2. На Windows Server 2012, 2012 R2, и 2016:
   - выбрать **Управление → Добавить роли и компоненты**:



в открывшемся окне **Мастер добавления ролей и компонентов** выбрать пункт **Установка ролей или компонентов**:



выбрать хост, на котором будут установлены компоненты:



на шаге **Выбор компонентов для установки** нажать кнопку **Далее**.

3. На Windows Server 2008 и 2008 R2 в дереве навигации выбрать **Компоненты** и нажать **Добавить компоненты**.

4. Выбрать компоненты для установки (см. Рекомендуемые компоненты для администрирования Samba AD):

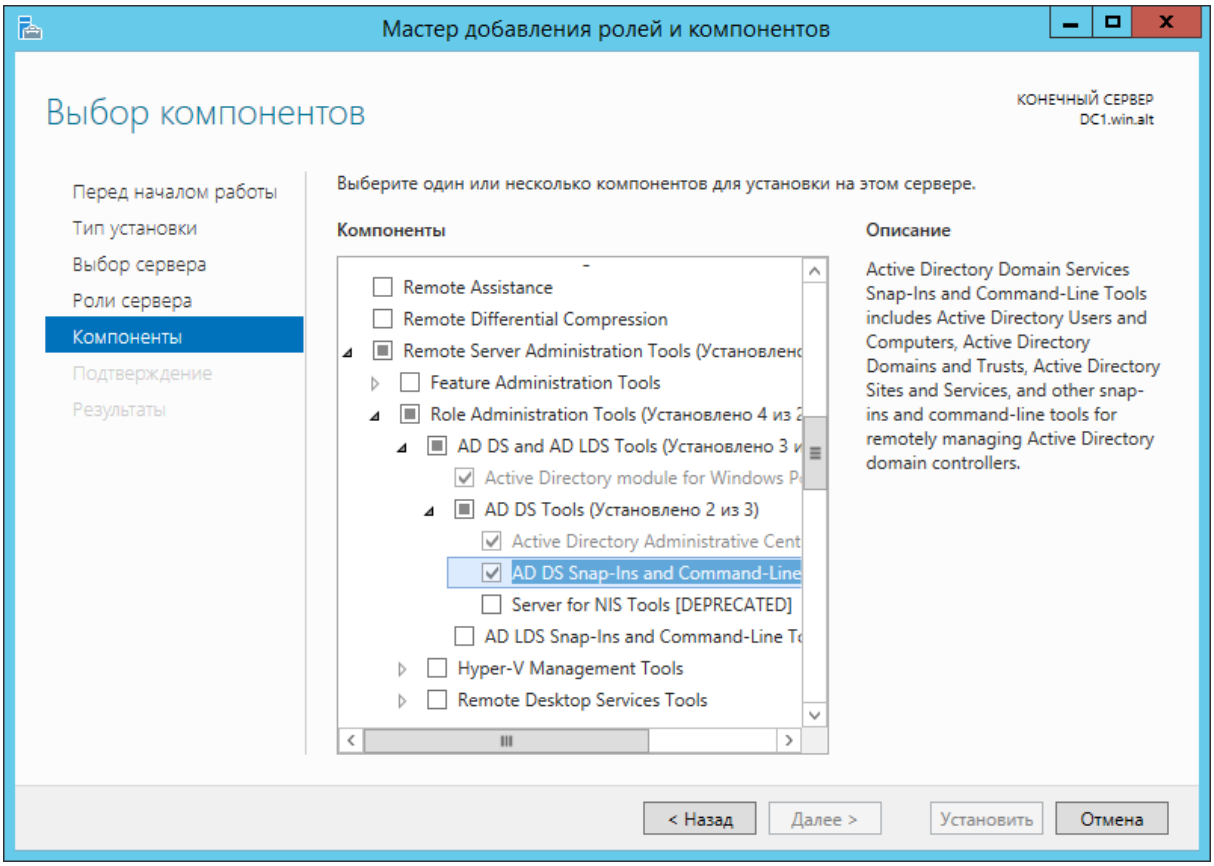


Таблица 25.1. Рекомендуемые компоненты для администрирования Samba AD

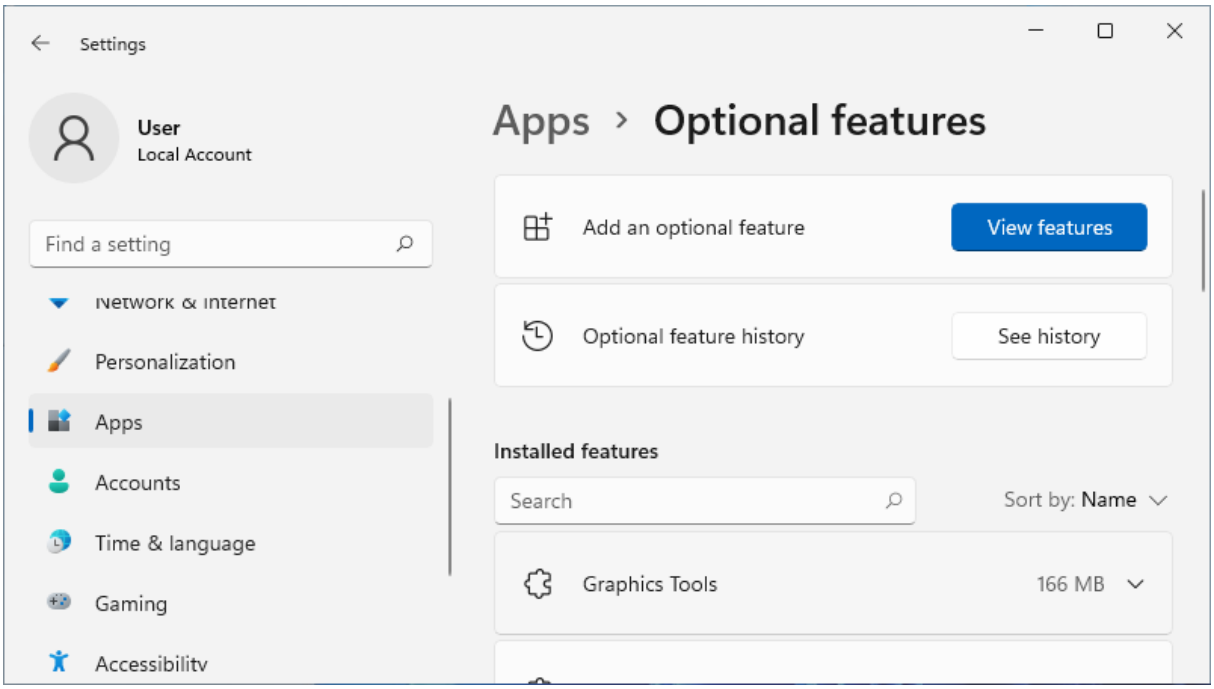
Компонент	Описание
Group Policy Management	Предоставляет оснастки для групповой политики: средство управления (GPMC), редактор управления (gpedit) и начальный редактор GPO
AD DS Snap-Ins and Command-Line Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS	Добавляет вкладку **`Атрибуты UNIX`** в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Эта функция не поддерживается в Windows Server 2016
Active Directory Module for Windows PowerShell	Включает командлеты Active Directory (AD) PowerShell
DNS Server tools	Оснастка MMC DNS для удаленного управления DNS

25.3.2. Windows 10 (1809 и более поздних версиях)

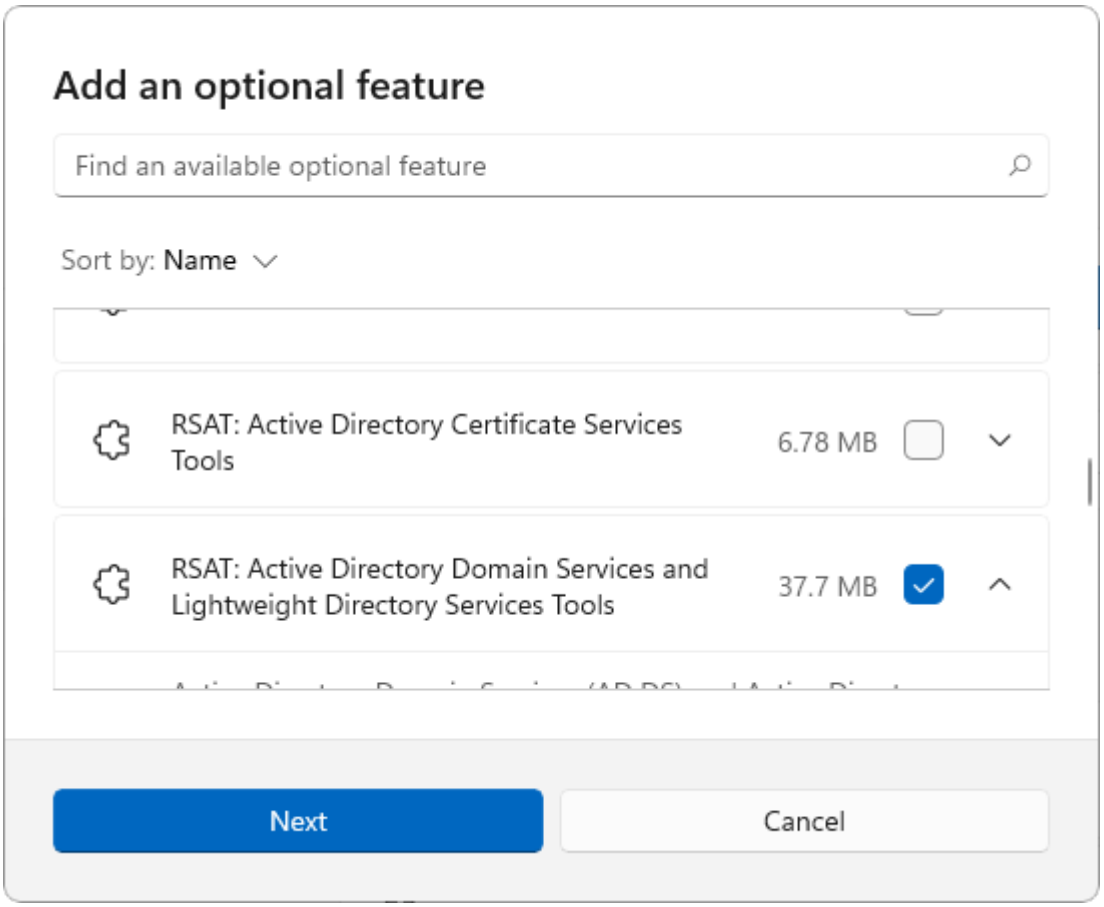
В Windows 10 1809 и более поздних версиях RSAT устанавливается в качестве дополнительной функции. Для установки компьютер должен иметь доступ в Интернет.

Установка:

1. Перейти в раздел **Settings** → **Apps** → **Optional Features** → **View features** (**Параметры Windows** → **Приложения** → **Дополнительные возможности** → **Добавить компонент**):



2. Выбрать нужные компоненты RSAT (см. Рекомендуемые компоненты для администрирования Samba AD) и нажать кнопку **`Next`**:



3. Нажать кнопку **`Install`**.

Таблица 25.2. Рекомендуемые компоненты для администрирования Samba AD

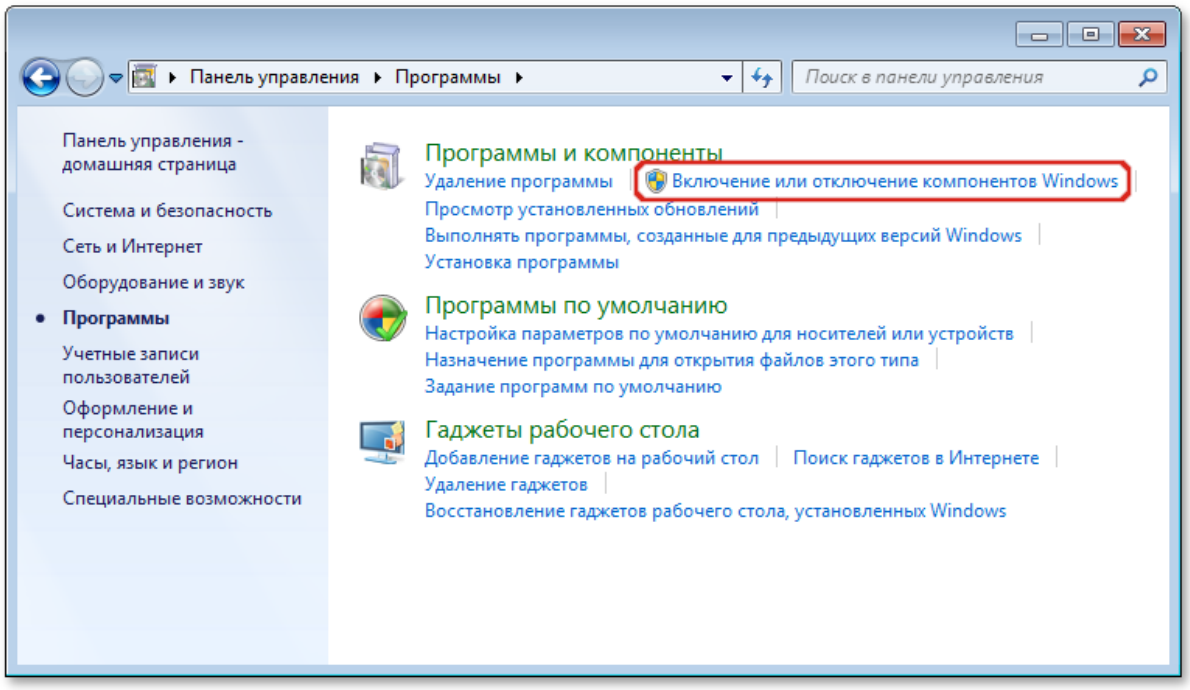
Компонент	Описание
RSAT: Group Policy Management Tools	Включают консоль управления групповыми политиками (gpmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
RSAT: Active Directory Domain Services and Lightweight Directory Services Tools	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
RSAT: DNS Server Tools	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки **`dnscmd.exe`**
RSAT: Remote Desktop Services Tool	Добавляет вкладку **`Профиль служб удаленных рабочих столов`** в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

25.3.3. Windows Vista и 7

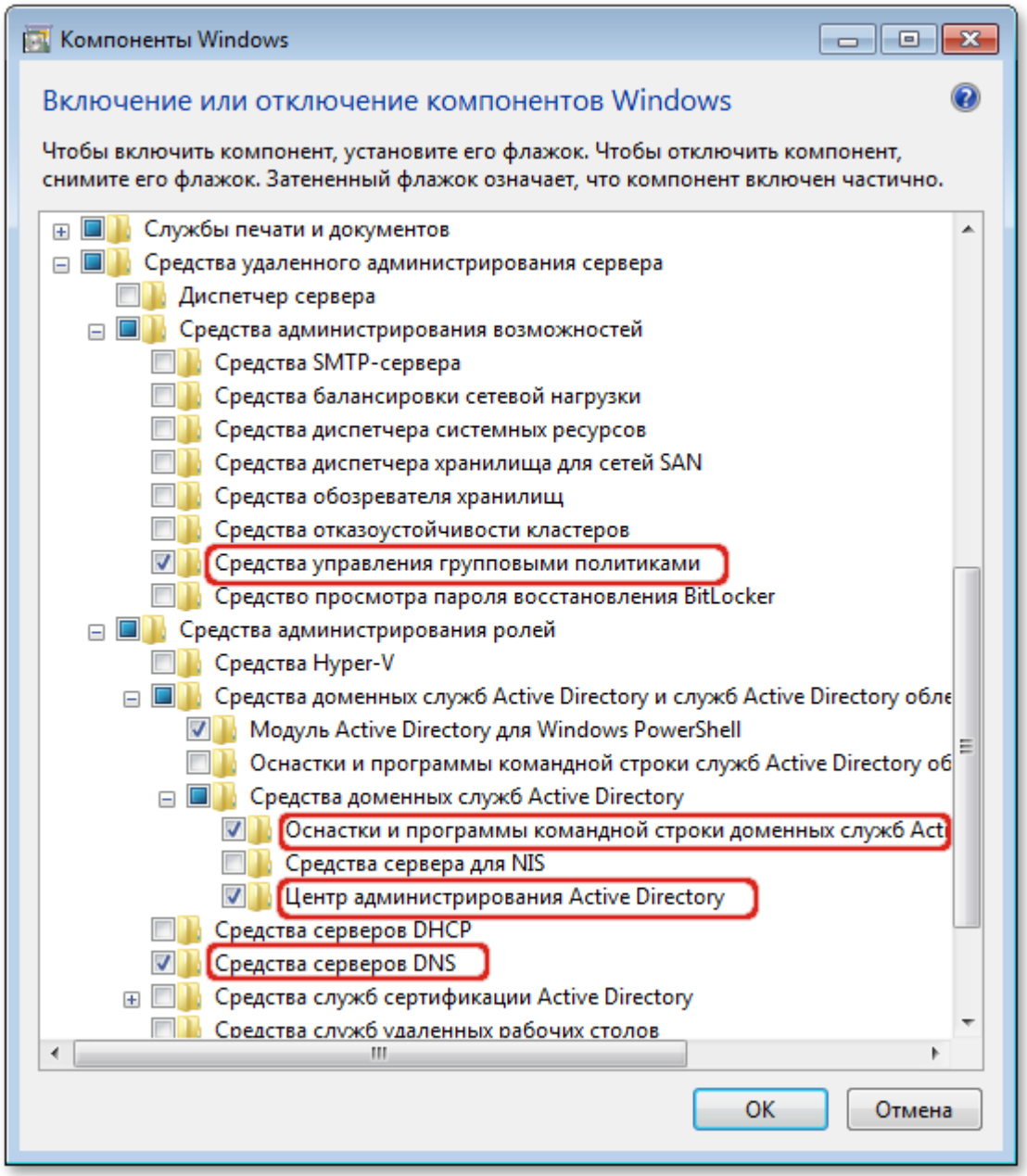
До версии Windows 10 1809 пакет удаленного администрирования серверов RSAT устанавливается в виде MSU обновления, которое нужно скачать с серверов Microsoft.

Установка:

1. Перейти в **Панель управления** → **Программы** → **Включение или отключение компонентов Windows**:



2. Включить компоненты (см. Рекомендуемые компоненты для администрирования Samba AD):



3. Нажать кнопку **OK**.

Таблица 25.3. Рекомендуемые компоненты для администрирования Samba AD

Компонент	Описание
Group Policy Management Tools (Средства управления групповыми политиками)	Включает консоль управления групповыми политиками (gpmc.msc), редактор управления групповыми политиками (gpme.msc) и редактор GPO инициализирующей программы групповой политики (gpedit.msc)
AD DS Tools (Оснастки и программы командной строки доменных служб Active Directory)	Предоставляет оснастку «Пользователи и компьютеры Active Directory» (ADUC) и «Сайты и службы Active Directory» (ADSS)
Server for NIS Tools (Средства сервера для NIS)	

Компонент	Описание
	Добавляет вкладку **Атрибуты UNIX** (**UNIX Attributes**) в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Включает программу командной строки **ypclear.exe**
Active Directory Module for Windows PowerShell (Модуль Active Directory для Windows PowerShell)	Обеспечивает централизованную среду для управления службами каталогов
DNS Server tools (Средства серверов DNS)	Включает оснастку «Диспетчер DNS» для удаленного управления DNS и программу командной строки **dnscmd.exe**
Remote Desktop Services Tool (Средства служб удалённых рабочих столов)	Добавляет вкладку **Профиль служб удаленных рабочих столов** в свойства объекта пользователя ADUC и устанавливает оснастку MMC «Удаленные рабочие столы» для администрирования RDP-сервера (tsmmc.msc).

Глава 26. Включение механизма применения конфигурации на клиентских машинах

Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах предназначен для управления включением работы групповых политик и выбором политики по умолчанию.

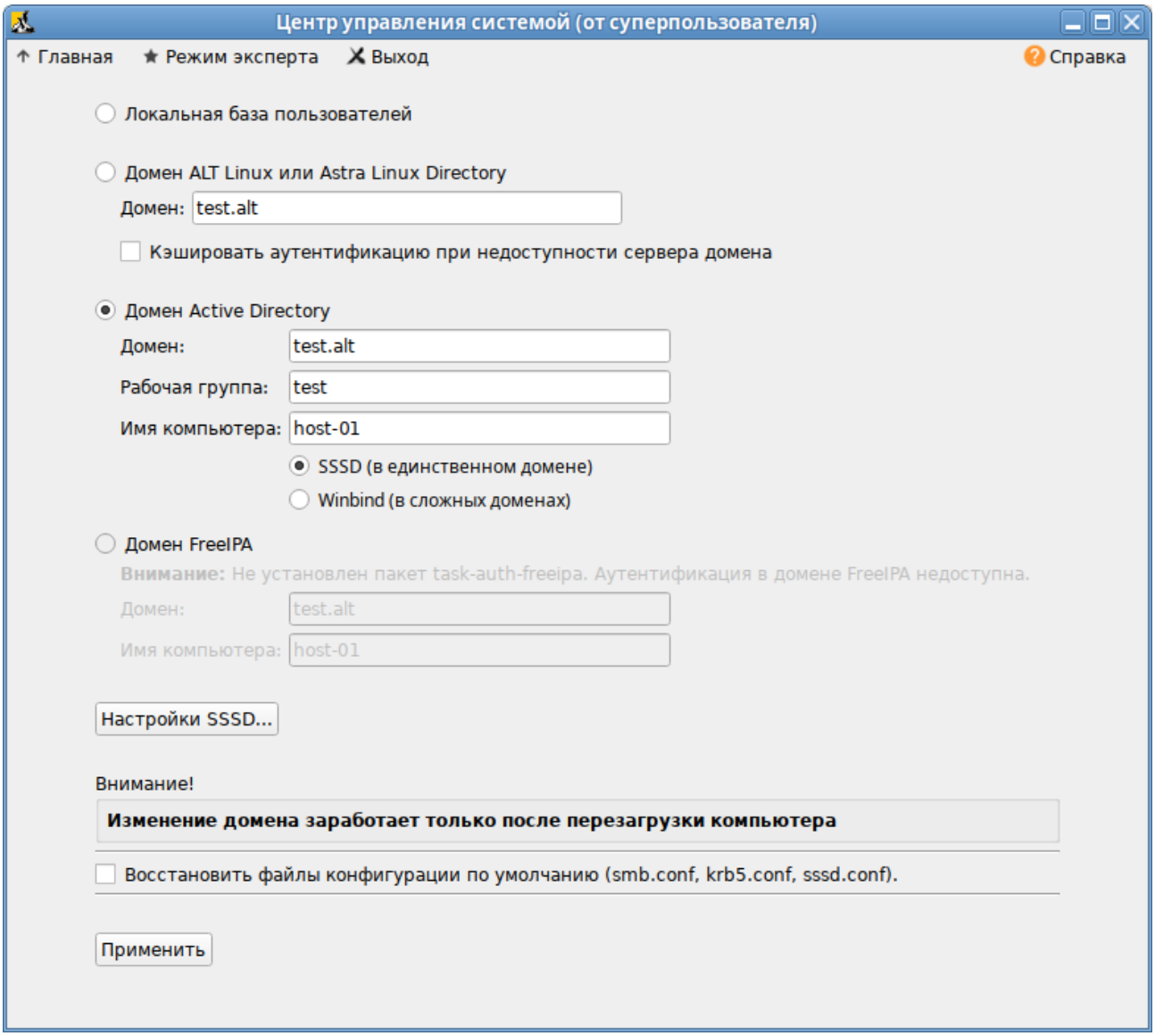
Данный модуль представляет собой следующие модули **ЦУС**: **Аутентификация** (пакет *alterator-auth*) и **Групповые политики** (пакет *alterator-gpupdate*).

Для возможности применения ГП на клиентских машинах должен быть установлен пакет *gpupdate* (подробнее см. Модуль клиентской машины для применения конфигурации), а для возможности включения ГП в ЦУС — пакет *alterator-gpupdate*:

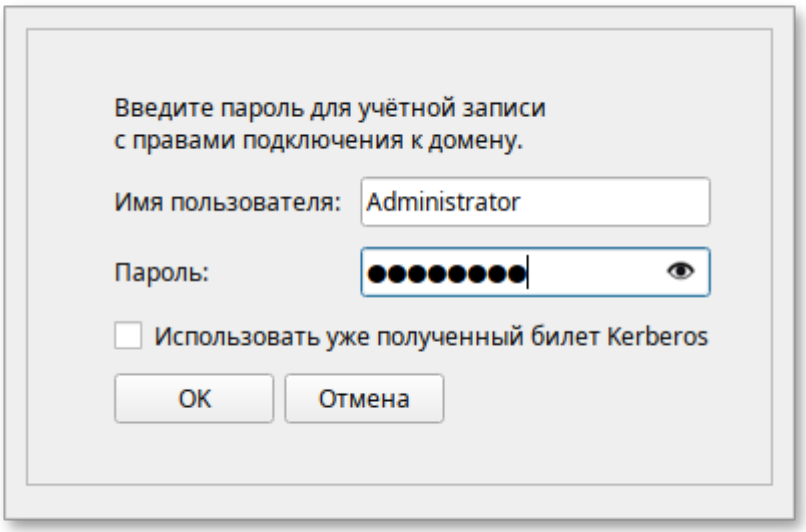
```
# apt-get install gpupdate alterator-gpupdate
```

Включить ГП можно как при вводе машины в Альт Домен, так и на уже включенной в домен рабочей станции.

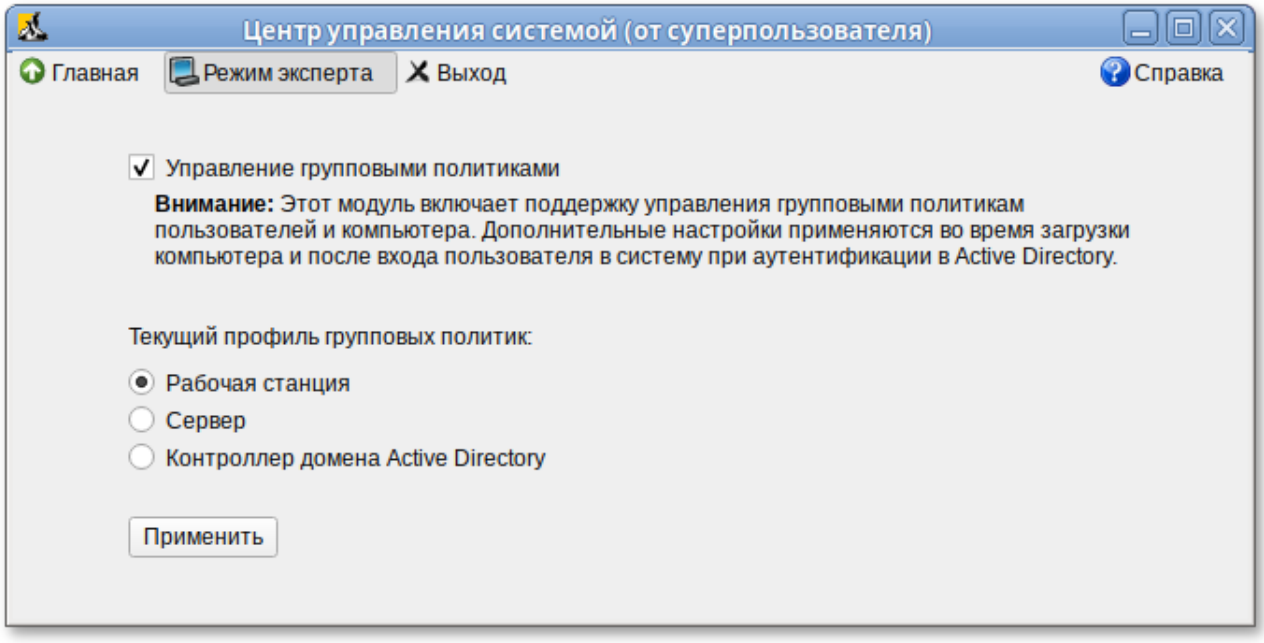
Для включения групповых политик при вводе машины в домен (см. Присоединение к домену в роли участника) следует в модуле ЦУС **Аутентификация** выбрать пункт **Домен Active Directory**, заполнить поля **Домен**, **Рабочая группа** и **Имя компьютера** и нажать кнопку **Применить**:



Затем в открывшемся окне ввести имя пользователя, имеющего право вводить машины в домен, и его пароль, отметить пункт **Включить групповые политики** и нажать кнопку **OK**:

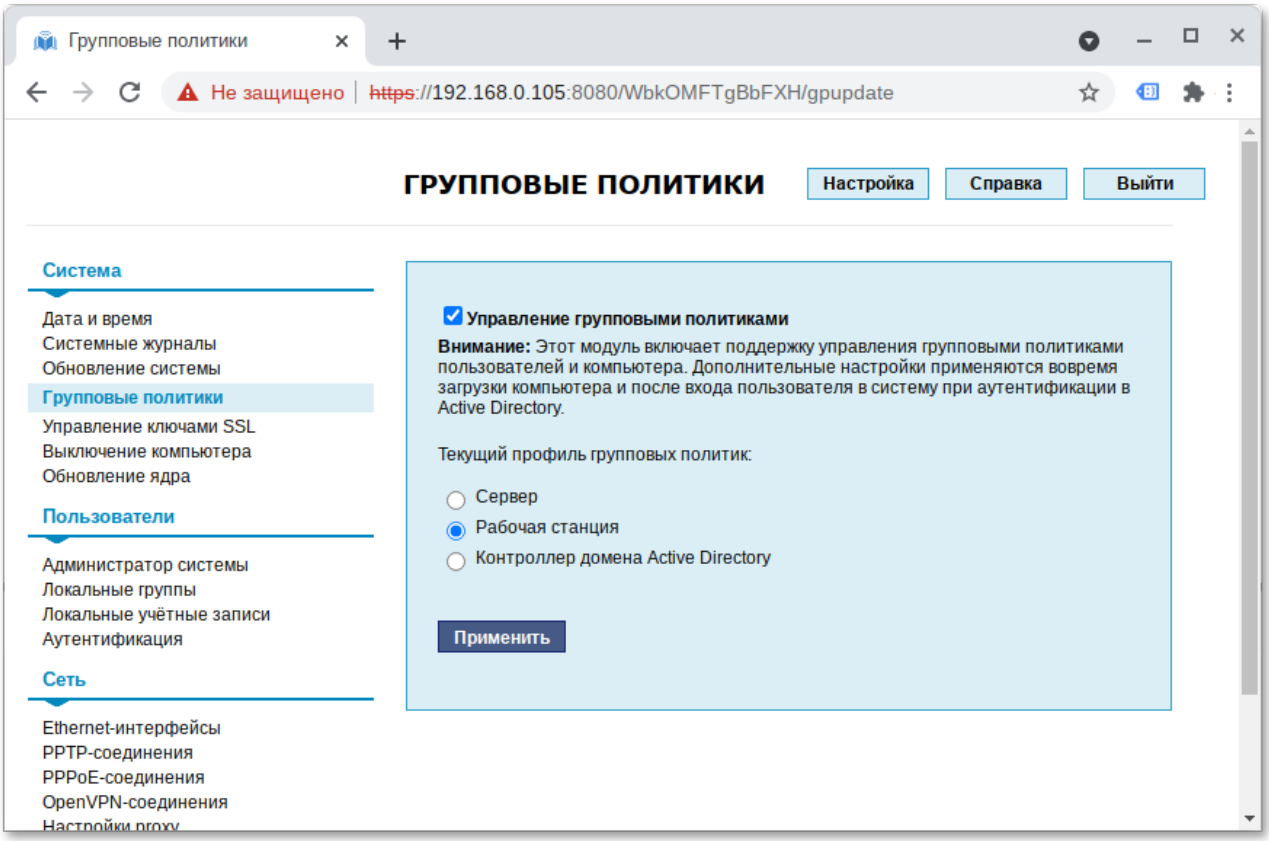


Включить поддержку управления групповыми политиками на машине уже введенной в домен можно в модуле ЦУС **Групповые политики**:



Модуль **Групповые политики** позволяет управлять включением/выключением поддержки групповых политик на машинах введенных в домен, а также выбирать профиль политики по умолчанию — **Сервер**, **Контроллер домена Active Directory** или **Рабочая станция**.

Для возможности включения групповых политик на машинах под управлением ОС «Альт», на которых не установлена графическая оболочка, модуль **Групповые политики** доступен также в веб-интерфейсе ЦУС:



Работа с веб-ориентированным интерфейсом ЦУС может происходить из любого веб-браузера с любого компьютера сети.

Глава 27. Модуль клиентской машины для применения конфигурации

27.1. Утилиты модуля gpupdate

27.2. Локальная политика

27.3. Ключи реестра

27.4. Модули клиентской стороны (Applier)

27.5. Периодичность запуска групповых политик

27.6. Утилита gpresult

Модуль клиентской машины для применения конфигурации (далее — gpupdate) отвечает за применение заданных администратором системы настроек конфигурации к клиентской машине и/или пользователю машины.

ПО состоит из компонента, который авторизуется в домене и выполняет скачивание файлов настроек на клиентскую машину. Далее происходит разбор файлов настроек и складывание полученных данных в хранилище, именуемое также «реестр». Это позволяет развязать методы доставки и применения настроек.

При успешной репликации настроек запускается часть системы называемая «фронтенд». Она отвечает за запуск различных модулей (appliers), каждый из которых отвечает за свою логическую функцию. Например, модуль firefox отвечает за вычитывание настроек для браузера Mozilla Firefox и создание файла политик для него, а модуль ntp отвечает за чтение настроек, касающихся NTP-сервера и создании подходящей конфигурации. Количество и функционал модулей может меняться по мере развития и актуализации продукта и компонентов системы, с которыми они работают.

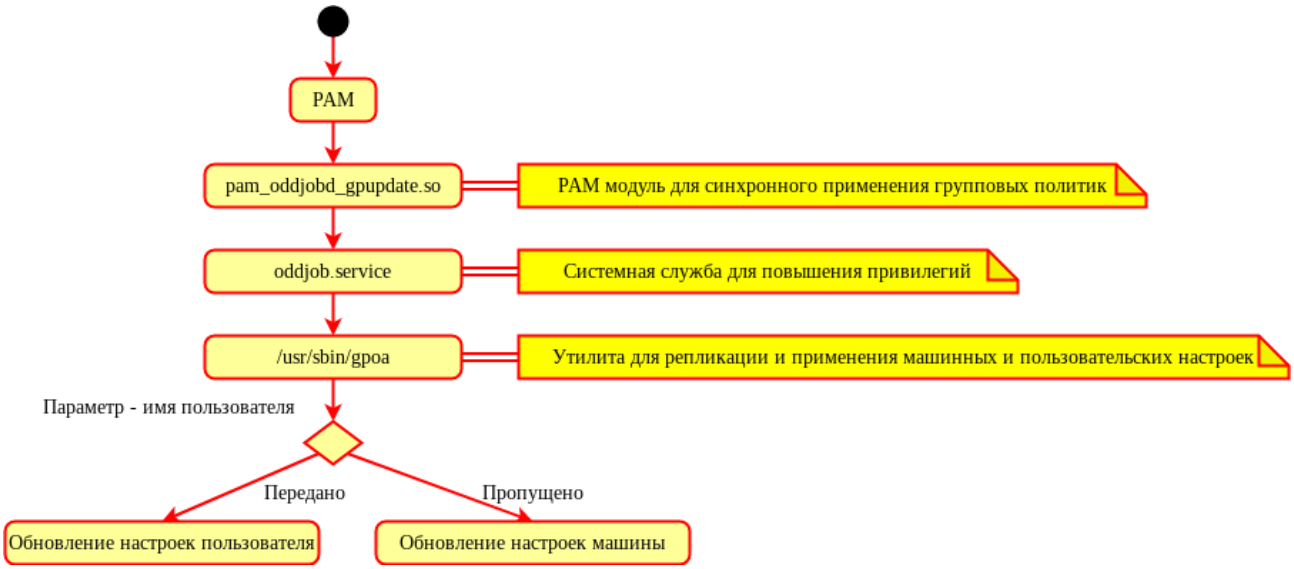
Групповые политики обрабатываются в следующем порядке:

- объект локальной групповой политики;
- объекты групповой политики, связанные с доменом (в рамках возможностей и ограничений поддержки леса доменов в Samba, как набора клиентских компонентов);
- объекты групповой политики, связанные с OU: сначала обрабатываются объекты групповой политики связанные с OU, находящиеся на самом высоком уровне в иерархии службы каталогов, затем объекты групповой политики, связанные с дочерним подразделением и т. д. Последними обрабатываются объекты групповой политики, связанные с OU, в которой находится пользователь или компьютер.

Процесс применения настроек:

- настройки для машины реплицируются при запуске компьютера и далее обновляются раз в час;
- настройки для пользователя реплицируются при входе пользователя в систему и далее обновляются раз в час.

Для работы механизмов применения пользовательских настроек задействовано множество компонентов ОС, таких как systemd, D-Bus, PAM.



Часть проекта, отвечающая за получение и применение групповых политик, внутри использует базу данных («реестр») для хранения настроек полученных из различных источников.

27.1. Утилиты модуля gpupdate

Модуль состоит из трёх утилит:

- **gpoa** — системная утилита, осуществляющая применение групповых политик для компьютера или пользователя (**gpoa** без параметра отрабатывает только для машины, для пользователя нужно указывать **username**);
- **gpupdate** — утилита, осуществляющая запрос на применение групповых политик. При запуске с привилегиями администратора может непосредственно выполнить применение групповых политик минуя необходимость повышения привилегий;
- **gpupdate-setup** — инструмент администрирования механизмов применения групповых политик. Позволяет включать и отключать применение групповых политик, а также задавать шаблон политики по умолчанию (**Рабочая станция**, **Сервер**, **Контроллер домена**).

Синтаксис команды **gpoa**:

```
gpoa [-h] [--dc DC] [--nodomain] [--noupdate] [--noplugins] [--list-backends] [--
loglevel LOGLEVEL] [пользователь]
```

Таблица 27.1. Опции команды gpoa

Ключ	Описание
-h, --help	Вывести справку о команде
--dc DC	Указать полное имя (FQDN) контроллера домена для реплицирования SYSVOL
--nodomain	Работать без домена (применить политику по умолчанию)
--noupdate	Не пытаться обновить хранилище, только запустить appliers
--noplugins	Не запускать плагины

Ключ	Описание
--list-backends	Показать список доступных бэкэндов
--loglevel LOGLEVEL	Установить уровень журналирования
пользователь	Имя пользователя домена

Примеры работы с командой **gpoa**:

- получить и применить настройки для текущей машины:

```
# gpoa --loglevel 0
```

- применить закешированные настройки для текущей машины:

```
# gpoa --noupdate
```

- получить и применить настройки с контроллера домена dc1.test.alt для пользователя ivanov:

```
# gpoa --dc dc1.test.alt --loglevel 3 ivanov
```

- применить политику по умолчанию:

```
# gpoa --nodomain --loglevel 0
```

Синтаксис команды **gpupdate**:

```
gpupdate [-h] [-u USER] [-t {ALL,USER,COMPUTER}] [-l LOGLEVEL] [-f] [-s]
```

Таблица 27.2. Опции команды gpupdate

Ключ	Описание
-h, --help	Вывести справку о команде
-u USER, --user USER	Имя пользователя для обновления GPO
--target TARGET	Указать политики, которые нужно обновить (пользователя или компьютера). Возможные значения: All (по умолчанию), Computer, User
-l LOGLEVEL, --loglevel LOGLEVEL	Установить уровень журналирования
-f, --force	Принудительно загрузить политики (GPT) с контроллера
-s, --system	Запустить gpupdate в системном режиме

Только root может указать любое имя пользователя для обновления. Пользователь может выполнять **gpupdate** только для машины или самого себя.

Примеры работы с командой **gpupdate**:

- получить и применить настройки для текущей машины:

```
$ gpupdate --target Computer
Apply group policies for computer.
```

- получить и применить настройки для текущего пользователя:

```
$ gpupdate --target User
Apply group policies for kudrin.
```

- получить и применить настройки для текущего пользователя и машины:

```
$ gpupdate
Apply group policies for kudrin.
```

- попытаться получить настройки для пользователя ivanov (с правами пользователя kudrin):

```
$ gpupdate -u ivanov --target User --loglevel 0
2024-06-10 17:17:18.113|[D00010]| Групповые политики будут обновлены для
указанной цели|{'target': 'USER'}
2024-06-10 17:17:18.113|[W00002]| Текущий уровень привилегий не позволяет
выполнить gpupdate для указанного пользователя. Будут обновлены настройки
текущего пользователя.|{'username': 'kudrin'}
2024-06-10 17:17:18.118|[D00013]| Запускается GPOA обращением к oddjobd через
D-Bus|{}
2024-06-10 17:17:18.119|[D00900]| Неизвестный отладочный код|{'bus_name':
'ru.basealt.oddjob_gpupdate'}
2024-06-10 17:17:18.119|[D00006]| Запускается GPOA для пользователя обращением
к oddjobd через D-Bus|{'username': 'kudrin'}
2024-06-10 17:17:37.972|[D00012]| Получен код возврата из утилиты|{'retcode':
dbus.Int32(0)}
Apply group policies for kudrin.
```

- попытаться получить настройки для пользователя ivanov (с правами суперпользователя):

```
# gpupdate -u ivanov --target User --loglevel 0
2024-06-10 17:19:53.960|[D00010]| Групповые политики будут обновлены для
указанной цели|{'target': 'USER'}
2024-06-10 17:19:53.978|[D00013]| Запускается GPOA обращением к oddjobd через
D-Bus|{}
2024-06-10 17:19:53.979|[D00900]| Неизвестный отладочный код|{'bus_name':
'ru.basealt.oddjob_gpupdate'}
2024-06-10 17:19:53.979|[D00006]| Запускается GPOA для пользователя обращением
к oddjobd через D-Bus|{'username': 'ivanov'}
2024-06-10 17:20:13.852|[D00012]| Получен код возврата из утилиты|{'retcode':
dbus.Int32(0)}
Apply group policies for ivanov.
```

Примечание

Изменения политик меняют версию в объекте ГП (GPO), **gpupdate** сравнивает версию и загружает только измененные политики.

Синтаксис команды **gpupdate-setup**:

```
gpupdate-setup [-h] действие …
```

Таблица 27.3. Список возможных действий для команды gpupdate-setup

Ключ	Описание
list	Показать список доступных типов локальной политики
list-backends	Показать список доступных бэкэндов
status	Показать текущий статус групповой политики (действие по умолчанию)
enable	Включить подсистему групповой политики
disable	Отключить подсистему групповой политики
update	Обновить состояние. Проверяет в каком состоянии находилась служба gpupdate. В случае, если служба gpupdate запущена, gpupdate-setup также запустит весь перечень необходимых служб (например, gpupdate-run-scripts)
write	Операции с групповыми политиками (включить, отключить, указать тип политики по умолчанию)
set-backend	Установить или изменить активную в данный момент серверную часть (бэкэнд)
default-policy	Показать название политики по умолчанию
active-policy	Показать название текущего профиля политики
active-backend	Показать текущий настроенный бэкэнд

Примеры работы с командой **gpupdate-setup**:

- просмотр текущего состояния подсистемы групповых политик:

```
# gpupdate-setup
disabled
```

- включить групповые политики (для включения ГП через ЦУС доступен соответствующий графический модуль управления, а также отметка во время введения машины в домен см. раздел Включение механизма применения конфигурации на клиентских машинах):

```
# gpupdate-setup enable
workstation
Created symlink /etc/systemd/user/default.target.wants/gpupdate-user.service
→ /usr/lib/systemd/user/gpupdate-user.service.
Created symlink /etc/systemd/system/multi-user.target.wants/gpupdate-scripts-
run.service → /lib/systemd/system/gpupdate-scripts-run.service.
Created symlink /etc/systemd/user/default.target.wants/gpupdate-scripts-run-
user.service → /usr/lib/systemd/user/gpupdate-scripts-run-user.service.
Created symlink /etc/systemd/system/timers.target.wants/gpupdate.timer → /lib/
systemd/system/gpupdate.timer.
Created symlink /etc/systemd/user/timers.target.wants/gpupdate-user.timer → /
usr/lib/systemd/user/gpupdate-user.timer.
# control system-policy
gpupdate
```

- выключить групповые политики:

```
# gpupdate-setup disable
Removed /etc/systemd/system/multi-user.target.wants/gpupdate.service.
Removed /etc/systemd/user/default.target.wants/gpupdate-user.service.
Removed /etc/systemd/system/timers.target.wants/gpupdate.timer.
Removed /etc/systemd/user/timers.target.wants/gpupdate-user.timer.
Removed /etc/systemd/system/multi-user.target.wants/gpupdate-scripts-
run.service.
Removed /etc/systemd/user/default.target.wants/gpupdate-scripts-run-
user.service.
```

- вывести список доступных бэкендов:

```
# gpupdate-setup list-backends
local
samba
```

- включить групповые политики и установить профиль политики по умолчанию server:

```
# gpupdate-setup write enable server
```

Gpupdate устанавливается с набором преднастроек. По умолчанию нет необходимости конфигурировать gpupdate. Однако в файле **/etc/gpupdate/gpupdate.ini** можно указать в явном виде следующие опции:

- раздел [gpoa]:
  - backend — способ получения настроек;
  - local-policy — профиль политики по умолчанию, который будет применен сразу после загрузки ОС (ad-domain-controller, workstation, server, default);
- раздел [samba]:
  - dc — контроллер домена, с которого нужно обновлять групповые политики.

Пример, файла **/etc/gpupdate/gpupdate.ini** на контроллере домена:

```
[gpoa]
backend = samba
local-policy = ad-domain-controller
```

Пример, файла **/etc/gpupdate/gpupdate.ini** на рабочей станции:

```
[gpoa]
backend = samba
local-policy = workstation
```

В следующем примере указан пустой профиль локальной политики. Указать пустой профиль бывает необходимо для тестирования групповых политик, чтобы они не наслаивались на локальные политики:

```
[gpoa]
backend = samba
local-policy = /usr/share/local-policy/default

[samba]
dc = dc1.test.alt
```

27.2. Локальная политика

Настройки локальной политики находятся в каталоге **/usr/share/local-policy/**. Данные настройки по умолчанию поставляются пакетом *local-policy*. Администраторы инфраструктур имеют возможность поставлять собственный пакет с локальной политикой и разворачивать её единообразно на всех клиентах. Формат шаблонов политик по умолчанию представляет собой архивный формат политик Samba с дополнительными модификациями. Локальную политику рекомендуется править только опытным администраторам. Состав локальной политики может меняться или адаптироваться системным администратором.

Таблица 27.4. Состав локальной политики

Параметры	Описание	Комментарий
sshd-gssapi-auth, ssh-gssapi-auth	Включает поддержку аутентификации с использованием GSSAPI на сервере OpenSSH (механизм Control)	Отвечает за возможность аутентификации в домене при доступе через SSH
sshd-allow-groups, sshd-allow-groups-list	Ограничение аутентификации на сервере OpenSSH по группам wheel и remote (механизм Control)	Необходимо для ограничения доступа через SSH для всех пользователей домена (только при наличии соответствующей привилегии)
system-policy	Применяет групповые политики при логине (механизм Control)	
oddjobd.service	Включение oddjobd.service (механизм Systemd)	Необходимо для обеспечения возможности запуска **gpupdate** для пользователя с правами администратора
gpupdate.service	Включение gpupdate.service (механизм Systemd)	Необходимо для регулярного обновления настроек машины
sshd.service	Включение sshd.service (механизм Systemd)	Необходимо для обеспечения возможности удалённого администрирования
OpenSSH	Открытие порта 22	Необходимо для обеспечения возможности подключения по SSH на машинах при старте Firewall applier

Пример локальной политики для рабочей станции (файл **/usr/share/local-policy/workstation/Machine/Registry.pol.xml**):

```
<?xml version="1.0" encoding="utf-8"?>
<PolFile num_entries="9" signature="PReg" version="1">
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>sshd-gssapi-auth</ValueName>
        <Value>enabled</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>ssh-gssapi-auth</ValueName>
        <Value>enabled</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>sshd-allow-groups</ValueName>
        <Value>enabled</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>sshd-allow-groups-list</ValueName>
        <Value>remote</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>Software\BaseALT\Policies\Control</Key>
        <ValueName>system-policy</ValueName>
        <Value>gpupdate</Value>
    </Entry>
    <Entry type="4" type_name="REG_DWORD">
        <Key>Software\BaseALT\Policies\SystemdUnits</Key>
        <ValueName>oddjobd.service</ValueName>
        <Value>1</Value>
    </Entry>
    <Entry type="4" type_name="REG_DWORD">
        <Key>Software\BaseALT\Policies\SystemdUnits</Key>
        <ValueName>sshd.service</ValueName>
        <Value>1</Value>
    </Entry>
    <Entry type="4" type_name="REG_DWORD">
        <Key>Software\BaseALT\Policies\SystemdUnits</Key>
        <ValueName>gpupdate.service</ValueName>
        <Value>1</Value>
    </Entry>
    <Entry type="1" type_name="REG_SZ">
        <Key>SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules</Key>
        <ValueName>OpenSSH</ValueName>
        <Value>v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|
Name=Open SSH port|Desc=Open SSH port|</Value>
    </Entry>
</PolFile>
```

27.3. Ключи реестра

Ключи реестра, полученные из объектов групповой политики (GPO), хранятся в Dconf.

Машинные политики хранятся в файле **/etc/dconf/db/policy.d/policy.ini**, политики пользователя — в файле **/etc/dconf/db/policy<UID>.d/policy<UID>.ini** (где UID — идентификатор пользователя в системе).

Отследить какие политики «прилетели» на машину клиента можно, выполнив команду:

```
dconf dump /
```

При выполнении этой команды с правами доменного пользователя будут выведены машинные политики и политики данного пользователя, при выполнении с правами пользователя root будут выведены только машинные политики.

Пример результата выполнения команды **`dconf dump /`** с правами доменного пользователя:

```
$ dconf dump /
[SOFTWARE/Policies/Microsoft/WindowsFirewall/FirewallRules]
OpenSSH='v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=22|Name=Open SSH
port|Desc=Open SSH port|'

[Software/BaseALT/Policies/Control]
ssh-gssapi-auth='enabled'
sshd-allow-groups='enabled'
sshd-allow-groups-list='remote'
sshd-gssapi-auth='enabled'
system-policy='gpupdate'

[Software/BaseALT/Policies/ReadQueue/Machine]
0="('Local Policy', '/var/cache/gpupdate/local-policy', None)"
1="('Firefox', '/var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{0CCFA74C-57F5-42B5-98E2-007D4A59C4C4}', 262148)"

[Software/BaseALT/Policies/ReadQueue/User]
0="('nm', '/var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{6F65CD4D-9209-4A81-9801-17A35CEE5CFD}', 131074)"

[Software/BaseALT/Policies/SystemdUnits]
gpupdate.service=1
oddjobd.service=1
sshd.service=1

[Software/Policies/Mozilla/Firefox]
DisableMasterPasswordCreation=1
PasswordManagerEnabled=1
ShowHomeButton=1

[Software/Policies/Mozilla/Firefox/Authentication]
SPNEGO="['.test.alt']"

[Software/Policies/Mozilla/Firefox/Homepage]
Locked=1
URL='https://basealt.ru'

[org/gnome/evolution-data-server]
migrated=true
network-monitor-gio-name=''

[org/mate/caja/window-state]
geometry='800x550+310+75'
maximized=false
start-with-sidebar=true
start-with-status-bar=true
start-with-toolbar=true
```

```
[org/mate/desktop/accessibility/keyboard]
bouncekeys-beep-reject=true
bouncekeys-delay=300
bouncekeys-enable=false
enable=false
feature-state-change-beep=false
mousekeys-accel-time=1200
mousekeys-enable=false
mousekeys-init-delay=160
mousekeys-max-speed=750
slowkeys-beep-accept=true
slowkeys-beep-press=true
slowkeys-beep-reject=false
slowkeys-delay=300
slowkeys-enable=false
stickykeys-enable=false
stickykeys-latch-to-lock=true
stickykeys-modifier-beep=true
stickykeys-two-key-off=true
timeout=120
timeout-enable=false
togglekeys-enable=false

[org/mate/desktop/session]
session-start=1718111448

[org/mate/mate-menu/plugins/applications]
last-active-tab=0

[org/mate/panel/general]
object-id-list=['menu-bar', 'show-desktop', 'workspace-switcher', 'window-list',
'notification-area', 'clock']
toplevel-id-list=['bottom']

[org/mate/panel/objects/clock]
applet-iid='ClockAppletFactory::ClockApplet'
locked=true
object-type='applet'
panel-right-stick=true
position=0
toplevel-id='bottom'

[org/mate/panel/objects/clock/prefs]
custom-format=''
format='24-hour'

[org/mate/panel/objects/menu-bar]
applet-iid='MateMenuAppletFactory::MateMenuApplet'
has-arrow=false
locked=true
object-type='applet'
position=0
toplevel-id='bottom'

[org/mate/panel/objects/notification-area]
applet-iid='NotificationAreaAppletFactory::NotificationArea'
locked=true
object-type='applet'
```

```
panel-right-stick=true
position=10
toplevel-id='bottom'

[org/mate/panel/objects/show-desktop]
applet-iid='WnckletFactory::ShowDesktopApplet'
locked=true
object-type='applet'
position=1
toplevel-id='bottom'

[org/mate/panel/objects/window-list]
applet-iid='WnckletFactory::WindowListApplet'
locked=true
object-type='applet'
position=20
toplevel-id='bottom'

[org/mate/panel/objects/workspace-switcher]
applet-iid='WnckletFactory::WorkspaceSwitcherApplet'
locked=true
object-type='applet'
position=10
toplevel-id='bottom'

[org/mate/panel/toplevels/bottom]
expand=true
orientation='bottom'
screen=0
size=28
y=836
y-bottom=0

[org/mate/terminal/profiles/default]
background-color='#2C2C2C2C2C2C'
background-darkness=0.94999999999999996
background-type='transparent'
bold-color='#000000000000'
foreground-color='#F5F5F5F5E4E4'
palette='#2E2E34343636:#CCCC00000000:#4E4E9A9A0606:#C4C4A0A00000:#34346565A4A4:#7
57550507B7B:#060698209A9A:#D3D3D7D7CFCF:#555557575353:#EFEF29292929:#8A8AE2E23434
:#FCFCE9E94F4F:#72729F9FCFCF:#ADAD7F7FA8A8:#3434E2E2E2E2:#EEEEEEEEECEC'
use-theme-colors=false
visible-name='По умолчанию'
```

27.4. Модули клиентской стороны (Applier)

На клиентский компьютер должны распространяться параметры политики, указанные в соответствующем объекте ГП.

Каждая группа параметров групповой политики обслуживается определенным модулем (Applier) клиентской стороны.

Таблица 27.5. Список модулей

Расширение клиентской стороны	Модуль	Описание
Управление control framework	control	Управляет фреймворком control. Может быть вызван только машинной политикой. Принцип работы — вызвать утилиту **`control`** с нужным параметром
Управление настройками службы Polkit	polkit	Управляет генерацией настроек PolicyKit. Работа с правилами PolicyKit ведется методом генерации файлов **`.rules`**
Управление настройками службы Polkit	polkit_user	Управляет генерацией настроек PolicyKit в контексте пользователя
Включение или выключение различных служб	systemd	Управление включением или выключением сервисов systemd. Данный applier реализован только для машин. Его функция — включение или выключение systemd units (при их наличии). Applier способен обрабатывать параметры, полученные из PReg файлов (через ADMX) в виде ветвей реестра
Настройка браузера Chromium	chromium	Генерирует файл политики для Chromium (**`policies.json`**). Данные настройки устанавливаются из ADMX-файлов для Chromium. Может быть вызван только машинной политикой
Настройка браузера Firefox	firefox	Генерирует файл политики для Firefox (**`policies.json`**). Данные настройки устанавливаются из ADMX-файлов для Firefox. Может быть вызван только машинной политикой
Настройка Яндекс.Браузера	yandex	Генерирует файл политики для Яндекс.Браузера (**`policies.json`**). Данные настройки устанавливаются из ADMX-файлов для Яндекс.Браузера. Может быть вызван только машинной политикой
Управление ярлыками запуска программ	shortcut	Управляет **`.desktop`** файлами (создание/удаление/замена)
Управление ярлыками запуска программ	shortcut_user	Управляет **`.desktop`** файлами в контексте пользователя. Способен реагировать на опцию выполнения операций в контексте администратора или пользователя
Управление подключением сетевых дисков	cifs	Управляет подключением сетевых дисков
Управление подключением сетевых дисков	cifs_user	Управляет подключением сетевых дисков в контексте пользователя
Управление каталогами файловой системы	folder	Управляет каталогами файловой системы (создание/удаление/пересоздание)

Расширение клиентской стороны	Модуль	Описание
Управление каталогами файловой системы	folder_user	Управляет каталогами файловой системы в контексте пользователя
Управление файлами	files	Управляет файлами (создание/удаление/пересоздание)
Управление файлами	files_user	Управляет файлами в контексте пользователя
Управление INI-файлами	ini	Управляет INI-файлами (создание/удаление/пересоздание)
Управление INI-файлами	ini_user	Управляет INI-файлами в контексте пользователя
Управление переменными среды	envvar	Управляет переменными среды
Управление переменными среды	envvar_user	Управляет переменными среды в контексте пользователя
Управление общими каталогами	networkshare	Управляет общими каталогами
Управление общими каталогами	networkshare_user	Управляет общими каталогами в контексте пользователя
Управление gsettings (настройки графической среды Mate)	gsettings	Разворачивает системные настройки gsettings. Редактирование системных настроек осуществляется методом развертывания файлов с расширением **`.gschema.override`** (в формате INI) в директории с XML схемами. После разворачивания необходимо осуществить вызов glib-compile-schemas, для того чтобы настройки вступили в силу
Управление gsettings (настройки графической среды Mate)	gsettings_user	Устанавливает настройки gsettings для пользователя
Управление настройками графической среды KDE	kde	Средство управления настройками среды рабочего стола KDE
Управление настройками графической среды KDE	kde_user	Устанавливает настройки KDE в контексте пользователя
Управление пакетами	package	Средство работы с пакетным менеджером для установки и удаления пакетов программ
Управление пакетами	package_user	Управление пакетами в контексте пользователя
Управление logon-скриптами	scripts	Управление скриптами запуска и завершения работы компьютера, входа и выхода из системы пользователя

Расширение клиентской стороны	Модуль	Описание
Управление logon-скриптами	scripts_user	Управление скриптами в контексте пользователя

Модель групповых политик вызывает расширение клиентской стороны, отвечающие за внесение изменений, согласно параметрам политики. Для выполнения настроек, указанных в параметрах групповой политики, расширения клиентской стороны изменяют конкретные параметры операционной системы. Изменения, внесённые в операционную систему при помощи модуля групповых политик, записываются в журналы событий.

27.5. Периодичность запуска групповых политик

Каждый фронтенд срабатывает на определённые ветки настроек. Запуск фронтенда для машины по умолчанию производится раз в час средством Systemd — **gpupdate.timer**. Запуск фронтенда для пользователя в административном контексте производится с помощью модуля pam_oddjob при входе в систему и далее раз в час (по умолчанию) также средством Systemd — **gpupdate-user.timer**.

Для мониторинга и контроля времени выполнения службы **gpupdate.service** используются системный таймер **gpupdate.timer** и пользовательский таймер **gpupdate-user.timer**. Для управления периодом запуска групповых политик достаточно изменить параметр соответствующего таймера systemd (по умолчанию период запуска составляет 1 час).

Изменить периодичность запуска системного таймера можно, изменив значение параметра **OnUnitActiveSec** в файле **/lib/systemd/system/gpupdate.timer**:

```
[Unit]
Description=Run gpupdate every hour

[Timer]
OnStartupSec=60min
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

По умолчанию таймер **gpupdate.timer** запустится после загрузки ОС, а затем будет запускаться каждый час во время работы системы. Просмотреть статус системного таймера можно, выполнив команду:

```
# systemctl status gpupdate.timer
● gpupdate.timer - Run gpupdate every hour
     Loaded: loaded (/lib/systemd/system/gpupdate.timer; enabled; vendor preset:
disabled)
     Active: active (waiting) since Mon 2024-06-10 16:39:44 EET; 5min ago
    Trigger: Mon 2024-06-10 17:29:17 EET; 43min left
   Triggers: ● gpupdate.service

июн 10 16:39:44 w2.test.alt systemd[1]: Started Run gpupdate every hour..
```

Изменить периодичность запуска пользовательского таймера можно, изменив значение параметра **OnUnitActiveSec** в файле **/usr/lib/systemd/user/gpupdate-user.timer**:

```
[Unit]
Description=Run gpupdate-user every hour

[Timer]
OnStartupSec=60min
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

По умолчанию таймер **gpupdate-user.timer** запустится после входа пользователя в систему, а затем будет запускаться каждый час пока активен сеанс соответствующего пользователя. Просмотреть статус пользовательского таймера можно, выполнив команду от имени пользователя:

```
$ systemctl --user status gpupdate-user.timer
● gpupdate-user.timer - Run gpupdate-user every hour
     Loaded: loaded (/usr/lib/systemd/user/gpupdate-user.timer; enabled; vendor
preset: enabled)
     Active: active (waiting) since Mon 2024-06-10 16:29:32 EET; 10min ago
    Trigger: Mon 2024-06-10 17:29:32 EET; 49min left
   Triggers: ● gpupdate-user.service

июн 10 16:29:32 w2.test.alt systemd[3469]: Started Run gpupdate-user every hour.
```

Чтобы изменения, внесённые в файл **/usr/lib/systemd/user/gpupdate-user.timer**, вступили в силу следует выполнить команду:

```
$ systemctl --user daemon-reload
```

Примечание

Управлять периодичностью запуска **gpupdate** можно также через групповые политики (см. раздел Настройка периодичности запроса конфигураций).

Просмотреть список запущенных системных таймеров можно, выполнив команду:

```
$ systemctl list-timers
```

Просмотреть список запущенных пользовательских таймеров можно, выполнив команду:

```
$ systemctl --user list-timers
```

27.6. Утилита gpresult

GPResult (**gpresult**) отображает сведения о результирующем наборе групповых политик для текущего пользователя (для которого запущена сессия) на текущей машине.

Для возможности использования утилиты должен быть установлен пакет *gpresult*:

```
# apt-get install gpresult
```

Сведения о примененных групповых политиках генерируются из данных, полученных после последнего выполнения **gpupdate**. GPResult не вызывает утилиту **gpupdate**.

Синтаксис команды **gpresult**:

```
gpresult [-h] [-r] [-c] [-v] [-l] [-p] [-w WIDTH] [-i POLICY_GUID] [-n
POLICY_NAME] [-u] [-m]
```

Таблица 27.6. Опции команды gpresult

Ключ	Описание
-h, --help	Вывести справку о команде
-r, --raw	Формат вывода: отображаются ключи групповых политик, текущие и предыдущие значения
-c, --common	Формат вывода: отображаются сведения о системе и имена групповых политик
-v, --verbose	Формат вывода (по умолчанию): отображаются подробные сведения о групповых политиках
-l, --list	Формат вывода: отображаются имена групповых политик и их GUID
-p, --previous	Включить информацию о предыдущих значениях ключей групповых политик
-w WIDTH, --width WIDTH	Задать ширину столбцов для вывода внутренних таблиц (ключи и значения, настройки): ▸по умолчанию ширина столбцов равна максимальной длине строки; ▸если указано значение ≤0, то ширина столбцов будет равна максимальной длине строки; ▸если длина максимальной строки меньше заданного значения, ширина столбцов не изменяется
-i POLICY_GUID, --policy_guid POLICY_GUID	Получить информацию о примененных ключах и значениях политики по GUID
-n POLICY_NAME, --policy_name POLICY_NAME	Получить информацию о примененных ключах и значениях политики по имени
-u, --user	Отобразить информацию для текущего пользователя
-m, --machine	Отобразить информацию для текущей машины

Примечание

Опция **-l** не применяется с опциями **-i** и **-n**. Опция **-l** может использоваться вместе с опцией **-r** — вывод не будет форматированным. Имя GPO и GUID разделяются одним пробелом. Без выбора опции формата вывода по умолчанию используется **-v**.

Примечание

GUID групповой политики можно передавать как в фигурных скобках, так и без: {1BA9EB0C-7B29-49CC-813D-75D8701FC221} и 1BA9EB0C-7B29-49CC-813D-75D8701FC221

Примеры работы с командой **gpresult**:

- получить полный отчет о примененных ГП для пользователя и машины:

```
$ gpresult -v
Отчет сформирован 30-01-2025 10:47

Результирующий набор политик
----------------------------
     Операционная система:    ALT
     Версия ОС:               10.4 (SorbaroniaMitschurinii)

ПОЛЬЗОВАТЕЛЬСКИЕ НАСТРОЙКИ
--------------------------
    Примененные Объекты Групповой Политики
    ---------------------------------------
         GPO          Файлы
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{96D5897A-
CEFB-4A1B-90AF-5D83707130C4}
         Версия       65537
         GUID         {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
         Ключи        -
         Настройки    -

         GPO          Local Policy
         Путь         /var/cache/gpupdate/local-policy
         Версия       -
         GUID         -
         Ключи        -
         Настройки    -

         GPO          Экспериментальные политики
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{377A04D4-213E-4783-9B37-5FEE4FF112AA}
         Версия       65537
         GUID         {377A04D4-213E-4783-9B37-5FEE4FF112AA}
         Ключи        -
         Настройки    -

         GPO          Default Domain Policy
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{31B2F340-016D-11D2-945F-00C04FB984F9}
         Версия       0
         GUID         {31B2F340-016D-11D2-945F-00C04FB984F9}
         Ключи        -
         Настройки    -

         GPO          KDE
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{3C70AD47-
E9D5-415F-A565-C1E1472C6D55}
         Версия       655370
         GUID         {3C70AD47-E9D5-415F-A565-C1E1472C6D55}
         Ключи        -
```

```
         Настройки    -

МАШИННЫЕ НАСТРОЙКИ
------------------
    Примененные Объекты Групповой Политики
    --------------------------------------
         GPO          Экспериментальные политики
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{377A04D4-213E-4783-9B37-5FEE4FF112AA}
         Версия       65537
         GUID         {377A04D4-213E-4783-9B37-5FEE4FF112AA}
         Ключи        -
         Настройки    -

         GPO          KDE
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{3C70AD47-
E9D5-415F-A565-C1E1472C6D55}
         Версия       655370
         GUID         {3C70AD47-E9D5-415F-A565-C1E1472C6D55}
         Ключи        /Software/BaseALT/Policies/GPUpdate/
KdeApplier                          1
                      /Software/BaseALT/Policies/GPUpdate/
KdeApplierUser                      1
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
Autolock            1
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
LockGrace           20
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
LockOnResume        1
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
Timeout             5
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.Autolock       0
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.LockGrace      1
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.LockOnResume   1
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.Timeout        0
         Настройки    -

         GPO          Local Policy
         Путь         /var/cache/gpupdate/local-policy
         Версия       -
         GUID         -
         Ключи        /SOFTWARE/Policies/Microsoft/WindowsFirewall/
FirewallRules/OpenSSH   v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|
LPort=22|Name=Open SSH port|Desc=Open SSH port|
                      /Software/BaseALT/Policies/Control/ssh-gssapi-
auth                   enabled
                      /Software/BaseALT/Policies/Control/sshd-allow-
groups                 enabled
                      /Software/BaseALT/Policies/Control/sshd-allow-groups-
list            remote
                      /Software/BaseALT/Policies/Control/sshd-gssapi-
auth                  enabled
                      /Software/BaseALT/Policies/Control/system-
policy                     gpupdate
                      /Software/BaseALT/Policies/SystemdUnits/
```

```
gpupdate.service            1
                    /Software/BaseALT/Policies/SystemdUnits/
oddjobd.service             1
                    /Software/BaseALT/Policies/SystemdUnits/
sshd.service                1
        Настройки   -

        GPO         Default Domain Policy
        Путь        /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{31B2F340-016D-11D2-945F-00C04FB984F9}
        Версия      0
        GUID        {31B2F340-016D-11D2-945F-00C04FB984F9}
        Ключи       -
        Настройки   -

        GPO         Файлы
        Путь        /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{96D5897A-
CEFB-4A1B-90AF-5D83707130C4}
        Версия      65537
        GUID        {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
        Ключи       /Software/BaseALT/Policies/GPUpdate/GlobalExperimental
1
        Настройки   Тип                 Файлы
                    Источник файла(ов)  //test.alt/sysvol/test.alt/test.txt
                    Источник            -
                    Действие            U
                    Место назначения    %DesktopDir%/new2.txt
                    Только для чтения   0
                    Архивный            0
                    Скрытый             0
                    Подавление ошибок   0
                    Исполняемый         0

        GPO         Сетевой диск
        Путь        /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{1F4C3297-9355-4098-B9C8-53CAD6FFEBEF}
        Версия      720907
        GUID        {1F4C3297-9355-4098-B9C8-53CAD6FFEBEF}
        Ключи       /Software/BaseALT/Policies/GPUpdate/DriveMapsName
my_share
        Настройки   Тип               Сетевые диски
                    Пароль
                    Имя диска         I
                    Путь              \\dc1.test.alt\sysvol
                    Действие          U
                    Этот диск         SHOW
                    Все диски         SHOW
                    Название
                    Переподключиться  1
                    Использовать      0

                    Тип               Сетевые диски
                    Пароль
                    Имя диска         O
                    Путь              \\dc1.test.alt\Free
                    Действие          U
                    Этот диск         SHOW
```

```
                      Все диски          SHOW
                      Название
                      Переподключиться   0
                      Использовать       1
```

- получить полный отчет о примененных ГП для машины:

```
$ gpresult -v -m
Отчет сформирован 30-01-2025 10:48

Результирующий набор политик
---------------------------
     Операционная система:    ALT
     Версия ОС:               10.4 (SorbaroniaMitschurinii)

МАШИННЫЕ НАСТРОЙКИ
------------------
    Примененные Объекты Групповой Политики
    --------------------------------------
         GPO          Экспериментальные политики
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{377A04D4-213E-4783-9B37-5FEE4FF112AA}
         Версия       65537
         GUID         {377A04D4-213E-4783-9B37-5FEE4FF112AA}
         Ключи        -
         Настройки    -

         GPO          KDE
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{3C70AD47-
E9D5-415F-A565-C1E1472C6D55}
         Версия       655370
         GUID         {3C70AD47-E9D5-415F-A565-C1E1472C6D55}
         Ключи        /Software/BaseALT/Policies/GPUpdate/
KdeApplier                          1
                      /Software/BaseALT/Policies/GPUpdate/
KdeApplierUser                      1
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
Autolock            1
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
LockGrace           20
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
LockOnResume        1
                      /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/
Timeout             5
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.Autolock       0
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.LockGrace      1
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.LockOnResume   1
                      /Software/BaseALT/Policies/KDELocks/
kscreenlockerrc.Daemon.Timeout        0
         Настройки    -

         GPO          Local Policy
         Путь         /var/cache/gpupdate/local-policy
         Версия       -
         GUID         -
         Ключи        /SOFTWARE/Policies/Microsoft/WindowsFirewall/
```

```
FirewallRules/OpenSSH   v2.20|Action=Allow|Active=TRUE|Dir=In|Protocol=6|
LPort=22|Name=Open SSH port|Desc=Open SSH port|
                      /Software/BaseALT/Policies/Control/ssh-gssapi-
auth                   enabled
                      /Software/BaseALT/Policies/Control/sshd-allow-
groups                 enabled
                      /Software/BaseALT/Policies/Control/sshd-allow-groups-
list            remote
                      /Software/BaseALT/Policies/Control/sshd-gssapi-
auth                  enabled
                      /Software/BaseALT/Policies/Control/system-
policy                     gpupdate
                      /Software/BaseALT/Policies/SystemdUnits/
gpupdate.service             1
                      /Software/BaseALT/Policies/SystemdUnits/
oddjobd.service              1
                      /Software/BaseALT/Policies/SystemdUnits/
sshd.service                 1
         Настройки    -

         GPO          Default Domain Policy
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{31B2F340-016D-11D2-945F-00C04FB984F9}
         Версия       0
         GUID         {31B2F340-016D-11D2-945F-00C04FB984F9}
         Ключи        -
         Настройки    -

         GPO          Файлы
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/{96D5897A-
CEFB-4A1B-90AF-5D83707130C4}
         Версия       65537
         GUID         {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
         Ключи        /Software/BaseALT/Policies/GPUpdate/GlobalExperimental
1
         Настройки    Тип                  Файлы
                      Источник файла(ов)   //test.alt/sysvol/test.alt/test.txt
                      Источник             -
                      Действие             U
                      Место назначения     %DesktopDir%/new2.txt
                      Только для чтения    0
                      Архивный             0
                      Скрытый              0
                      Подавление ошибок    0
                      Исполняемый          0

         GPO          Сетевой диск
         Путь         /var/cache/samba/gpo_cache/TEST.ALT/POLICIES/
{1F4C3297-9355-4098-B9C8-53CAD6FFEBEF}
         Версия       720907
         GUID         {1F4C3297-9355-4098-B9C8-53CAD6FFEBEF}
         Ключи        /Software/BaseALT/Policies/GPUpdate/DriveMapsName
my_share
         Настройки    Тип                Сетевые диски
                      Пароль
                      Имя диска          I
                      Путь               \\dc1.test.alt\sysvol
                      Действие           U
                      Этот диск          SHOW
```

```
                        Все диски          SHOW
                        Название
                        Переподключиться   1
                        Использовать       0

                        Тип                Сетевые диски
                        Пароль
                        Имя диска          O
                        Путь               \\dc1.test.alt\Free
                        Действие           U
                        Этот диск          SHOW
                        Все диски          SHOW
                        Название
                        Переподключиться   0
                        Использовать       1
```

- вывести список (примененных) имен групповых политик и их GUID:

```
$ gpresult -lm
 Экспериментальные политики    {377A04D4-213E-4783-9B37-5FEE4FF112AA}
 KDE                           {3C70AD47-E9D5-415F-A565-C1E1472C6D55}
 Local Policy                  -
 Default Domain Policy         {31B2F340-016D-11D2-945F-00C04FB984F9}
 Файлы                         {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
 Сетевой диск                  {1F4C3297-9355-4098-B9C8-53CAD6FFEBEF}
```

- получить информацию о примененных ключах групповой политики по GUID:

```
$ gpresult -c -i 6F65CD4D-9209-4A81-9801-17A35CEE5CFD
/Software/BaseALT/Policies/Polkit/org.freedesktop.NetworkManager.enable-
disable-network         Auth_admin
/Software/BaseALT/Policies/Polkit/
org.freedesktop.NetworkManager.settings.modify.system         No
/Software/BaseALT/Policies/PolkitLocks/org.freedesktop.NetworkManager.enable-
disable-network    0
/Software/BaseALT/Policies/PolkitLocks/
org.freedesktop.NetworkManager.settings.modify.system    0
```

- получить информацию о примененных ключах групповой политики по имени политики:

```
$ gpresult -c -n KDE
 /Software/BaseALT/Policies/GPUpdate/KdeApplier                              1
 /Software/BaseALT/Policies/GPUpdate/KdeApplierUser                          1
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/Autolock              1
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/LockGrace             20
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/LockOnResume          1
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/Timeout               5
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.Autolock         0
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.LockGrace        1
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.LockOnResume     1
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.Timeout          0
```

где KDE — имя групповой политики;

- получить информацию о текущих и предыдущих ключах групповой политики по имени политики:

```
$ gpresult -c -p -n KDE
 /Software/BaseALT/Policies/GPUpdate/KdeApplier
1     -
 /Software/BaseALT/Policies/GPUpdate/KdeApplierUser
1     -
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/Autolock
1     -
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/LockGrace
20    11
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/LockOnResume
1     -
 /Software/BaseALT/Policies/KDE/kscreenlockerrc/Daemon/Timeout
5     12
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.Autolock
0     1
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.LockGrace
1     -
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.LockOnResume
1     -
 /Software/BaseALT/Policies/KDELocks/kscreenlockerrc.Daemon.Timeout
0     1
```

Глава 28. Модуль удаленного управления базой данных конфигурации (ADMC)

28.1. Запуск ADMC

28.2. Интерфейс ADMC

28.3. Свойства объектов

28.4. Выбор контейнера

28.5. Управление пользователями

28.6. Управление контактами

28.7. Управление группами

28.8. Управление компьютерами

28.9. Управление подразделениями

28.10. Делегирование административных полномочий

28.11. Управление объектами парольных настроек

28.12. Управление общими папками

28.13. Управление объектами групповых политик

28.14. Добавление/Удаление UPN суффиксов

28.15. Прсмотр и передача ролей FSMO

28.16. Выбор объектов

28.17. Поиск объектов

28.18. Использование сохранённых результатов поиска

Компонент удаленного управления базой данных конфигурации (далее — ADMC) предназначен для управления:

- объектами в домене (пользователями, группами, компьютерами, подразделениями);
- групповыми политиками.

ADMC позволяет:

- создавать и администрировать учётные записи пользователей, компьютеров и групп;
- менять пароли пользователя;
- создавать организационные подразделения, для структурирования и выстраивания иерархической системы распределения учётных записей в AD;
- просматривать и редактировать атрибуты объектов;
- создавать и просматривать объекты групповых политик;
- выполнять поиск объектов по разным критериям;
- сохранять поисковые запросы;
- переносить поисковые запросы между компьютерами (выполнять экспорт и импорт поисковых запросов).

В **ADMC** реализована функция поиска объектов групповых политик.

28.1. Запуск ADMC

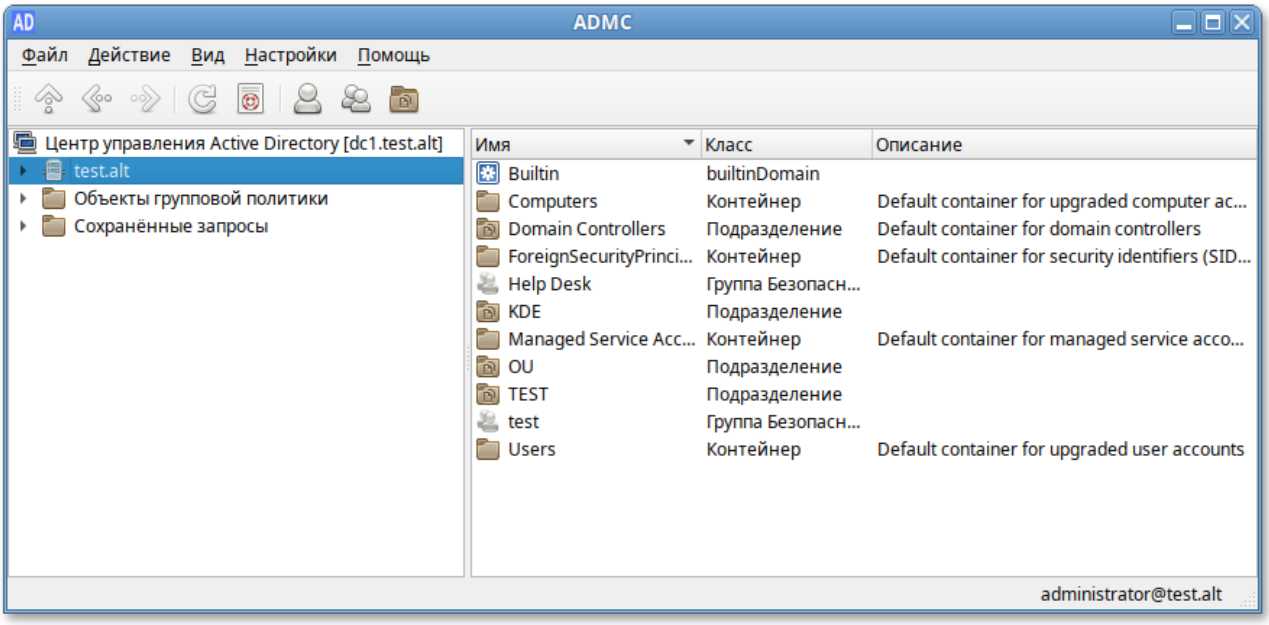
Запуск **ADMC** осуществляется из меню запуска приложений: пункт **Системные** → **ADMC** или из командной строки (команда **admc**).

Примечание

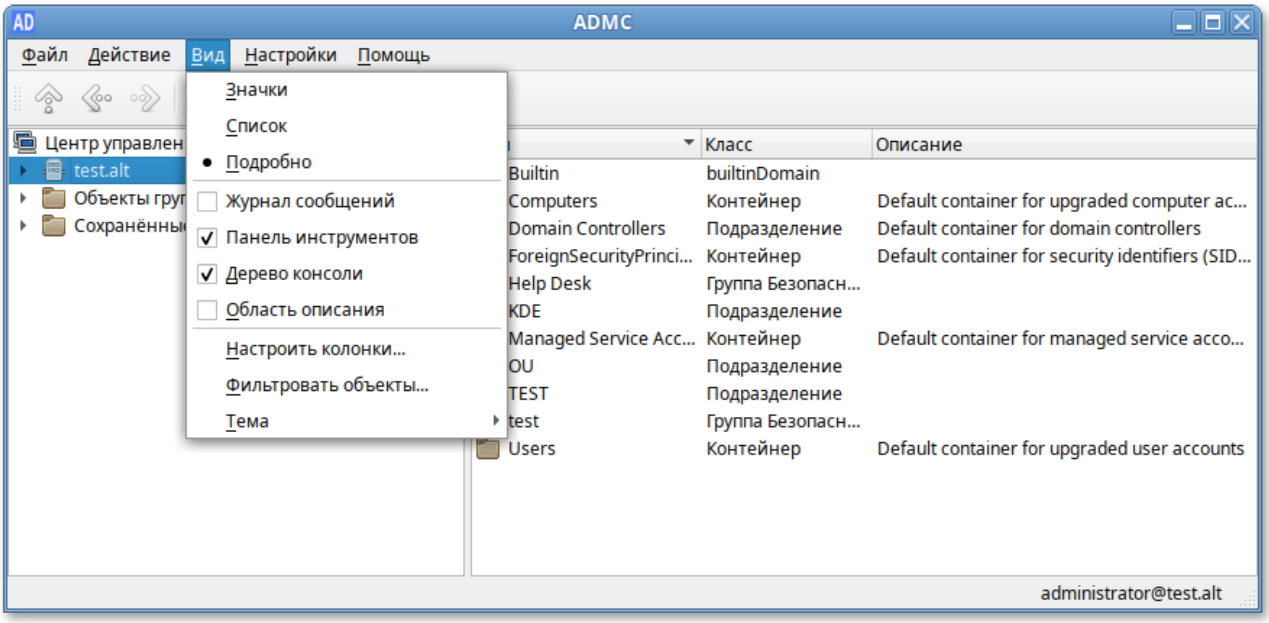
Для использования **ADMC** необходимо предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

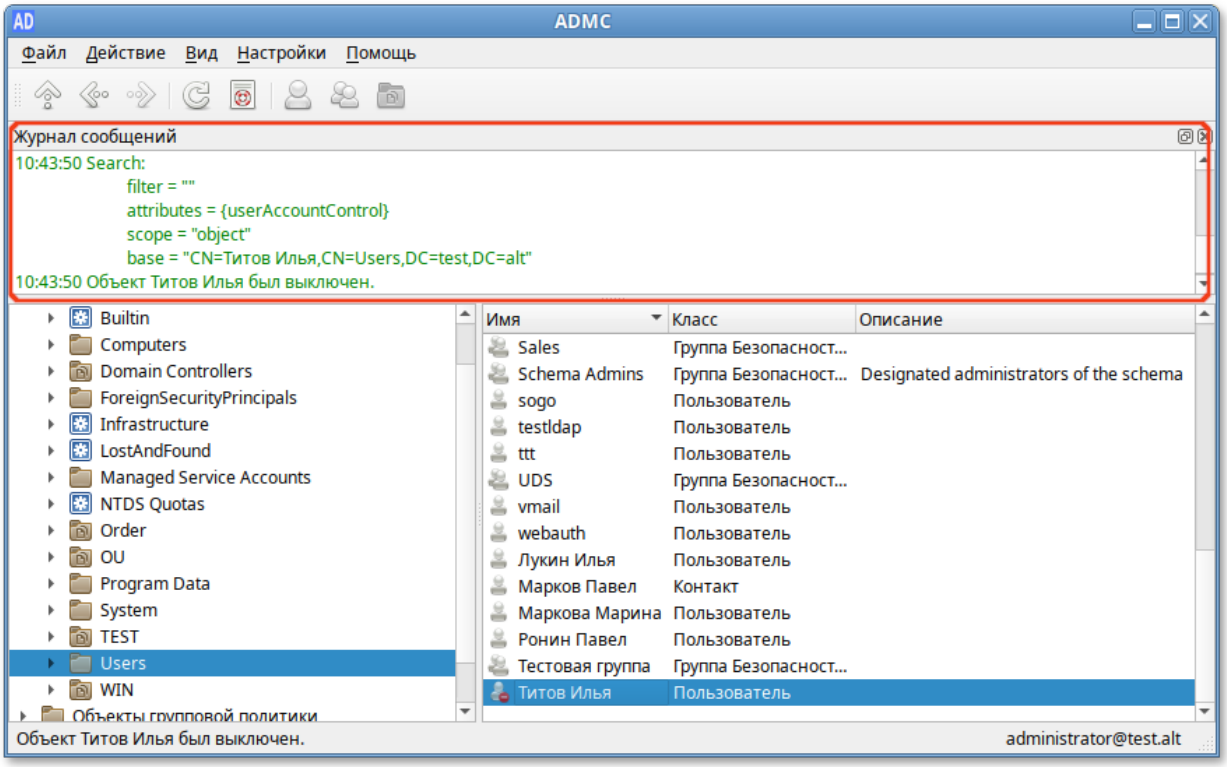
28.2. Интерфейс ADMC



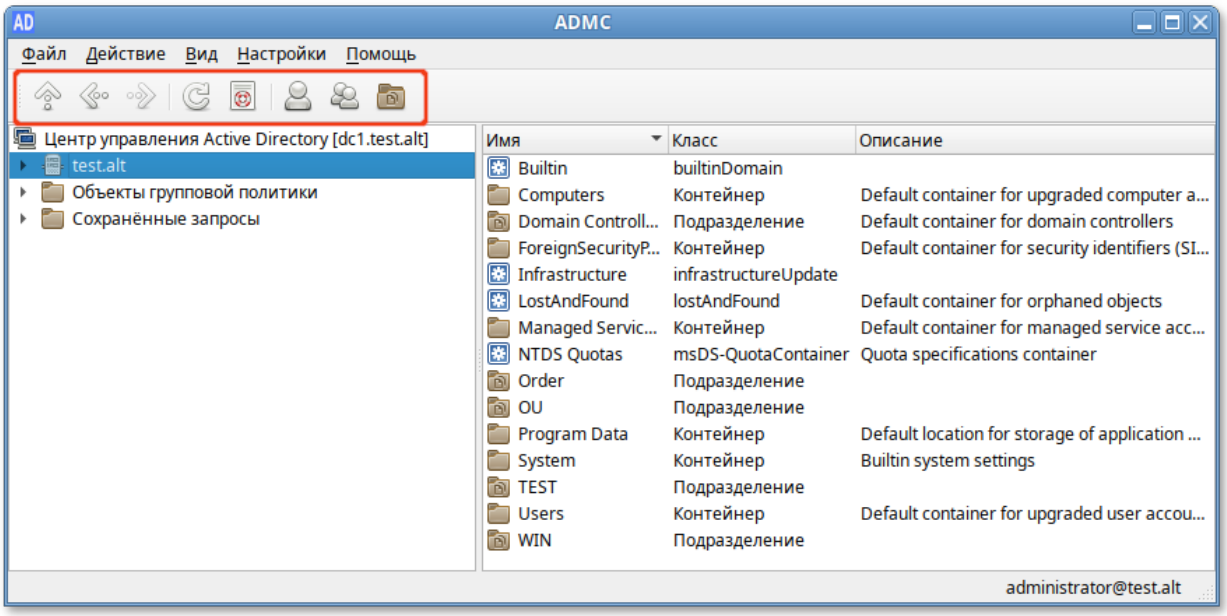
Включить/выключить отображение панелей можно, отметив соответствующий пункт в меню **Вид**:



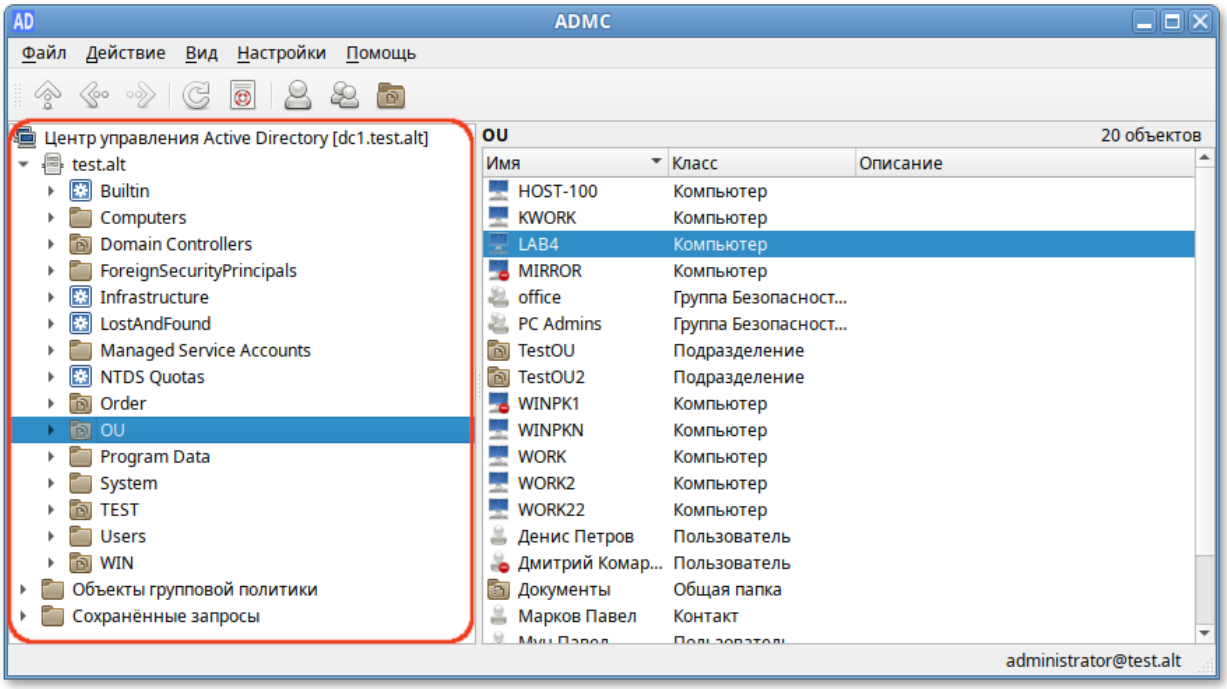
- **Журнал сообщений** — показать/скрыть панель журнала. В панели журнала отображаются сообщения о статусе приложения. Эти сообщения содержат отчеты обо всех выполненных действиях над объектами:



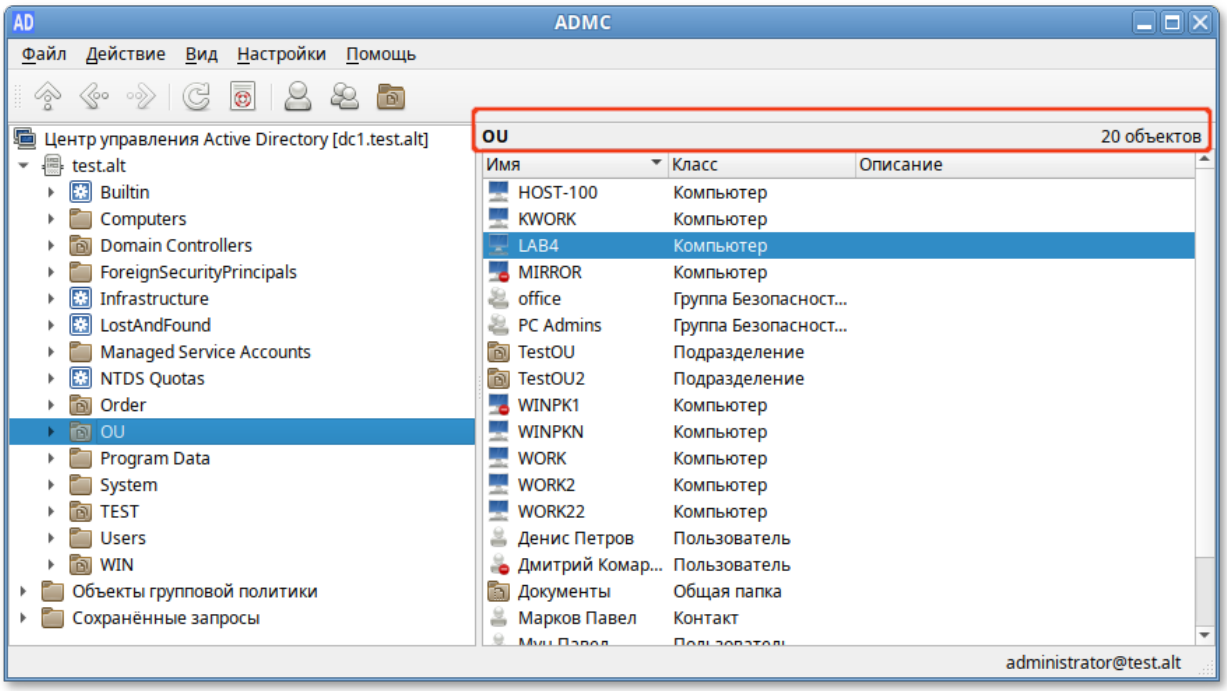
Панель инструментов — показать/скрыть панель инструментов;



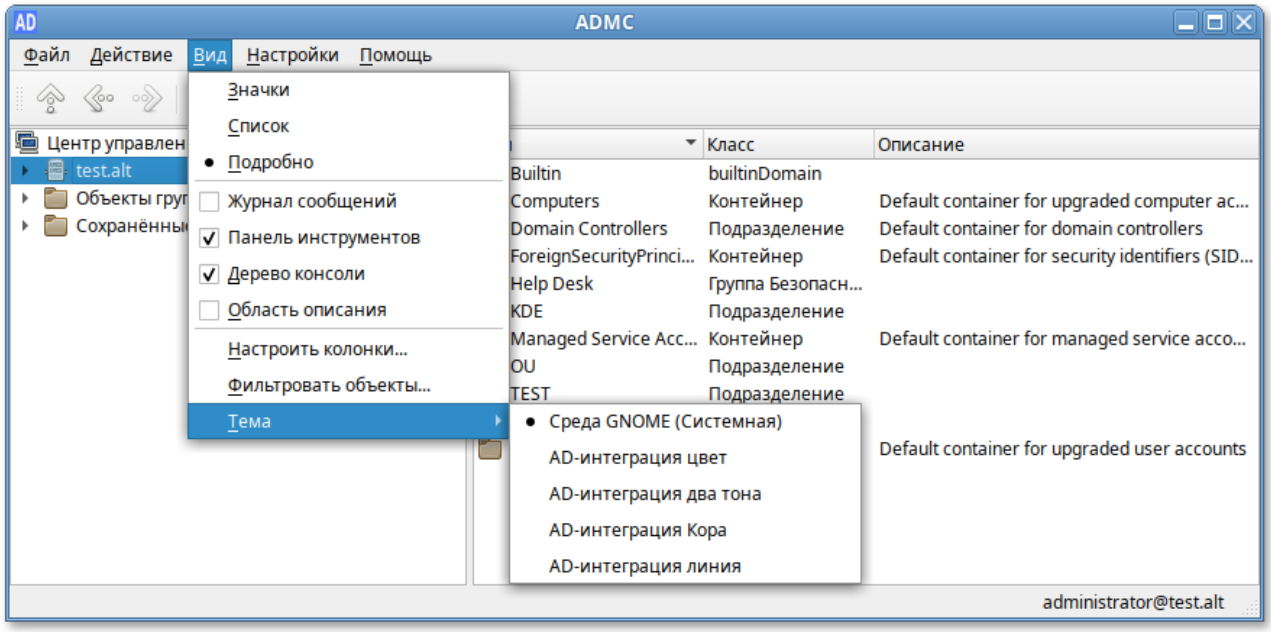
Дерево консоли — показать/скрыть панель дерева объектов Active Directory. Панель дерева объектов Active Directory отображается слева, в правой панели будут отображаться сведения о выбранном объекте. По умолчанию дерево показывает объекты типа «контейнер»:



Область описания — выводить описание контейнера. В области описания отображается название контейнера и количество объектов в контейнере:



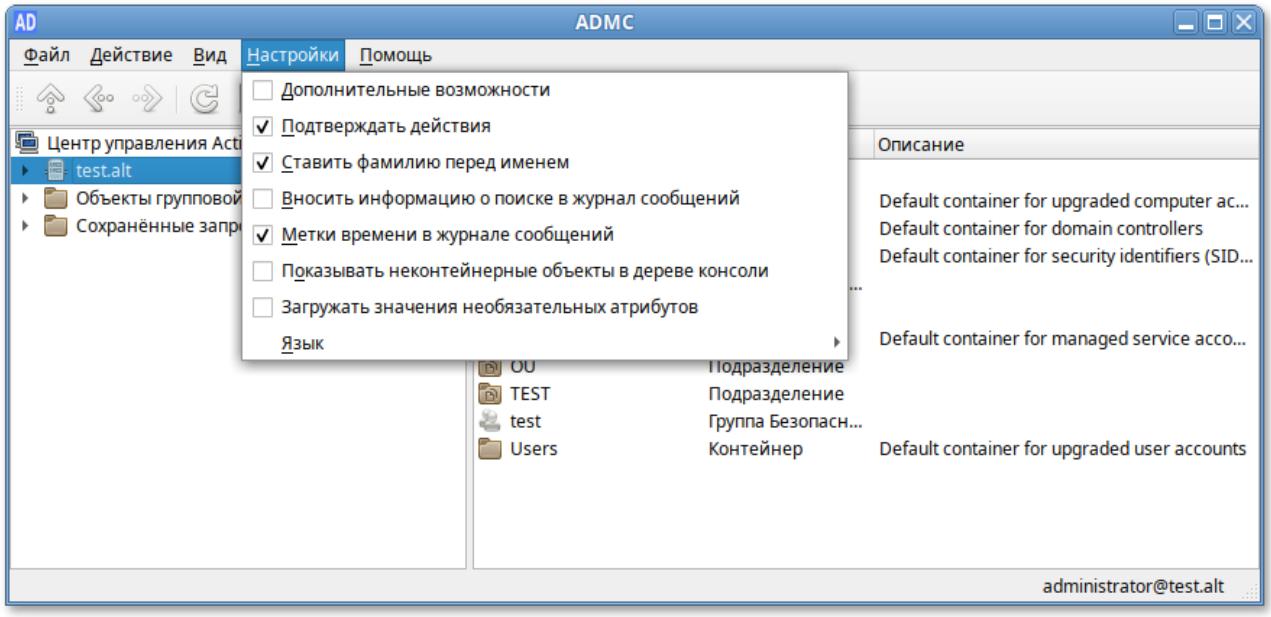
В меню **Вид** → **Тема** можно выбрать тему значков:



Примечание

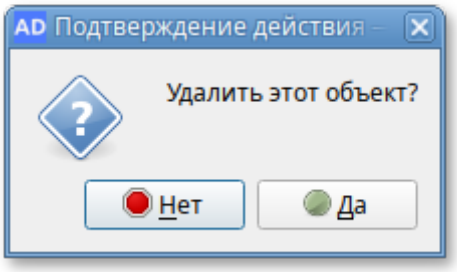
Системная тема берётся из каталога **`/usr/share/icons`**, пользовательские темы берутся по умолчанию из каталога **`/usr/share/ad-integration-themes`**. Каталоги с темами определяются по наличию в них файла **`index.theme`** и могут быть символическими ссылками.

В меню **Настройки** можно изменить параметры **ADMC**:



- **Дополнительные возможности** — показывать расширенные объекты и элементы приложения;

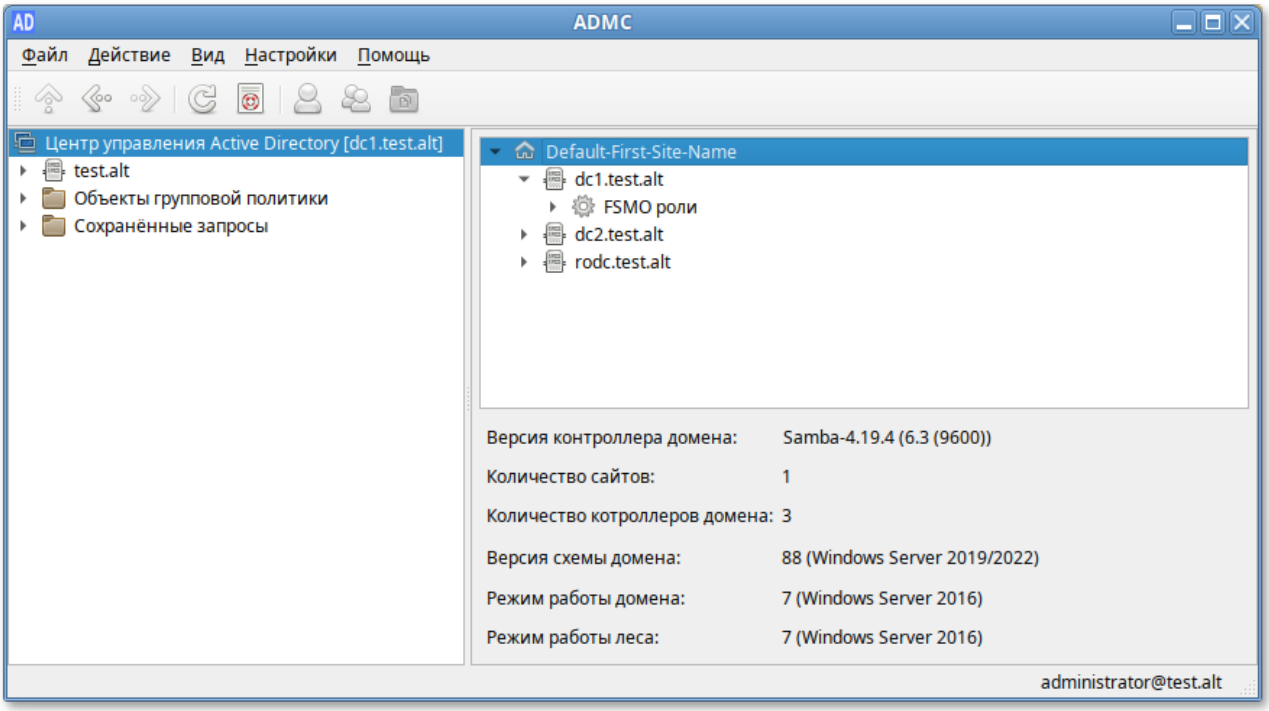
- **Подтверждать действия** — выводить окно **Подтвердить действие** при выполнении потенциально опасных действий, например, удалении объекта:



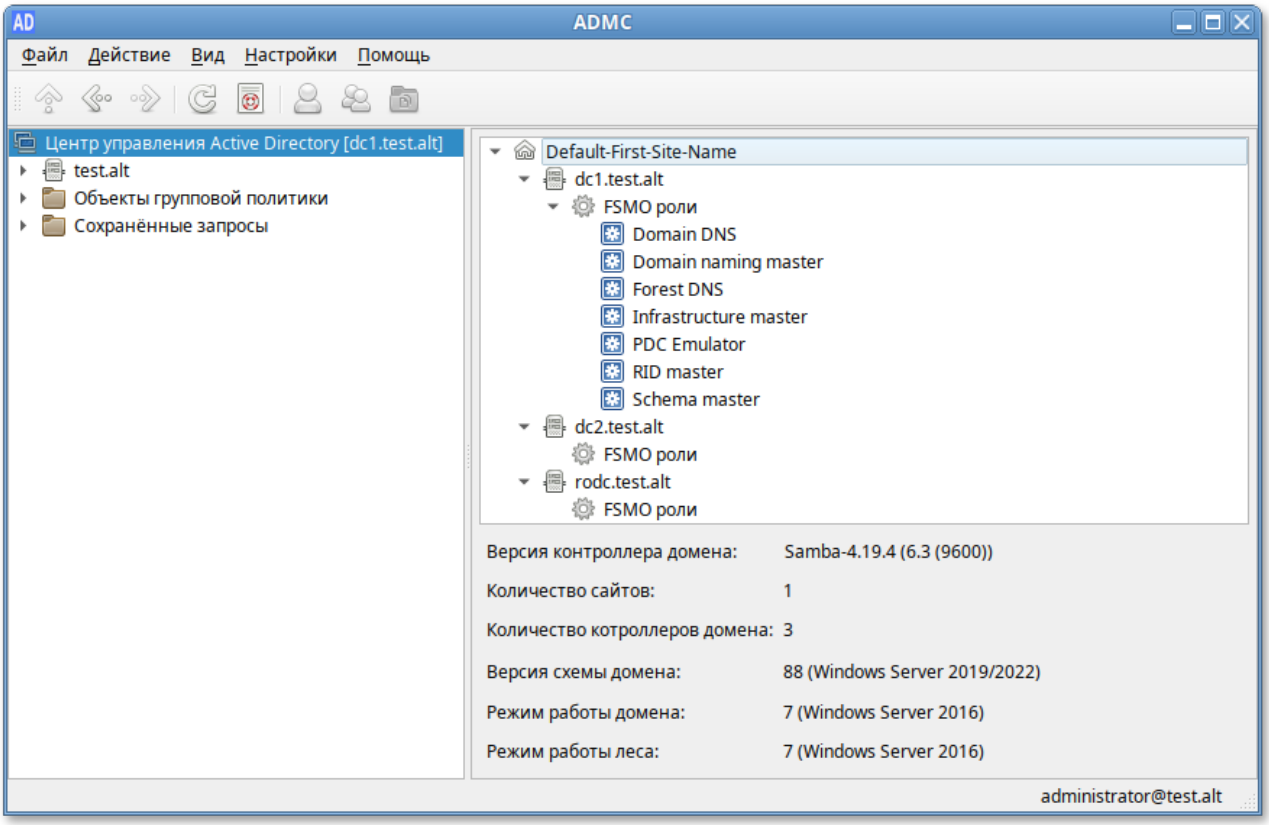
- **Ставить фамилию перед именем** — изменить формат полного имени (поле «cn») по умолчанию на «Фамилия Имя»;
- **Вносить информацию о поиске в журнал сообщений** — вносить в журнал поисковые запросы;
- **Метки времени в журнале сообщений** — показывать в журнале время события;
- **Показывать неконтейнерные объекты в дереве консоли** — показывать неконтейнерные объекты (например, учётные записи пользователей и компьютерные учётные записи) в панели дерева объектов Active Directory;
- **Загрузить необязательные атрибуты** — позволяет загрузить значения необязательных атрибутов на вкладке **Атрибуты** в окне свойств пользователя;
- **Язык** — выбрать язык интерфейса (русский или английский).

Выбранные параметры сохраняются и восстанавливаются при каждом запуске программы.

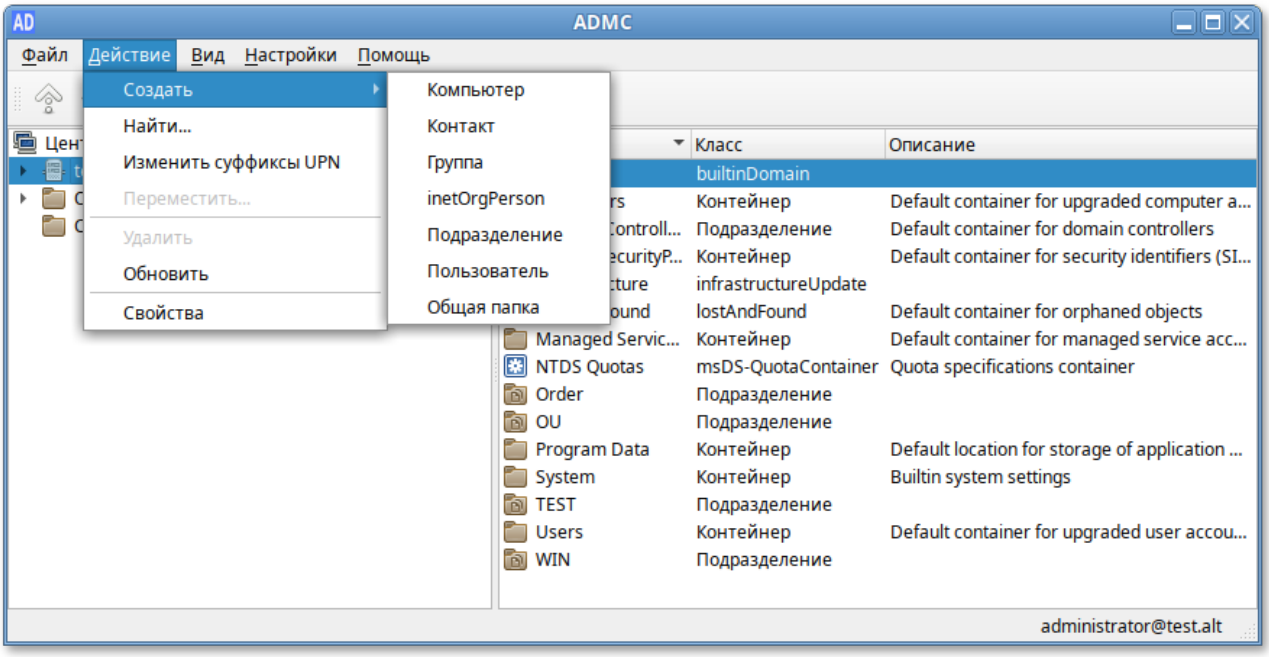
При выборе корневого элемента в дереве консоли будет отображена информация о домене: дерево с сайтами, контроллерами домена и ролями FSMO. Данный виджет также содержит версию контроллера домена, количество сайтов и контроллеров домена, режимы работы домена и леса, версию схемы домена:



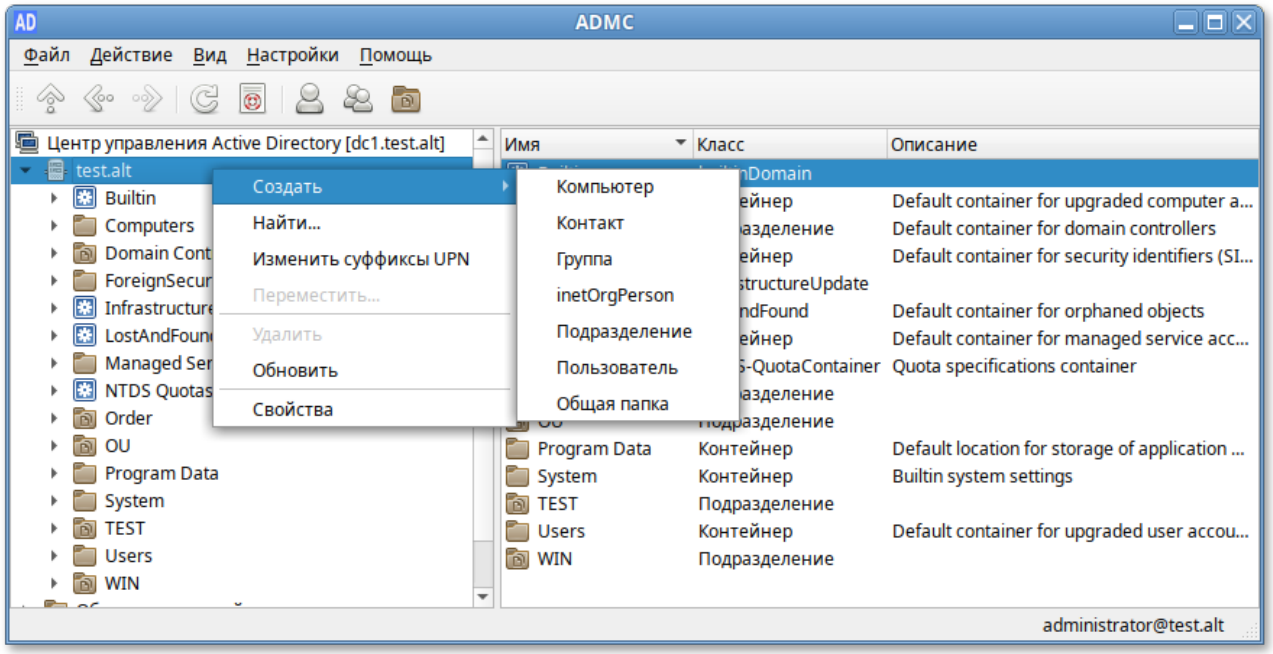
Роли FSMO:



Меню операций с объектом открывается из строки меню (пункт **Действие**) после выбора объекта:



или в контекстном меню объекта:

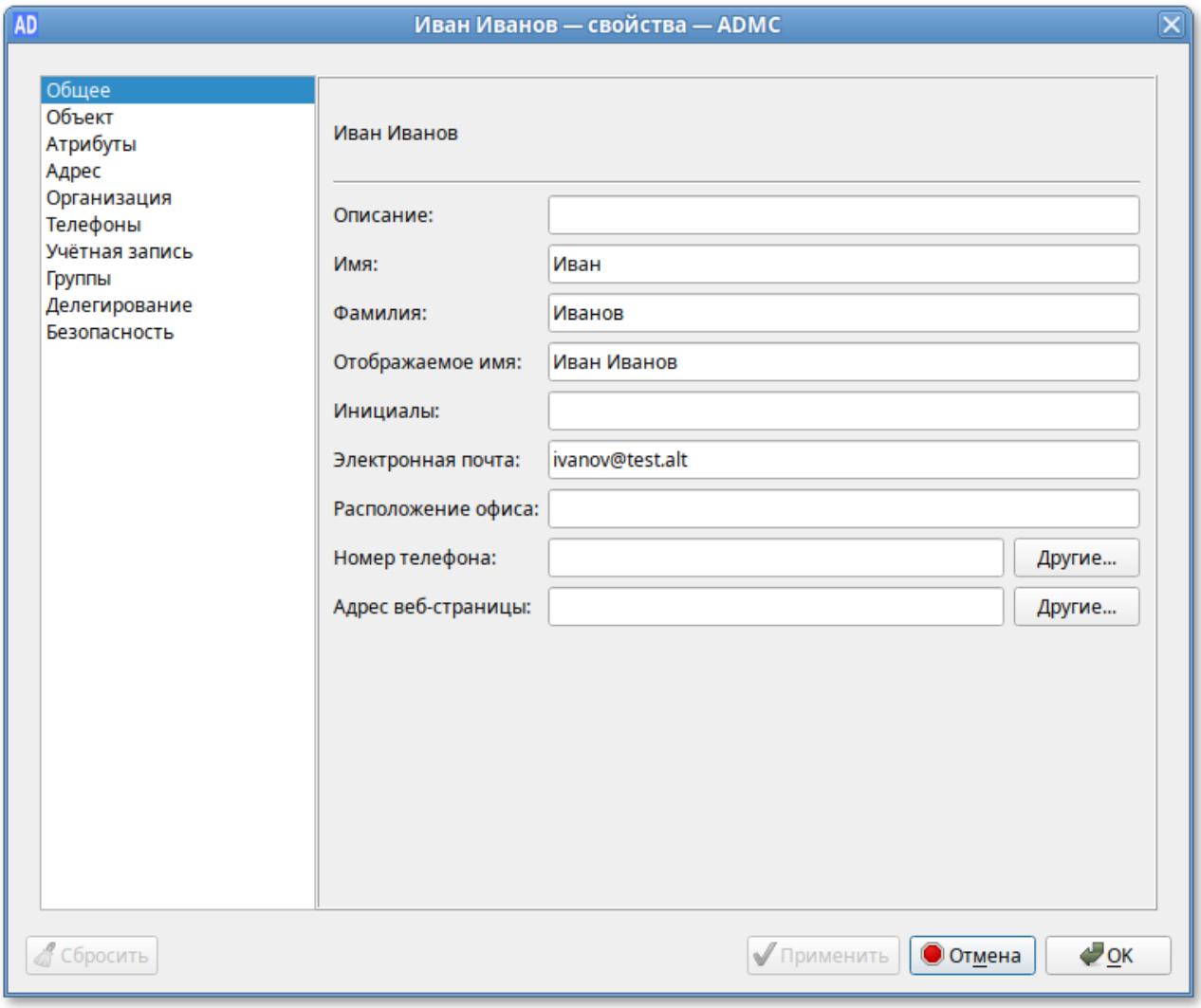


Меню операций содержит действия, применимые к выделенному объекту.

28.3. Свойства объектов

Существует два режима работы ADMC: обычный и расширенный режим. При включении расширенного режима (**Настройки** → **Дополнительные возможности**) в свойствах всех объектов появляются дополнительно две вкладки: **Атрибуты** и **Объект**. Для объекта пользователь также появляется вкладка **Безопасность**.

Окно **Учетная запись пользователя — Свойства** в расширенном режиме:



По умолчанию отображается вкладка **Общее**.

Таблица 28.1. Назначение вкладок окна «Свойства учётной записи пользователя»

Вкладка	Описание	Расширенный режим
Общее	Основная вкладка, содержащая информацию, идентифицирующую личность пользователя, которой соответствует данная учётная запись	-
Учётная запись	Характеристики учётной записи пользователя, настройка правил регистрации в сети	-
Адрес	Почтовый адрес пользователя	-
Организация	Данные о сотруднике согласно штатному расписанию	-
Телефоны	Настройка телефонии	-
Группы	Управление членством в группах безопасности	-

Вкладка	Описание	Расширенный режим
Атрибуты	Список атрибутов объекта	+
Объект	Информация об объекте	+
Делегирование		-
Безопасность	Права доступа к объекту	+

Во вкладке **Общее** задаются личные данные сотрудника и его контактная информация: телефоны, размещение, адрес электронной почты и др. Вкладка **Общее** отображается по умолчанию при вызове свойств учётной записи любого объекта AD. В качестве значений параметров указаны названия соответствующих им полей в AD.

Таблица 28.2. Соответствие параметров на вкладке «Общее» полям в AD

Поле на вкладке Общее	Примечание	Поле в Active Directory	Тип
Полное имя	Во вкладке **Общее** значение этого поля изменить нельзя	cn, name	Юникод
Описание		description	Юникод
Имя		givenName	Юникод
Фамилия		sn	Юникод
Отображаемое имя	Значение этого параметра складывается из значений трёх параметров: First Name, Initials и Last Name	diplayName	Юникод
Инициалы	Длина не более 6 символов	initials	Юникод
Электронная почта	Автоматически заполняемое поле в соответствии с форматом UPN (RFC 822) при создании почтового ящика для учётной записи пользователя. По умолчанию поле пустое	mail	Юникод
Расположение офиса	Указывается физическое месторасположение пользователя: комната, офис и т.д.	physicalDeliveryOfficeName	Юникод
Номер телефона		telephoneNumber	Юникод
Другие телефоны	Можно задать, нажав кнопку **Другие...**	otherTelephone	Юникод
Адрес веб-страницы		wWWHomePage	Юникод

Поле на вкладке Общее	Примечание	Поле в Active Directory	Тип
Другие адреса веб-страниц	Можно задать, нажав кнопку **Другие...**	url	Юникод

Во вкладке **Учетная запись** сосредоточены настройки, характеризующие правила доступа пользователя к сети, включая имя входа в сеть:

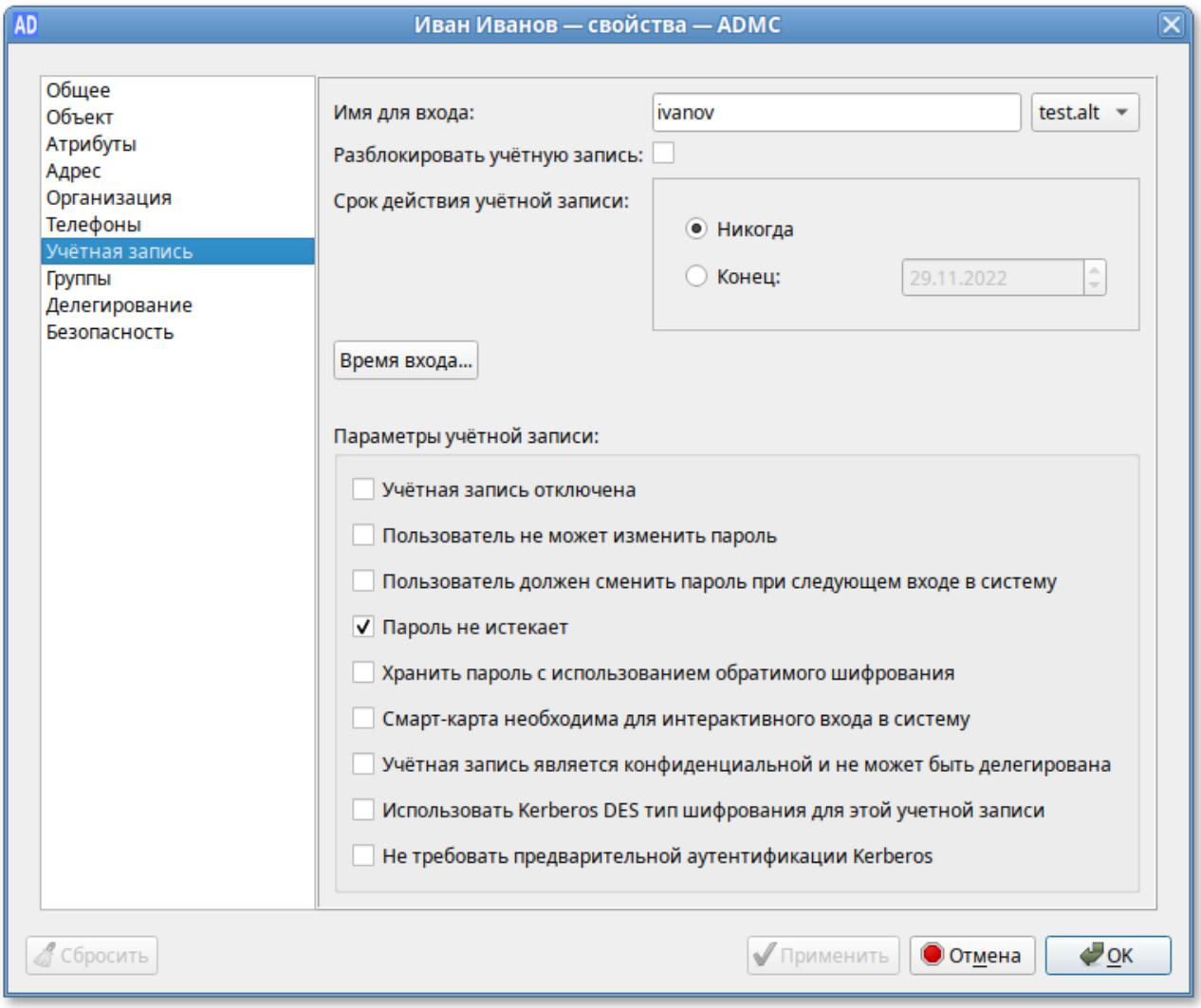


Таблица 28.3. Соответствие параметров на вкладке «Учетная запись» полям в AD

Поле на вкладке Учетная запись	Примечание	Поле в Active Directory	Тип
Имя для входа	Имя пользователя для входа (логин пользователя)	userPrincipalName	Юникод
Разблокировать учётную запись	Позволяет разблокировать учётную запись пользователя, если она была заблокирована, например, из-за	userAccountControl = 16	Целое число

Поле на вкладке Учетная запись	Примечание	Поле в Active Directory	Тип
	слишком большого количества неудачных попыток входа		
Срок действия учётной записи	Дата отключения учётной записи (по умолчанию **Никогда** — неограниченный срок действия). Если нужно задать дату окончания срока действия учётной записи пользователя, следует выбрать **Конец** и затем выбрать дату	accountExpires	Большое целое число
Время входа…	Часы, в которые пользователю разрешено выполнять вход в домен	logonHours	Октет
Учетная запись отключена (ACCOUNTDISABLE)	Если эта опция включена, пользователь не сможет войти в систему	userAccountControl = 0x0002 (2)	Целое число
Пользователь не может изменить пароль (PASSWD_CANT_CHANGE)		userAccountControl = 0x0040 (64)	Целое число
Пользователь должен сменить пароль при следующем входе в систему		pwdLastSet	Большое целое число
Пароль не истекает (DONT_EXPIRE_PASSWORD)	Срок действия пароля для этой учётной записи никогда не истечет	userAccountControl = 0x10000 (65536)	Целое число
Хранить пароль с использованием обратимого шифрования (ENCRYPTED_TEXT_PWD_ALLOWED)	Для шифрования ключей использовать DES-шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы,	userAccountControl = 0x0080 (128)	Целое число

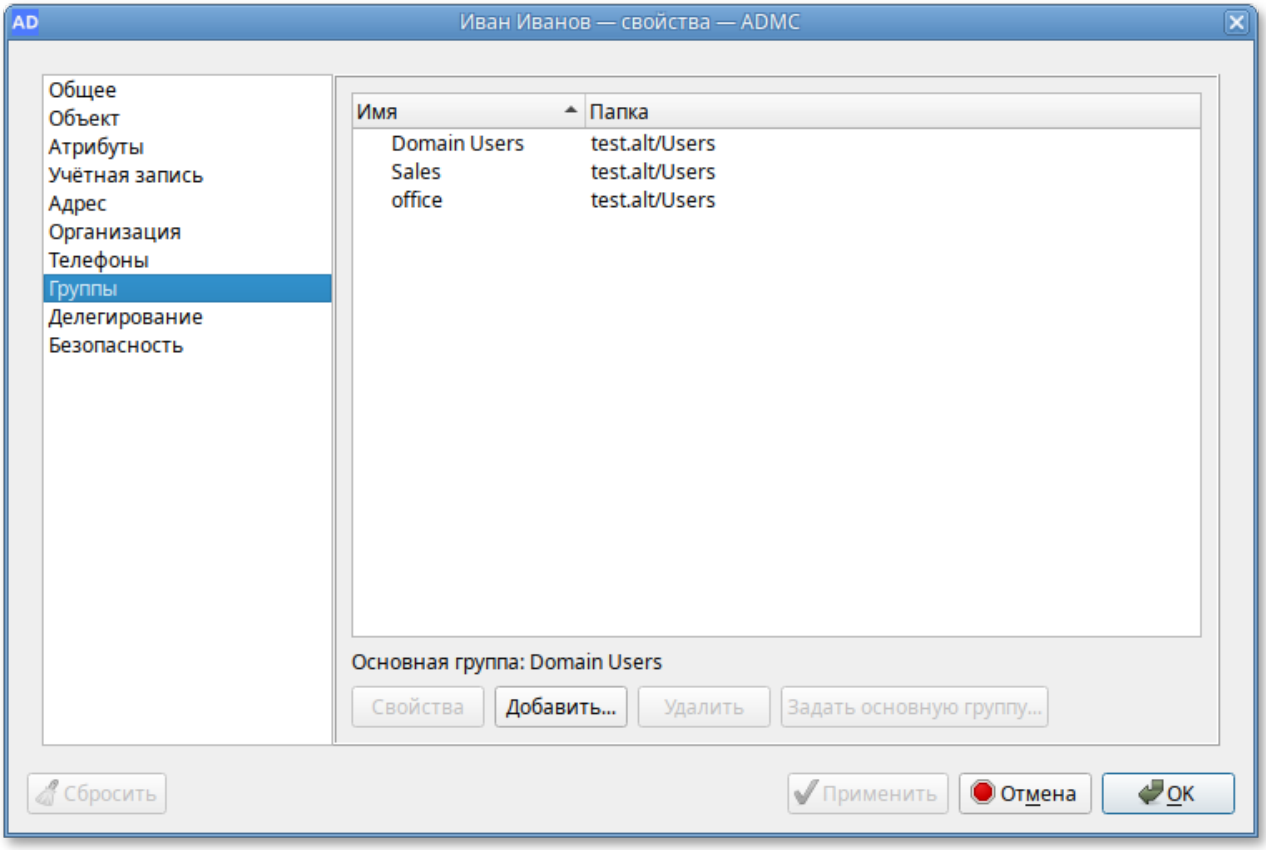
Поле на вкладке Учетная запись	Примечание	Поле в Active Directory	Тип
	требующие знание пароля пользователя для проверки подлинности		
Смарт-карта необходима для интерактивного входа в систему (SMARTCARD_REQUIRED)	Пользователь должен войти в систему с помощью смарт-карты	userAccountControl = 0x40000 (262144)	Целое число
Учетная запись является конфиденциальной и не может быть делегирована (NOT_DELEGATED)	Пользователю нельзя доверять делегирование полномочий	userAccountControl = 0x100000 (1048576)	Целое число
Использовать Kerberos DES тип шифрования для этой учётной записи (USE_DES_KEY_ONLY)	Ограничить этот субъект использованием только типов шифрования DES (стандарт шифрования данных) для ключей	userAccountControl = 0x200000 (2097152)	Целое число
Не требовать предварительной аутентификации Kerberos (DONT_REQ_PREAUTH)	Для доступа к ресурсам сети не нужно предварительно проверять подлинность с помощью протокола Kerberos	userAccountControl = 0x400000 (4194304)	Целое число
Доверять делегирование (TRUSTED_FOR_DELEGATION)	Учетная запись пользователя или компьютера, под которой выполняется служба, является доверенной для делегирования Kerberos. Любая такая служба может олицетворять клиента, запрашивающего службу	userAccountControl = 0x80000 (524288)	Целое число

Примечание

userAccountControl — атрибут управления учётной записью пользователя. Значение атрибута userAccountControl, образуется путем суммирования всех установленных значений. В таблице приведены только те значения, которые можно изменить явным образом на вкладках **Учетная запись** и **Делегирование**. Значения UserAccountControl по умолчанию для определенных объектов:

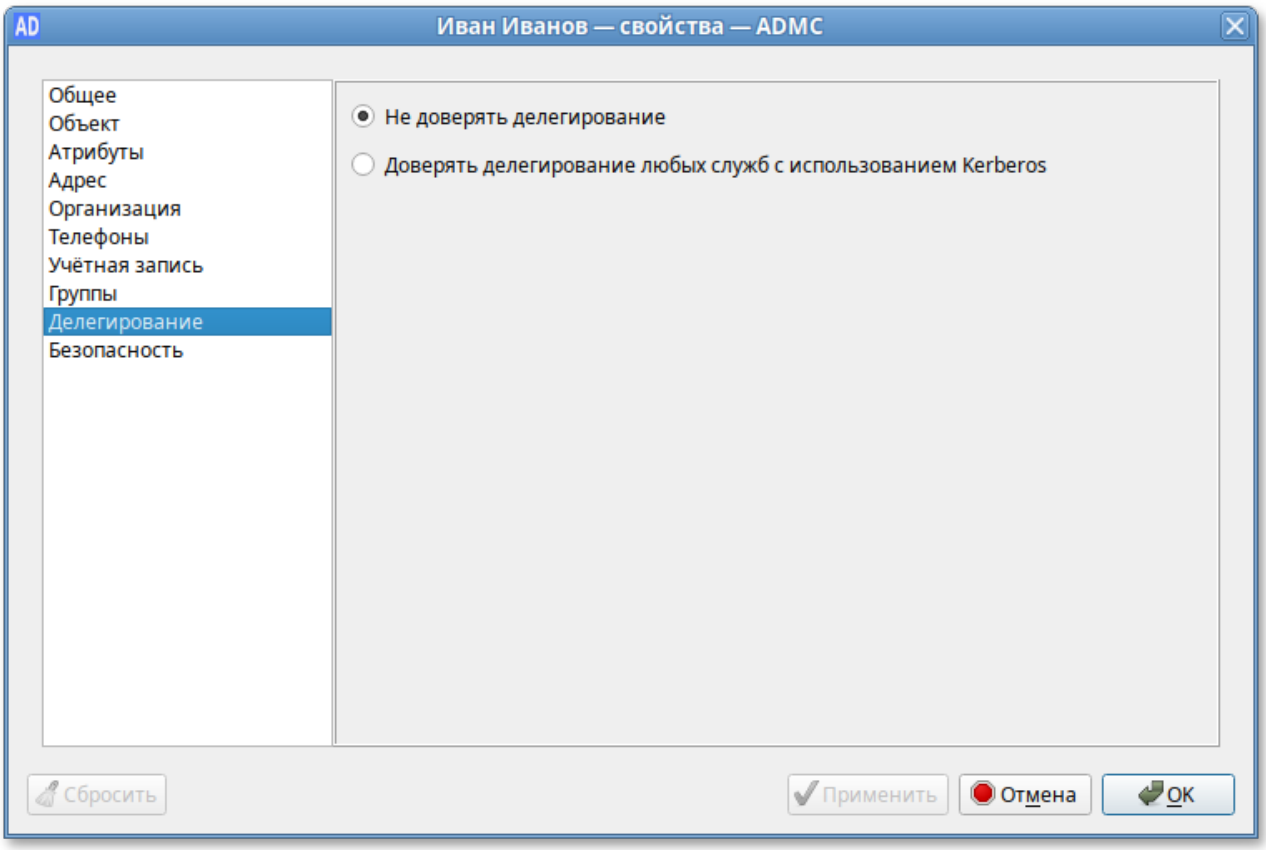
- обычный пользователь (NORMAL_ACCOUNT): 0x200 (512);
- контроллер домена (SERVER_TRUST_ACCOUNT): 0x2000 (8192);
- рабочая станция или сервер (WORKSTATION_TRUST_ACCOUNT): 0x1000 (4096).

На вкладке **Группы** формируется список групп, членом которых является текущий пользователь. Здесь также можно назначить основную группу (Primary Group). Для управления членством пользователя в группах безопасности AD используются две кнопки, находящиеся под списком групп, членами которой является пользователь: **Добавить** и **Удалить**. По умолчанию пользователь входит в группу Domain Users.



На вкладке **Делегирование** доступно два параметра:

- **Не доверять делегирование** — запрещение делегирования услуг;
- **Доверять делегирование любых служб с использованием Kerberos** — задает возможность делегирования услуг только с помощью протокола Kerberos.

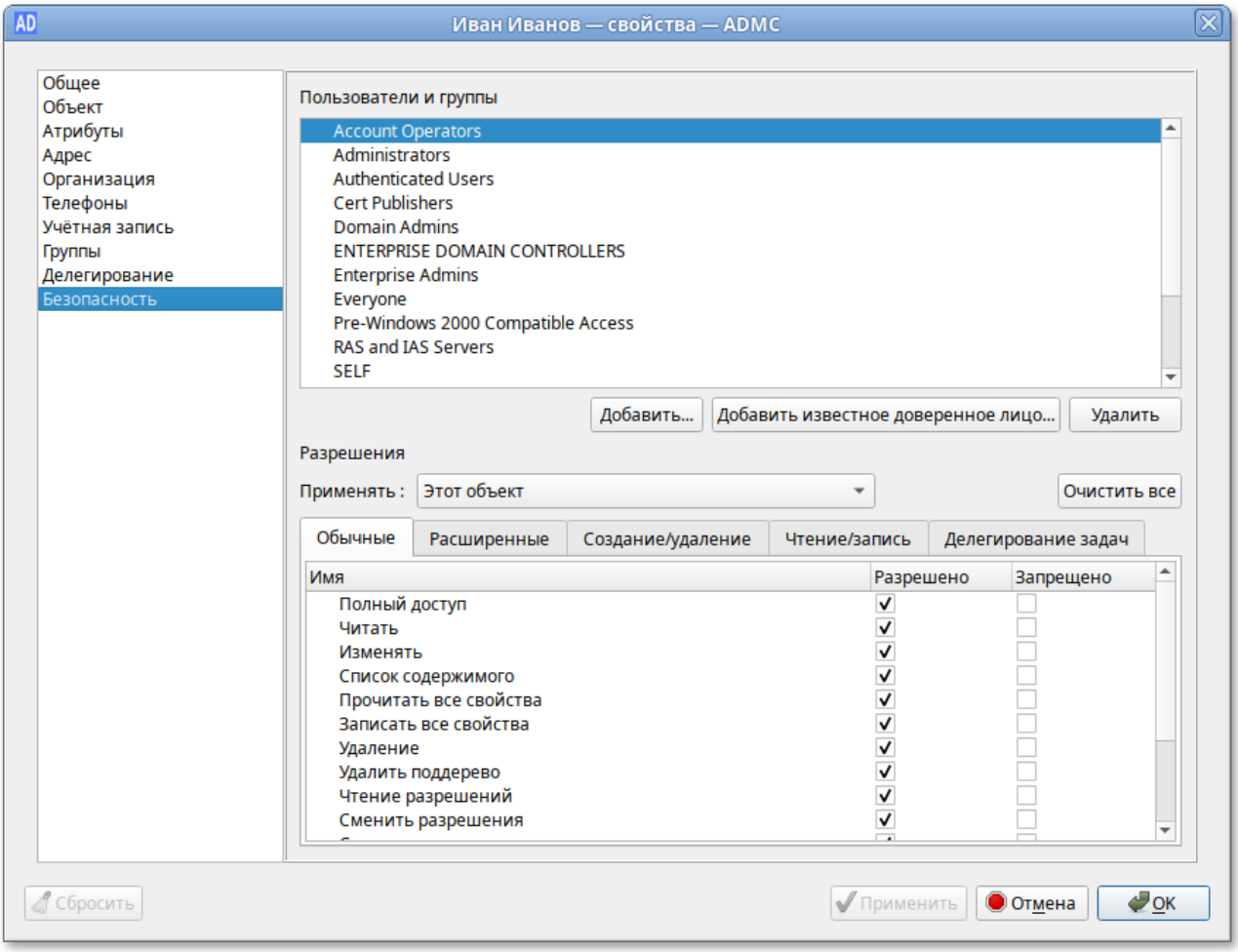


Примечание

Протокол проверки подлинности Kerberos — это основной протокол безопасности для проверки подлинности в домене. Он проверяет подлинность пользователя и системы.

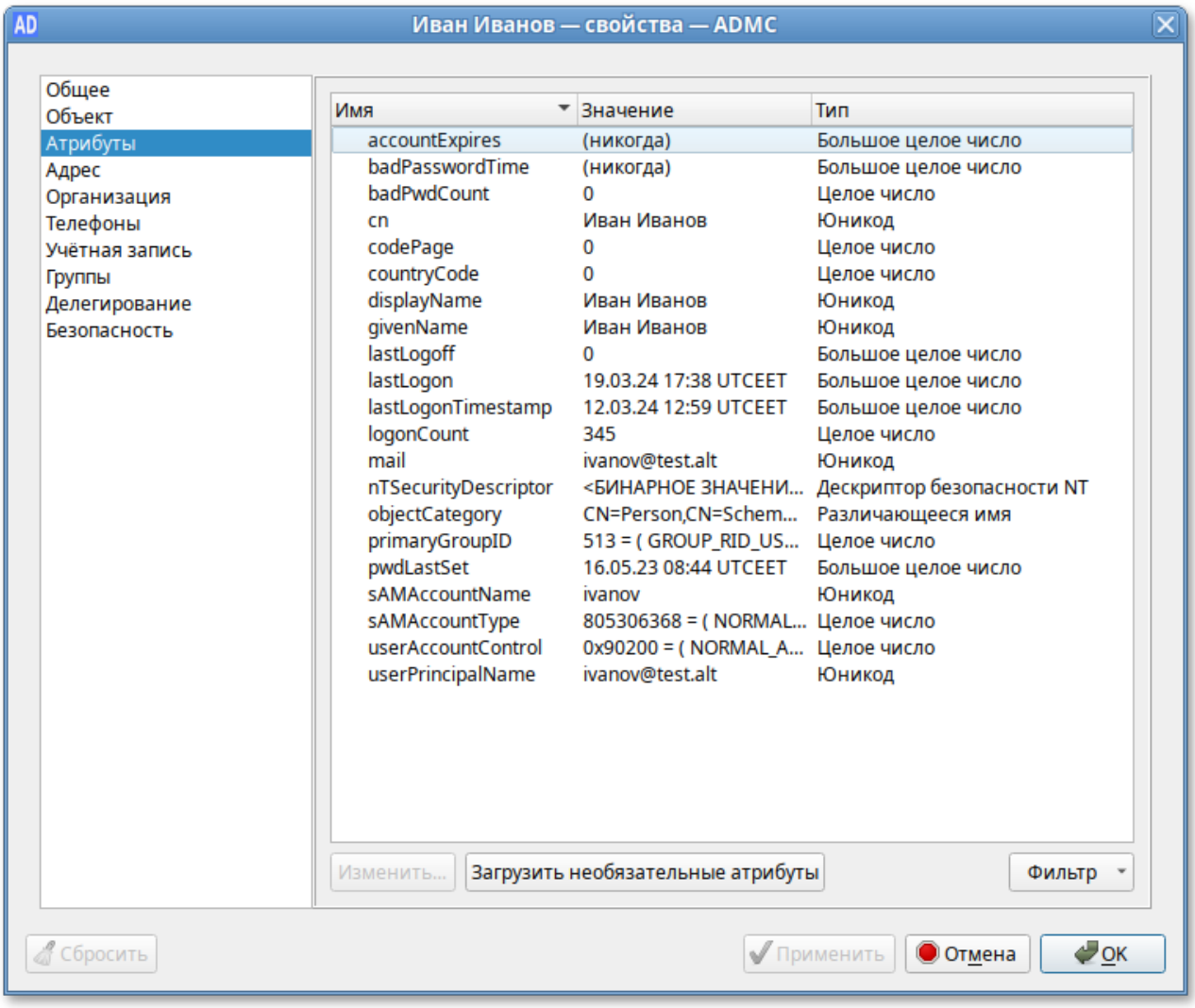
Каждому объекту в сети назначается набор данных об управлении доступом. Этот набор данных определяет, какой тип доступа разрешается пользователям и группам.

Управление разрешениями для выбранного объекта доступно на вкладке **Безопасность**:



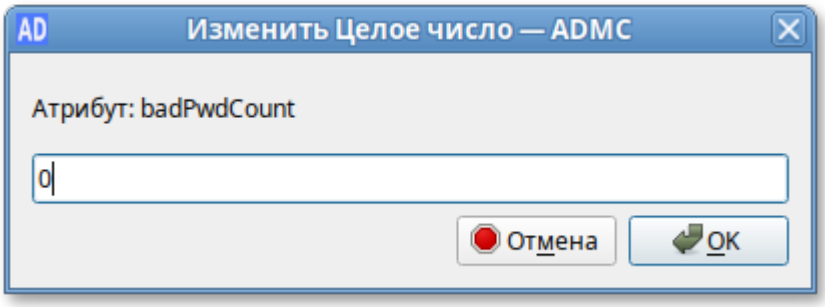
В разделе **Разрешения** отображается список действующих разрешений и запретов для каждой выбранной группы. Чтобы установить разрешения для группы, которая отсутствует в списке можно воспользоваться кнопкой **Добавить…** или **Добавить известное доверенное лицо…**.

Для тонкого редактирования свойств объектов домена (пользователей, компьютеров, групп) можно воспользоваться вкладкой **Атрибуты**:

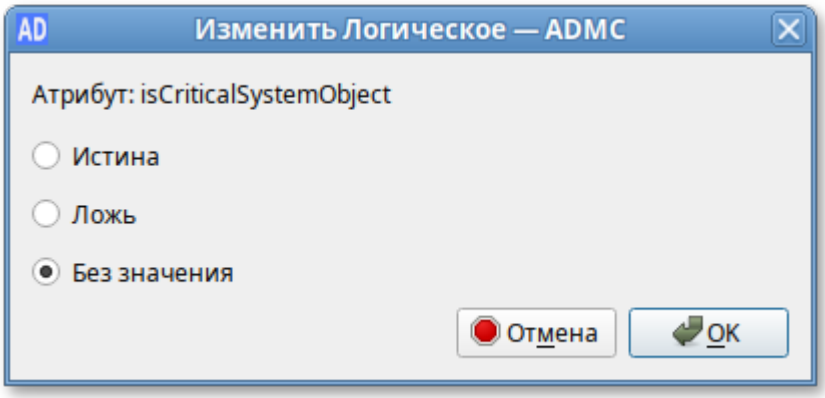


Эту вкладку можно использовать для просмотра и редактирования атрибутов, недоступных через другие вкладки окна **Свойства объекта** (например, для просмотра значений неизменяемых атрибутов).

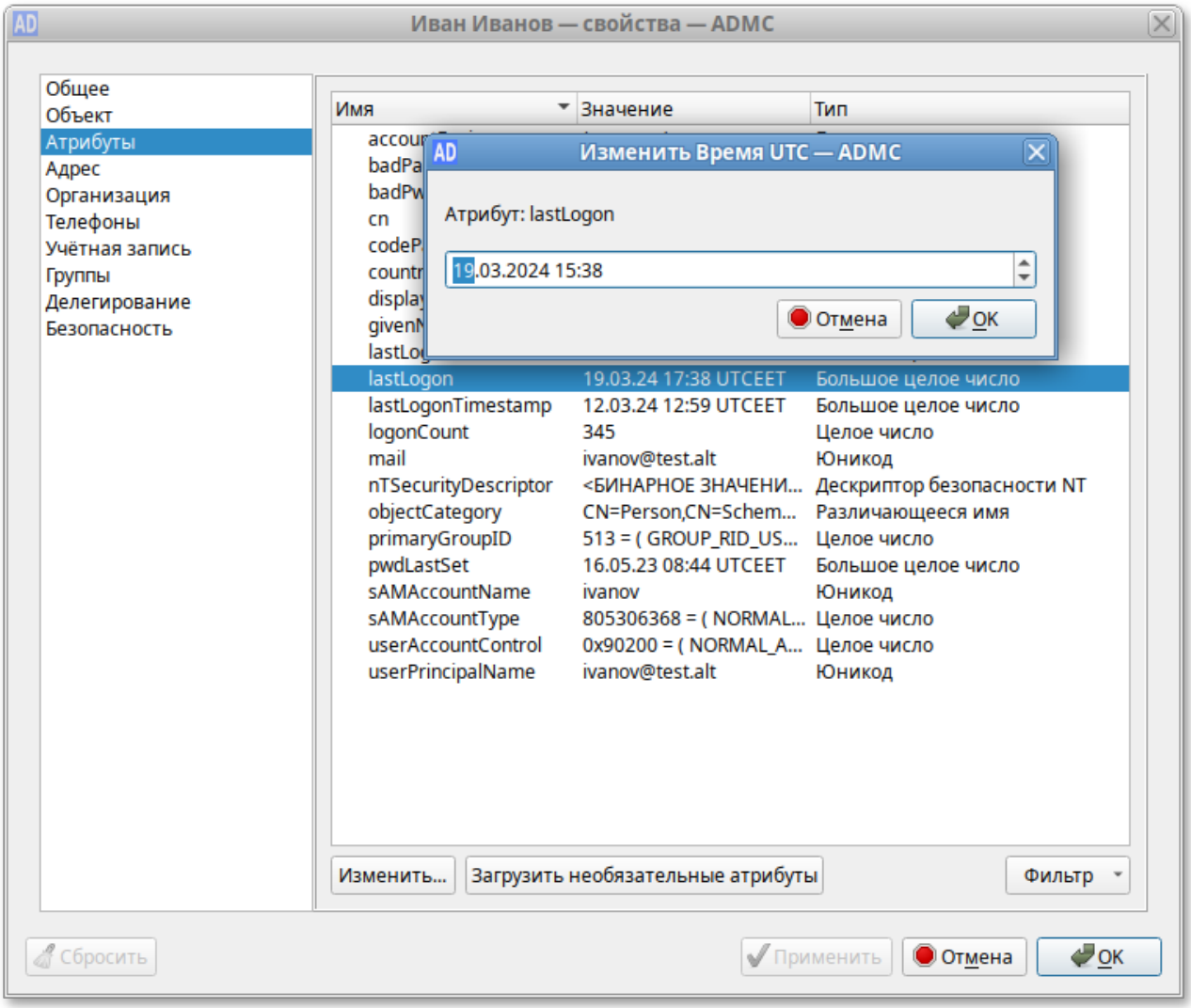
Содержимое окна редактирования атрибута зависит от типа атрибута. Окно редактирования атрибута целого типа:



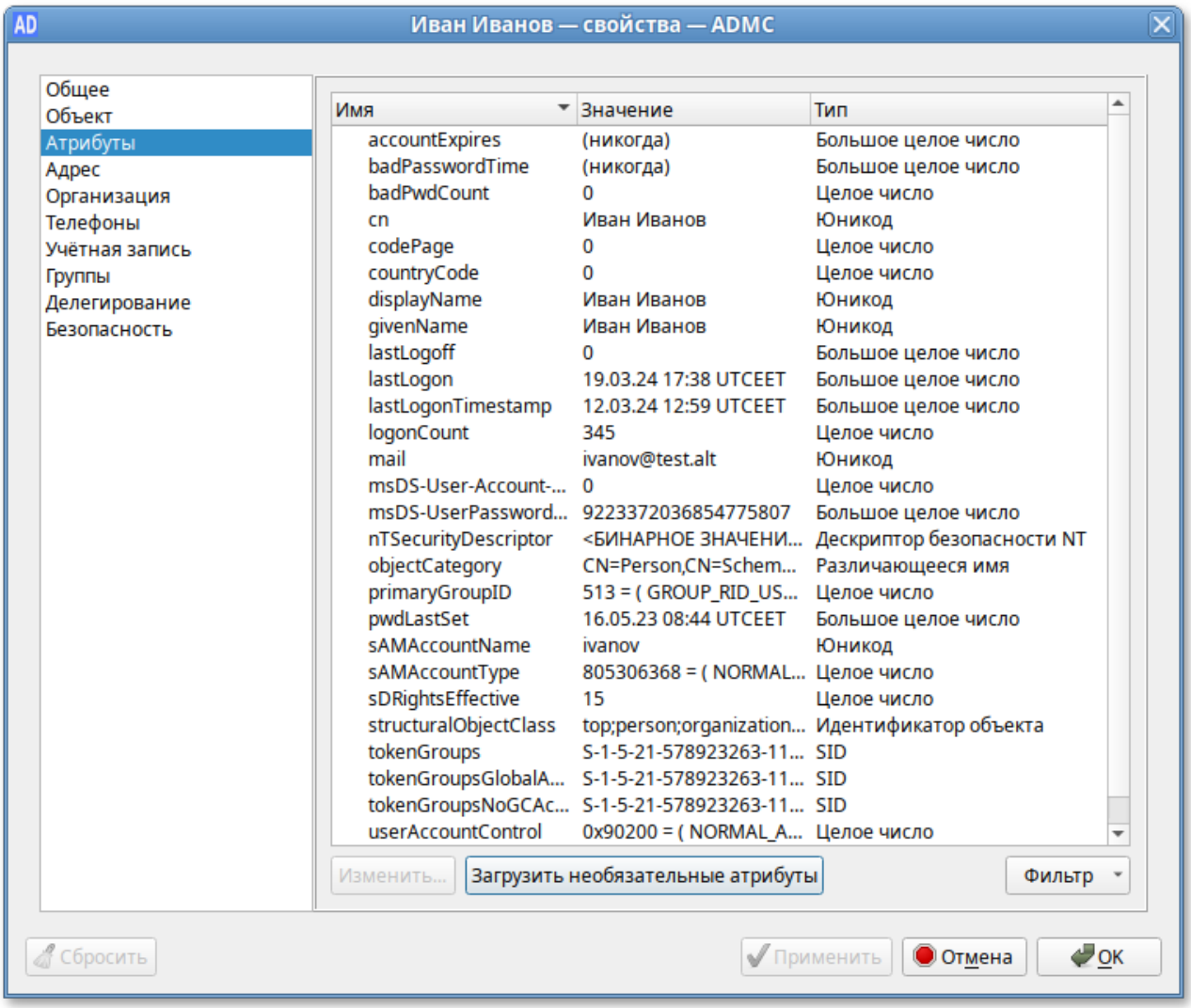
Окно редактирования атрибута логического типа:



Для большинства атрибутов AD имеется встроенная функция декодирования значений. Например, значение атрибута lastLogon или lastLogonTimestamp (информация о времени последнего входа пользователя в домен) во вкладке **Атрибуты** и в окне редактирования атрибута отображается в формате «Дата Время», хотя время хранится в виде большого целого числа, представляющего число 100-наносекундных интервалов с 1 января 1601 (UTC):

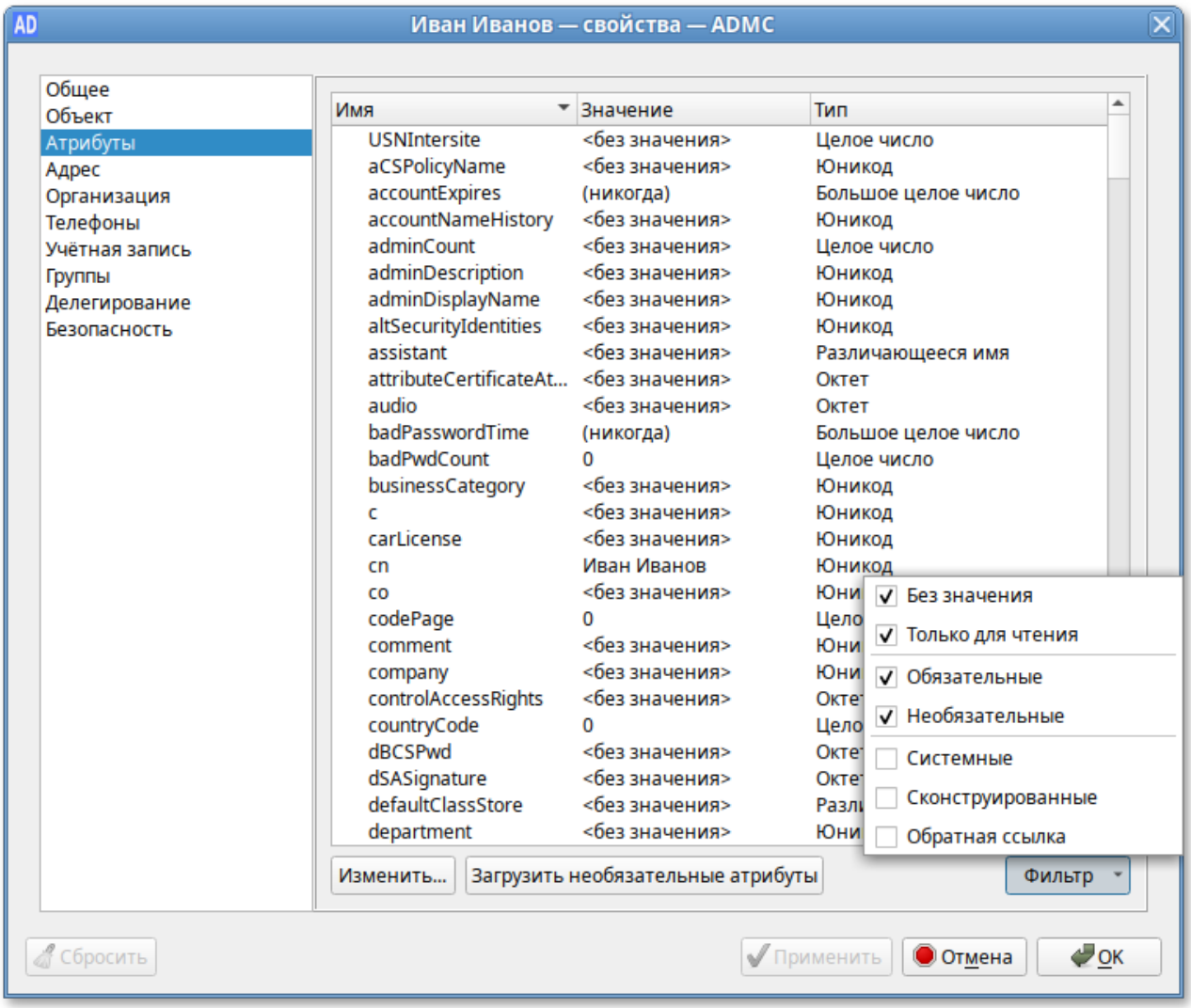


Кнопка **Загрузить необязательные атрибуты** позволяет загрузить значения необязательных атрибутов:



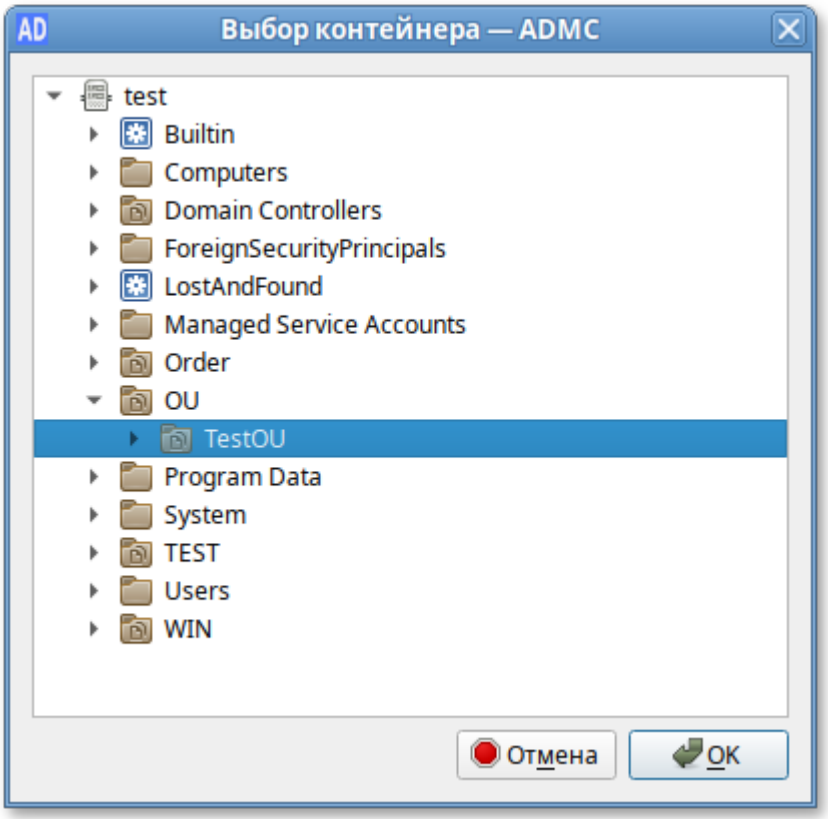
Кнопка **Фильтр** позволяет управлять отображением списка атрибутов:

- **Без значения** — показывать пустые атрибуты;
- **Только для чтения** — показывать все атрибуты, в том числе те, на правку которых нет полномочий. Если снять отметку с этого пункта, будут показаны только те атрибуты, на правку которых делегированы полномочия (например, если у пользователя нет полномочий на изменение атрибутов данного объекта, список атрибутов будет пуст);
- **Обязательные** — показывать обязательные атрибуты;
- **Необязательные** — показывать необязательные (дополнительные) атрибуты;
- **Системные** — показывать системные атрибуты, которые может изменять только сервер AD (например, objectClass);
- **Сконструированные** — показывать атрибуты, которые не хранятся в каталоге, но вычисляются контроллером домена (например, canonicalName);
- **Обратные ссылки** — показывать связанные атрибуты (например, memberOf).



28.4. Выбор контейнера

При перемещении объекта в новый контейнер (пункт **Переместить…** в контекстном меню объекта) открывается окно, в котором можно выбрать контейнер, в который следует переместить объект.



28.5. Управление пользователями

Учетная запись пользователя домена:

- удостоверяет личность пользователя;
- разрешает или запрещает доступ к ресурсам домена.

В ADMC предусмотрена возможность создания новых учётных записей пользователей в доменных службах Альт Домен и управления существующими учётными записями пользователей.

Примечание

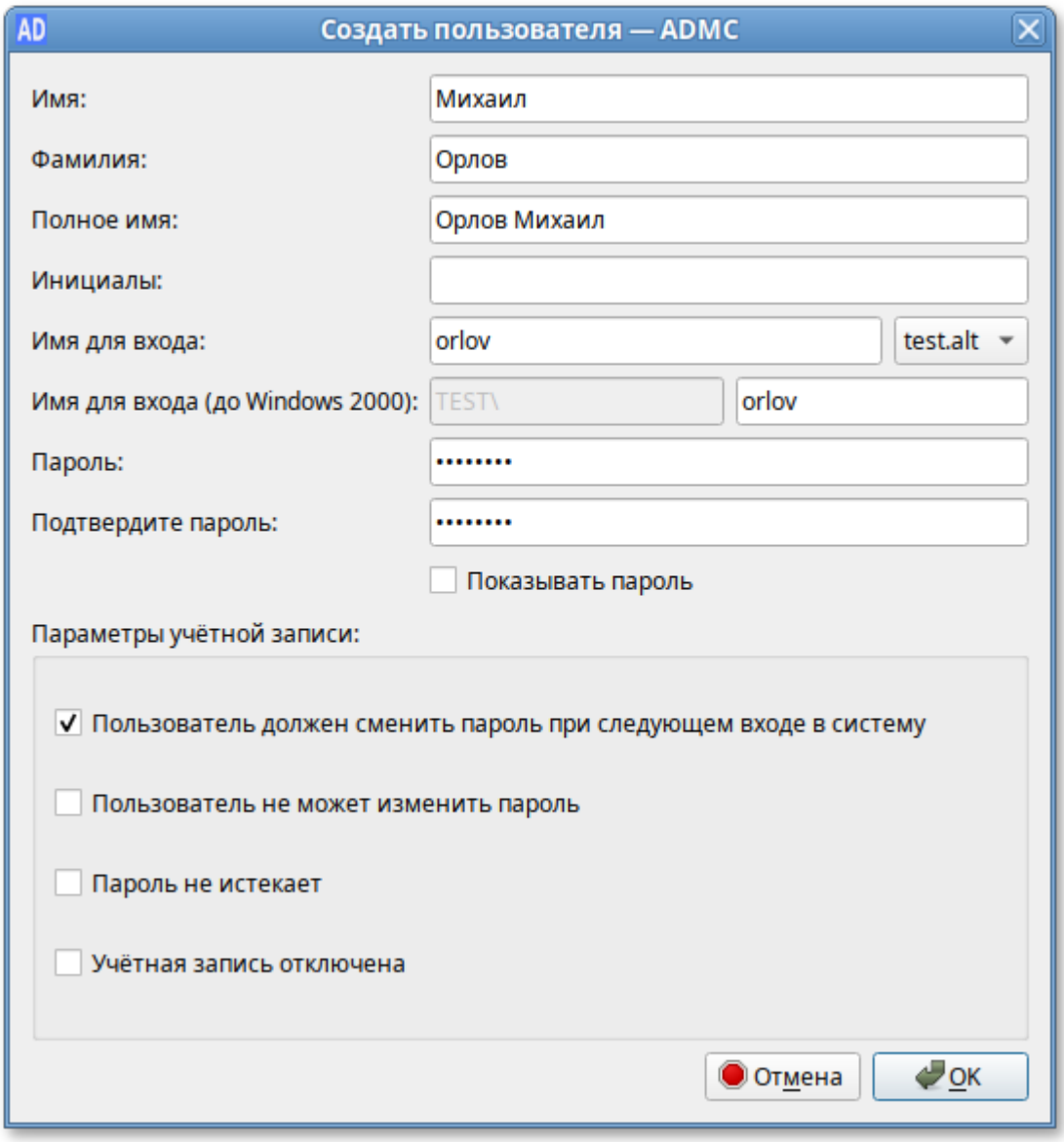
Для доступа к некоторым операциям необходимо быть членом одной из этих групп: Account Operators, Domain Admins, Enterprise Admins.

Примечание

Объект InetOrgPerson является производным от класса пользователь (user). Он может работать в качестве субъекта безопасности так же, как и объект класса пользователь. Для создания учётной записи InetOrgPerson в контекстном меню контейнера следует выбрать пункт **Создать** → **inetOrgPerson**.

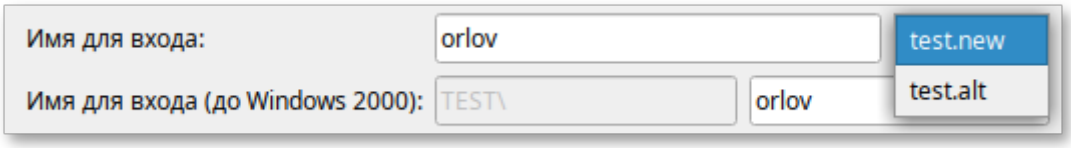
28.5.1. Создание учётной записи пользователя

Для создания учётной записи пользователя в контекстном меню контейнера следует выбрать пункт **Создать** → **Пользователь**. Окно мастера создания учётной записи пользователя:



При создании учётной записи пользователя можно указать следующие параметры (атрибуты):

- **Имя** — имя пользователя;
- **Фамилия** — фамилия пользователя;
- **Полное имя** — полное имя пользователя (в это поле можно добавить отчество или поменять имя и фамилию местами);
- **Инициалы** — инициалы пользователя;
- **Имя для входа** — имя пользователя для входа (логин пользователя). В раскрывающемся списке перечисляются доступные суффиксы основного имени пользователя (UPN), которые можно использовать для создания имени пользователя для входа. Список содержит полное имя системы доменных имен (DNS) текущего домена и все альтернативные суффиксы UPN:



- **Имя для входа (до Windows 2000)** — имя пользователя для входа в старые системы (пред-Windows 2000);
- **Пароль**/**Подтвердите пароль** — пароль пользователя;
- **Пользователь должен сменить пароль при следующем входе в систему** — пользователь должен изменить пароль при следующем входе в систему. Если эта опция включена, только пользователь будет знать свой пароль;
- **Пользователь не может изменить пароль** — предотвращает изменение пароля пользователем;
- **Пароль не истекает** — установить бессрочный пароль. Если эта опция включена, срок действия учётной записи пользователя не ограничен (по умолчанию срок действия пароля задан атрибутом minPwdAge);
- **Учетная запись отключена** — отключить учётную запись пользователя. Если эта опция включена, пользователь не сможет войти в систему.

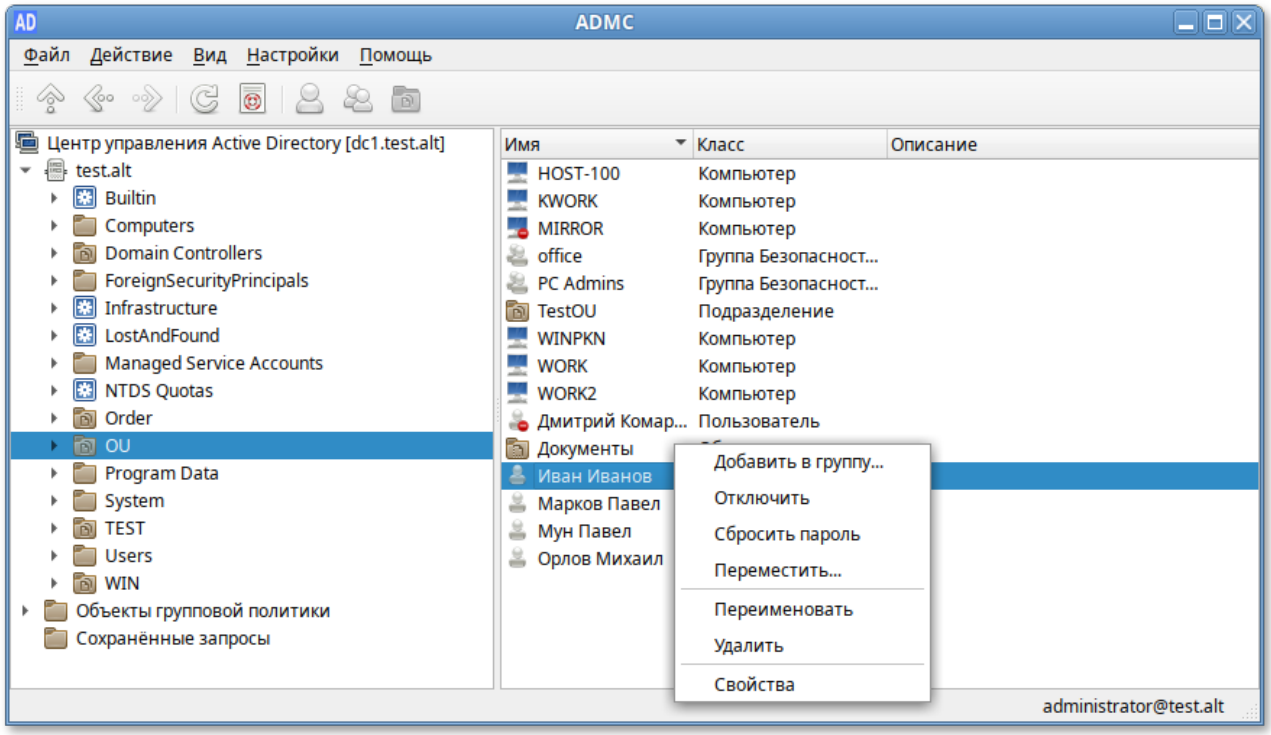
Примечание

Для совместимости с доменами пред-Windows 2000 (Windows NT) в AD задается два имени пользователя, значения которых имеют разный формат. Первое имя, используемое в доменах Window 2k, — UPN-имя, которому в AD соответствует поле userPrincipalName, имеющее формат user@domain, где domain — DNS-имя домена, например, TEST.ALT; user — имя пользователя в сети. Для удобства назначения имен UPN-имя разделено на две части (префикс UPN и суффикс UPN). Второе задаваемое имя пользователя — SAM-имя, которое используется для совместимости в доменах Windows NT. Структура SAM-имени следующая: domain\user, где domain — сокращенное имя домена, например, TEST; user — имя пользователя. В AD хранится только имя пользователя в поле samAccountName. Первая часть SAM-имени однозначно вычисляется из DNS-имени домена.

По умолчанию суффиксом основного имени (UPN) для учётной записи пользователя является DNS имя домена AD, которое содержит учётную запись пользователя. Для упрощения процессов администрирования и входа пользователя в систему можно добавить альтернативные суффиксы UPN.

28.5.2. Изменение учётной записи пользователя

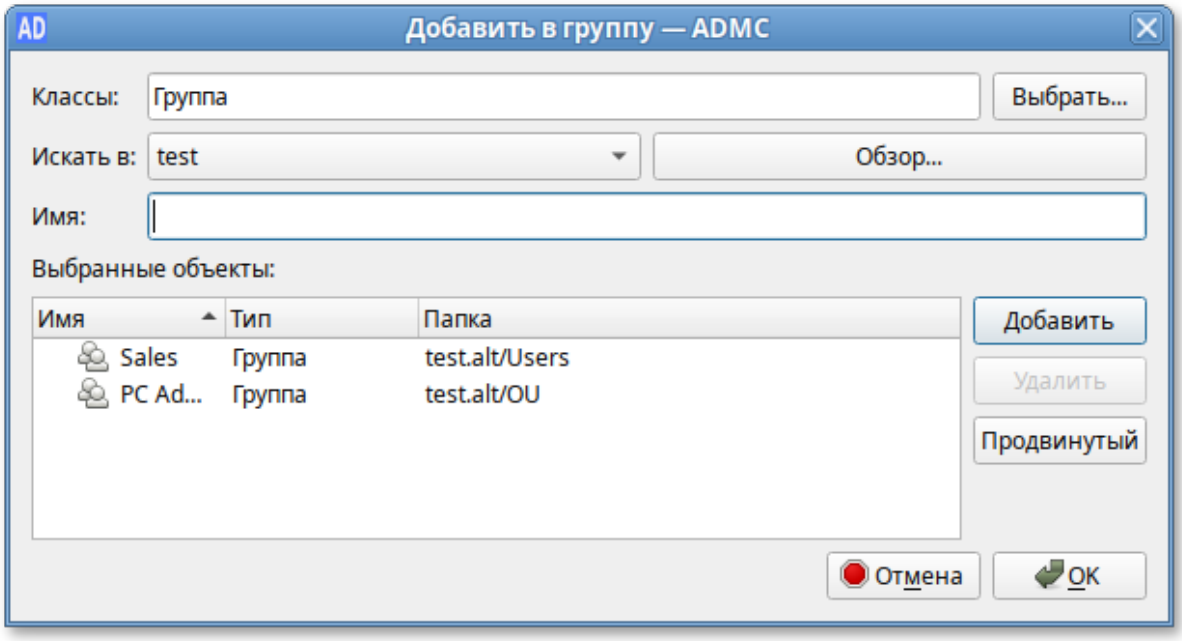
Для изменения учётной записи пользователя следует в контекстном меню пользователя выбрать соответствующее действие:



Для добавления пользователя в группу:

1. В контекстном меню пользователя выбрать пункт **Добавить в группу…**.

2. В открывшемся окне выбрать группы, в которые следует добавить учётную запись пользователя в качестве участника:

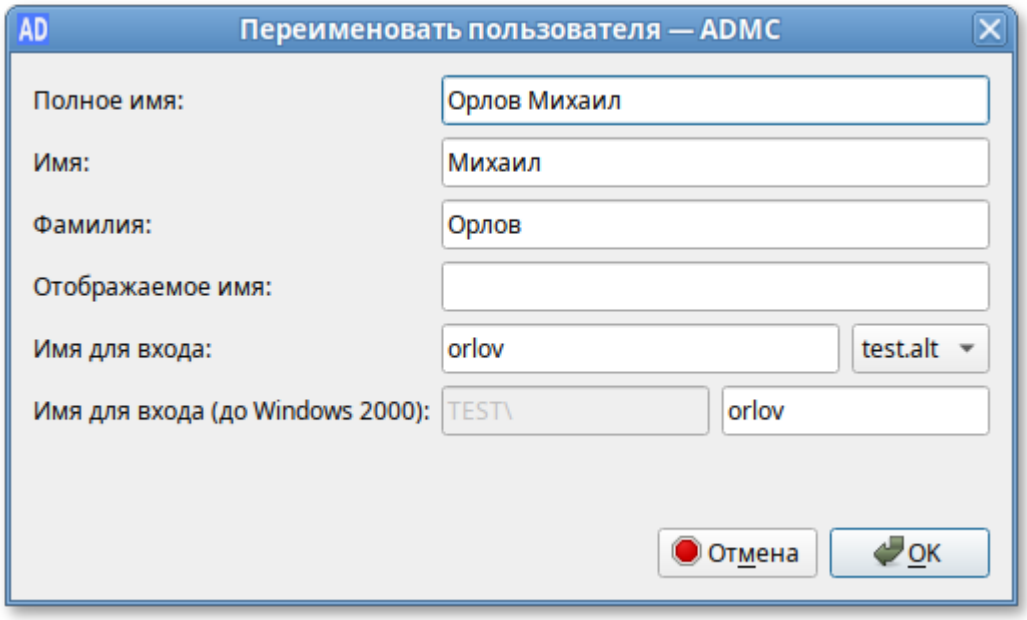


3. Нажать кнопку **OK**.

Для переименования пользователя:

1. В контекстном меню пользователя выбрать пункт **Переименовать**.

2. В открывшемся окне, если необходимо, изменить соответствующие поля:

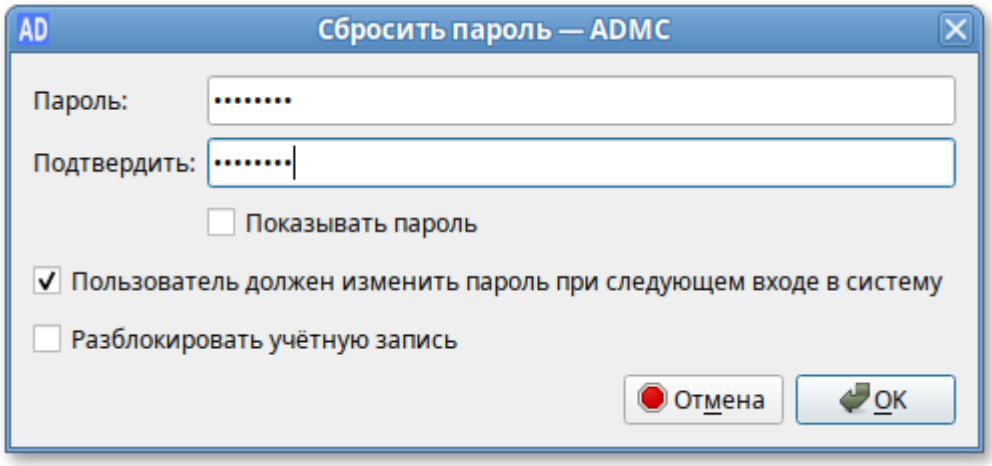


3. Нажать кнопку **OK** для сохранения изменений.

Для изменения пароля пользователя:

1. В контекстном меню пользователя выбрать пункт **Сбросить пароль**.

2. В открывшемся окне ввести новый пароль и подтвердить его:



3. Если необходимо, чтобы пользователь изменил этот пароль при следующем входе в систему, установить отметку **Пользователь должен изменить пароль при следующем входе в систему**.

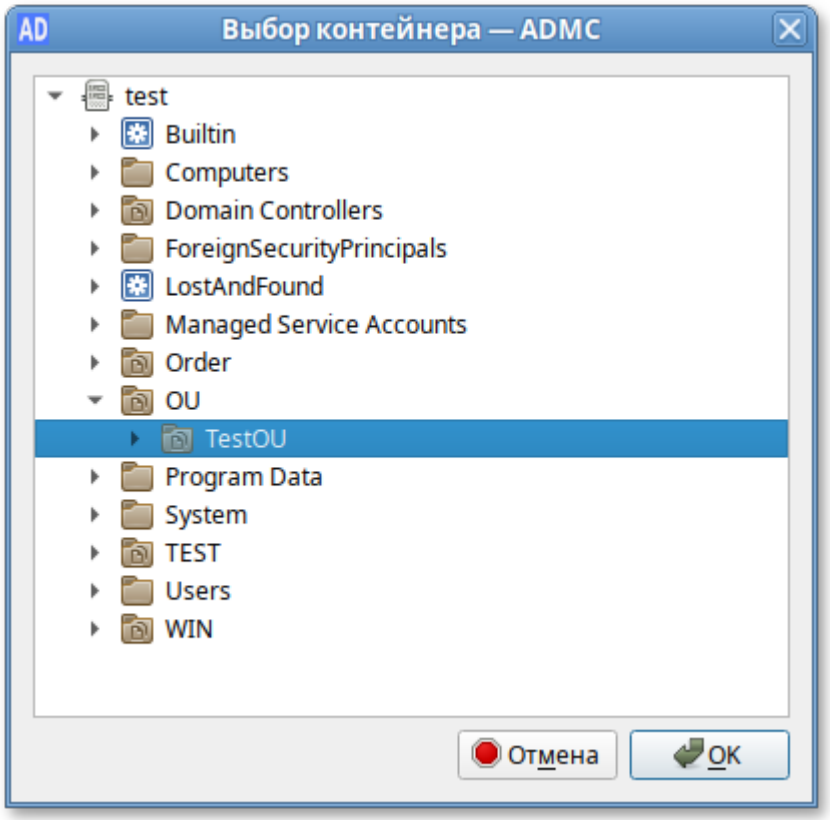
4. Установить отметку **Разблокировать учётную запись**, если необходимо разблокировать учётную запись пользователя.

5. Нажать кнопку **OK** для сохранения изменений.

Для перемещения пользователя в другой контейнер:

1. В контекстном меню пользователя выбрать пункт **Переместить…**.

2. В открывшемся окне выбрать контейнер, в который следует переместить учётную запись пользователя:

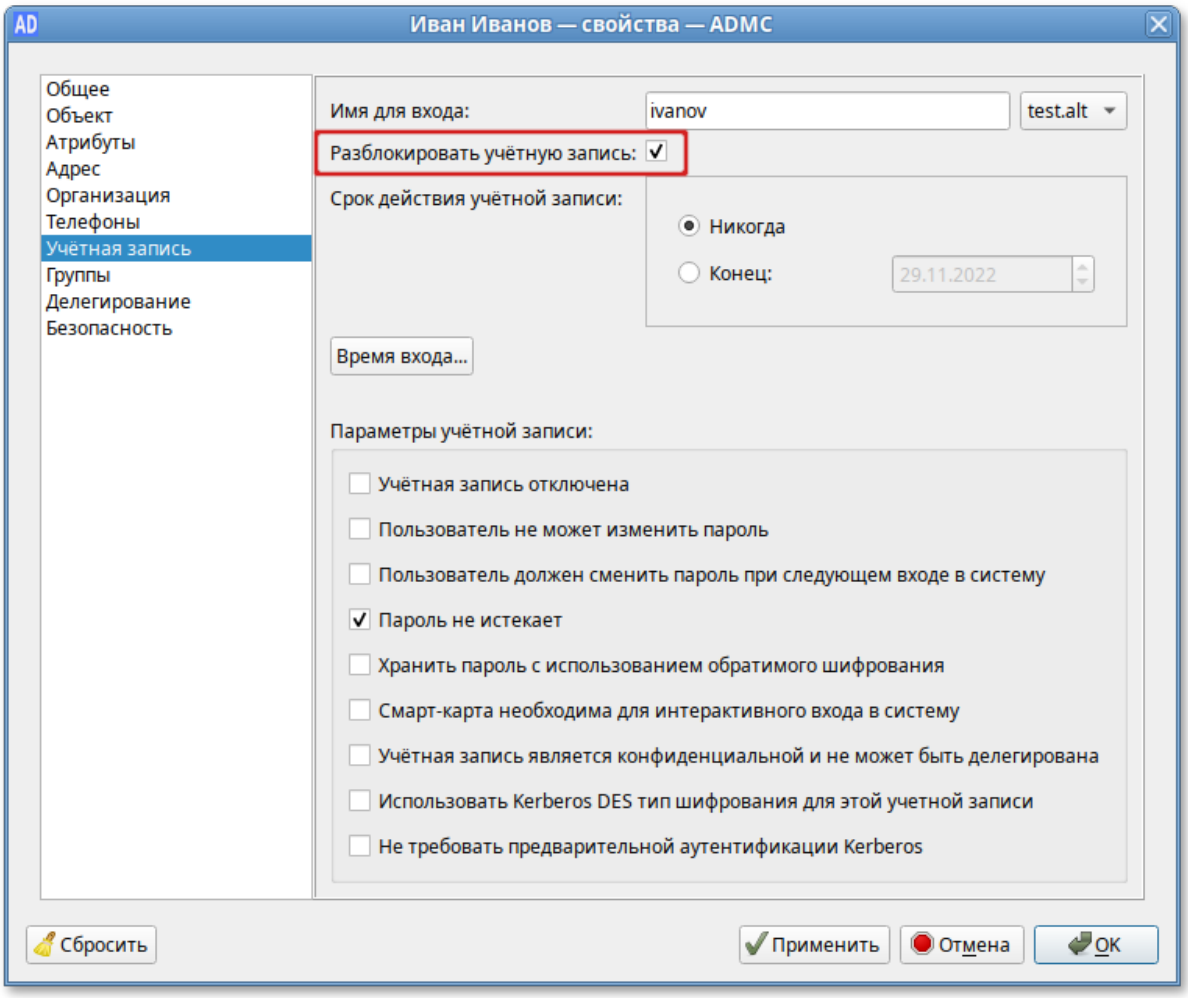


3. Нажать кнопку **OK**.

Для включения/отключения учётной записи пользователя необходимо в контекстном меню пользователя выбрать пункт **Отключить** или **Включить** (в зависимости от состояния учётной записи будет доступно одно из этих действий).

Чтобы разблокировать учётную запись пользователя:

1. В контекстном меню пользователя выбрать пункт **Свойства**.
2. В открывшемся окне на вкладке **Учетная запись** отметить пункт **Разблокировать учётную запись**:



3. Нажать кнопку **OK** или **Применить**.

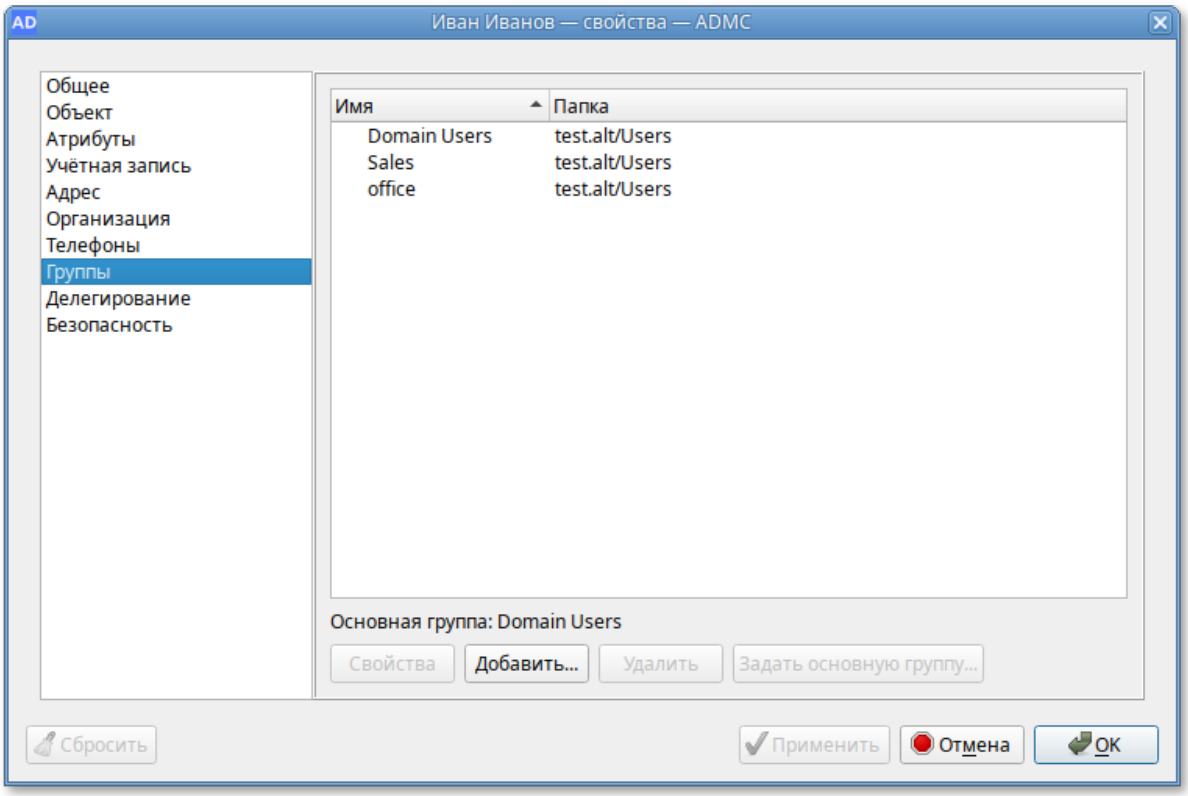
Для удаления учётной записи пользователя следует в контекстном меню пользователя выбрать пункт **Удалить**.

Предупреждение

Если в настройках ADMC не отмечен пункт **Подтверждать действия**, пользователь будет удален сразу после выбора пункта меню **Удалить**.

Для того чтобы найти группы, участником которых является пользователь:

1. В контекстном меню пользователя выбрать пункт **Свойства**.
2. В открывшемся окне на вкладке **Группы** будут отображаться группы, в которые входит данный пользователь:

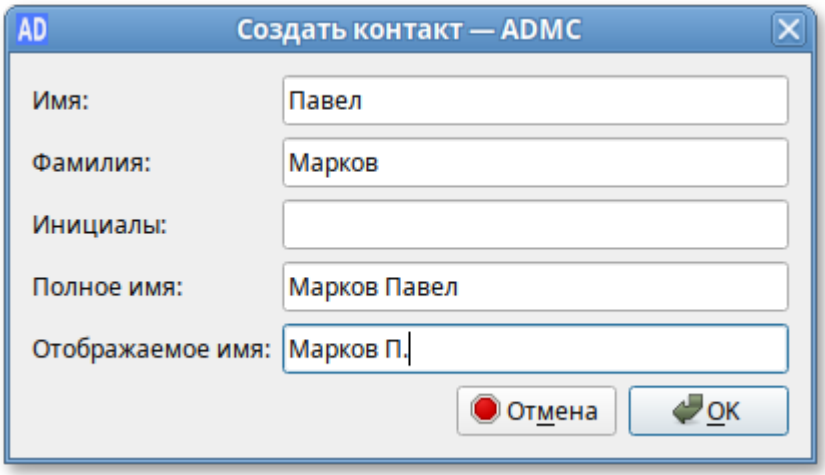


28.6. Управление контактами

Контакт предназначен для хранения информации о пользователях, которым не требуется регистрация в домене.

28.6.1. Создание контакта

Для создания контакта в контекстном меню контейнера следует выбрать пункт **Создать** → **Контакт**. Окно мастера создания контакта:



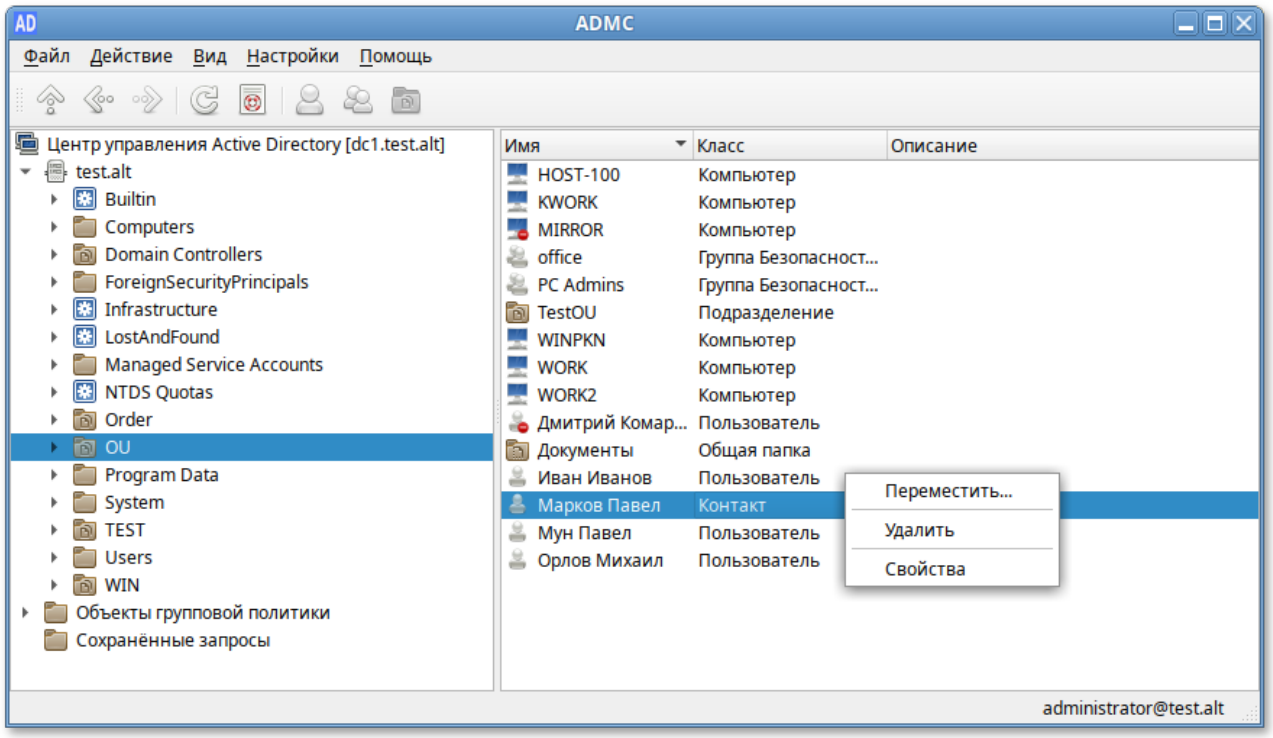
При создании контакта можно указать следующие параметры (атрибуты):

- **Имя** — имя пользователя;
- **Фамилия** — фамилия пользователя;

- **Инициалы** — инициалы пользователя;
- **Полное имя** — полное имя пользователя (в это поле можно добавить отчество или поменять имя и фамилию местами);
- **Отображаемое имя** — имя, отображаемое в адресной книге для определенной учётной записи.

28.6.2. Изменение свойств контакта

Для изменения учётной записи пользователя следует в контекстном меню контакта выбрать соответствующее действие:



Вкладки **Общие**, **Адрес**, **Телефоны** и **Организация** в окне **Свойства** контакта идентичны соответствующим вкладкам окна **Свойства** учётной записи пользователя.

На вкладке **Группы** можно, по аналогии с учётными записями пользователей, указать, членом каких групп является контакт. Возможность членства в группах не даёт контакту никаких прав в рамках домена и предназначена для организации групп рассылки. Для контакта нельзя указать основную группу, так как это не требуется для функционирования групп рассылки.

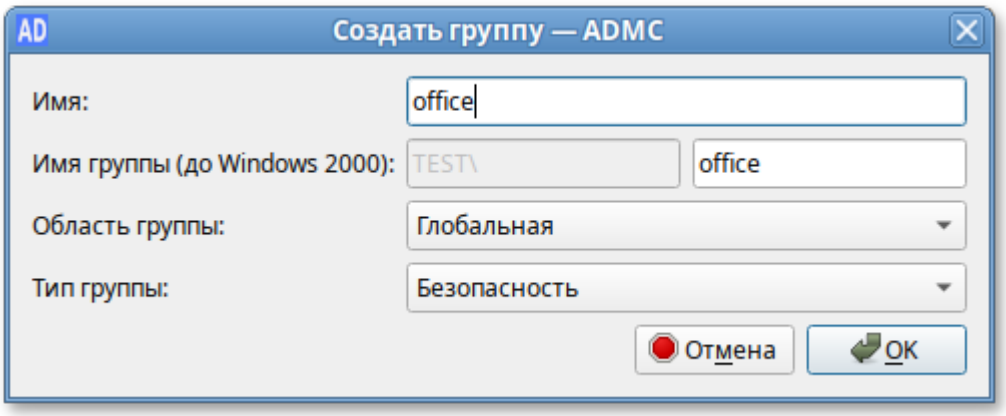
28.7. Управление группами

Группа состоит из учётных записей пользователей и компьютеров, контактов и других групп и может управляться как единое целое. Пользователи и компьютеры, входящие в определённую группу, являются членами группы.

Группы характеризуются областью действия и типом. Область действия группы определяет пределы применения группы внутри домена или леса. Тип группы определяет возможность использования группы для назначения разрешений с ресурса общего доступа (для групп безопасности) или только для списков рассылки электронной почты (для групп рассылки).

28.7.1. Создание группы

Для создания группы следует в контекстном меню контейнера выбрать пункт **Создать** → **Группа**. Окно мастера создания группы:

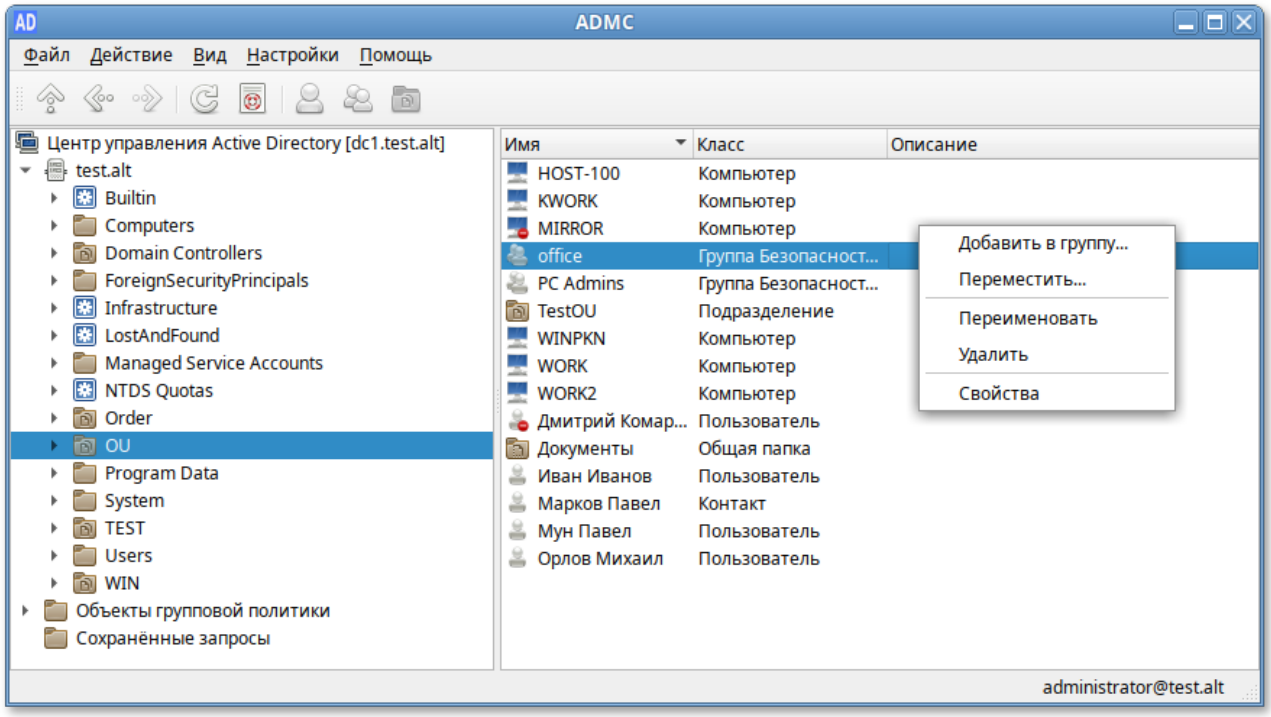


При создании группы можно указать следующие параметры (атрибуты):

- **Имя** — название группы;
- **Имя группы (до Windows 2000)** — название группы для старых систем (пред-Windows 2000);
- **Область группы** — область действия группы:
  - **Глобальная** — членами глобальной группы могут быть другие группы и учётные записи только из того домена, в котором определена группа. Членам этой группы разрешения могут назначаться в любом домене леса;
  - **Домен локальная** — членам такой группы разрешения могут назначаться только внутри домена (доступ к ресурсам одного домена);
  - **Универсальная** — членами универсальных групп могут быть другие группы и учётные записи из любого домена дерева доменов или леса. Членам такой группы разрешения могут назначаться в любом домене дерева доменов или леса;
- **Тип группы** — тип группы:
  - **Безопасность** — используется для назначения разрешений доступа к общим ресурсам;
  - **Рассылка** — используется для создания списков рассылки электронной почты.

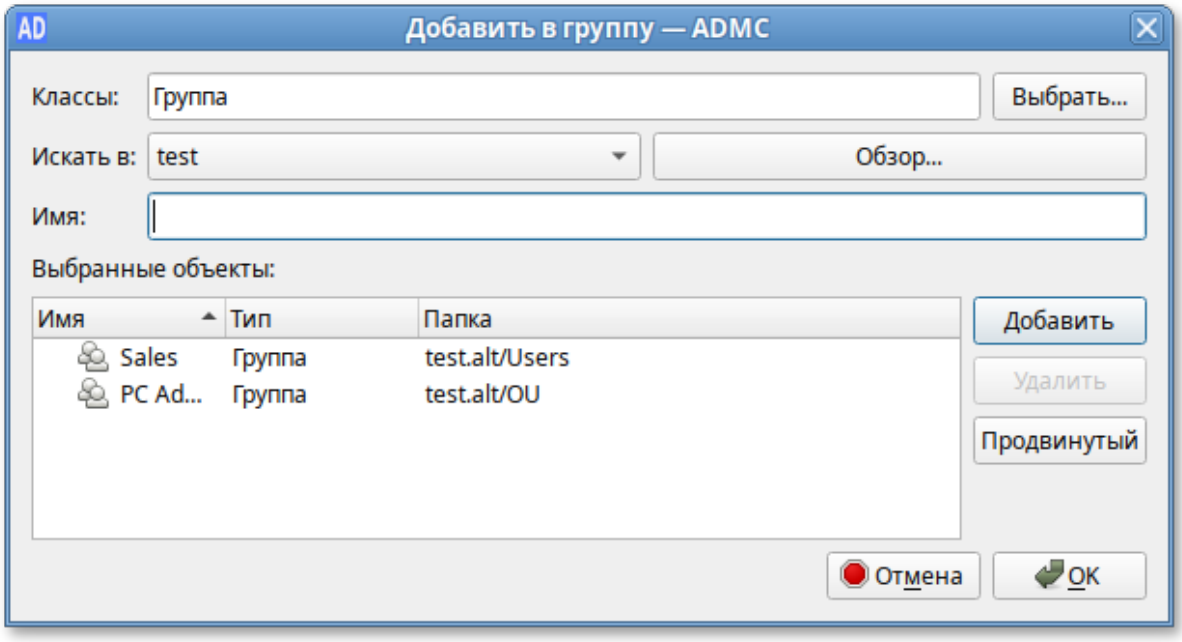
28.7.2. Изменение группы

Для изменения группы следует в контекстном меню группы выбрать соответствующее действие:



Для добавления группы в другую группу:

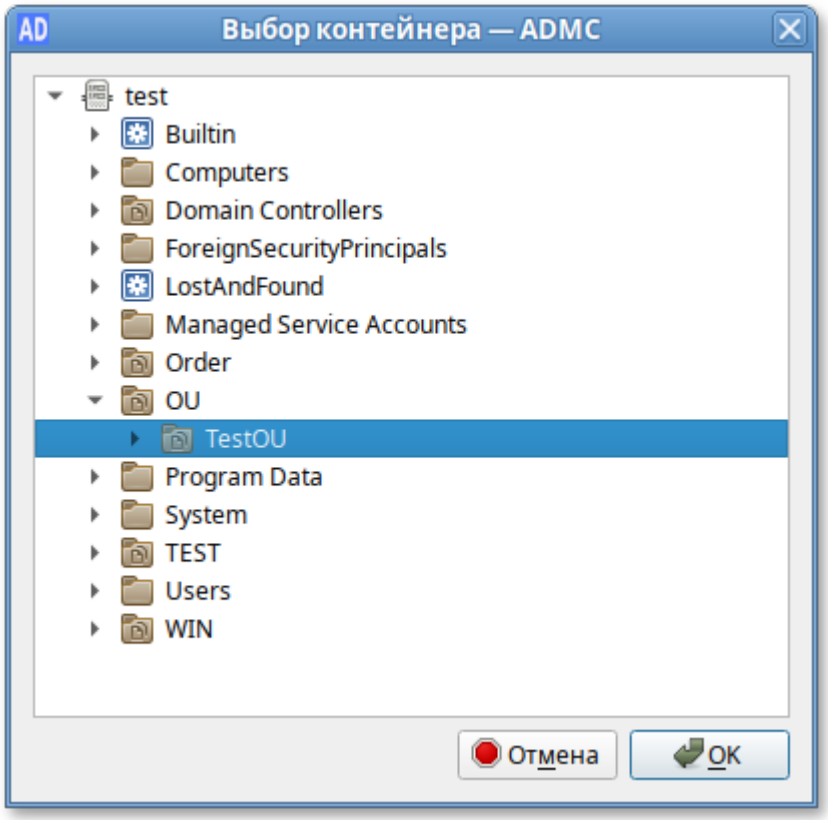
1. В контекстном меню группы выбрать пункт **Добавить в группу…**.
2. В открывшемся окне выбрать группы, в которые следует добавить данную группу в качестве участника:



3. Нажать кнопку **OK**.

Для перемещения группы в другой контейнер:

1. В контекстном меню группы выбрать пункт **Переместить…**.
2. В открывшемся окне выбрать контейнер, в который следует переместить группу:

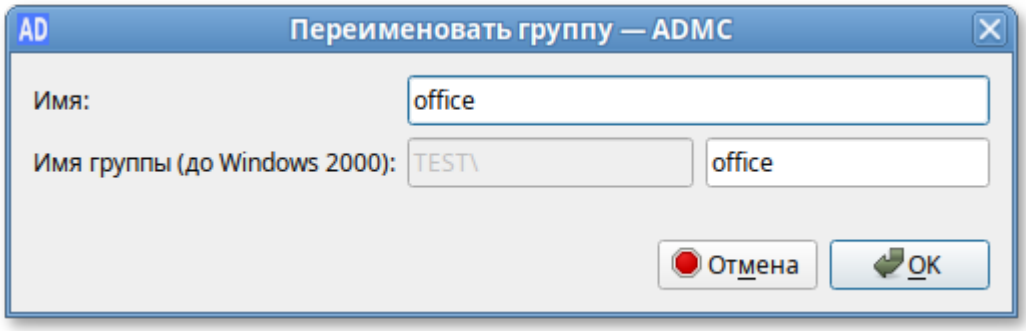


3. Нажать кнопку **OK**.

Для переименования группы:

1. В контекстном меню группы выбрать пункт **Переименовать**.

2. В открывшемся окне, если необходимо, изменить соответствующие поля:



3. Нажать кнопку **OK** для сохранения изменений.

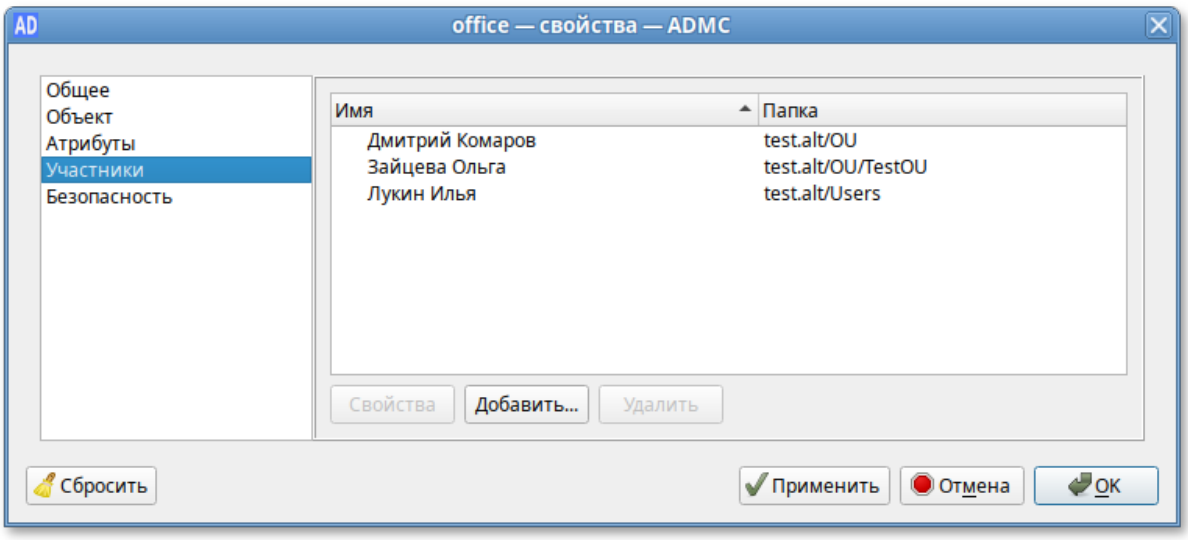
Для удаления группы следует в контекстном меню группы выбрать пункт **Удалить**.

Предупреждение

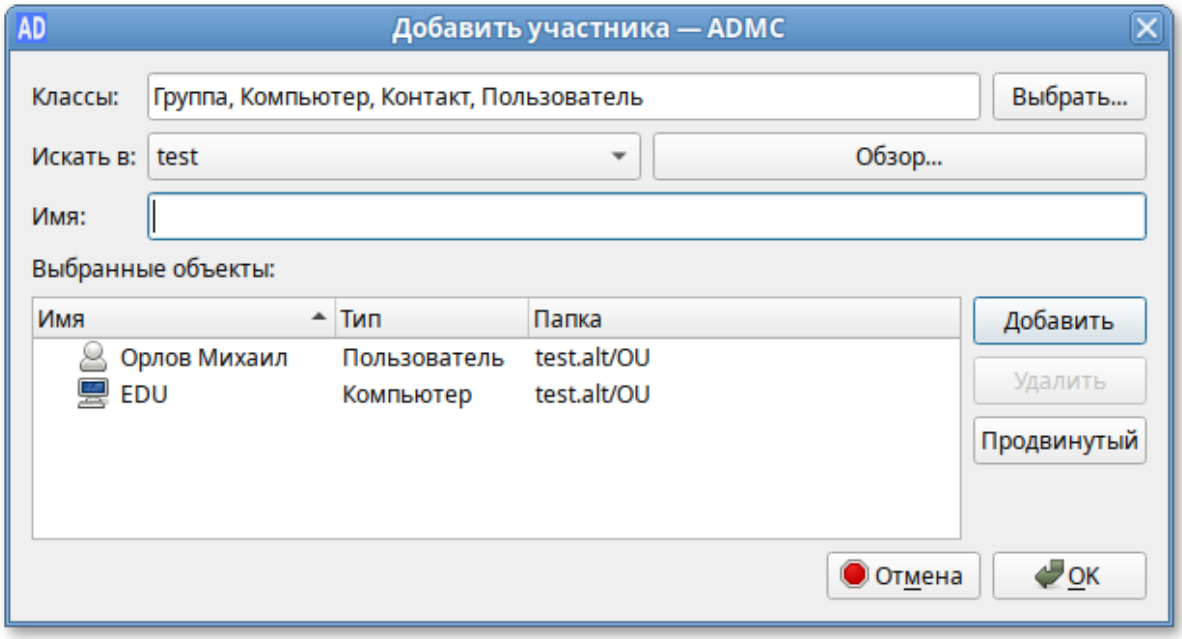
Если в настройках ADMC не отмечен пункт **Подтверждать действия**, группа будет удалена сразу после выбора пункта меню **Удалить**.

Для того чтобы добавить участников в группу:

1. В контекстном меню группы выбрать пункт **Свойства**.
2. В открывшемся диалоговом окне на вкладке **Участники** нажать кнопку **Добавить…**:



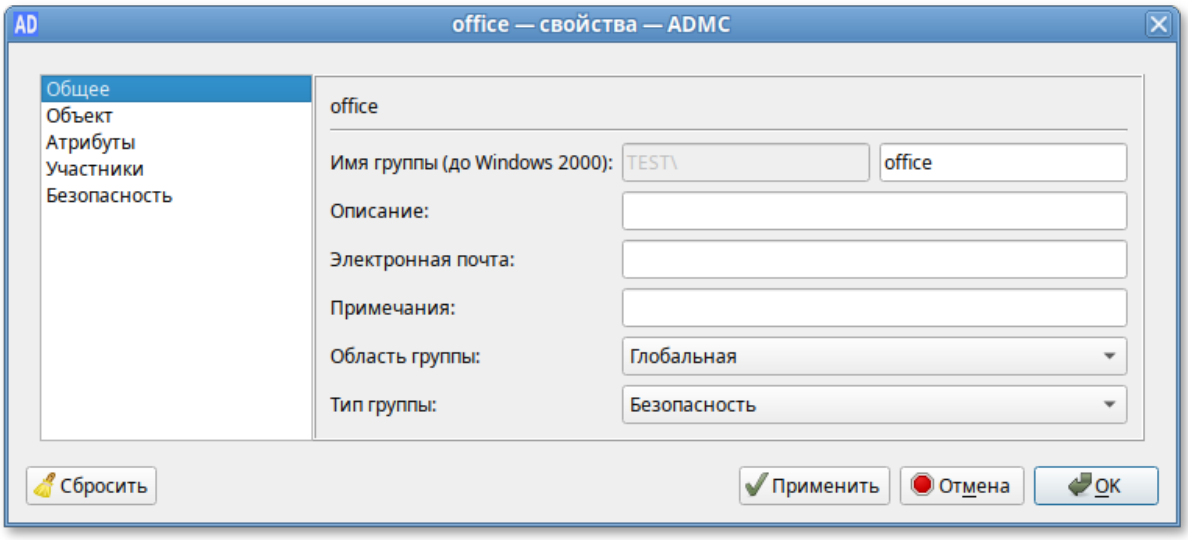
3. Выбрать объекты, которые необходимо добавить в группу:



4. Нажать кнопку **OK**.
5. Нажать кнопку **OK** или **Применить** для сохранения изменений.

Для изменения области действия/типа группы:

1. В контекстном меню группы выбрать пункт **Свойства**.
2. В открывшемся диалоговом окне на вкладке **Общее** в выпадающем списке **Тип группы** выбрать тип группы, в выпадающем списке **Область группы** выбрать область действия группы:



3. Нажать кнопку **OK** или **Применить** для сохранения изменений.

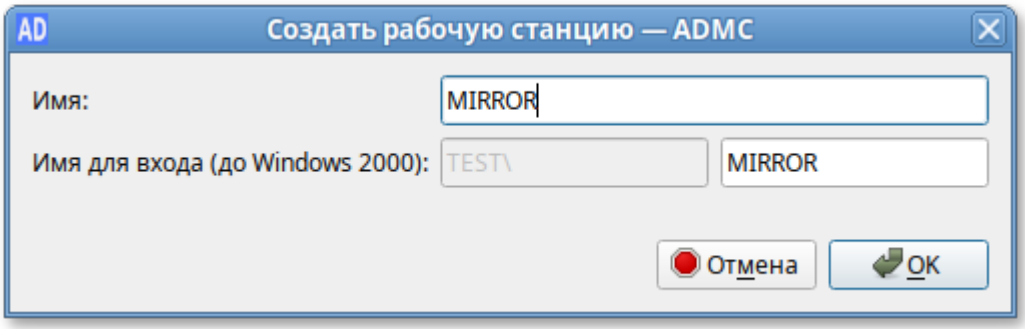
28.8. Управление компьютерами

Учетные записи компьютеров представляют собой устройства, подключенные к AD. Они хранятся в базе данных AD после того, как их подключат к домену.

28.8.1. Создание учётной записи компьютера

Учетная запись компьютера создается во время стандартной процедуры присоединения к домену.

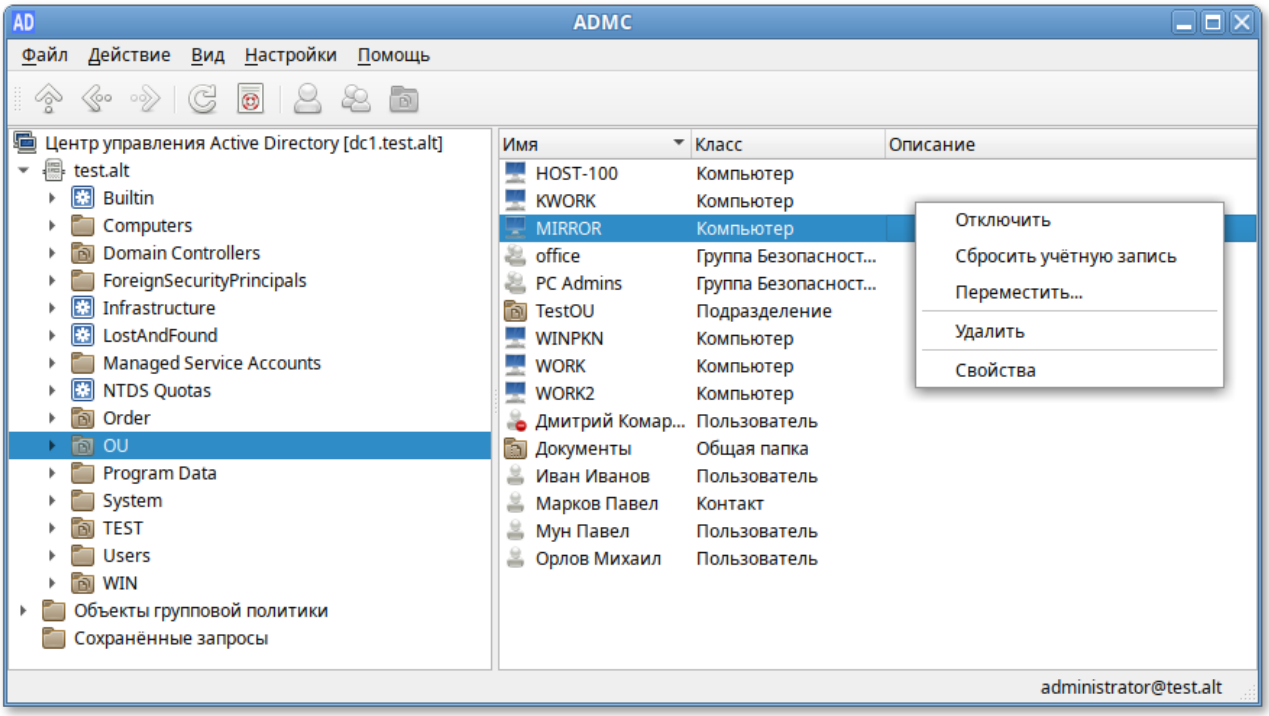
Для создания вручную учётной записи компьютера следует в контекстном меню контейнера выбрать пункт **Создать** → **Компьютер**. Окно мастера создания учётной записи компьютера:



При создании учётной записи компьютера необходимо указать название компьютера (поле **Имя**) и название компьютера для старых систем (поле **Имя для входа (до Windows 2000)**).

28.8.2. Изменение учётной записи компьютера

Для изменения учётной записи компьютера следует в контекстном меню компьютера выбрать соответствующее действие:



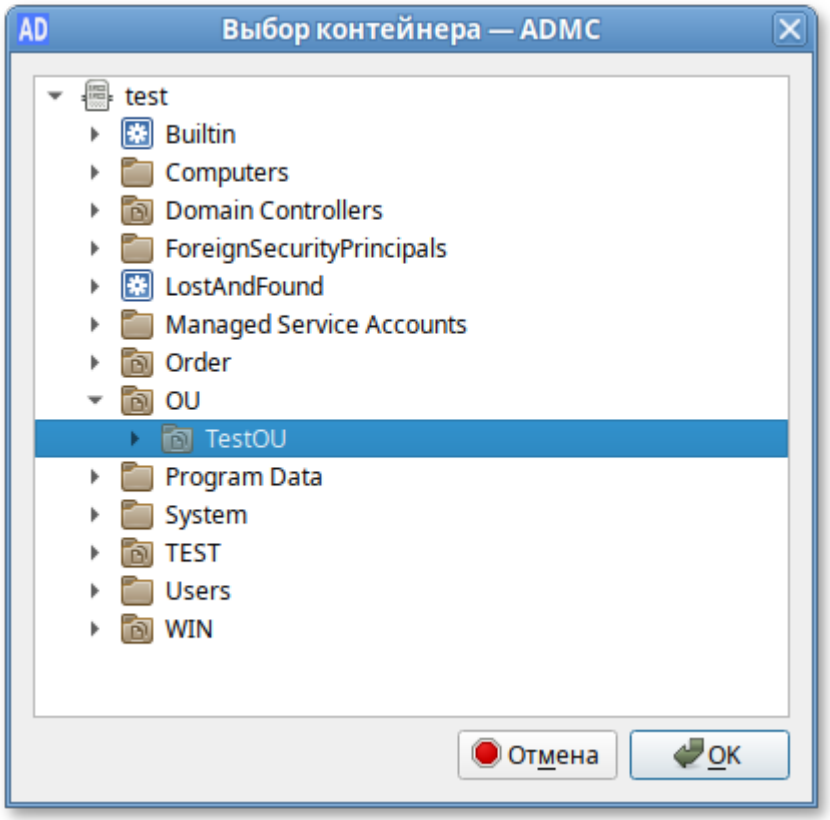
Для включения/отключения учётной записи компьютера необходимо в контекстном меню компьютера выбрать пункт **Отключить** или **Включить** (в зависимости от состояния учётной записи будет доступно одно из этих действий).

Для сброса учётной записи компьютера следует в контекстном меню компьютера выбрать пункт **Сбросить учётную запись**. При этом учётная запись выбранного компьютера будет переустановлена. Переустановка учётной записи компьютера прекращает его подключение к домену и требует заново ввести данный компьютер в домен.

Для перемещения компьютера в другой контейнер:

1. В контекстном меню компьютера выбрать пункт **Переместить…**.

2. В открывшемся окне выбрать контейнер, в который следует переместить учётную запись компьютера:



3. Нажать кнопку **OK**.

Для удаления учётной записи компьютера следует в контекстном меню компьютера выбрать пункт **Удалить**.

Предупреждение

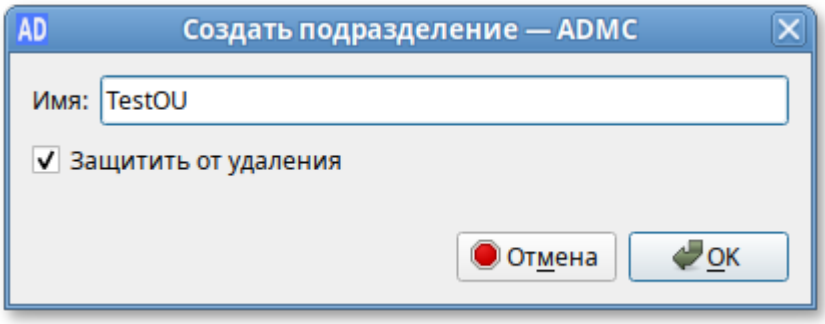
Если в настройках ADMC не отмечен пункт **`Подтверждать действия`**, компьютер будет удалён сразу после выбора пункта меню **Удалить**.

28.9. Управление подразделениями

Организационная единица или подразделение (Organizational Unit, OU) — это субконтейнер в AD, в который можно помещать пользователей, группы, компьютеры и другие объекты AD. Подразделение — самая маленькая область или единица, для которой можно назначить параметры групповой политики. Подразделения могут быть вложенными.

28.9.1. Создание подразделения

Для создания подразделения следует в контекстном меню контейнера выбрать пункт **Создать** → **Подразделение**. Окно мастера создания подразделения:



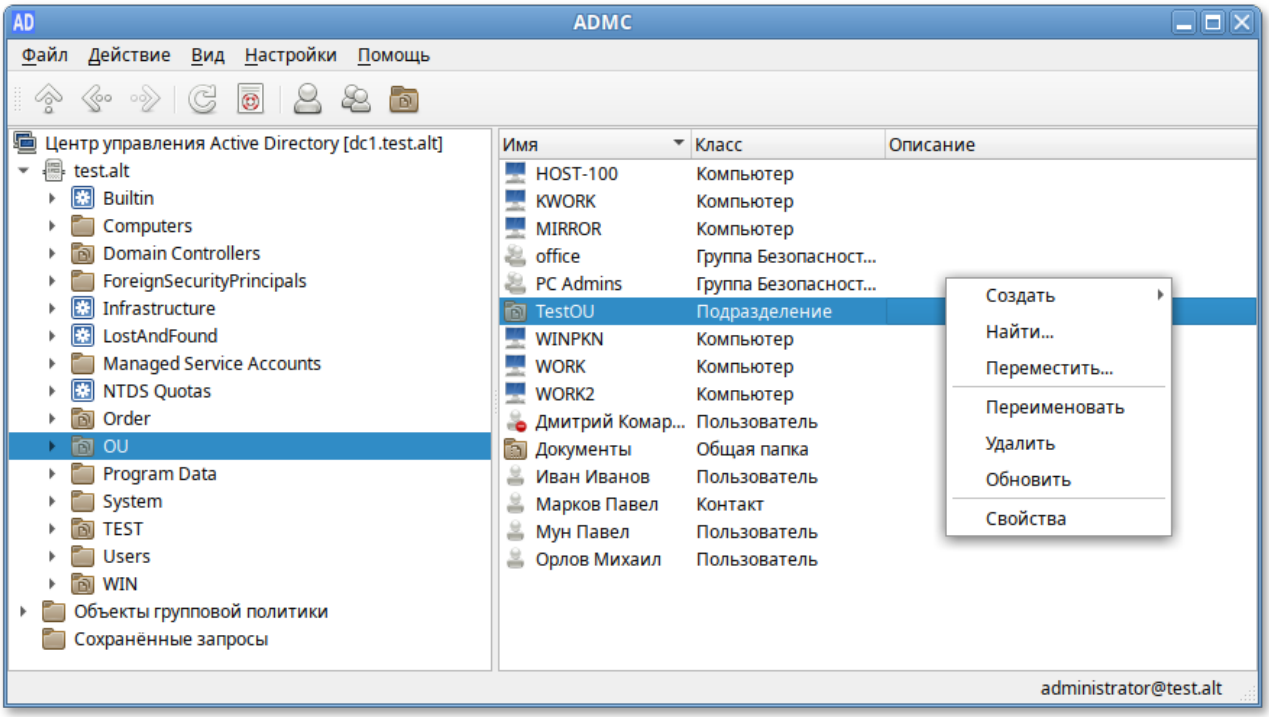
При создании подразделения необходимо указать название подразделения (поле **Имя**).

Примечание

Если при создании подразделения отметить пункт **Защитить от удаления**, то для удаления данного подразделения, необходимо сначала снять данную отметку в окне свойств подразделения.

28.9.2. Изменение подразделения

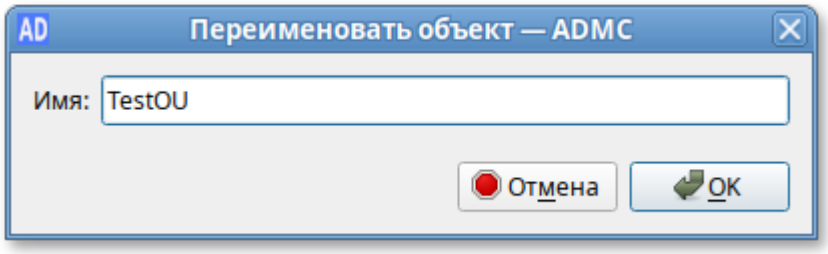
Для изменения подразделения следует в контекстном меню подразделения выбрать соответствующее действие:



Для переименования подразделения:

1. В контекстном меню подразделения выбрать пункт **Переименовать**.

2. В открывшемся окне изменить имя подразделения:

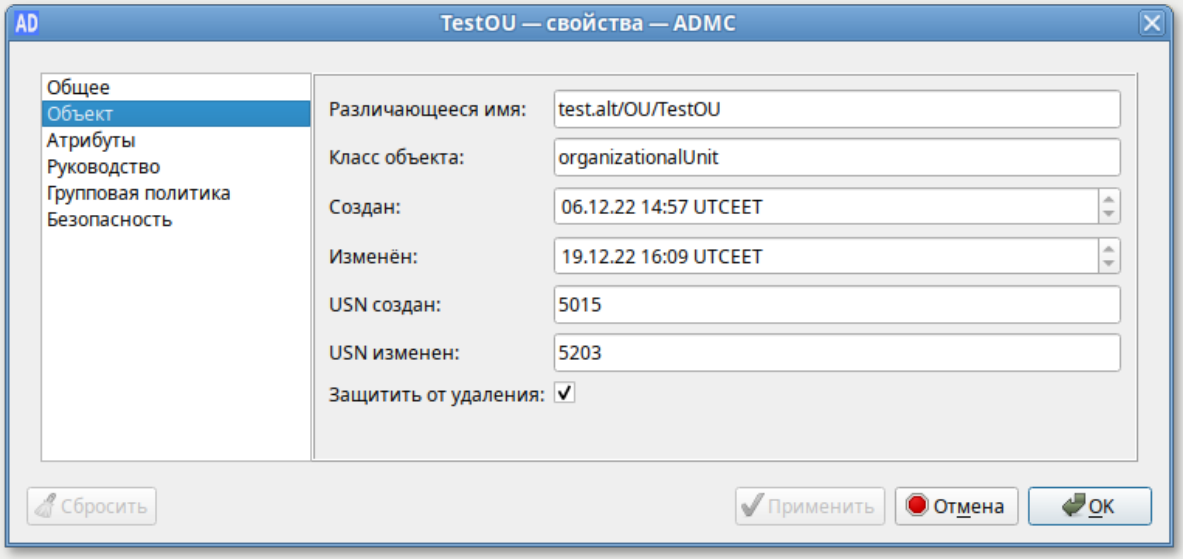


3. Нажать кнопку **OK** для сохранения изменений.

Для удаления подразделения следует в контекстном меню подразделения выбрать пункт **Удалить**.

Предупреждение

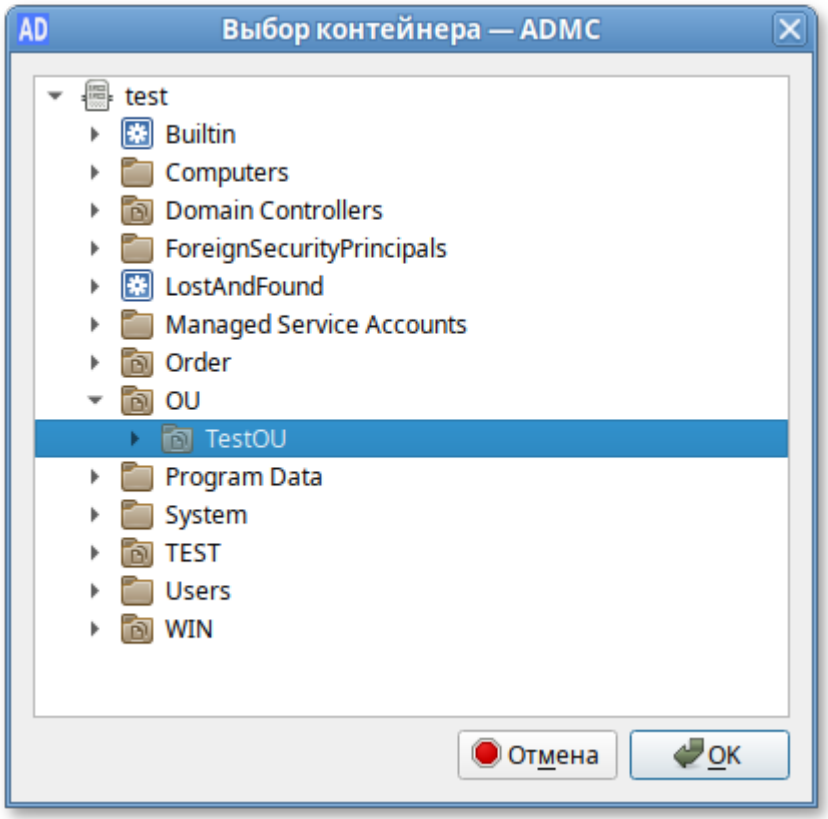
Если при создании подразделения был отмечен пункт **Защитить от удаления**, то сразу удалить подразделение не получится, необходимо сначала снять данную отметку в окне свойств подразделения:



Для перемещения подразделения в другой контейнер:

1. В контекстном меню подразделения выбрать пункт **Переместить…**.

2. В открывшемся окне выбрать контейнер, в который следует переместить подразделение:



3. Нажать кнопку **OK**.

28.10. Делегирование административных полномочий

Разрешения — это набор правил, которые определяют, насколько объект имеет полномочия просматривать или изменять другие объекты в домене.

Делегирование позволяет предоставить право на выполнение некоторых задач управления доменом обычным пользователям домена, не включая их в привилегированные доменные группы, такие как «Domain Admins», «Account Operators» и т.д. Например, с помощью делегирования можно предоставить определённой группе пользователей право на добавление пользователей в группы, заведение новых пользователей в домене и сброс пароля.

Делегировать полномочия можно на уровне домена или конкретной OU.

Важно:

- Разрешения наследуются от родительских объектов, если не настроено иное.
- Изменение разрешений может повлиять на безопасность и функциональность, поэтому рекомендуется тщательно проверять изменения перед их применением.
- Для управления разрешениями на уровне объектов рекомендуется использовать группы, а не отдельных пользователей, чтобы упростить администрирование.
- Не следует предоставлять делегировать права на управление OU, в котором содержатся административные аккаунты. Все чувствительные пользователи и группы с повышенными привилегиями нужно размещать в отдельной OU, на которую не распространяется правила делегирования.

- Запрещающие правила имеют приоритет над разрешающими.

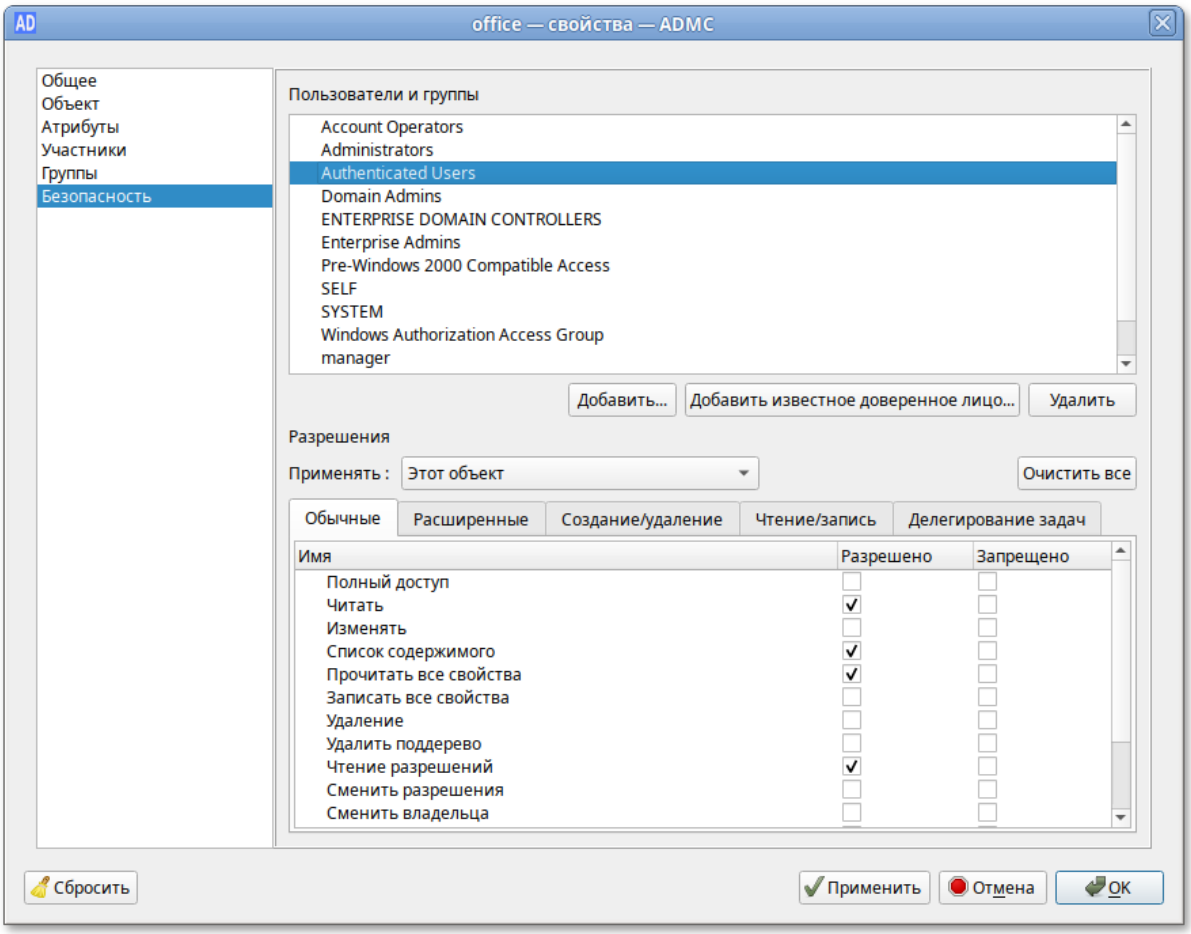
Примечание

Для возможности редактирования разрешений необходимо в меню **Настройки** отметить пункт **Дополнительные возможности**.

28.10.1. Управление разрешениями

Просмотр разрешений пользователя или объекта можно выполнить в окне свойств объекта:

1. В контекстном меню объекта выбрать пункт **Свойства**:



2. В окне свойств объекта перейти на вкладку **Безопасность**.

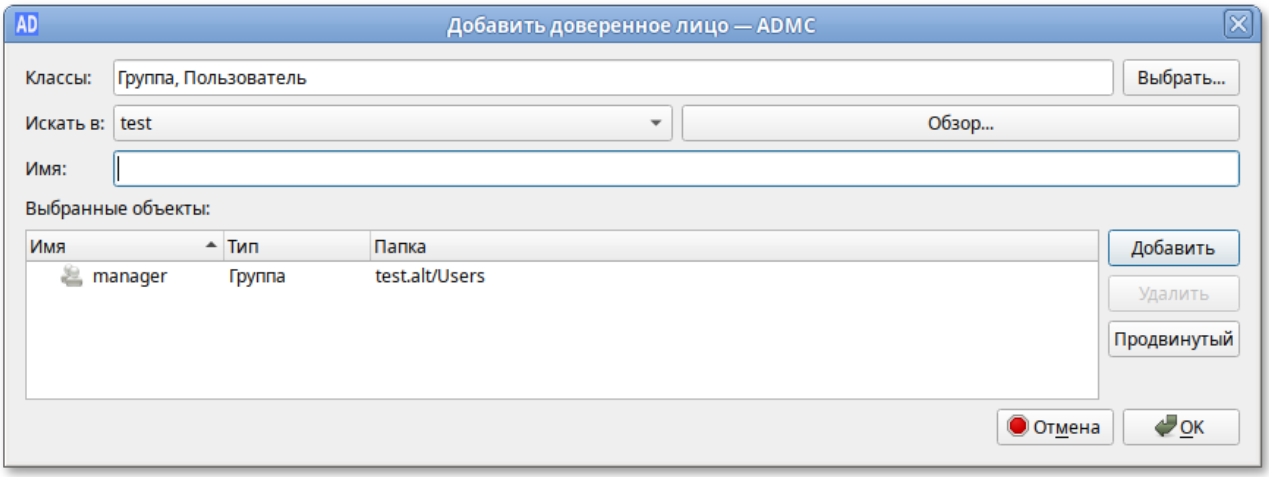
Каждому объекту в сети назначается набор данных об управлении доступом. Этот набор данных определяет, какой тип доступа разрешается пользователям и группам.

В поле **Пользователи и группы** отображаются группы и пользователи, которым назначены разрешения на доступ к данному объекту. Это поле показывает, кто имеет права на выполнение определенных действий с объектом (например, чтение, запись, изменение и т.д.). В этом поле отображаются встроенные группы безопасности:

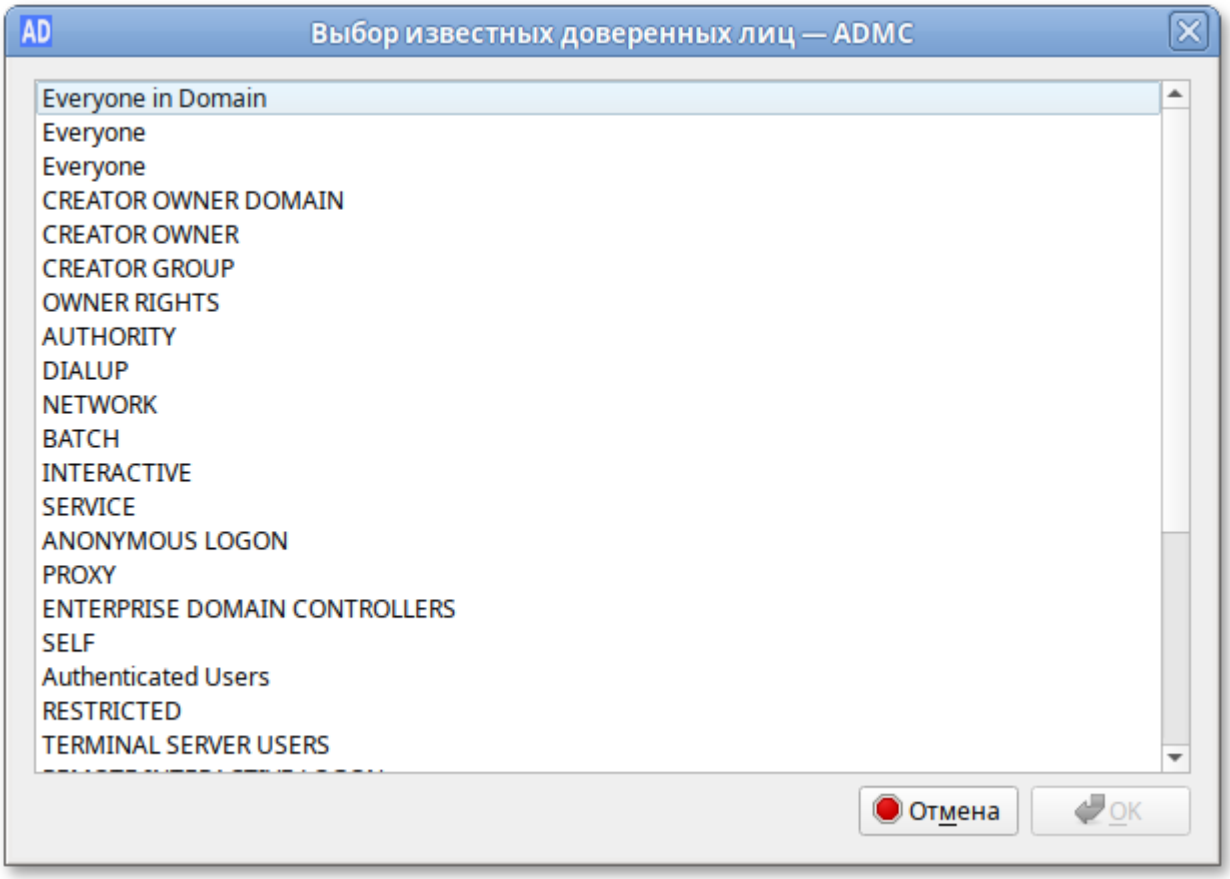
- **Domain Admins** — администраторы домена, которые имеют полный контроль над объектами в домене;

- **Enterprise Admins** — администраторы предприятия, которые имеют полный контроль над всеми доменами в лесу;
- **Administrators** — локальные администраторы;
- **Authenticated Users** — все аутентифицированные пользователи в домене;
- **SYSTEM** — встроенная учетная запись операционной системы, которая имеет полный контроль над объектами;
- **Self** — специальная группа, представляющая сам объект (используется для делегирования управления).

Чтобы установить разрешения для группы (или пользователя), которая отсутствует в списке можно воспользоваться кнопкой **Добавить…**:



или **Добавить известное доверенное лицо…**:



В разделе **Разрешения** отображается список разрешений, назначенных группам или пользователям, выбранным в поле **Пользователи и группы**. Все разрешения разбиты на вкладки:

- **Обычные** — общие и стандартные разрешения;
- **Расширенные** — расширенные права;
- **Создание/Удаление** — создание/удаление дочерних объектов;
- **Чтение/Запись** — чтение/запись свойств;
- **Делегирование задач** — задачи управления доменом.

Разрешения определяют, какие действия могут выполнять пользователи или группы с данным объектом.

Примеры разрешений:

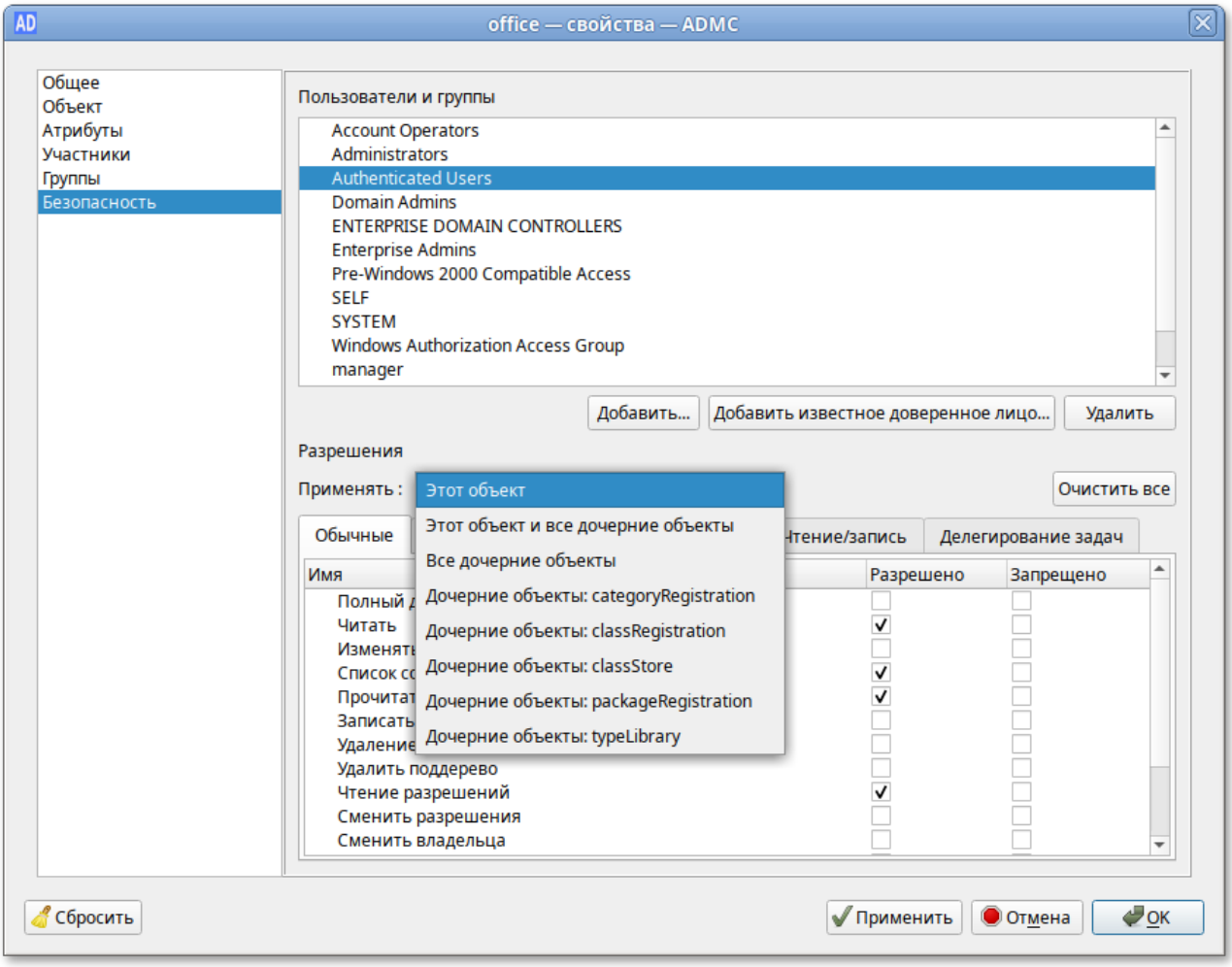
- **Полный доступ** — полный доступ к объекту, включая изменение разрешений;
- **Читать** — возможность просматривать свойства объекта;
- **Изменять** — возможность изменять свойства объекта;
- **Удаление** — возможность удалять объект;
- **Создавать дочерние объекты** — возможность создавать любые объекты в контейнере;
- **Удалять все дочерние объекты** — возможность удалять любые объекты в контейнере;
- **Чтение разрешений** — возможность просматривать разрешения объекта;
- **Сменить разрешения** — возможность изменять разрешения объекта.

Тип разрешения:

- **Разрешено** — разрешает выполнение указанного действия;
- **Запрещено** — явно запрещает выполнение указанного действия (имеет приоритет над разрешениями).

Область применения (поле **Применять**) определяет, к каким объектам применяются разрешения:

- **Этот объект** — разрешения применяются только к текущему объекту;
- **Этот объект и все дочерние объекты** — разрешения применяются к текущему объекту и всем объектам внутри него;
- **Все дочерние объекты** — разрешения применяются только к объектам внутри контейнера;
- **Дочерние объекты: <класс объекта>** — разрешения применяются только к объектам определенного типа (например, только к пользователям или только к группам).



Разрешения могут быть явно назначены или унаследованы от родительского объекта. Унаследованные разрешения отображаются серым цветом и не могут быть изменены на уровне дочернего объекта. Явно назначенные разрешения имеют приоритет над унаследованными.

Примечание

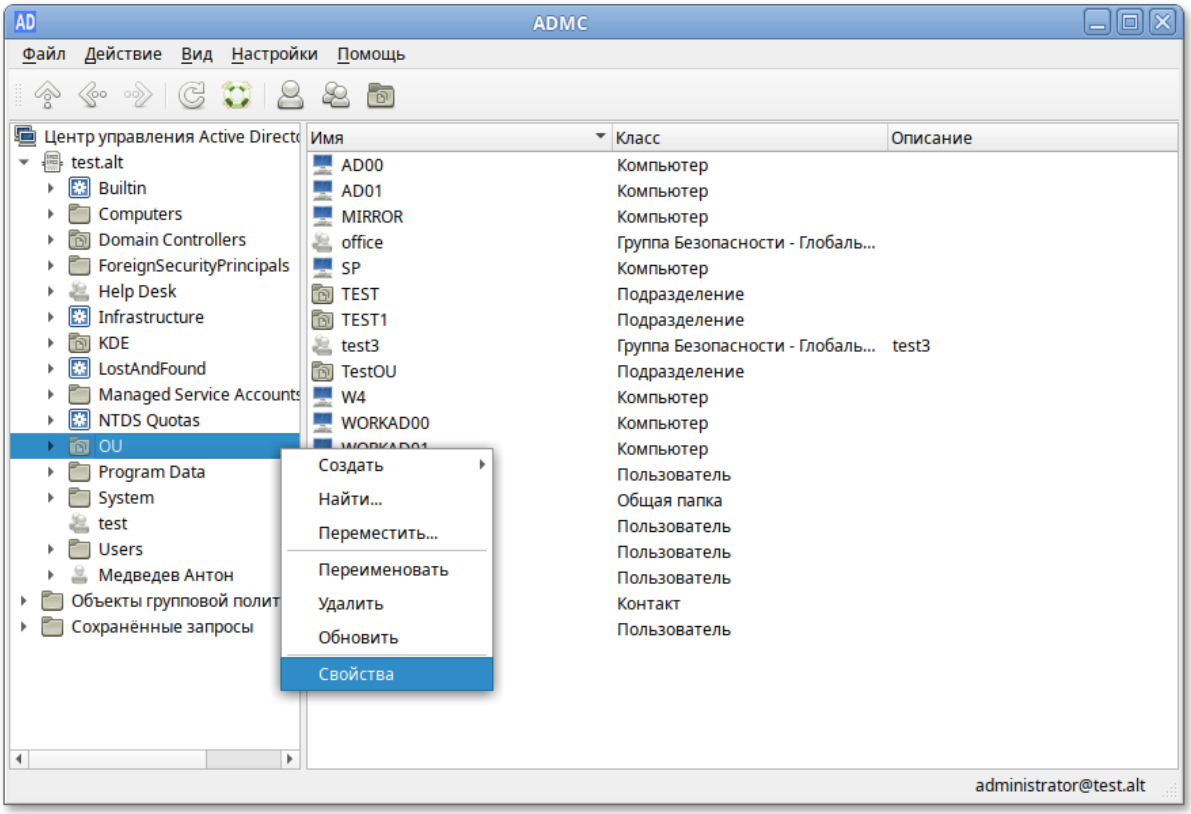
Снятие/установка бóльших разрешений снимает/устанавливает все меньшие тоже. Например, снятие разрешения **Полный доступ** снимает все остальные разрешения.

28.10.2. Настройка разрешений, необходимых для перемещения объектов между OU

Чтобы иметь возможность перемещать объекты (учетные записи пользователей, групп и компьютеров) из одного OU в другой, необходимо иметь права как на создание, так и на удаление этого типа объекта как в исходном, так и в целевом OU. Кроме того также нужны права на обновление свойств объекта. Если разрешения установлены для самого верхнего OU, все дочерние OU также унаследуют разрешения.

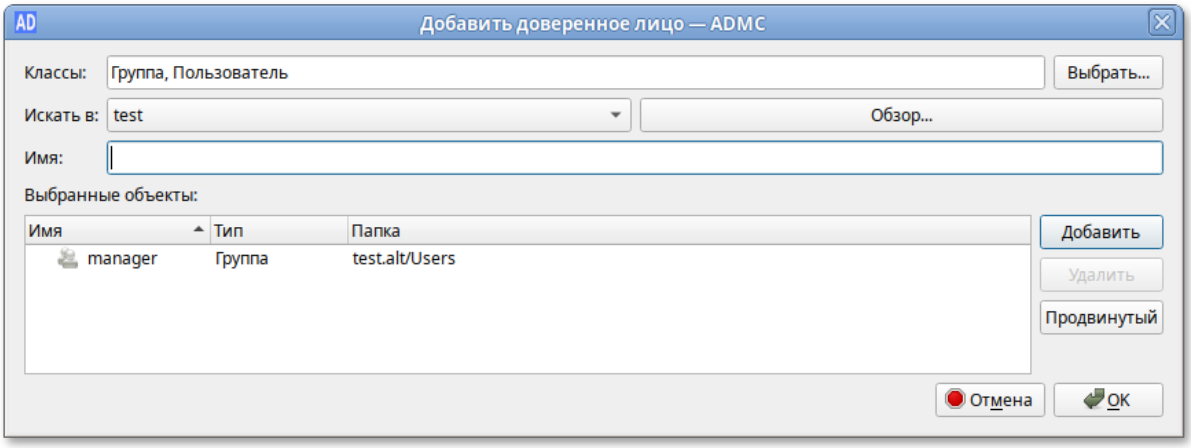
Для того чтобы предоставить членам группы «manager» разрешения на перемещение объектов из одного контейнера (OU) в другой, необходимо:

1. В контекстном меню контейнера (OU), из которого нужно разрешить перемещение, выбрать пункт **Свойства**:



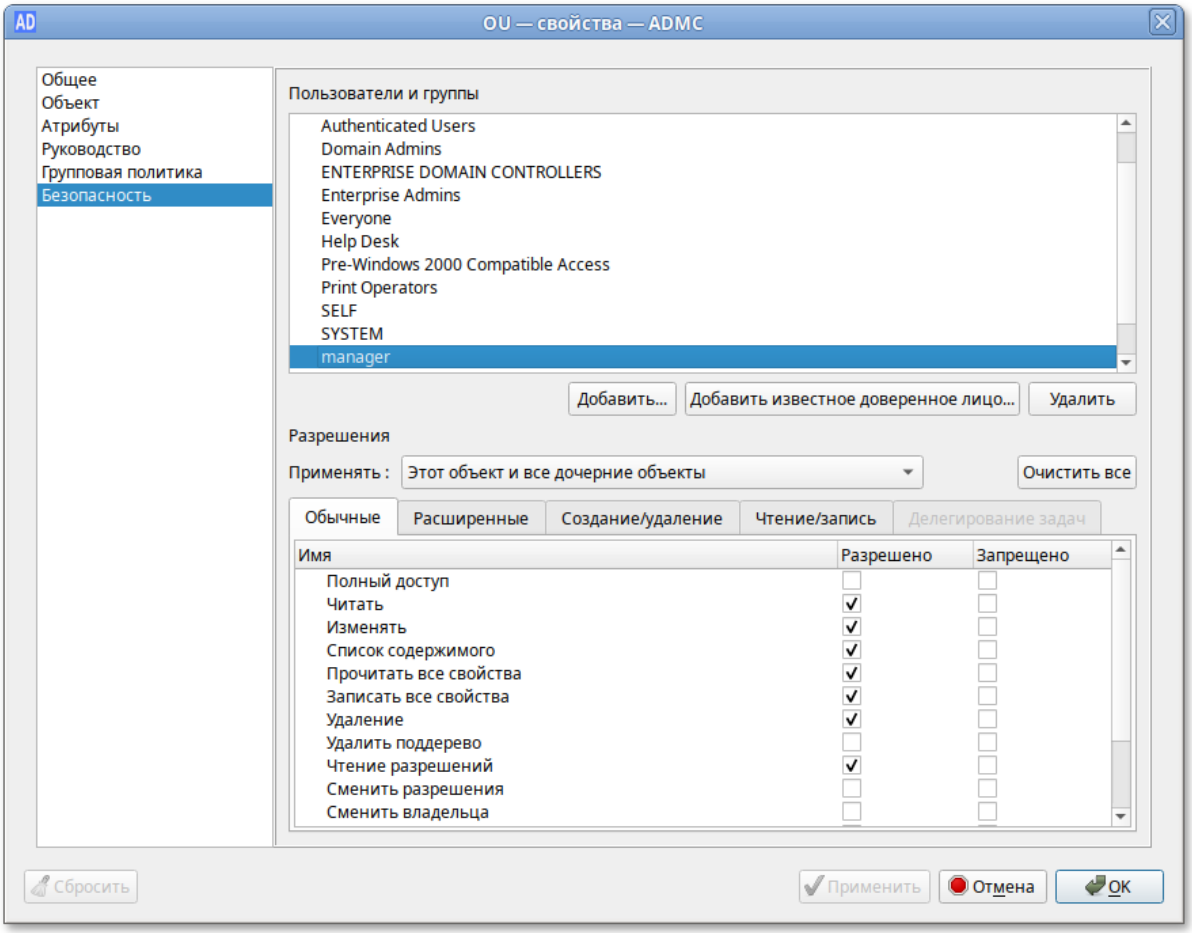
2. В окне свойств контейнера перейти на вкладку **Безопасность**.

3. Добавить объект, которому будут добавлены разрешения. Для этого нажать кнопку **Добавить…** и выбрать необходимый объект. В данном примере будет добавлена группа manager:



4. В окне списке **Применить** выбрать пункт **Этот объект и все дочерние объекты**.

5. Настроить разрешения для добавленной группы. Для этого в разделе **Разрешения** установить отметки **Разрешено** в полях **Читать**, **Изменять** и **Удаление**:



6. Нажать кнопку **OK**, чтобы сохранить изменения.

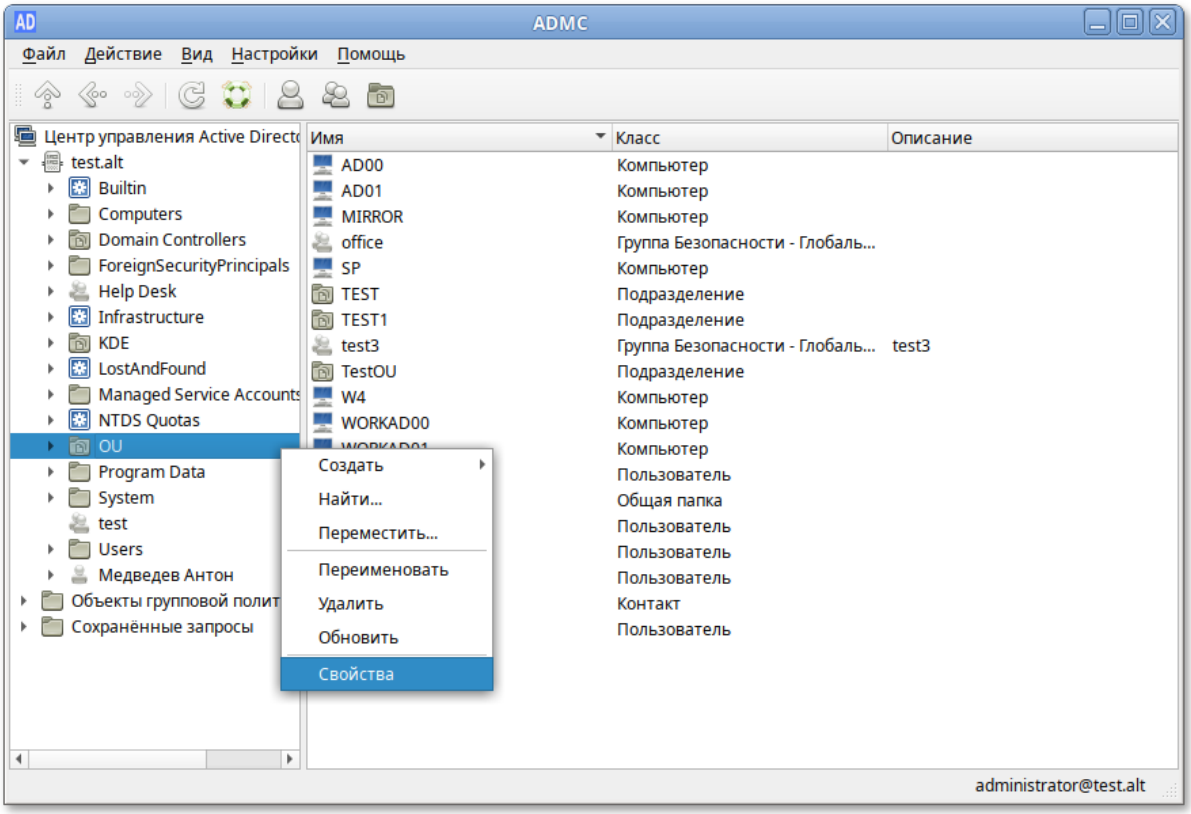
7. Повторить все шаги для целевого контейнера.

28.10.3. Делегация полномочий на управление учетными записями пользователей

В примере, рассмотренном ниже, членам группы *manager* делегируются права на управление учетными записями пользователей, входящих в организационную единицу *OU*.

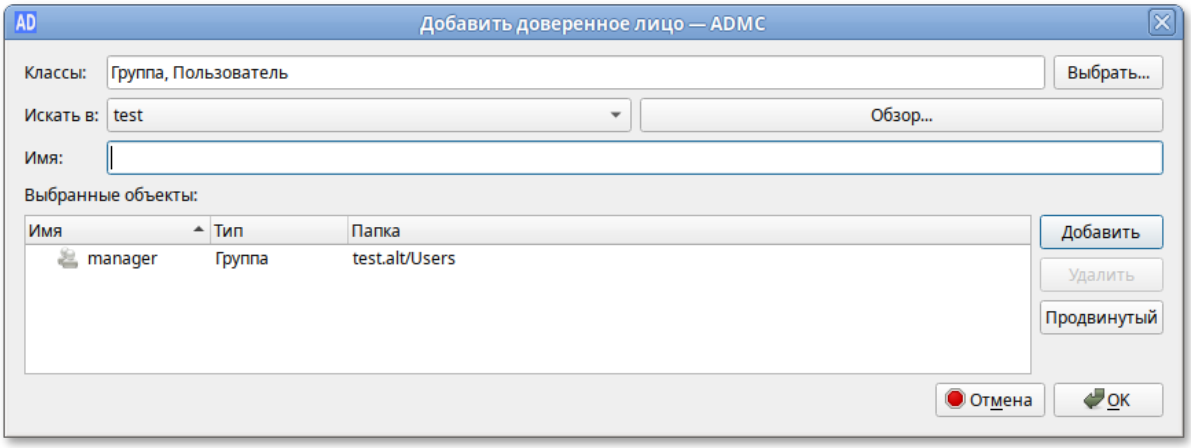
Для делегации полномочий необходимо выполнить следующие действия:

1. В контекстном меню организационной единицы выбрать пункт **Свойства**:

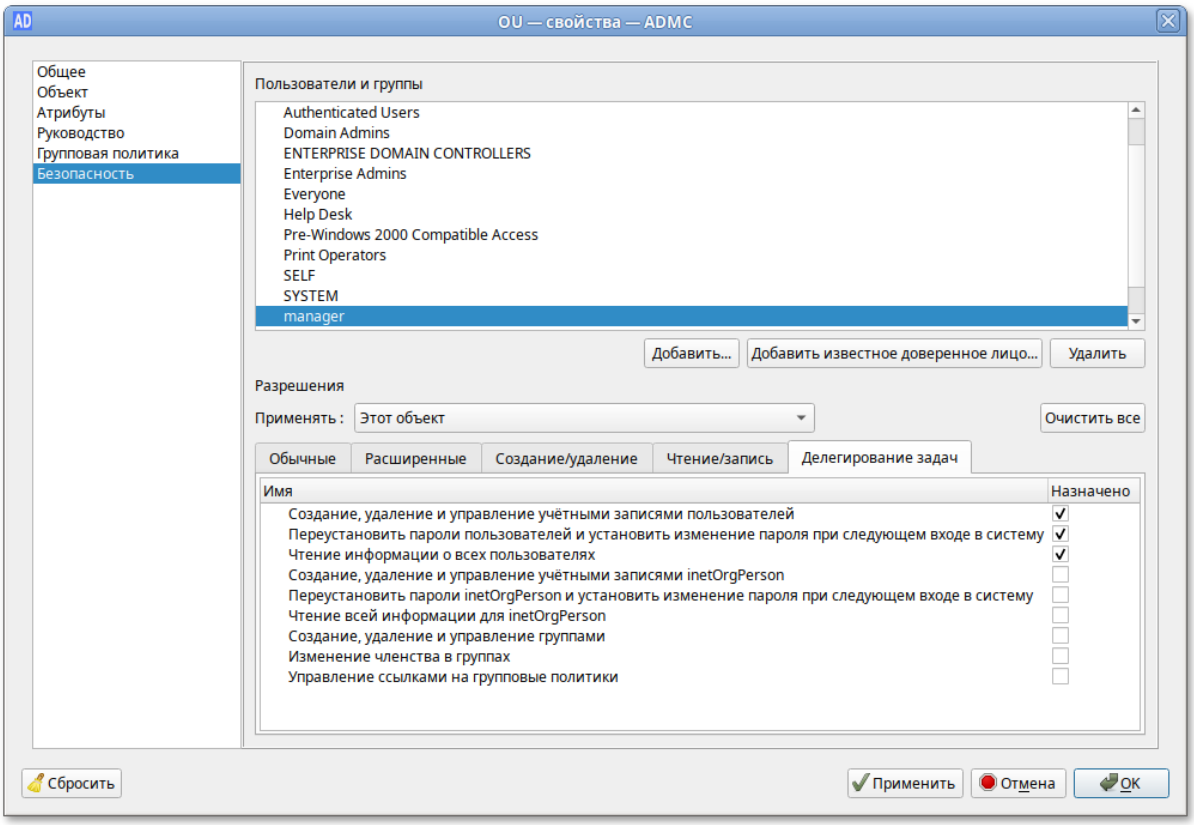


2. В окне свойств контейнера перейти на вкладку **Безопасность**.

3. Добавить объект, которому будут делегированы задачи. Для этого нажать кнопку **Добавить…** и выбрать необходимый объект. В данном примере будет добавлена группа manager:



4. Делегировать задачи добавленному объекту. Для этого в разделе **Разрешения** перейти на вкладку **Делегирование задач** и установить отметку в поле **Создание, удаление и управление учетными записями пользователей** (отметки в полях **Переустановить пароли пользователей и установить изменение пароля при следующем входе в систему** и **Чтение информации о всех пользователях** будут проставлены автоматически):



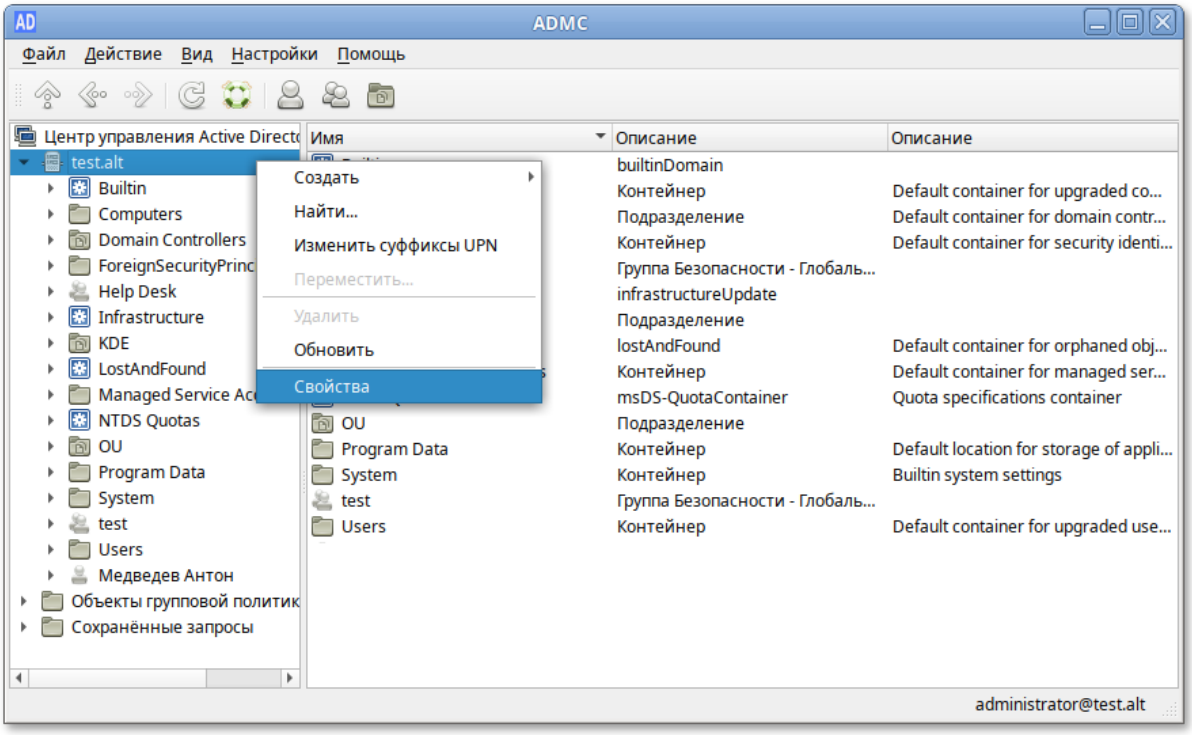
5. Нажать кнопку **Применить**.

Далее можно зарегистрироваться в системе с учетной записью члена группы manager и убедиться, что данный пользователь имеет разрешения, например, на переустановку пароля пользователя, входящего в организационную единицу OU.

28.10.4. Делегация полномочий на присоединение компьютеров в домен

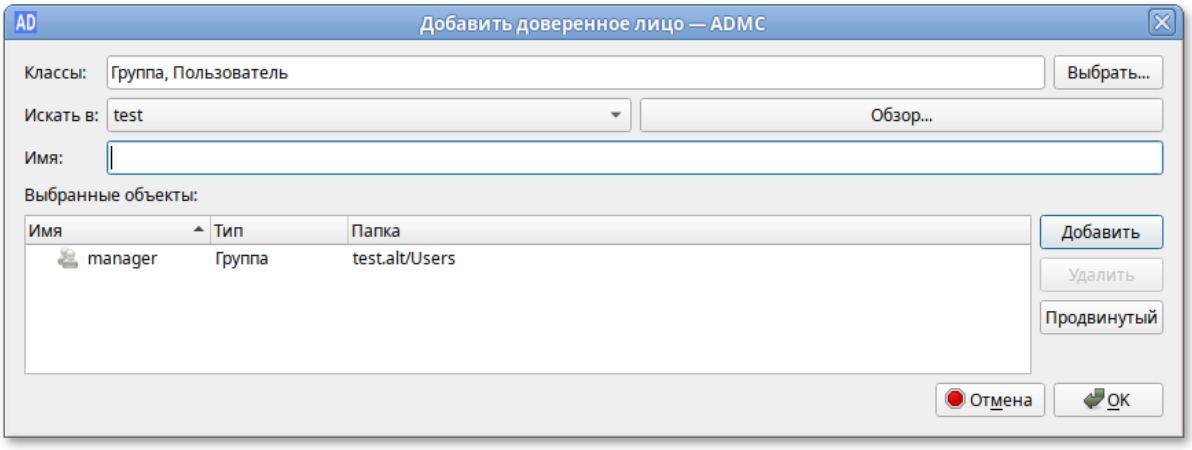
Делегация полномочий на присоединение компьютеров в домен членам группы *manager*:

1. В контекстном меню домена выбрать пункт **Свойства**:

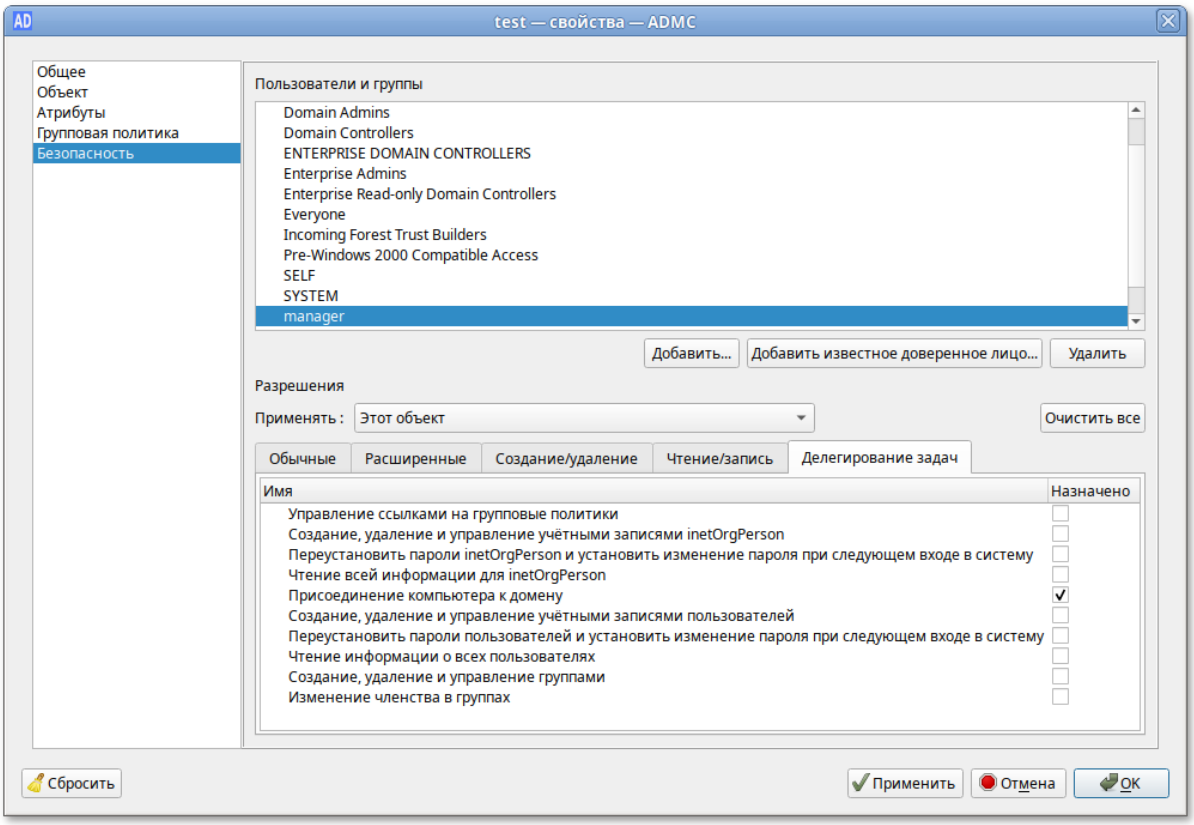


2. В окне свойств домена перейти на вкладку **Безопасность**.

3. Добавить объект, которому будут делегирована задача. Для этого нажать кнопку **Добавить…** и выбрать необходимый объект. В данном примере будет добавлена группа manager:



4. Делегировать задачи добавленному объекту. Для этого в разделе **Разрешения** перейти на вкладку **Делегирование задач** и установить отметку в поле **Присоединение компьютера к домену**:



5. Нажать кнопку **Применить**.

Далее можно зарегистрироваться в системе с учетной записью члена группы manager и убедиться, что данный пользователь имеет разрешения, например, на переустановку пароля пользователя, входящего в организационную единицу OU.

28.11. Управление объектами парольных настроек

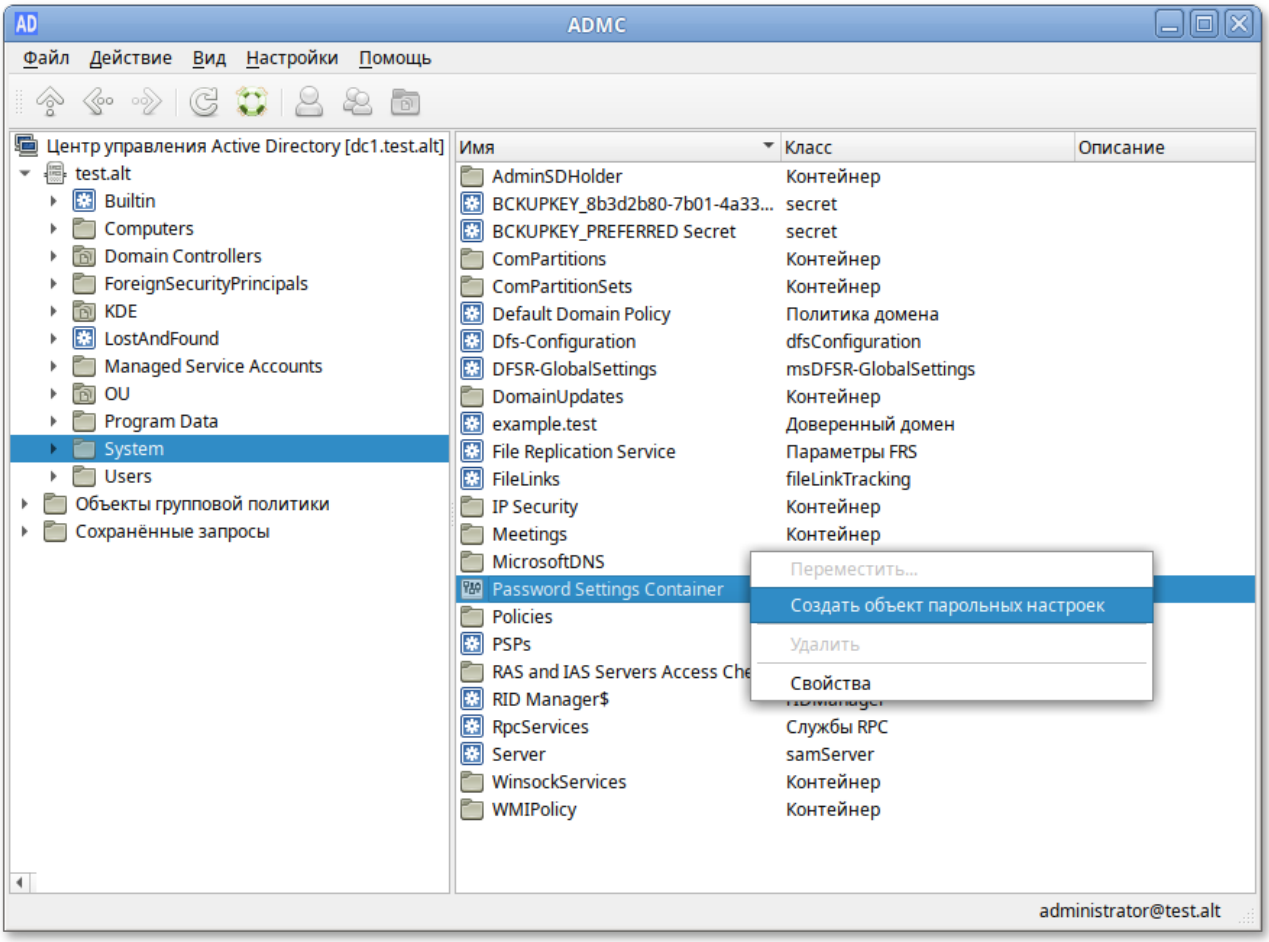
Объекты настроек паролей (Password Settings Object, PSO) позволяют администраторам домена переопределять параметры политики паролей домена и настраивать более точные параметры паролей для конкретных пользователей или групп пользователей. Например, для определённых пользователей можно установить требование минимальной длины пароля, ослабить ограничения сложности для других пользователей и т.д. PSO могут применяться к группам или к отдельным пользователям.

Примечание

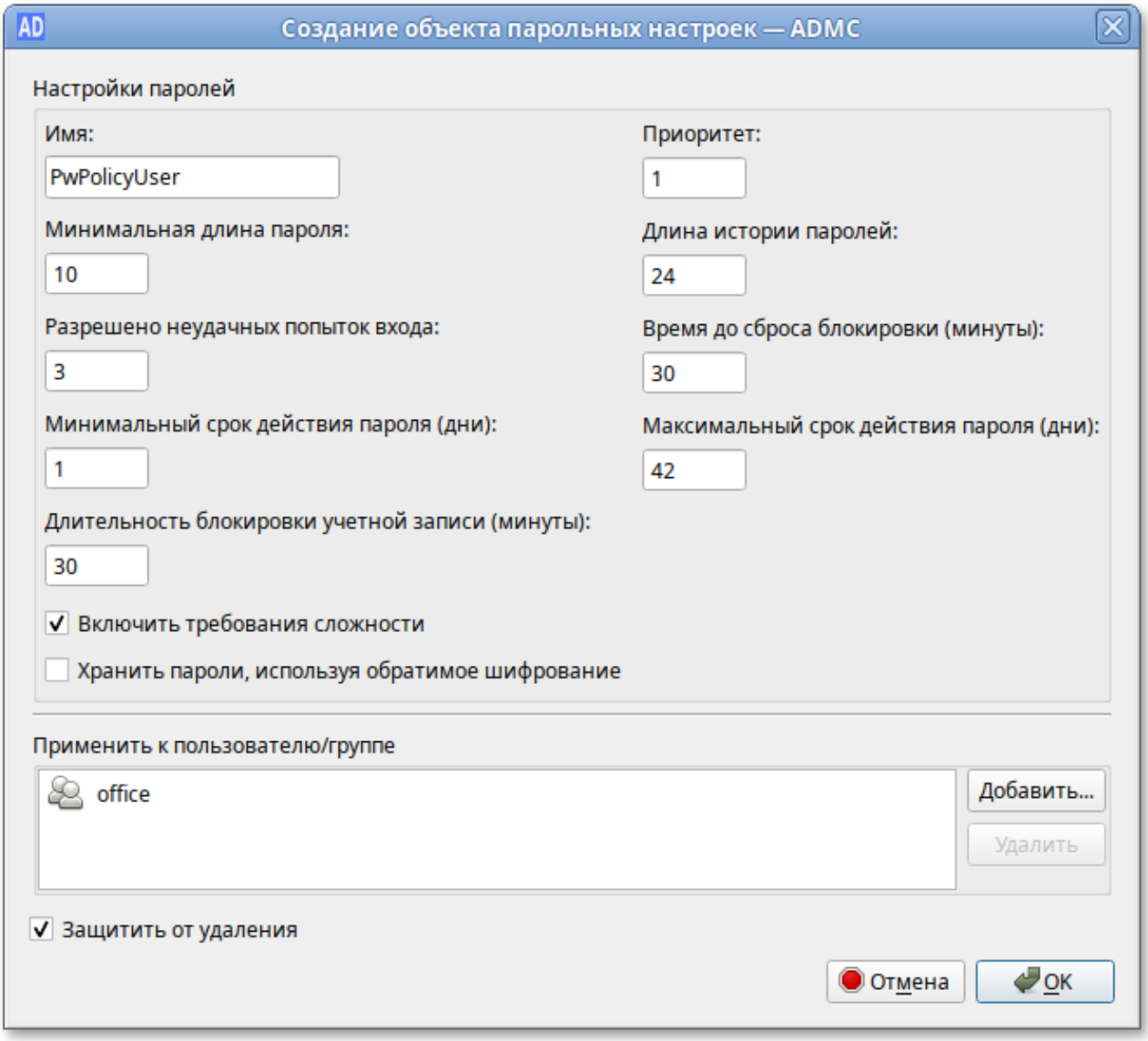
Для возможности работы с объектами парольных настроек необходимо в меню **Настройки** отметить пункт **Дополнительные возможности**.

28.11.1. Создание объекта парольных настроек

Для создания объекта парольных настроек следует в контекстном меню контейнера **`Password Settings Container`** (вкладка **System**) выбрать пункт **Создать объект парольных настроек**:



Окно мастера создания объекта парольных настроек:



При создании объекта парольных настроек необходимо в поле **Имя** указать имя объекта парольных настроек (имя должно быть уникальным на уровне домена).

В поле **Приоритет** можно указать приоритет политики (precedence), который будет учитываться в том случае, если к пользователю или группе пользователей применяются несколько политик. Чем меньше значение этого параметра, тем выше приоритет.

Далее можно указать следующие параметры объекта парольных настроек:

- **Минимальная длина пароля** — минимальное количество символов в пароле (по умолчанию 7);
- **Длина истории паролей** — число хранимых предыдущих паролей пользователей (требование неповторяемости паролей) (по умолчанию 24);
- **Разрешено неудачных попыток входа** — допустимое количество неудачных попыток ввода пароля перед блокировкой учетной записи (по умолчанию 0 — никогда не блокировать);
- **Время до сброса блокировки** — интервал времени (в минутах), по истечении которого записанное количество попыток начинается заново (по умолчанию 30);

- **Минимальный срок действия пароля** — минимальный срок действия пароля (по умолчанию один день);
- **Максимальный срок действия пароля** — максимальный срок действия пароля (по умолчанию 42 дня);
- **Длительность блокировки учетной записи** — интервал времени (в минутах), в течение которого возможность аутентификации для пользователя, превысившего количество попыток входа, будет заблокирована (по умолчанию 30);
- **Включить требования сложности** — должен ли пароль отвечать требованиям сложности (по умолчанию включено);
- **Хранить пароли, используя обратимое шифрование** — хранить пароли, используя обратимое шифрование (по умолчанию выключено).

Примечание

Для создания политики требуется передать новое значение хотя бы для одной парольной настройки.

В окне **Применить к пользователю/группе** следует добавить пользователей и/или группы, к которым должен применяться этот объект парольных настроек.

Примечание

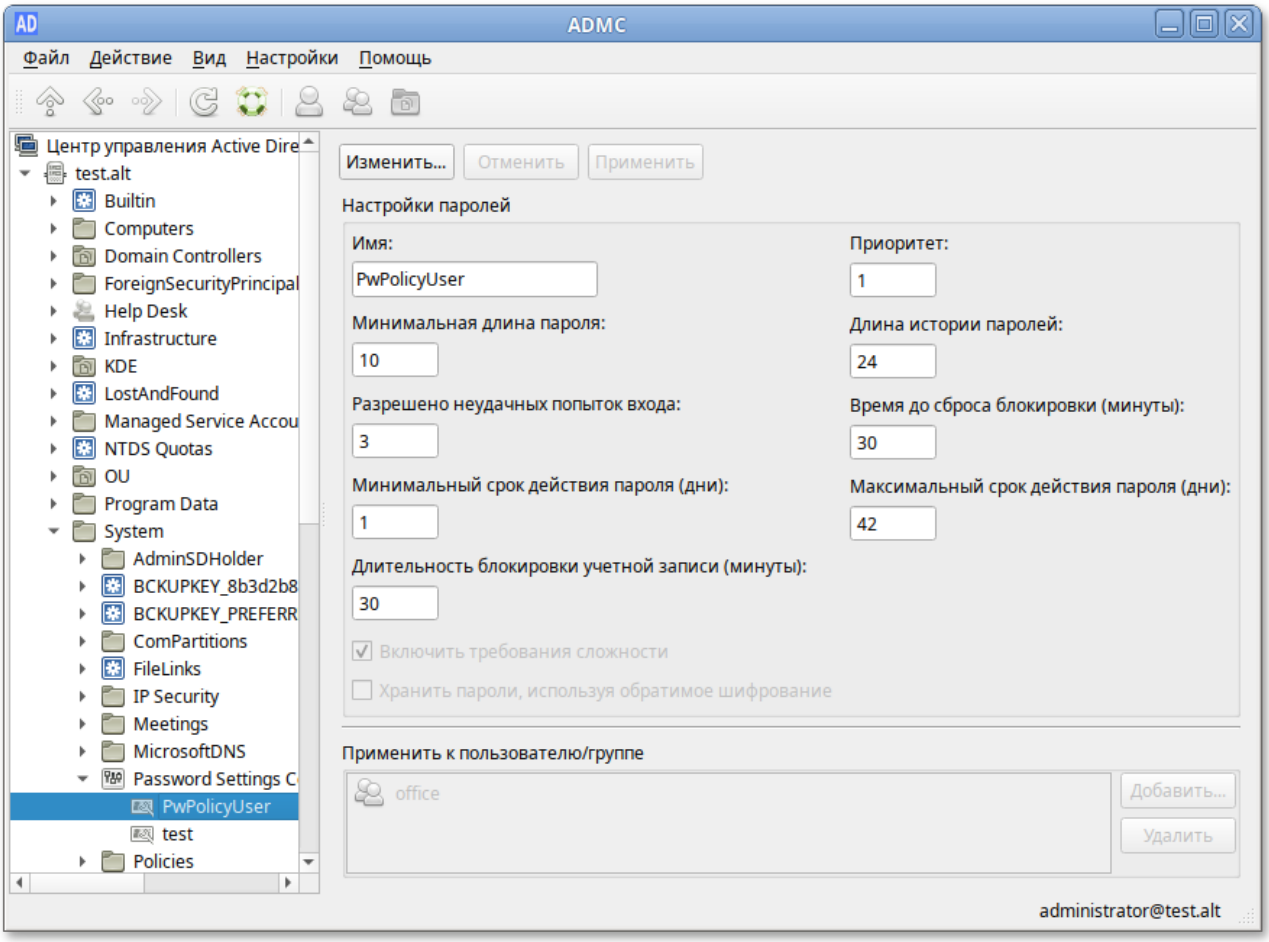
Если при создании объекта парольных настроек отметить пункт **Защитить от удаления**, то для удаления данного объекта, необходимо сначала снять данную отметку в окне свойств объекта.

28.11.2. Просмотр и изменение объекта парольных настроек

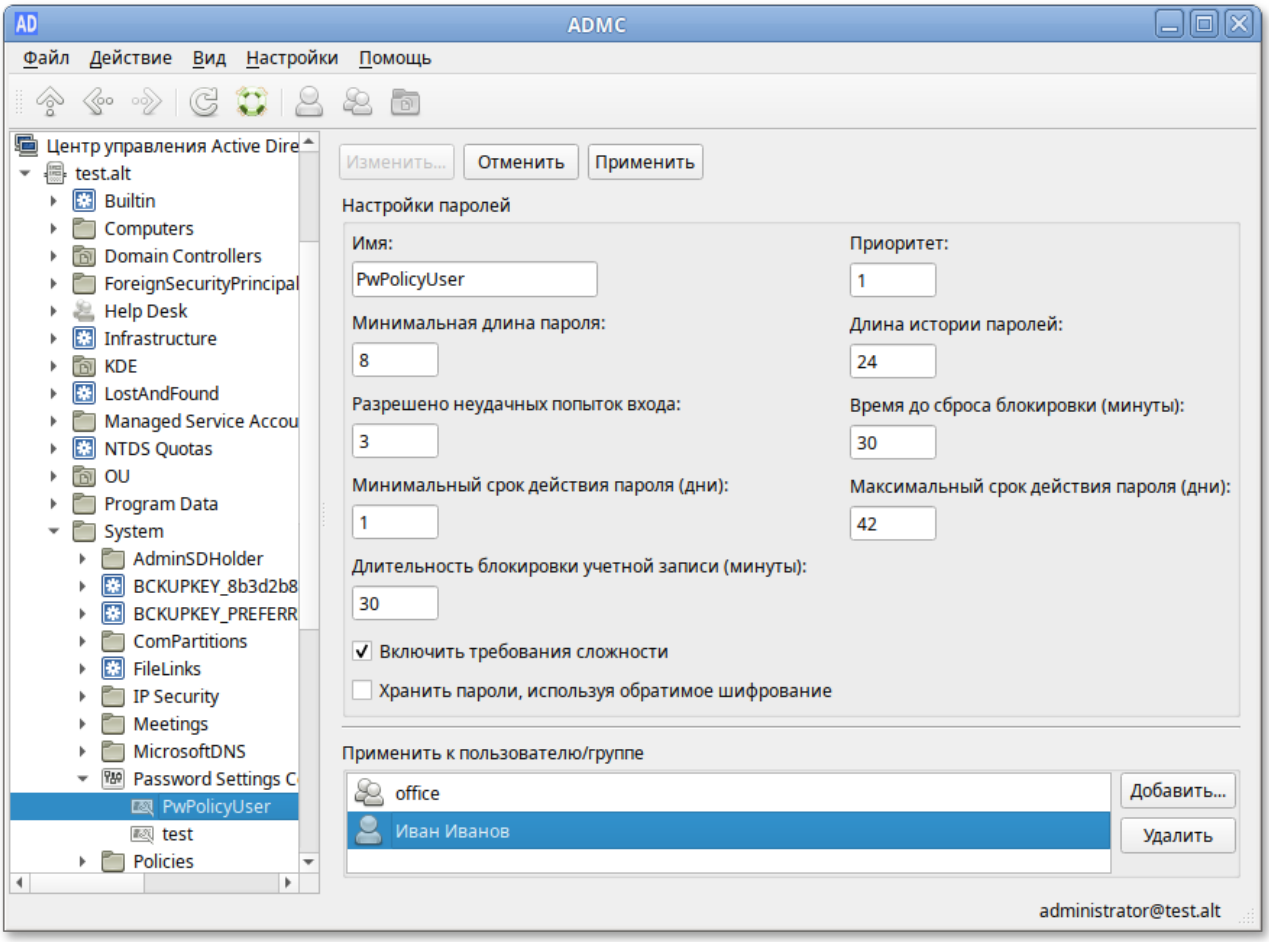
Примечание

Для того чтобы контейнер **Password Settings Container** отображался в дереве консоли, необходимо в меню **Настройки** отметить пункт **Показывать неконтейнерные объекты в дереве консоли**.

Для просмотра параметров объекта парольных настроек можно дважды щелкнуть мышью по объекту парольных настроек или выбрать объект в списке **Password Settings Container**:



Для изменения параметров объекта парольных настроек следует нажать кнопку **Изменить…**, внести изменения и нажать кнопку **Применить**:



Примечание

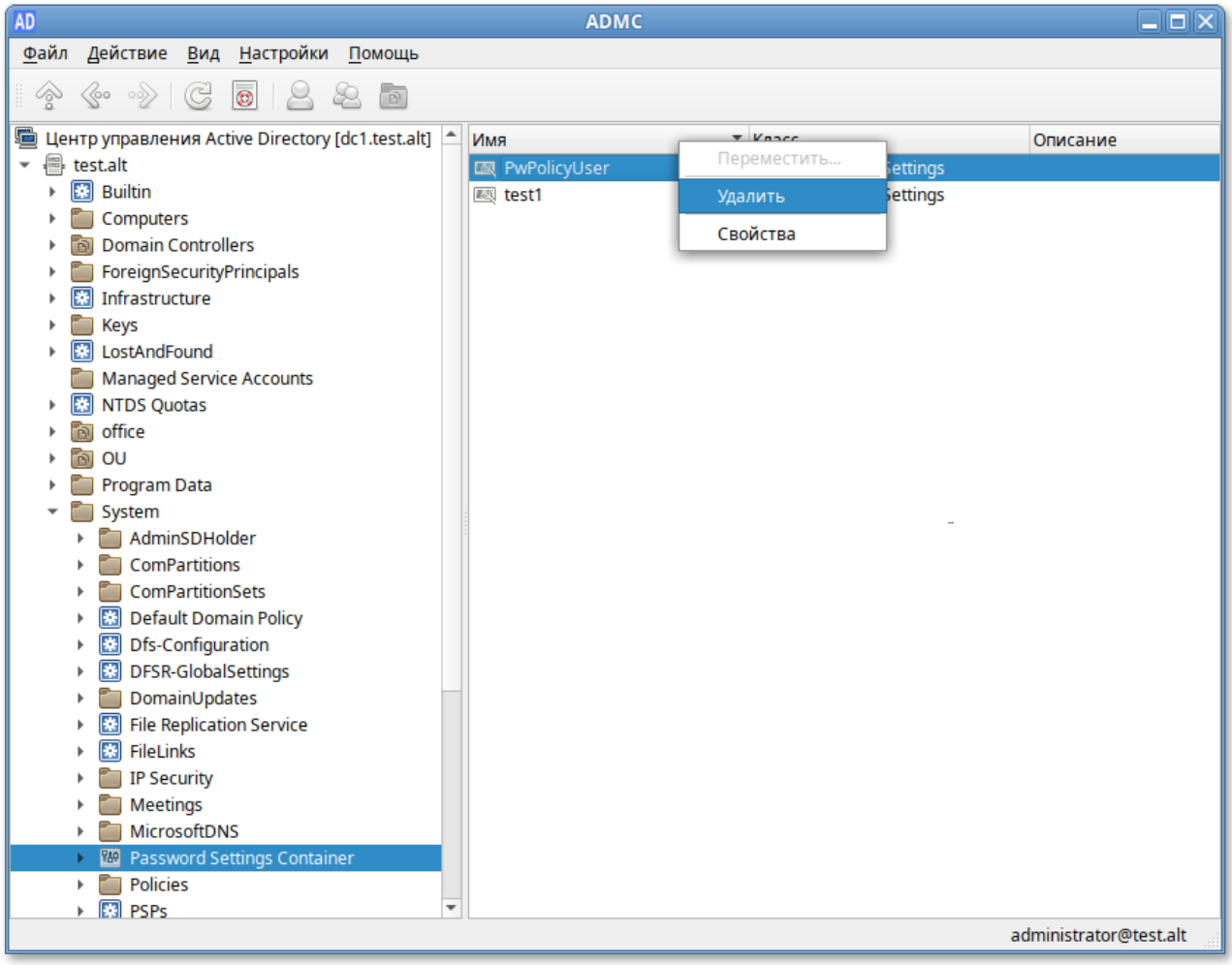
Изменить имя объекта парольных настроек нельзя.

28.11.3. Удаление объекта парольных настроек

Примечание

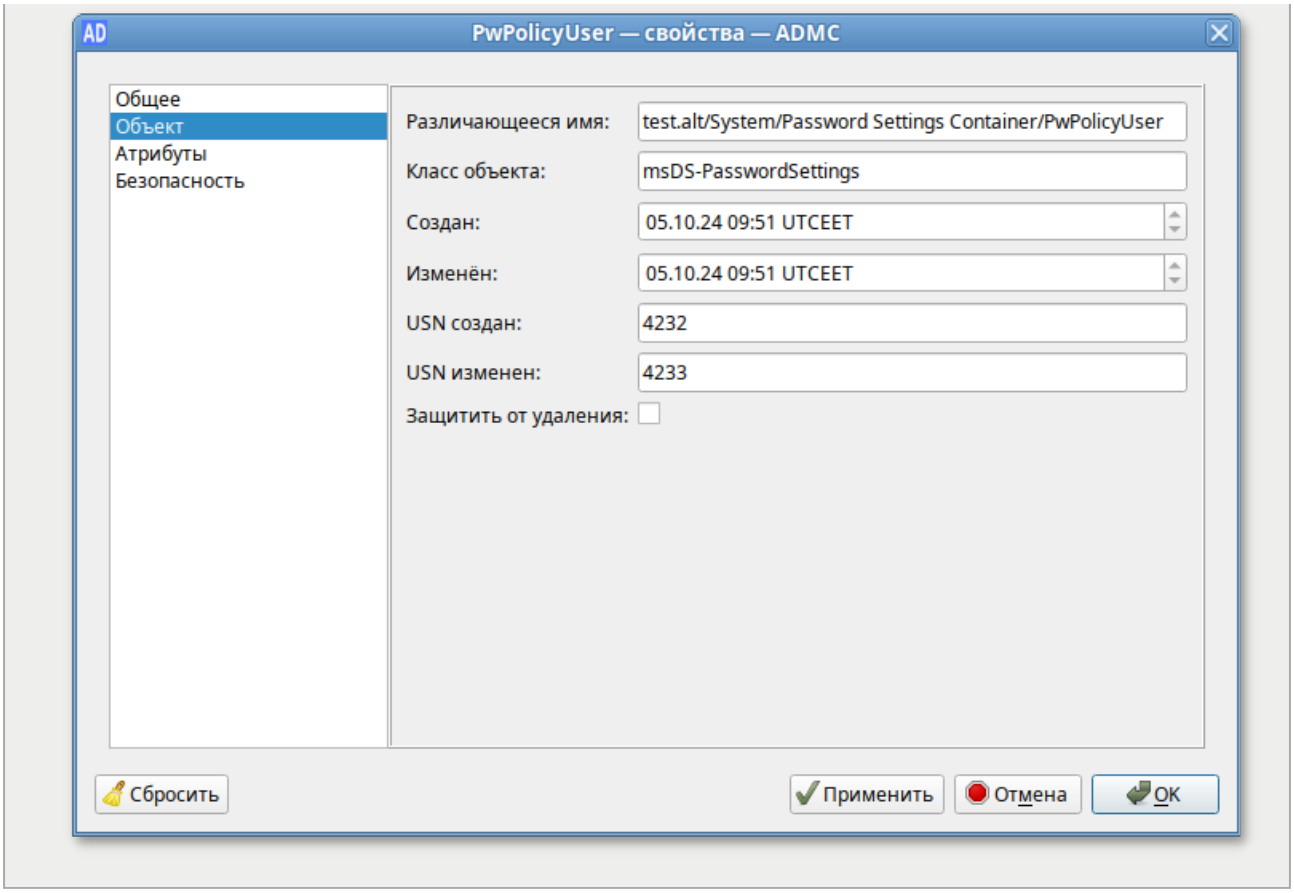
Для того чтобы контейнер **`Password Settings Container`** отображался в дереве консоли, необходимо в меню **Настройки** отметить пункт **Показывать неконтейнерные объекты в дереве консоли**.

Для удаления объекта парольных настроек следует в контекстном меню объекта выбрать пункт **Удалить**:



Предупреждение

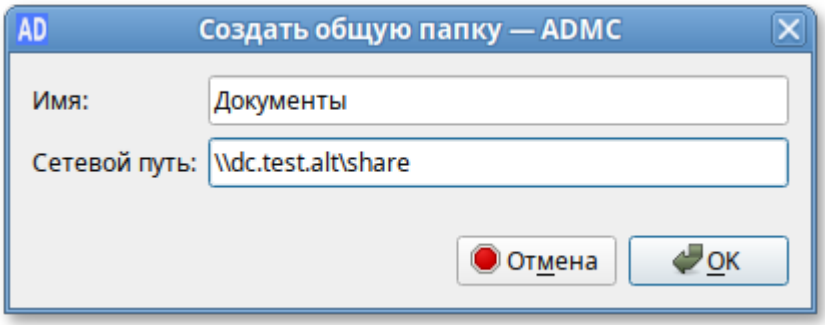
Если при создании объекта парольных настроек был отмечен пункт **Защитить от удаления**, то сразу удалить объект не получится, необходимо сначала снять данную отметку в окне свойств объекта парольных настроек:



28.12. Управление общими папками

Общая папка является ссылкой на общий сетевой ресурс и не содержит никаких данных.

Для создания общей папки следует в контекстном меню контейнера выбрать пункт **Создать** → **Общая папка**. Окно мастера создания общей папки:

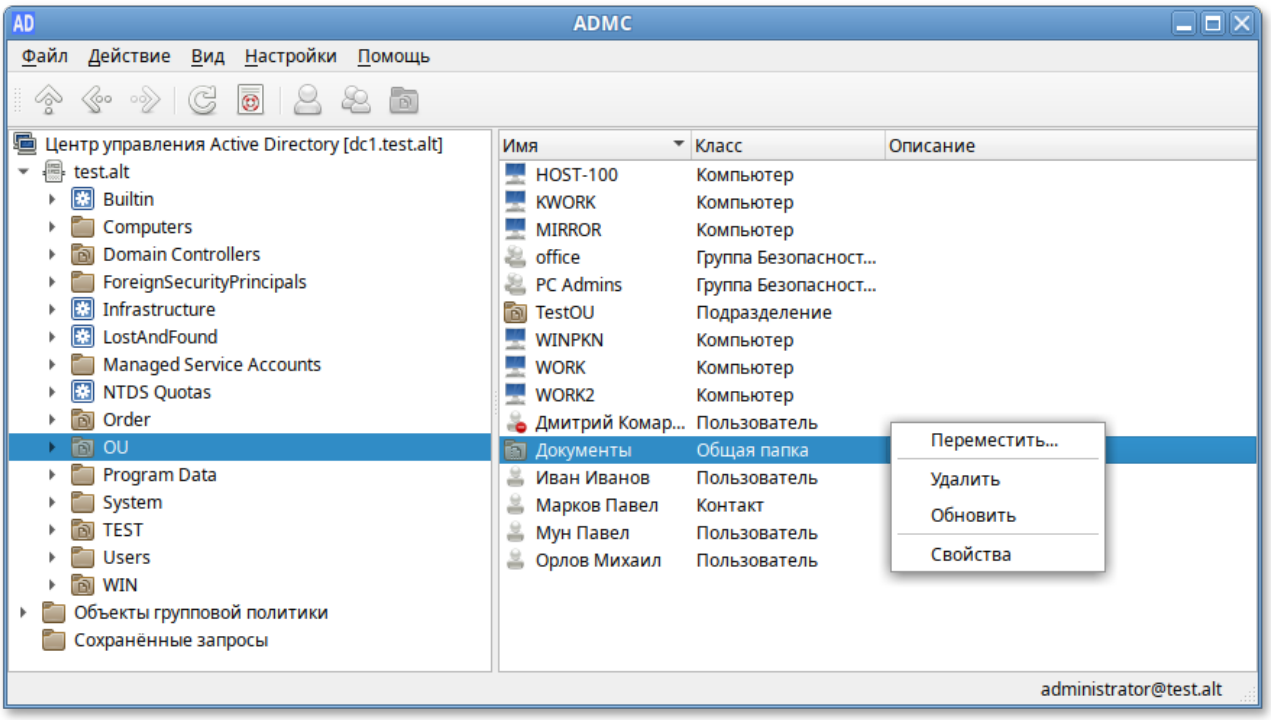


В поле **Имя** следует ввести название папки, под которым она будет отображаться в каталоге AD, а в поле **Сетевой путь** — полный сетевой путь к общей папке.

Примечание

Чтобы просмотреть содержимое общей папки, на машине Windows в дереве консоли управления «Active Directory — пользователи и компьютеры» в контекстном меню общей папки следует выбрать пункт **Проводник**. Откроется новое окно **Проводника**, в котором будет показано содержимое общей папки.

Для изменения общей папки следует в контекстном меню общей папки выбрать соответствующее действие:

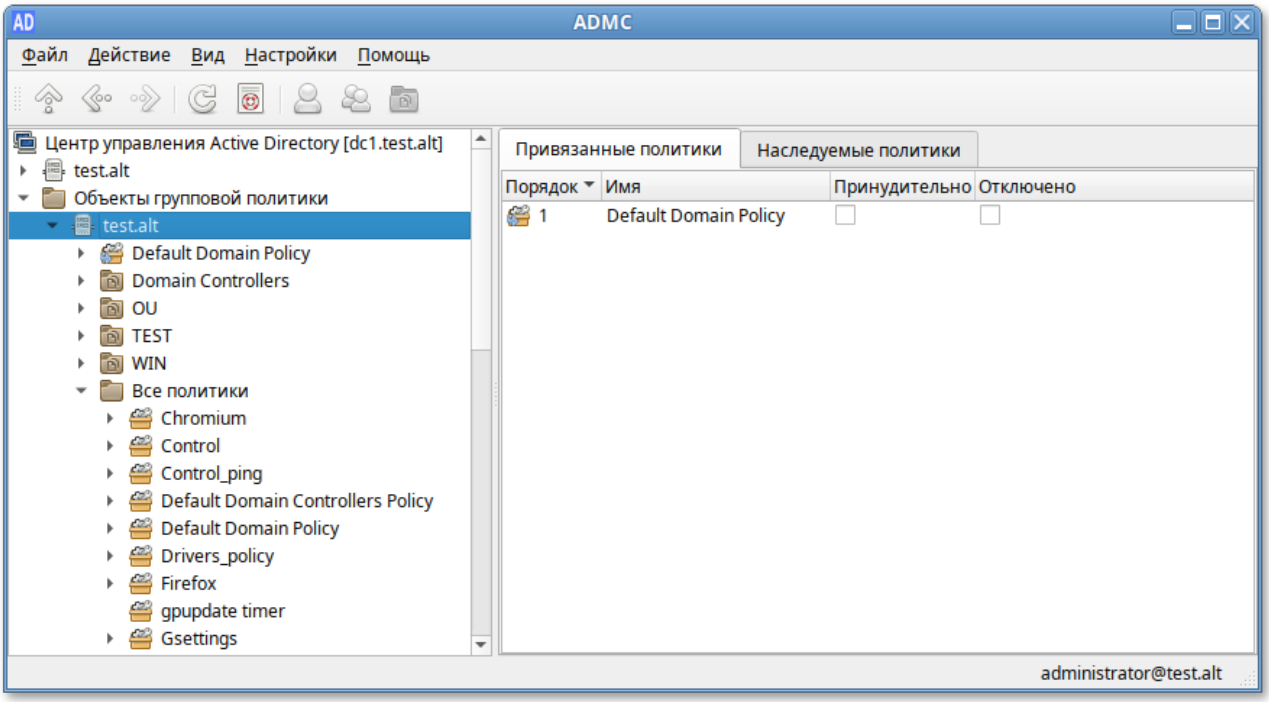


28.13. Управление объектами групповых политик

Групповая политика состоит из набора политик, называемых объектами групповой политики. Для вступления настроек в силу, объект групповой политики необходимо связать с одним или несколькими контейнерами AD. Любой объект групповой политики может быть связан с несколькими контейнерами, и, наоборот, с конкретным контейнером может быть связано несколько объектов групповой политики. Контейнеры наследуют объекты групповой политики, например, объект групповой политики, связанный с подразделением, применяется ко всем пользователям и компьютерам в его дочерних подразделениях. Аналогичным образом, объект групповой политики, применяемый к OU, применяется не только ко всем пользователям и компьютерам в этом OU, но и наследуется всем пользователям и компьютерам в дочерних OU.

ADMC позволяет управлять объектами групповых политик: создавать, удалять, создавать ссылки на групповые политики.

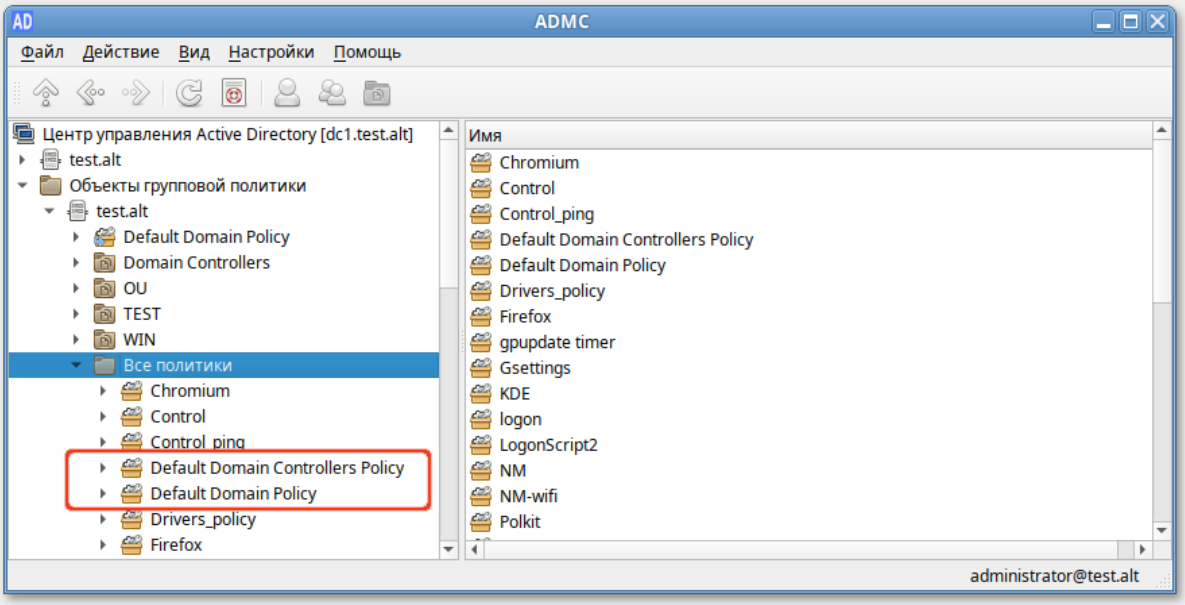
В разделе **Объекты групповой политики** отображаются групповые политики, которые назначены на различные OU (отображается вся структура OU). Полный список политик (GPO) в текущем домене доступен в разделе **Все политики**.



Примечание

В каждом домене Active Directory по умолчанию создаются два объекта групповой политики, которые действуют на все компьютеры и контроллеры домена соответственно:

- Default Domain Policy;
- Default Domain Controller Policy.



Эти объекты групповой политики очень важны, поэтому не рекомендуется вносить в них изменения без крайней необходимости.

Групповые политики Active Directory можно назначить на OU или весь домен. Чаще всего политики привязываются к OU с компьютерами или пользователями.

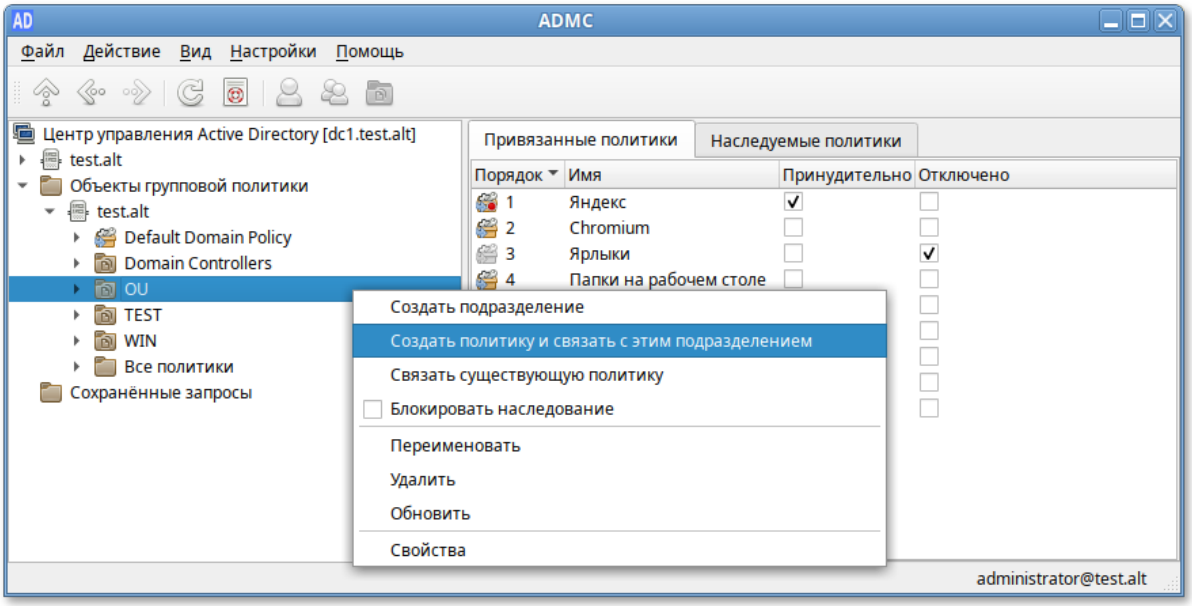
Примечание

Редактирование групповых политик реализуется в модуле редактирования настроек клиентской конфигурации (GPUI).

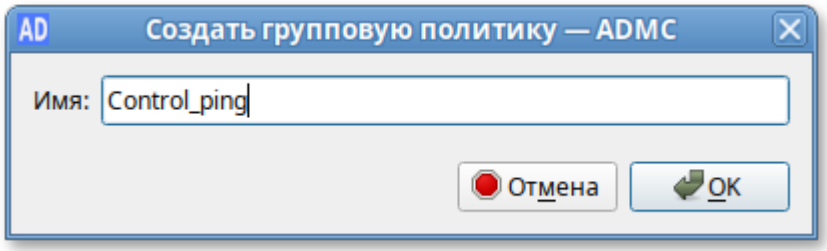
28.13.1. Создание объекта групповой политики

Для того чтобы создать новый объект групповой политики и сразу назначить его на OU, необходимо выполнить следующие действия:

1. В контекстном меню нужного контейнера выбрать пункт **Создать политику и связать с этим подразделением**:



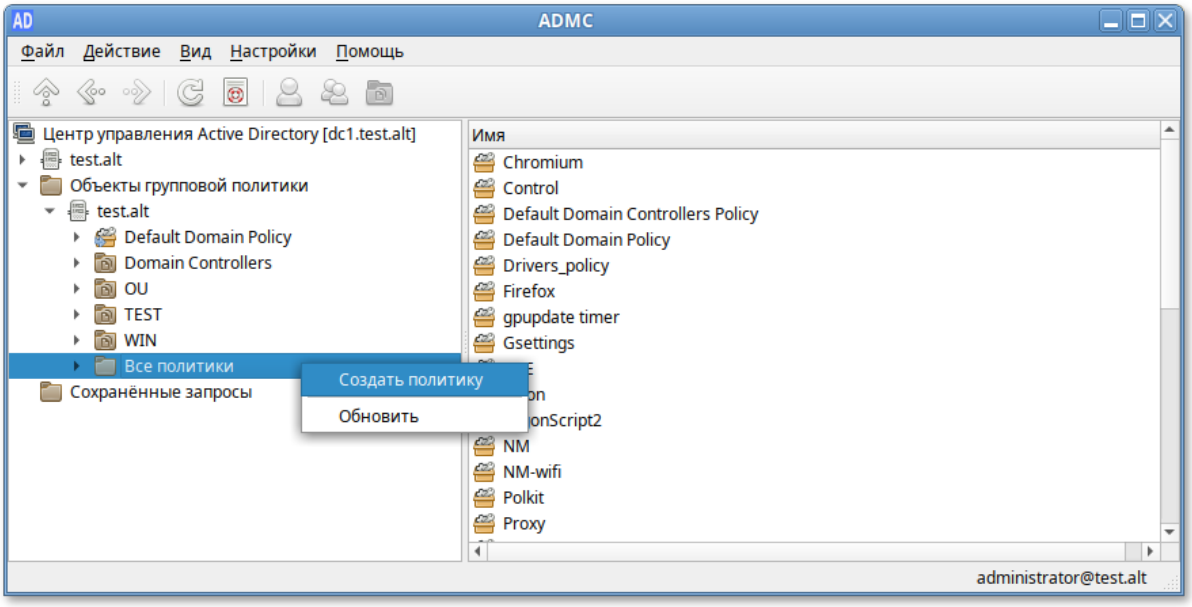
2. В открывшемся окне задать имя политики:



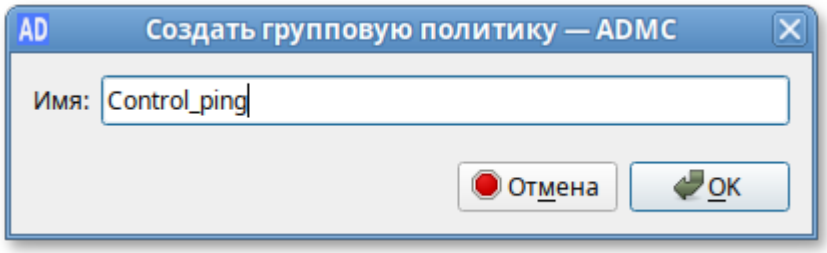
3. Нажать кнопку **OK**.

Для того чтобы создать новый объект групповой политики, не назначая его на OU, необходимо выполнить следующие действия:

1. В контекстном меню папки **Все политики** выбрать пункт **Создать политику**:



2. В открывшемся окне задать имя политики:

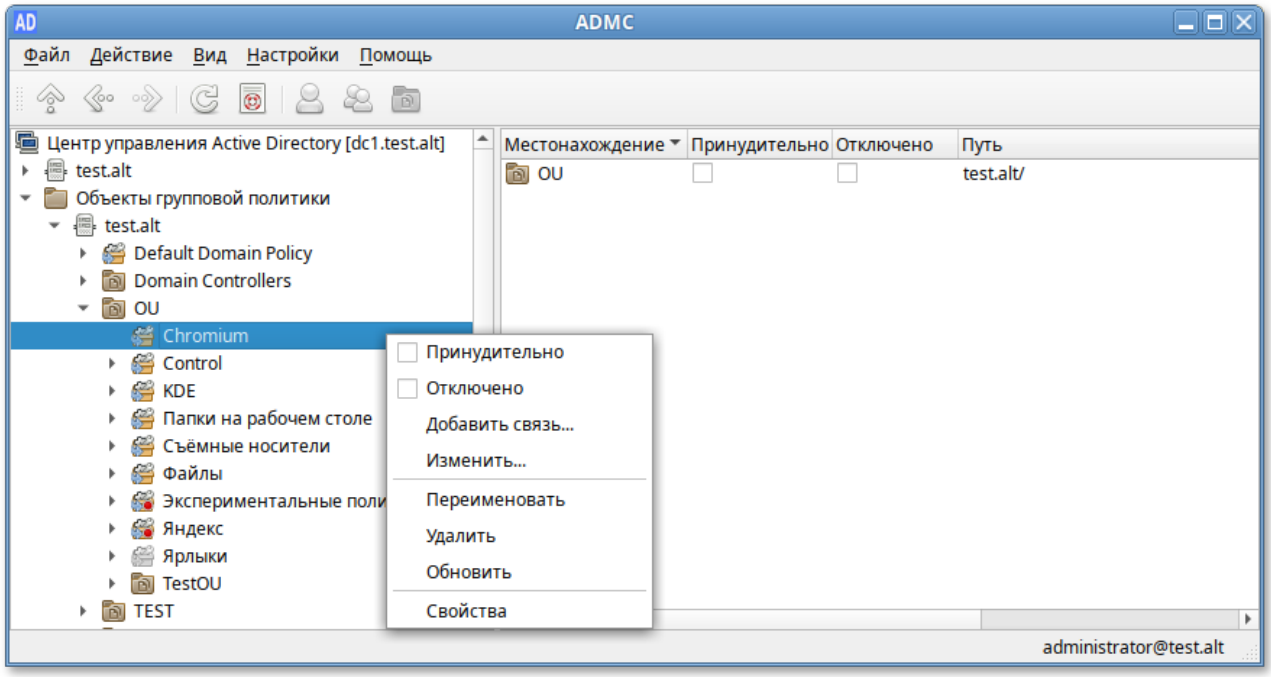


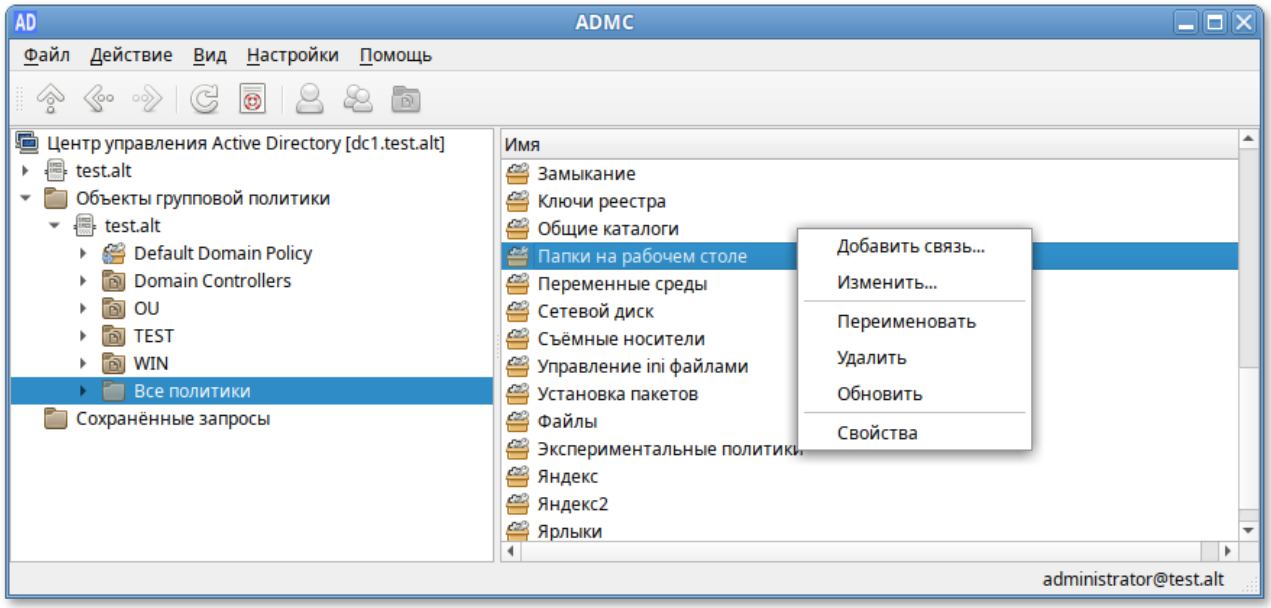
3. Нажать кнопку **OK**.

Созданный объект групповой политики не будет задействован, пока не будет привязан к подразделению.

28.13.2. Изменение объекта групповой политики

Для изменения объекта групповой политики следует в контекстном меню политики выбрать соответствующее действие:



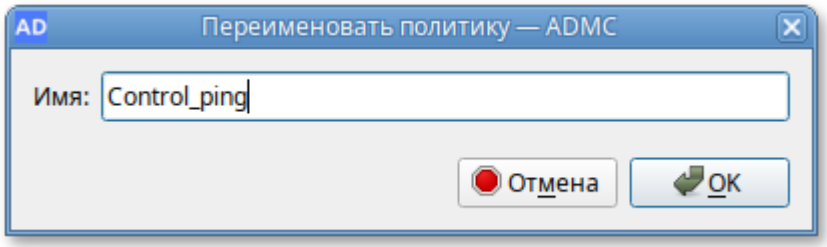


28.13.2.1. Переименование объекта групповой политики

Для переименования политики:

1. В контекстном меню политики выбрать пункт **Переименовать**.

2. В открывшемся окне ввести новое название:

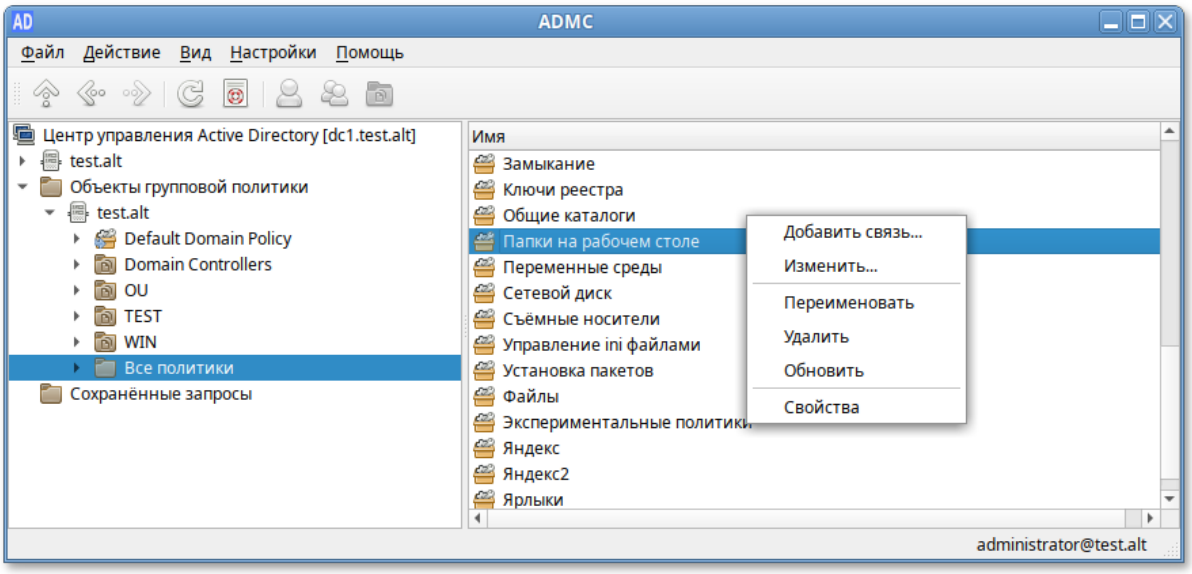


3. Нажать кнопку **OK** для сохранения изменений.

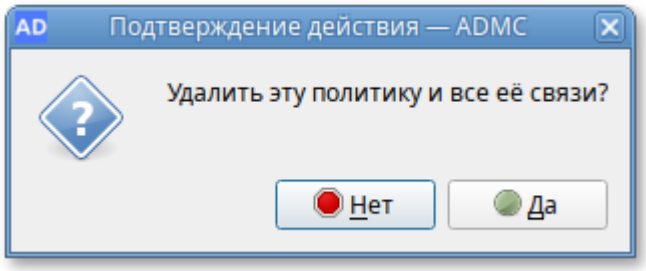
28.13.2.2. Удаление объекта групповой политики

Для удаления политики:

1. В контекстном меню политики в разделе **Все политики** выбрать пункт **Удалить**:

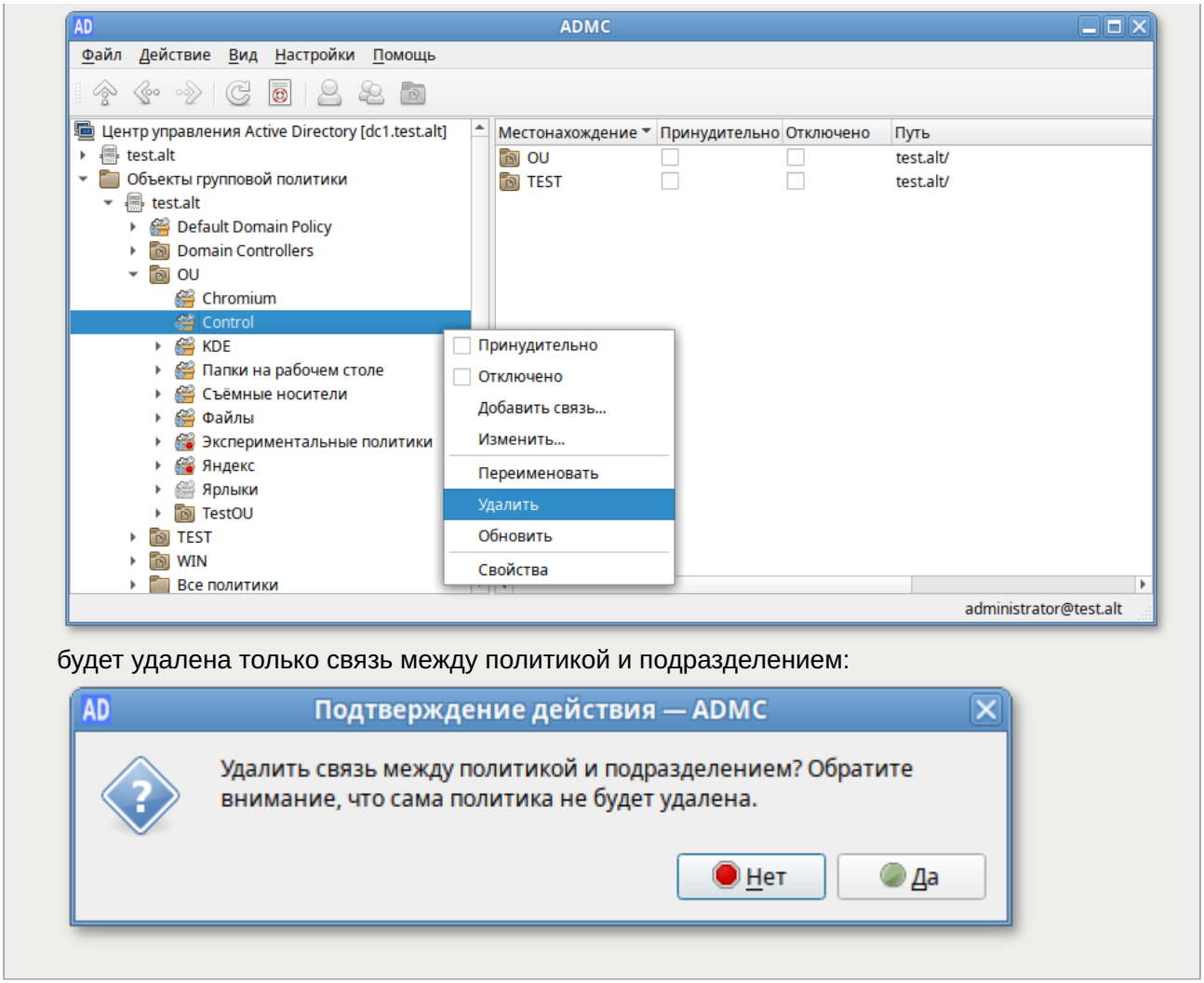


2. Подтвердить удаление, нажав кнопку **Да**:



Примечание

Если выбрать пункт **Удалить** в контекстном меню политики в подразделении, на которое она назначена:



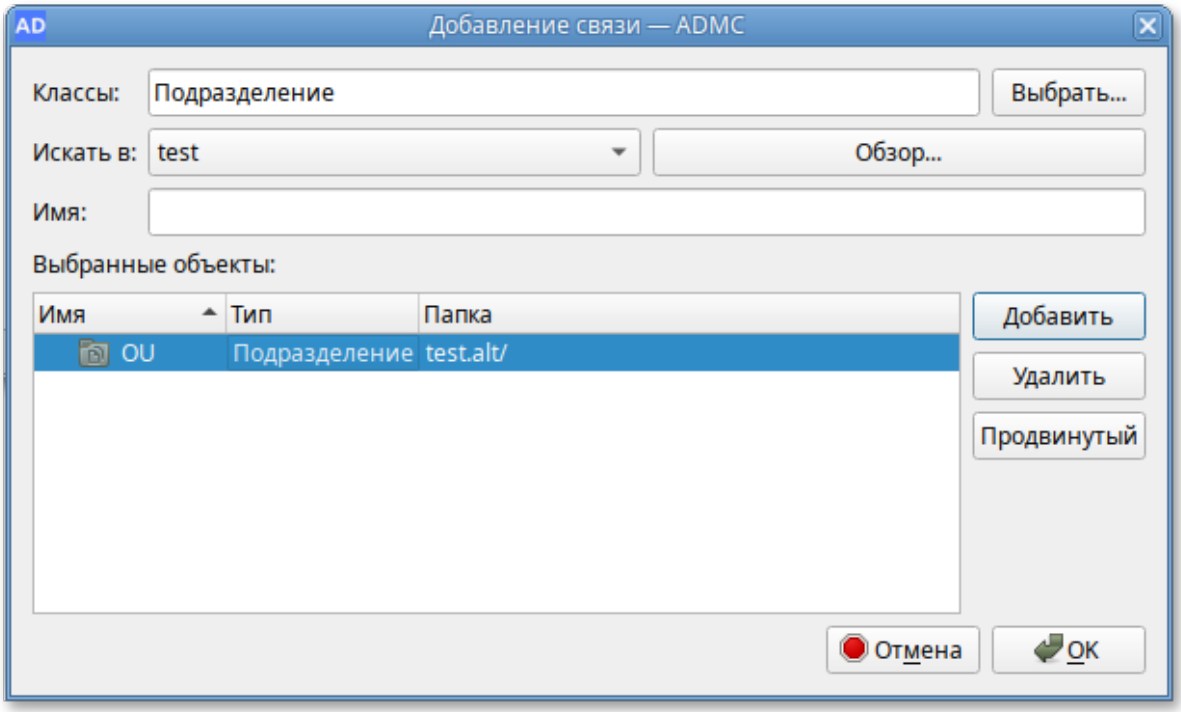
будет удалена только связь между политикой и подразделением:

28.13.2.3. Создание и удаление связи между политикой и подразделением

Для создания связи между политикой и подразделением (создания ссылки на политику):

1. В контекстном меню политики выбрать пункт **Добавить связь…**.

2. Выбрать объекты, которые необходимо связать с политикой:

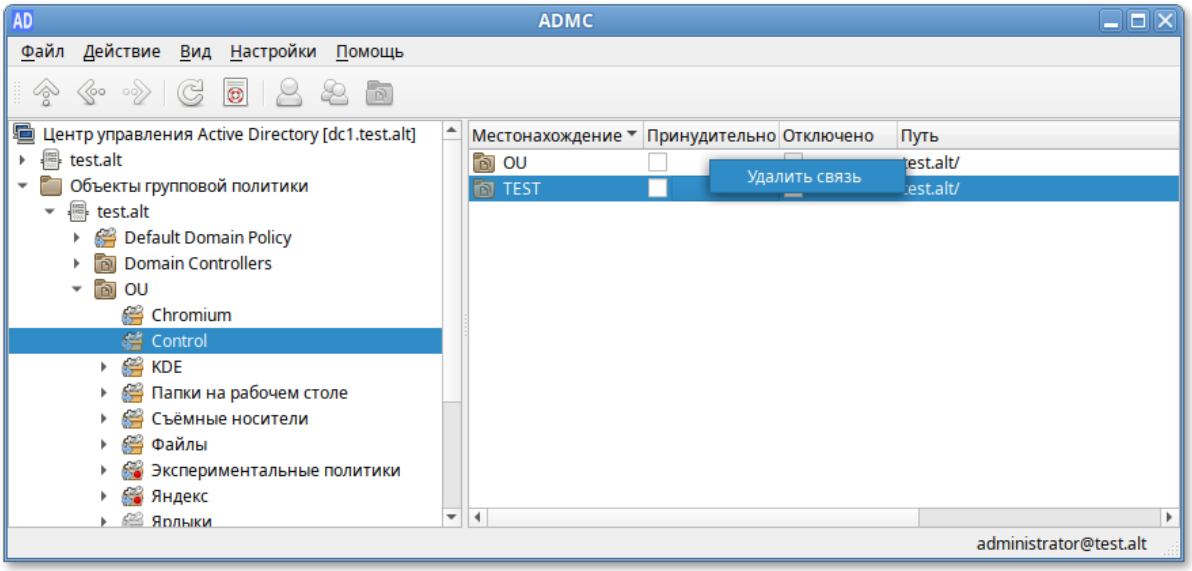


3. Нажать кнопку **ОК**.

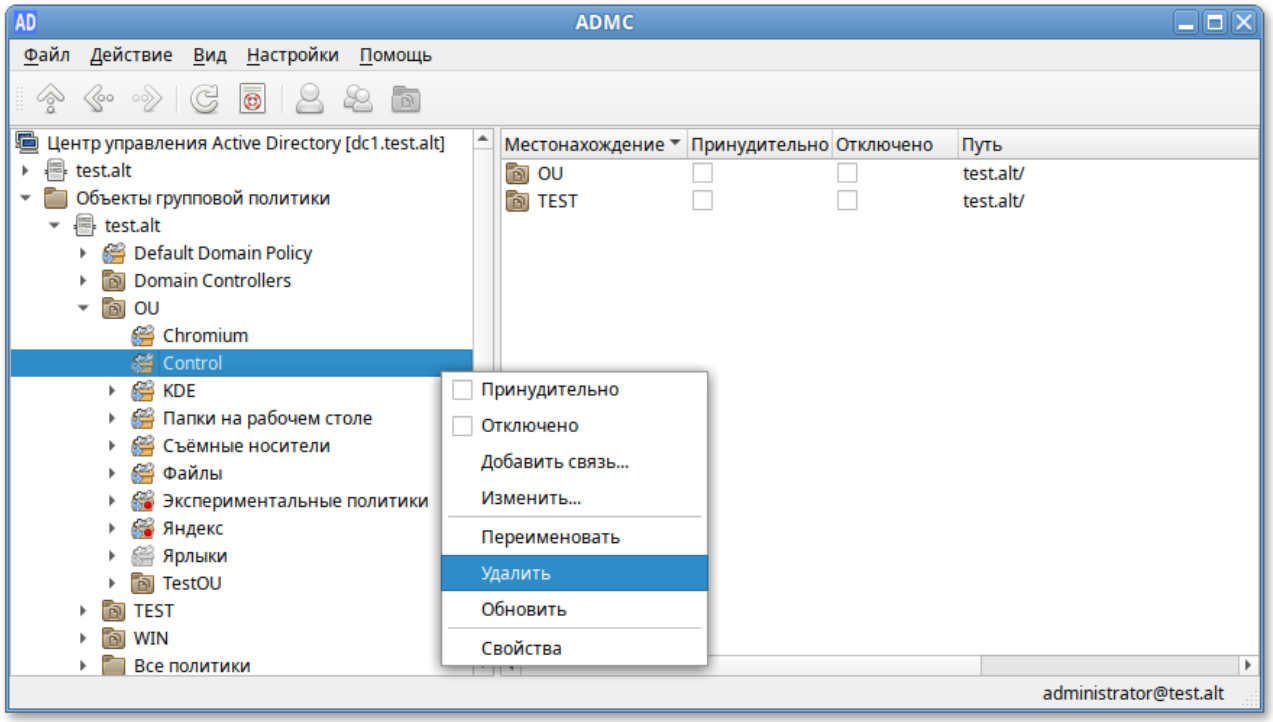
Для удаления ссылки на объект групповой политики:

1. Выбрать политику, которую следует изменить (в папке **Все политики** или в папке соответствующего OU).

2. В контекстном меню подразделения, связь с которым нужно отключить от политики, выбрать пункт **Удалить связь**:



Удалить связь между политикой и подразделением также можно, выбрав пункт **Удалить** в контекстном меню политики в подразделении, на которое она назначена:



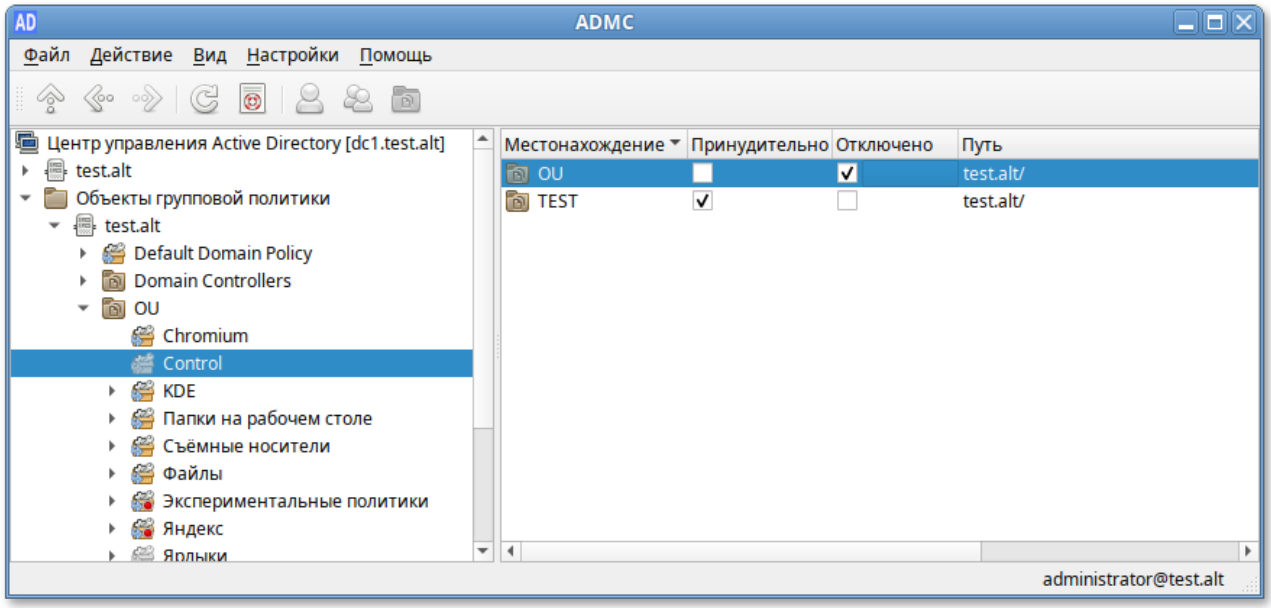
28.13.2.4. Параметры ссылки на объект групповой политики

В ADMC можно изменить параметры ссылки на объект групповой политики:

- опция **Принудительно** — принудительное применение политик более высокого уровня к объекту;
- опция **Отключено** — временно отключить связь политики с подразделением.

Чтобы отредактировать параметры ссылки, необходимо:

1. Выбрать политику, которую следует отредактировать.
2. На панели результатов найти подразделение, для которого нужно изменить параметры ссылки.
3. Включить опцию **Принудительно**, чтобы запретить переопределение параметров политик (см. Блокирование наследования). Политика, с включённой опцией **Принудительно**, отображается в списке политик с красным кружком.
4. Включить опцию **Отключено**, чтобы временно отключить действие политики. Отключённая политика, в списке политик отображается серым цветом.

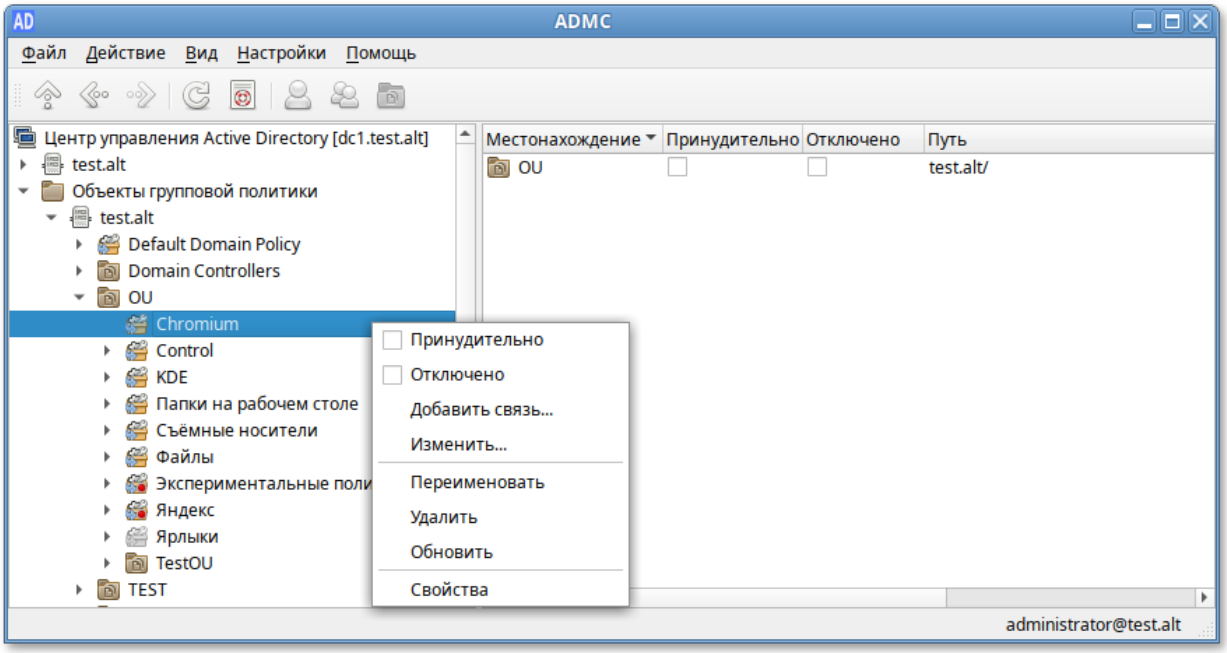


Примечание

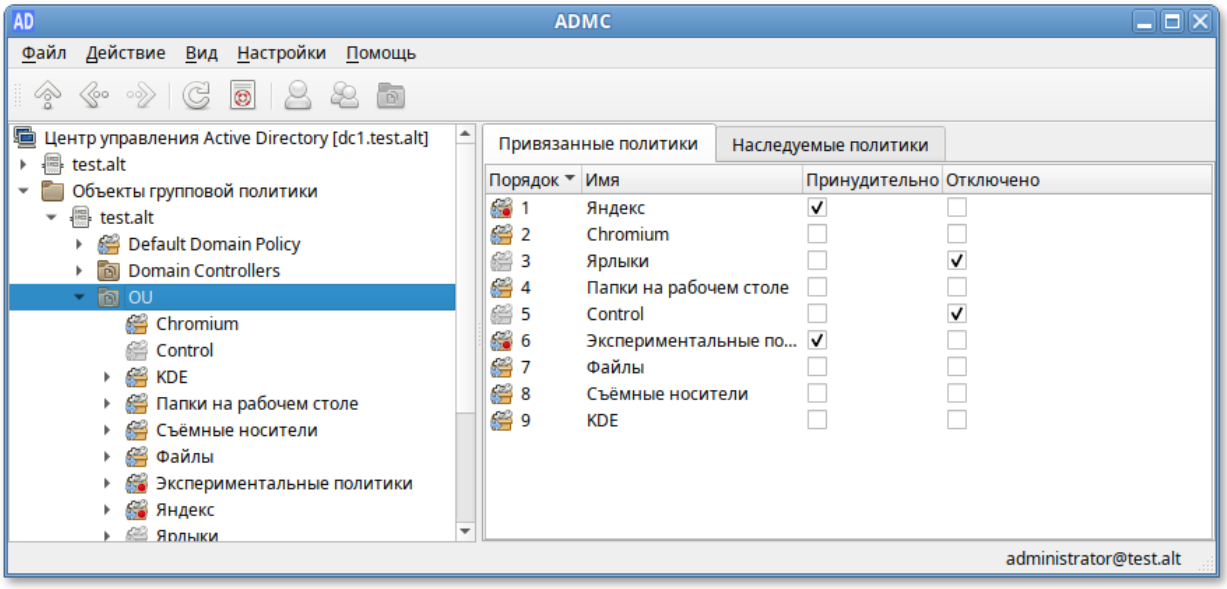
Если необходимо, чтобы политика перестала действовать на клиентов в данном подразделении, можно либо удалить ссылку (при этом сам объект ГП не будет удален), либо временно отключить действие политики.

Включить/отключить опции **Принудительно** и **Отключено** также можно:

- в контекстном меню политики в подразделении:



- на вкладке **Привязанные политики** подразделения:



28.13.2.5. Редактирование настроек групповой политики

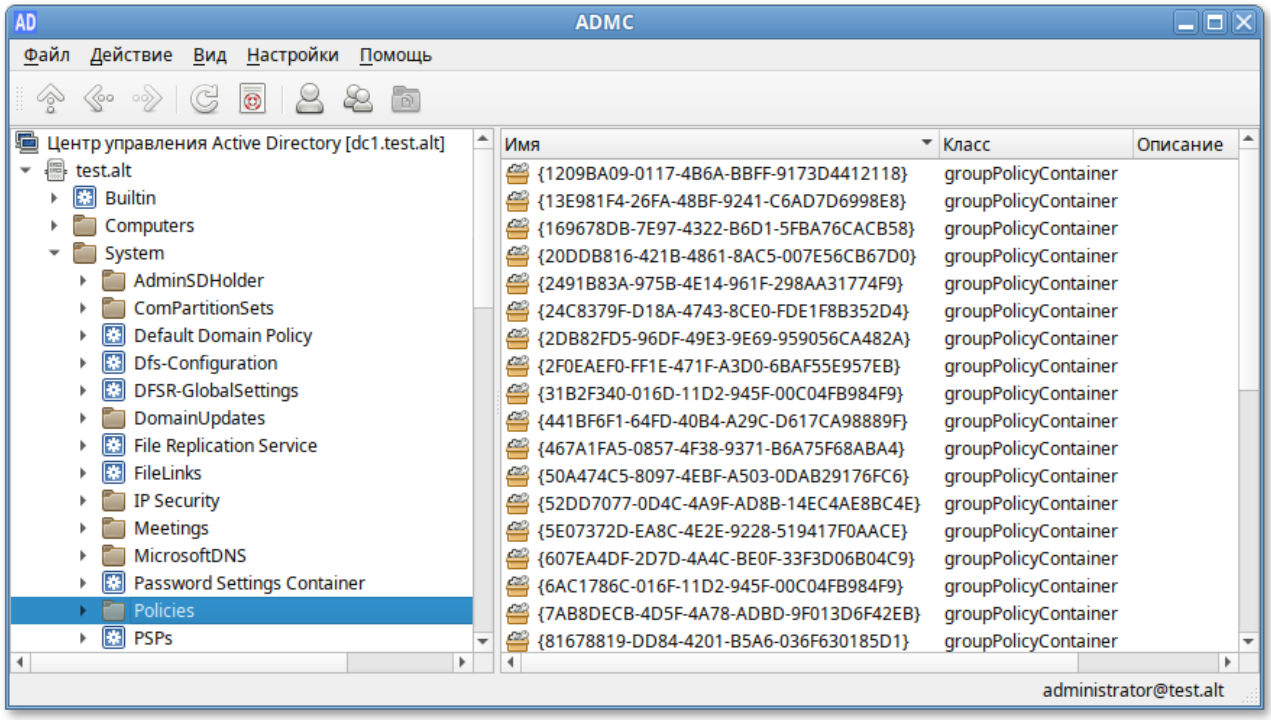
Примечание

Для возможности редактирования настроек политики, на машине должен быть установлен модуль редактирования настроек клиентской конфигурации (GPUI).

Для изменения настроек политики необходимо в контекстном меню политики выбрать пункт **Изменить…**, будет запущен модуль редактирования настроек клиентской конфигурации, где можно изменить параметры групповой политики.

При создании каждого нового объекта групповой политики, в базе данных AD создается контейнер групповой политики (Group Policy Container, GPC). Для возможности просмотра контейнера групповой политики (это дочерний контейнер Policies контейнера System) в настройках ADMC должен быть отмечен пункт **Дополнительные возможности**.

В AD контейнер групповой политики создается как тип groupPolicyContainer, причем его GUID можно увидеть в ADMC в столбце **Имя**:



Ниже перечислены некоторые атрибуты, позволяющие описать различные типы данных объекта групповой политики:

- displayName — атрибут, определяющий имя объекта групповой политики;
- gPCFileSysPath — атрибут, указывающий путь к расположению текущего шаблона групповой политики с соответствующим именем GUID;
- gPCMachineExtensionNames — атрибут, определяющий список расширений клиентской стороны конфигурации компьютера, используемых для обработки объекта групповой политики. Значение атрибута выглядит следующим образом: [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F72-3407-48AE-BA88-E8213C6761F1}], что представляет собой [{GUID CSE-расширения}{GUID расширения MMC}{GUID второго расширения MMC}][GUID-идентификаторы последующих CSE- и MMC-расширений];
- gPCUserExtensionNames — атрибут, определяющий список расширений клиентской стороны конфигурации пользователя, используемых для обработки объекта групповой политики;
- versionNumber — в этом атрибуте определен номер версии контейнера GPC объекта групповой политики, который, для осуществления синхронизации двух объектов, должен быть идентичным с номером версии шаблона групповой политики;
- flags — состояние объекта групповой политики: объект GPO включен (значение 0), отключен раздел «Конфигурация пользователя» (значение 1), отключен раздел «Конфигурация компьютера» (значение 2), объект GPO полностью отключен (значение 3).

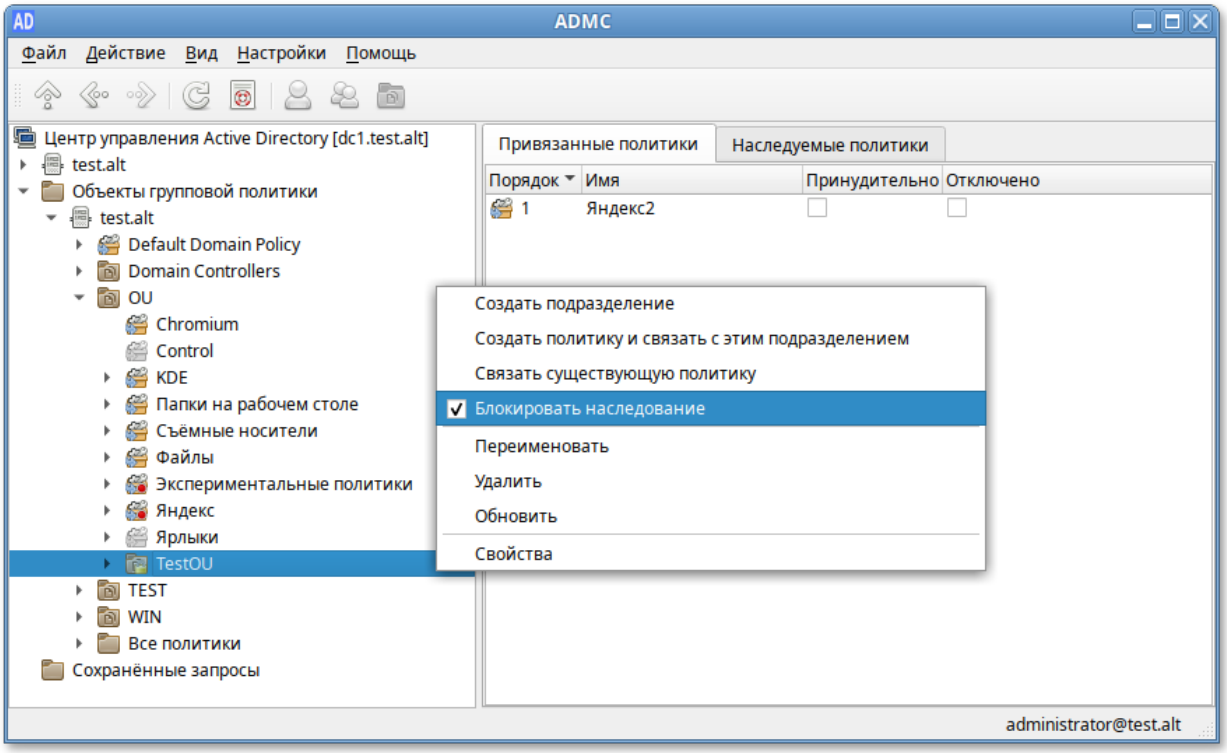
Примечание

Вручную изменять атрибуты объекта групповой политики не рекомендуется.

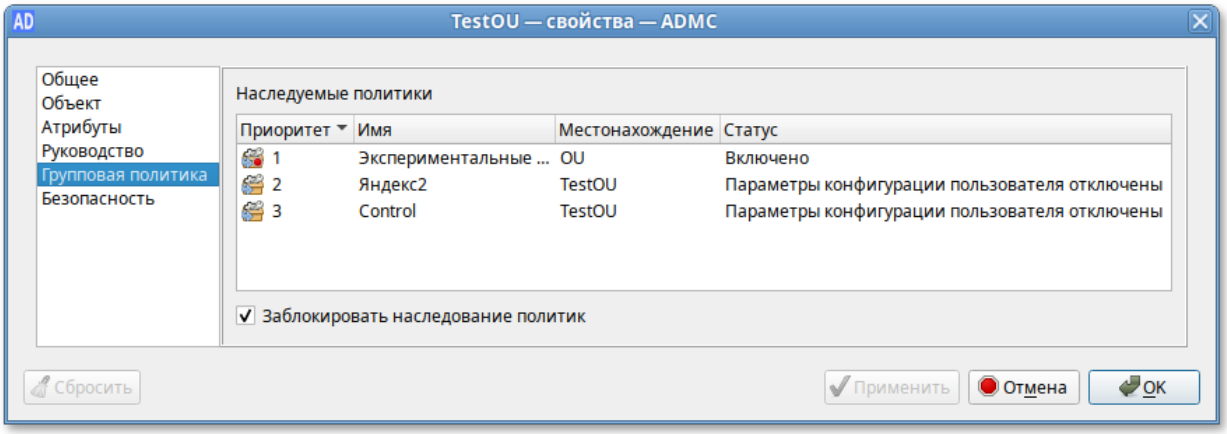
28.13.3. Блокирование наследования

Для того чтобы параметры групповой политики, определенные на уровне вышестоящих контейнеров, не распространялись на содержимое конфигурируемого контейнера, необходимо выполнить одно из следующих действий:

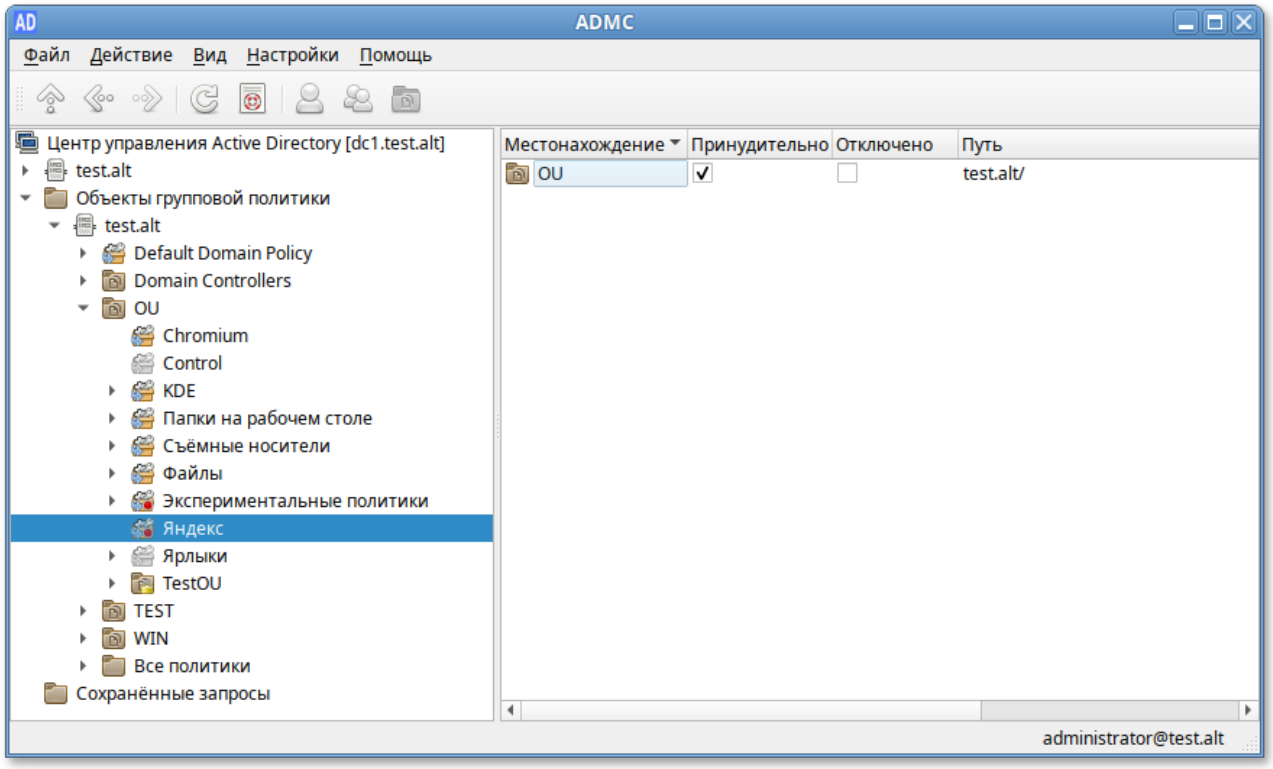
- в контекстном меню контейнера, к которому привязан объект групповой политики установить отметку **Блокировать наследование**:



- в окне свойств контейнера, к которому привязан объект групповой политики, на вкладке **Групповая политика** установить отметку **Заблокировать наследование политик**:



Так как администратор домена может не согласиться с тем, что администратор подразделения блокирует параметры политики домена, существует возможность запретить переопределение параметров с помощью отметки **Принудительно**:



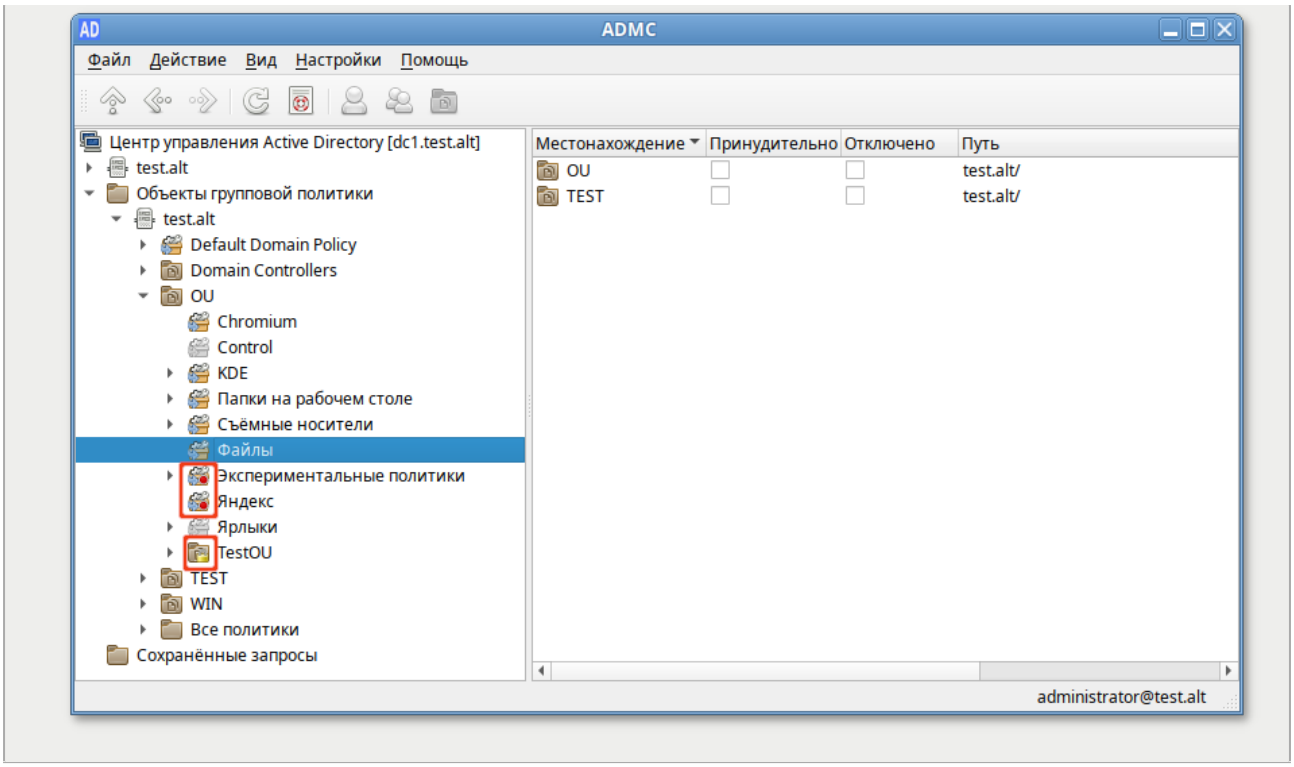
Отметка в поле **Принудительно** означает, что связь установлена принудительно. Это приведёт к принудительному применению политик более высокого уровня к объектам более низкого уровня, например, применение политики домена ко всем дочерним подразделениям, или применения политики сайта ко всем доменам и подразделениям в пределах сайта.

При использовании параметра **Принудительно** выигрывает та политика, которая находится выше в иерархии домена (например, политика Default Domain Policy будет выигрывать у всех других ГП, если у неё активирован параметр **Принудительно**).

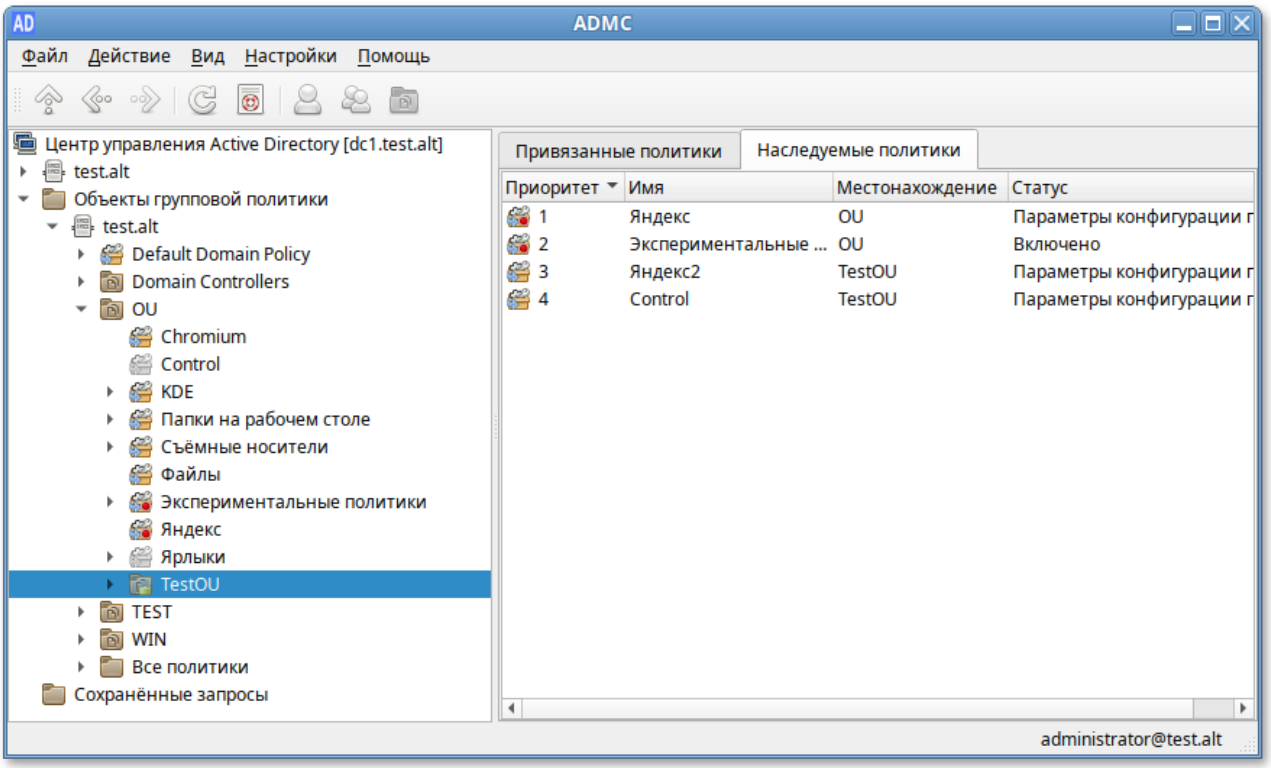
Примечание

Подразделение с блокированным наследованием отображается в дереве консоли со значком замка.

После установки параметра **Принудительно**, на значке групповой политики появится красный кружок, означающий, что для данной политики запрещено переопределение параметров.



На вкладке **Наследуемые политики** подразделения можно увидеть, какие политики применяются к подразделению, а также местонахождение политики:



28.13.4. Фильтрация безопасности ГП

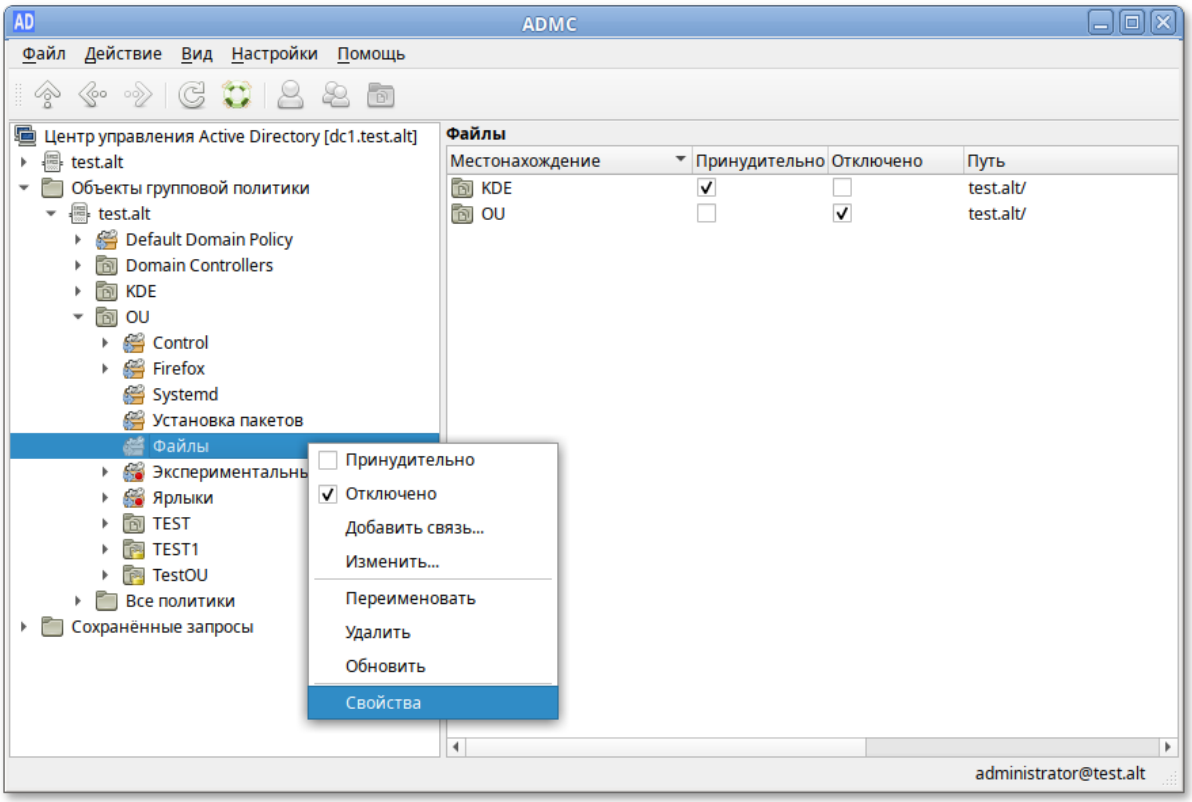
Фильтрация безопасности ГП (Security Filtering) предполагает выборочное применение параметров ГП к конкретным пользователям, компьютерам или группам на основе их разрешений безопасности.

По умолчанию, когда объект ГП связан с OU, он применяется ко всем пользователям и компьютерам в этой OU. Фильтрация безопасности позволяет администраторам сузить область применения объекта ГП, гарантируя, что только определенные объекты будут затронуты политиками, определенными в объекте групповой политики.

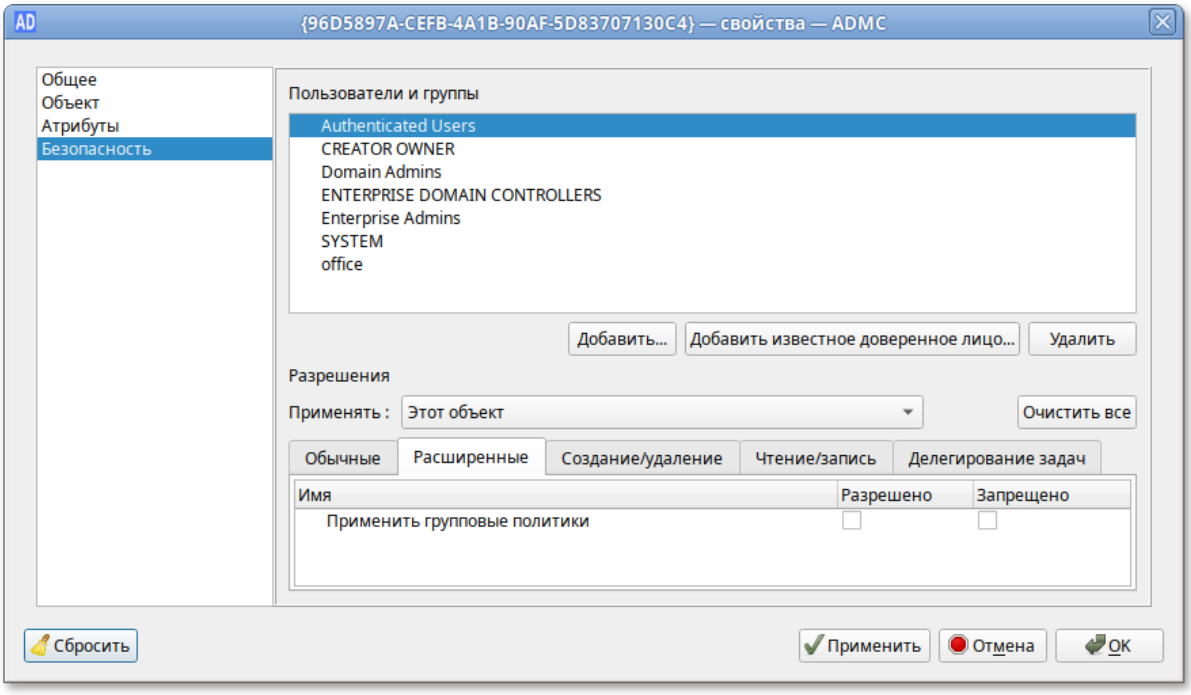
По умолчанию на всех новых объектах групповой политики в домене присутствуют разрешения для группы **`Authenticated Users`**, которая включает в себя всех пользователей и все компьютеры домена. Это означает, что данная политика будет применяться на всех компьютерах и для всех пользователей, которые попадают в область её действия.

Если необходимо сузить круг объектов, к которым будет применяться данная политика, то следует выполнить следующие действия:

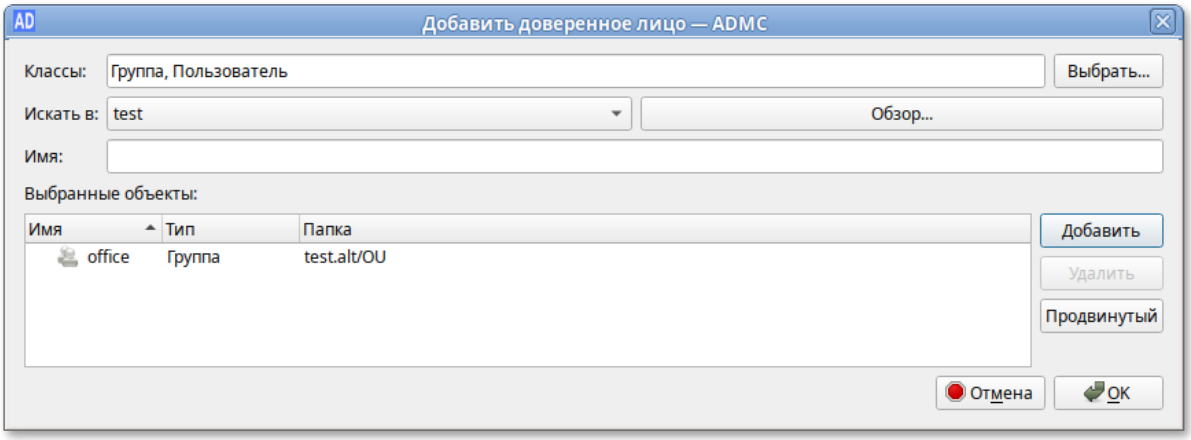
1. В контекстном меню групповой политики выбрать пункт **Свойства**:



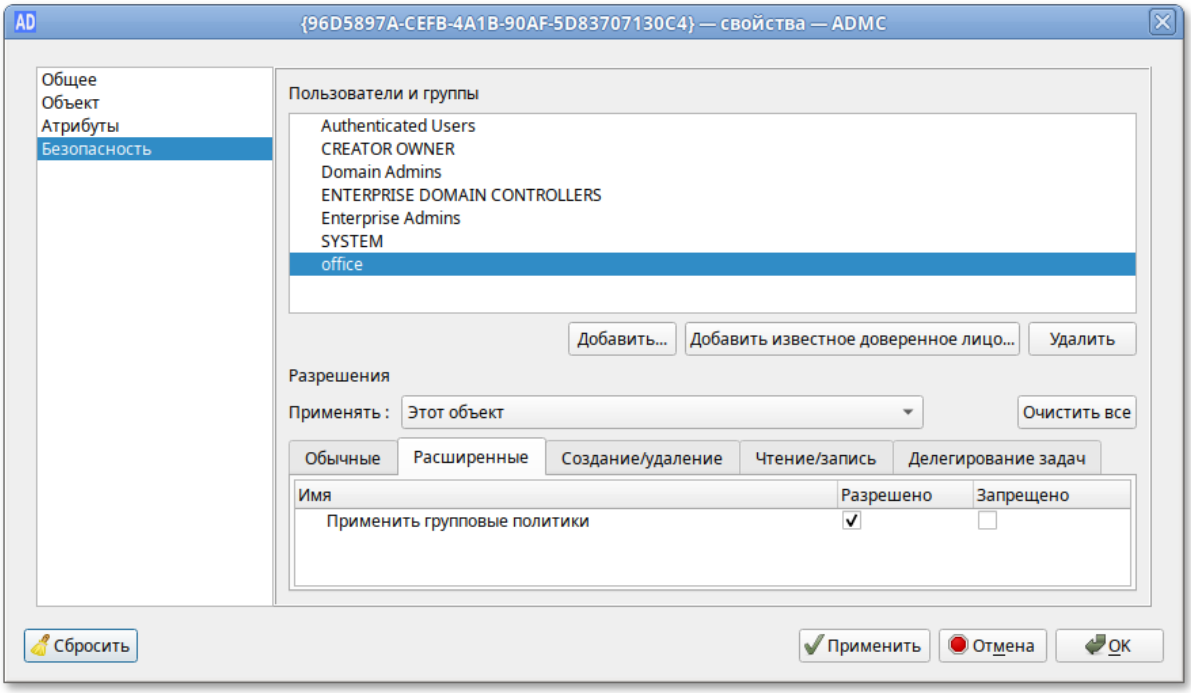
2. Перейти на вкладку **`Безопасность`**. У группы **`Authenticated Users`** убрать разрешение на применение групповых политик (в разделе **`Разрешения`** на вкладке **`Расширенные`** снять отметку с пункта **`Применить групповые политики`** в столбце **`Разрешено`**):



3. Добавить объект, к которому будет применяться групповая политика. Для этого нажать **Добавить…** и выбрать необходимый объект (можно выбрать пользователя, компьютер или группу). В данном примере будет добавлена группа **`office`**:



4. Для добавленного объекта выставить разрешения **`Читать`** (вкладка **Обычные**) и **`Применить групповые политики`** (вкладка **Расширенные**) и нажать кнопку **Применить**:

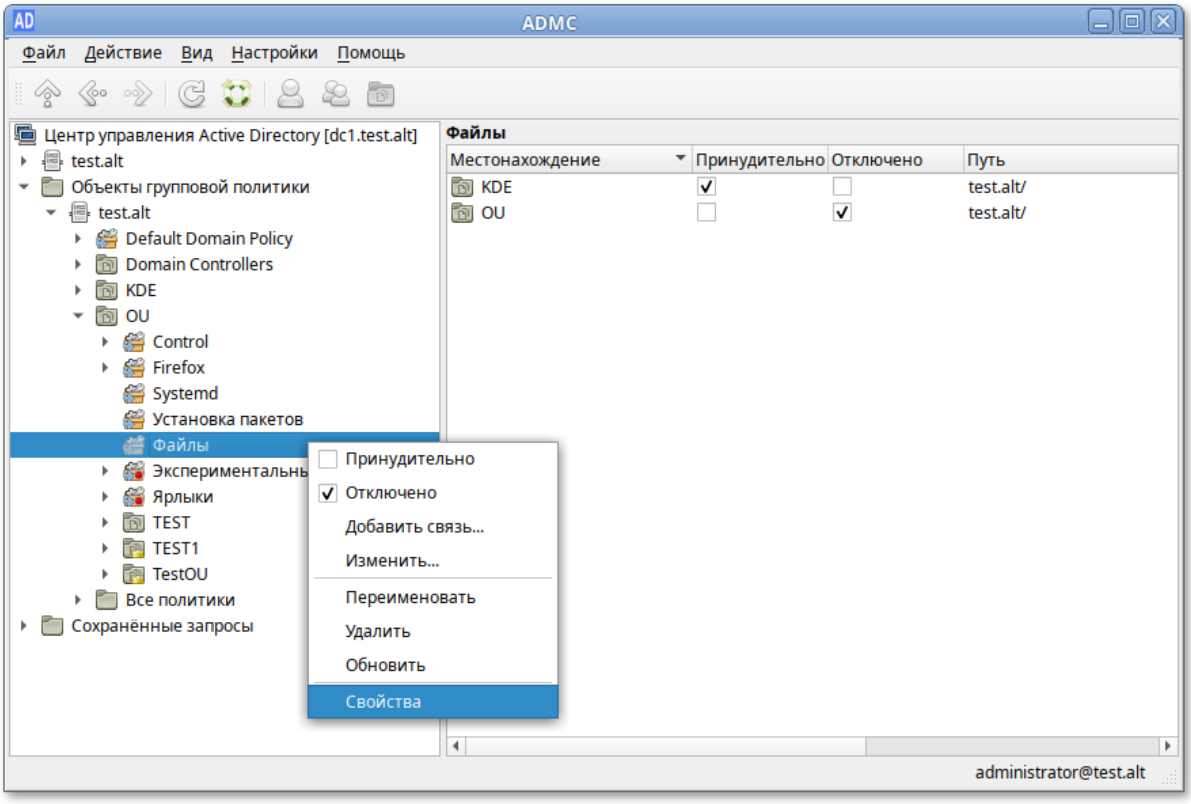


Примечание

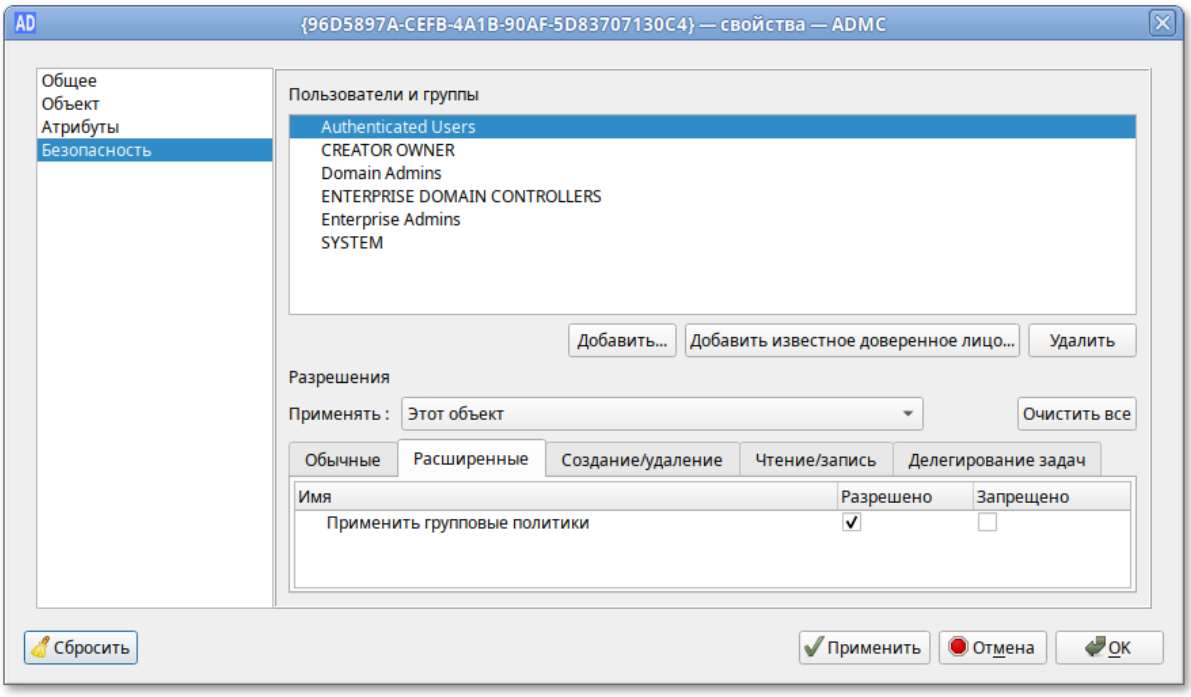
Если выставить все разрешения, групповые политики применяться не будут.

Чтобы определенному объекту запретить применение групповой политики, следует выполнить следующие действия:

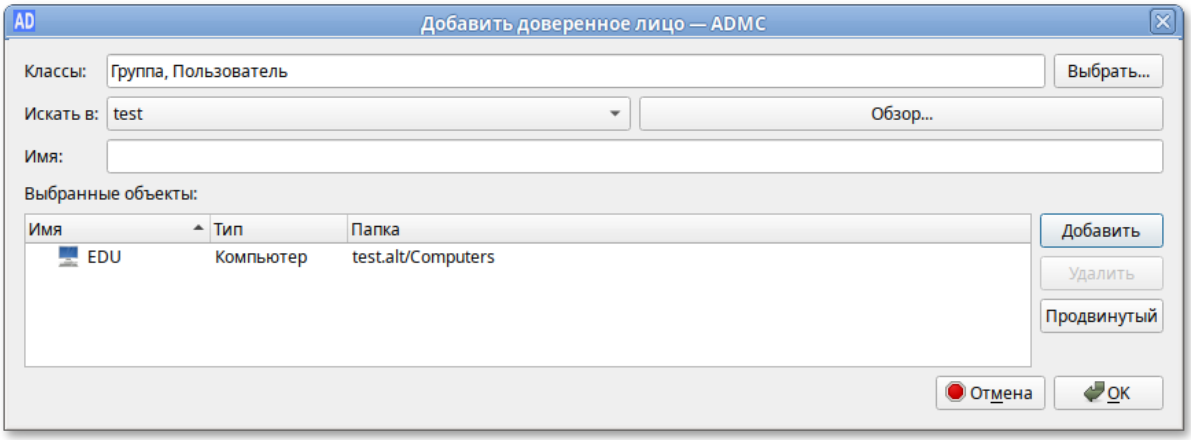
1. В контекстном меню групповой политики выбрать пункт **Свойства**:



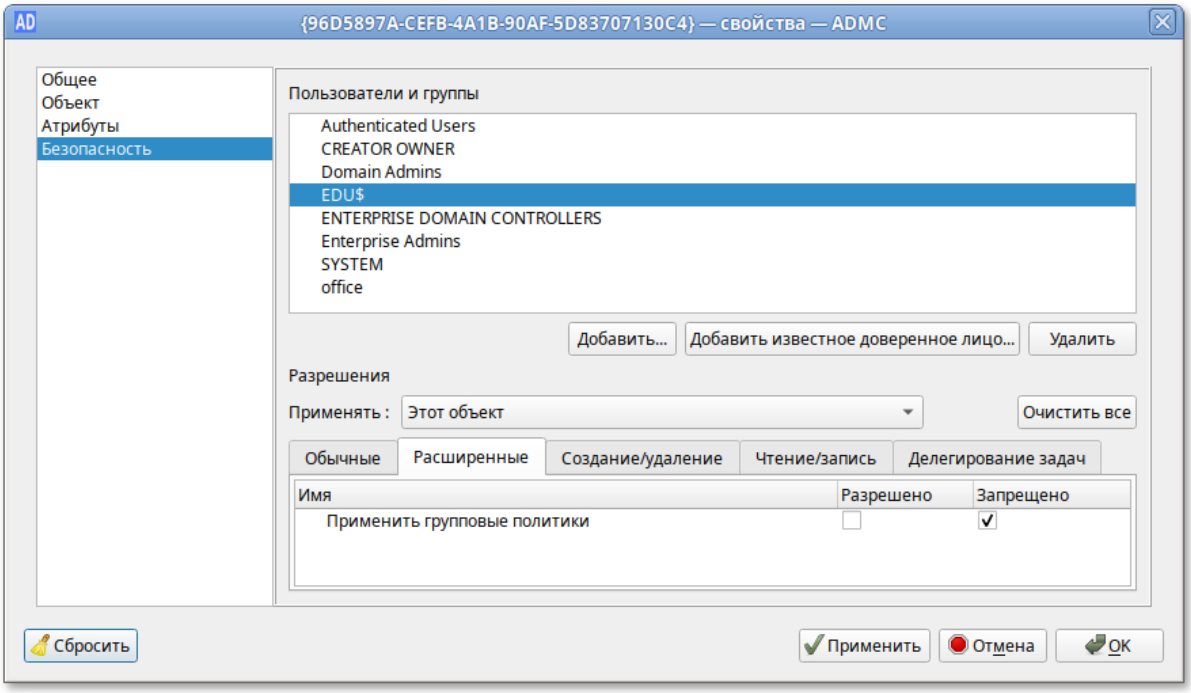
2. Перейти на вкладку **Безопасность**. У группы **Authenticated Users** оставить разрешение на применение групповых политик (не снимать отметку с пункта **Применить групповые политики** в столбце **Разрешено**):



3. Добавить объект, к которому не будет применяться групповая политика. Для этого нажать **Добавить…** и выбрать необходимый объект (можно выбрать пользователя, компьютер или группу). В данном примере будет добавлен компьютер **EDU**:



4. Для добавленного объекта установить запрет применения групповых политик (установить отметку в пункте **Применить групповые политики** в столбце **Запрещено**) и нажать кнопку **Применить**:

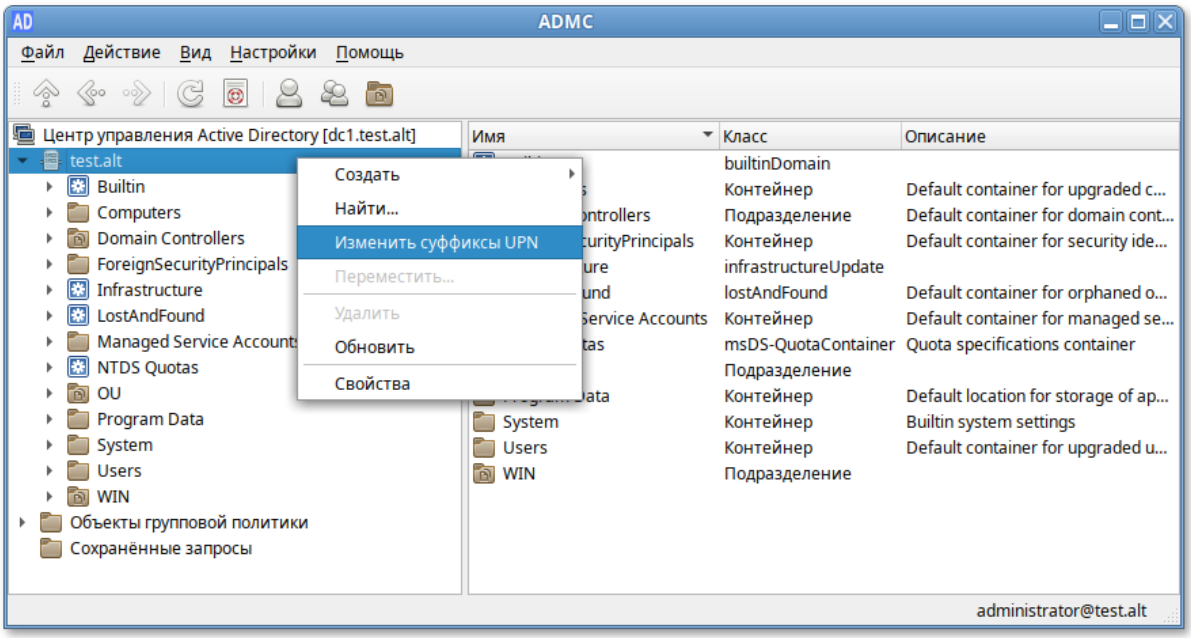


28.14. Добавление/Удаление UPN суффиксов

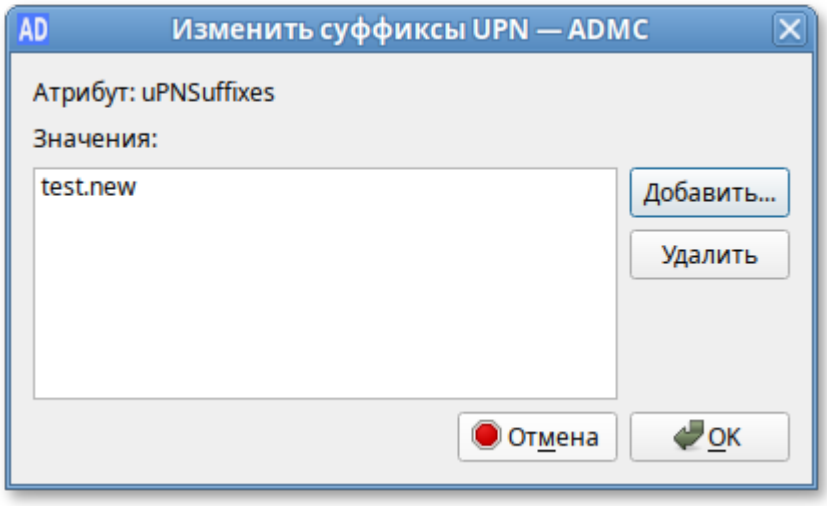
UserPrincipalName (UPN) — имя для входа пользователя в формате email-адреса, например, ivanov@test.alt. Здесь ivanov это UPN-префикс (имя пользователя в домене AD), test.alt — UPN-суффикс. По умолчанию в AD в качестве UPN-суффикса используется DNS имя домена AD. Добавление дополнительных имен доменов позволяет упростить процесс входа и повысить безопасность.

Для того чтобы добавить/удалить дополнительный UPN-суффикс, необходимо выполнить следующие шаги:

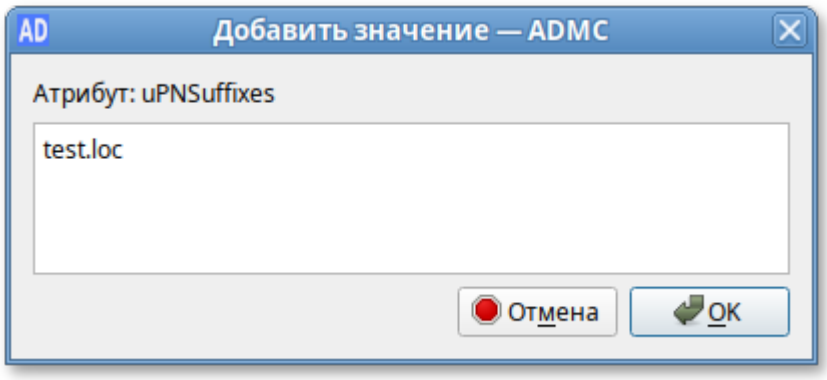
1. В контекстном меню домена выбрать пункт **Изменить суффиксы UPN**:



2. В открывшемся диалоговом окне нажать кнопку **Добавить…**:



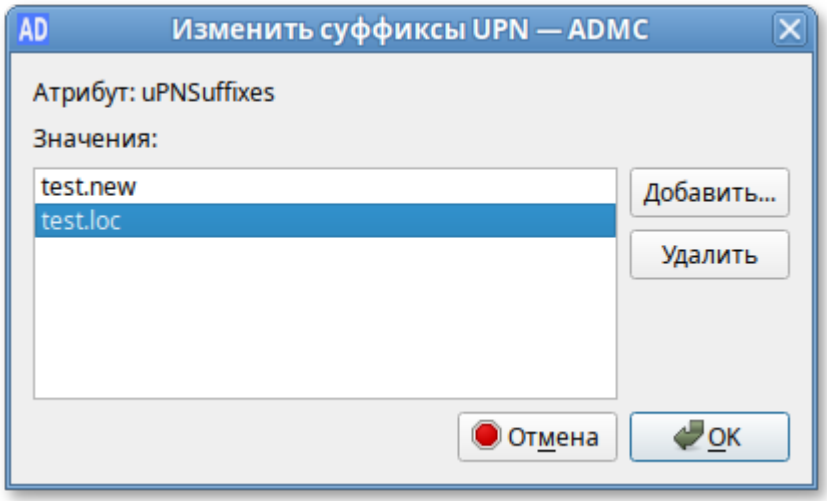
3. Ввести альтернативный суффикс:



Не требуется, чтобы суффикс UPN был действительным DNS-именем домена. Суффиксы UPN должны соответствовать условиям DNS-имен в отношении допустимых символов и синтаксиса.

4. Нажать кнопку **OK**, чтобы добавить новый суффикс в список.

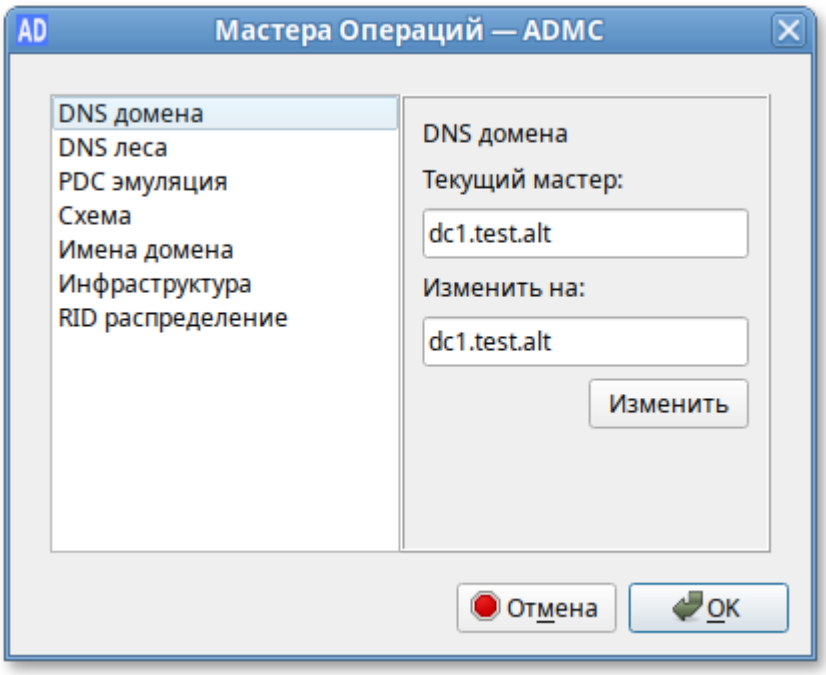
5. Чтобы удалить существующий суффикс, необходимо выбрать его в списке и нажать кнопку **Удалить**:



28.15. Прсмотр и передача ролей FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) — это операции, выполняемые контроллерами домена AD, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера — хозяевами операций.

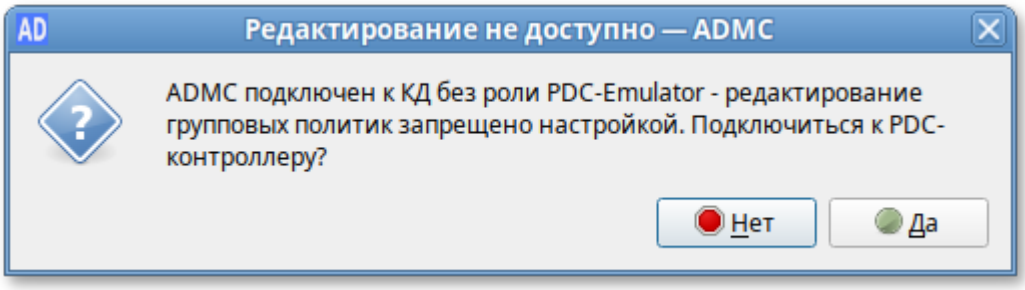
Для просмотра текущего владельца роли необходимо выбрать пункт меню **Файл → Мастера Операций**. В открывшемся окне в списке слева выбрать роль и в поле **Текущий мастер** будет показан владелец роли:



Список возможных ролей:

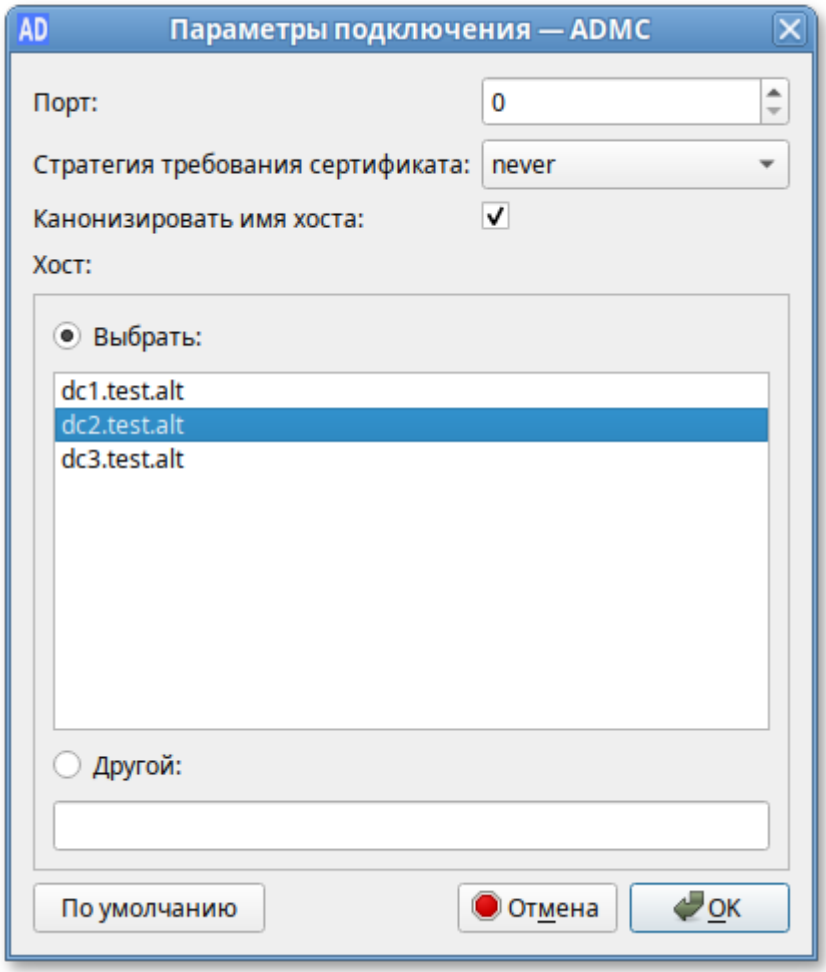
1. **DNS домена** — Domain DNS Zone Master role;
2. **DNS леса** — Forest DNS Zone Master role;
3. **PDC эмуляция** — эмулятор PDC;
4. **Схема** — хозяин схемы;
5. **Имена домена** — хозяин именования доменов;
6. **Инфраструктура** — хозяин инфраструктуры;
7. **RID распределение** — хозяин RID.

Если отмечен пункт **Редактирование политик только с подключением к PDC-Emulator**, при отсутствии подключения к контроллеру домена с ролью PDC-эмуляции, действия, затрагивающие шаблоны групповых политик (редактирование/изменение/удаление политик) будут запрещены:

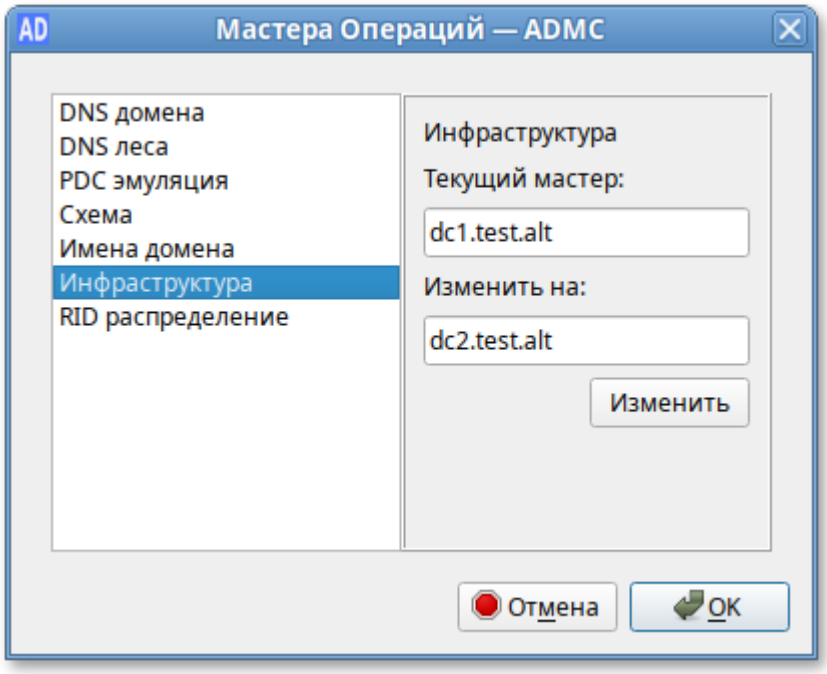


Для штатной передачи роли необходимо выполнить следующие действия:

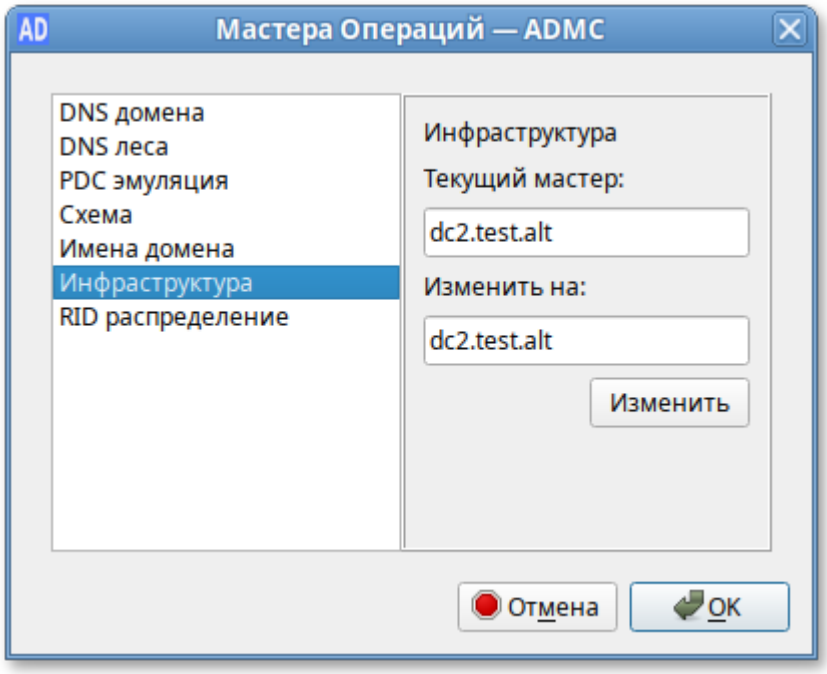
1. В окне **Параметры подключения — ADMC** (**Файл** → **Параметры подключения**) выбрать контроллер домена, который должен стать новым владельцем роли, и нажать кнопку **OK**:



2. В окне **Мастера Операций — ADMC** (**Файл** → **Мастера Операций**) выбрать роль (при этом в поле **Текущий мастер** будет показан текущий владелец роли, а в поле **Изменить на** — контроллер домена, который должен стать новым владельцем роли) и нажать кнопку **Изменить**:

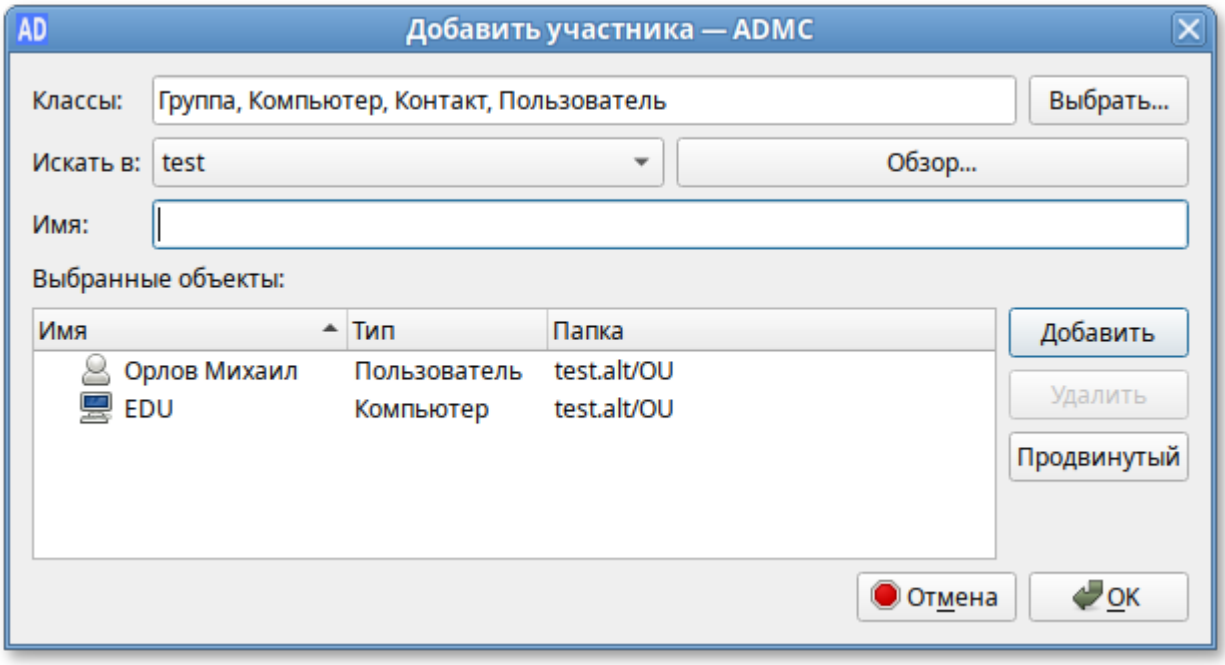


Владелец роли будет изменён:



28.16. Выбор объектов

Выбор объектов осуществляется в диалоговом окне **Выбрать объекты — ADMC**. Доступ к этому диалоговому окну можно получить из разных мест, например при выборе действия **Добавить в группу…** в контекстном меню учётной записи пользователя.



Для выбора объекта достаточно указать класс объекта, выбрать расположение, с которого требуется начать поиск, и в поле **Имя** ввести имена объектов:

1. В поле **Классы**, нажав кнопку **Выбрать…**, выбрать типы объектов, которые будут использоваться для поиска (в большинстве случаев это поле будет заполнено автоматически, в зависимости от контекста задачи).

2. В поле **Искать в** выбрать объект, который будет использоваться в качестве основы для поиска.

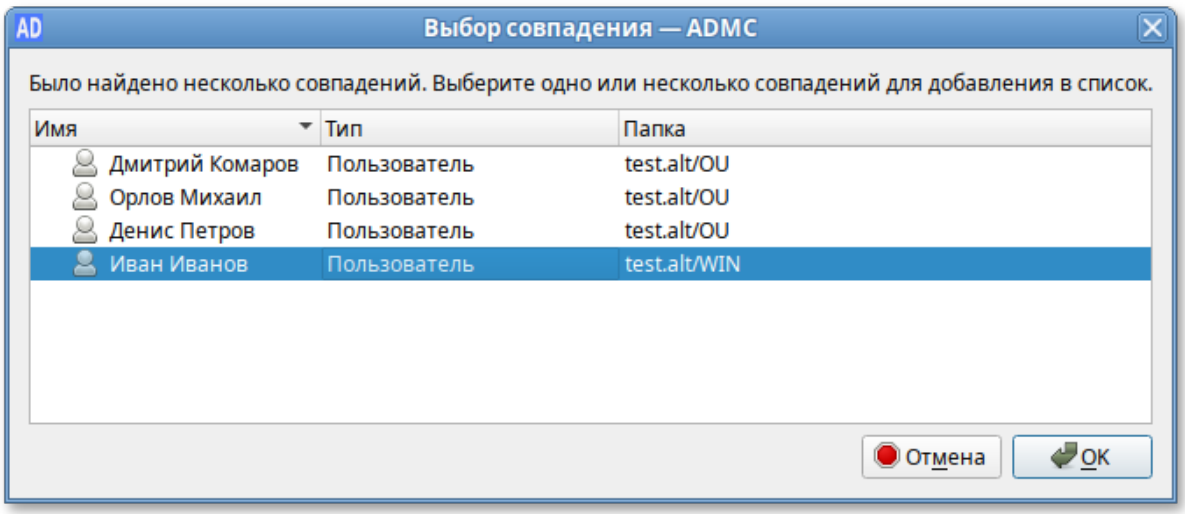
3. В поле **Имя** ввести имя объекта (можно ввести часть имени или выполнить поиск по имени для входа).

4. Нажать кнопку **Добавить** для поиска объекта по названию.

5. Если объект найден, он будет добавлен в список найденных объектов.

6. Если объект не найден, исправить имя и повторить попытку.

7. Если есть несколько совпадений, откроется диалоговое окно, в котором можно выбрать одно или несколько совпадений:



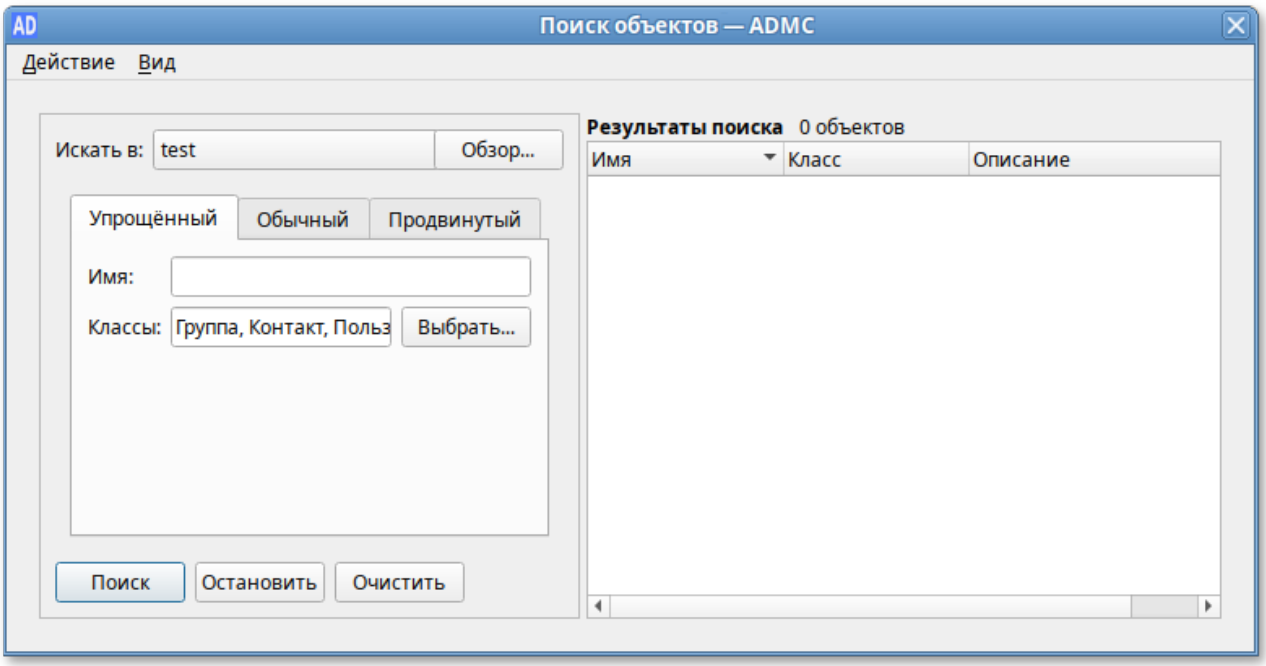
8. Повторить пункты 1-7, пока не будут добавлены все объекты.

9. Чтобы удалить объект из списка, нужно выбрать объект и нажать кнопку **Удалить**.

Для выбора объектов можно также использовать продвинутый поиск, который можно открыть, нажав кнопку **Продвинутый**.

28.17. Поиск объектов

Поиск объектов осуществляется в диалоговом окне **Поиск объектов — ADMC**. Доступ к этому диалоговому окну можно получить, выбрав пункт **Найти...** в меню **>Действие** или в контекстном меню контейнера.



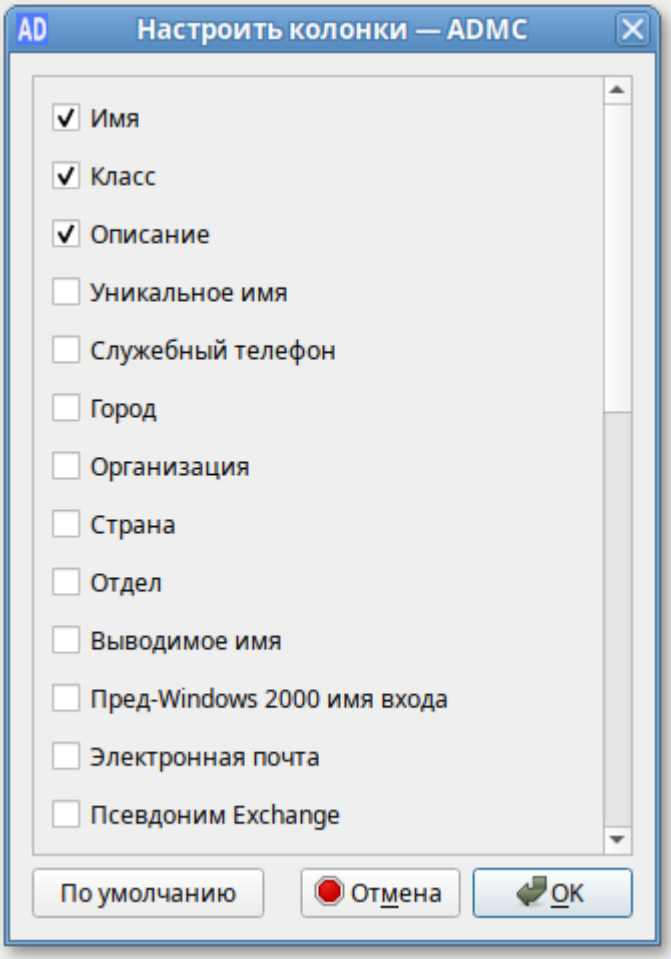
Поиск объектов в домене возможен по разным критериям:

- по типу и имени (простой поиск) — вкладка **Упрощенный**;
- по атрибутам — вкладка **Обычный**;

- в синтаксисе запросов LDAP — вкладка **Продвинутый**.

Примечание

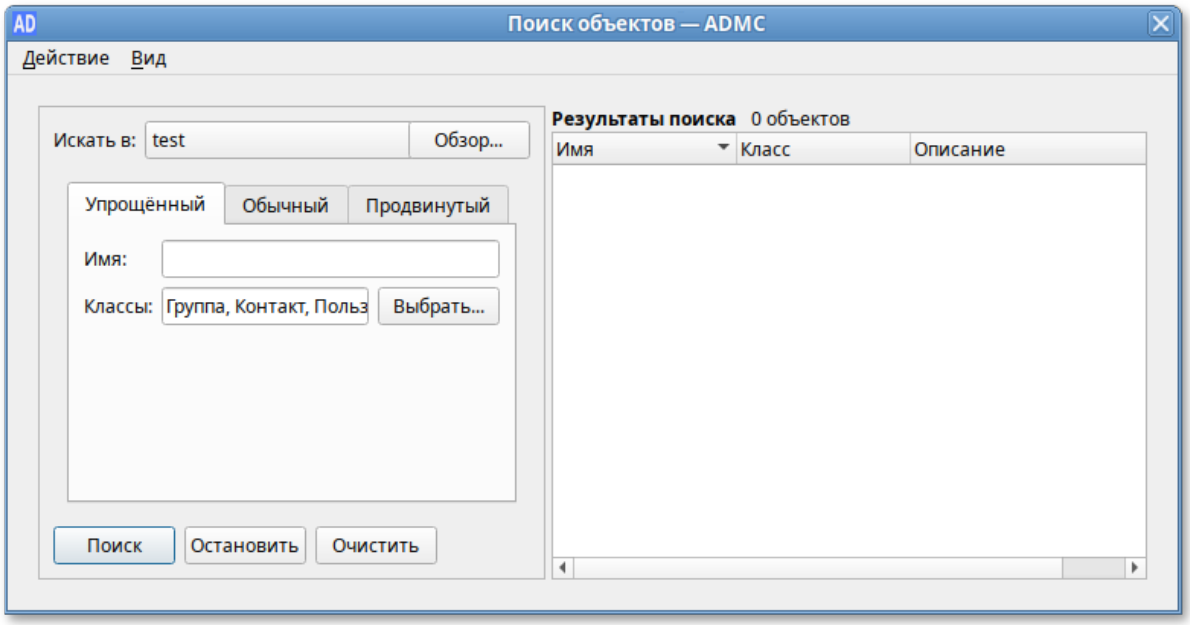
В диалоговом окне, вызываемом меню **Вид** → **Настроить колонки**, можно выбрать поля, которые будут отображаться в списке результатов поиска.



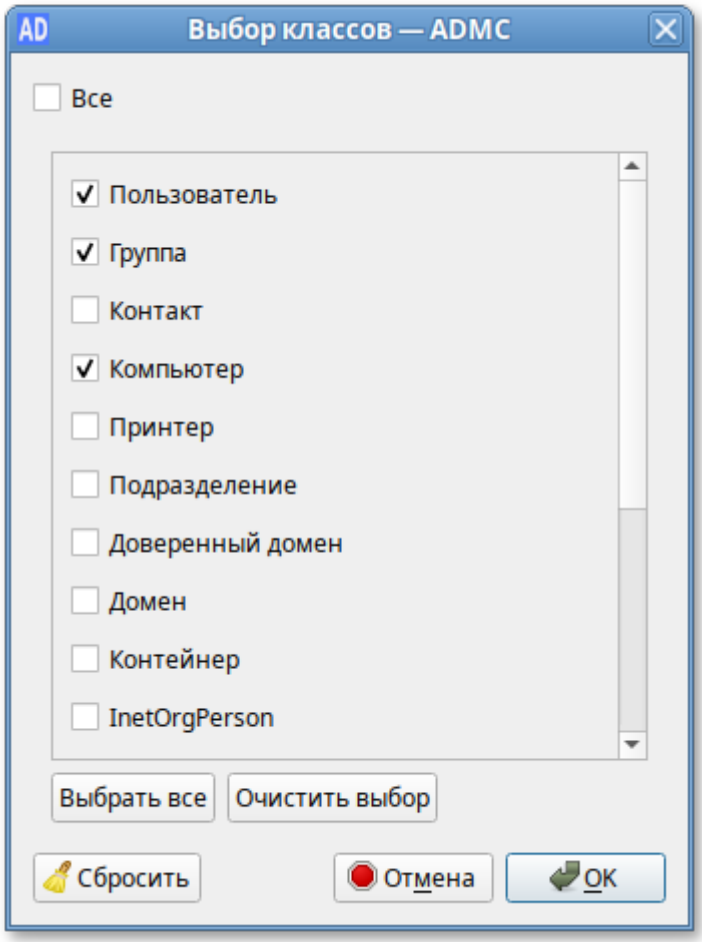
28.17.1. Простой поиск

Процедура простого поиска:

1. В диалоговом окне **Поиск объектов — ADMC** выбрать вкладку **Упрощенный**:

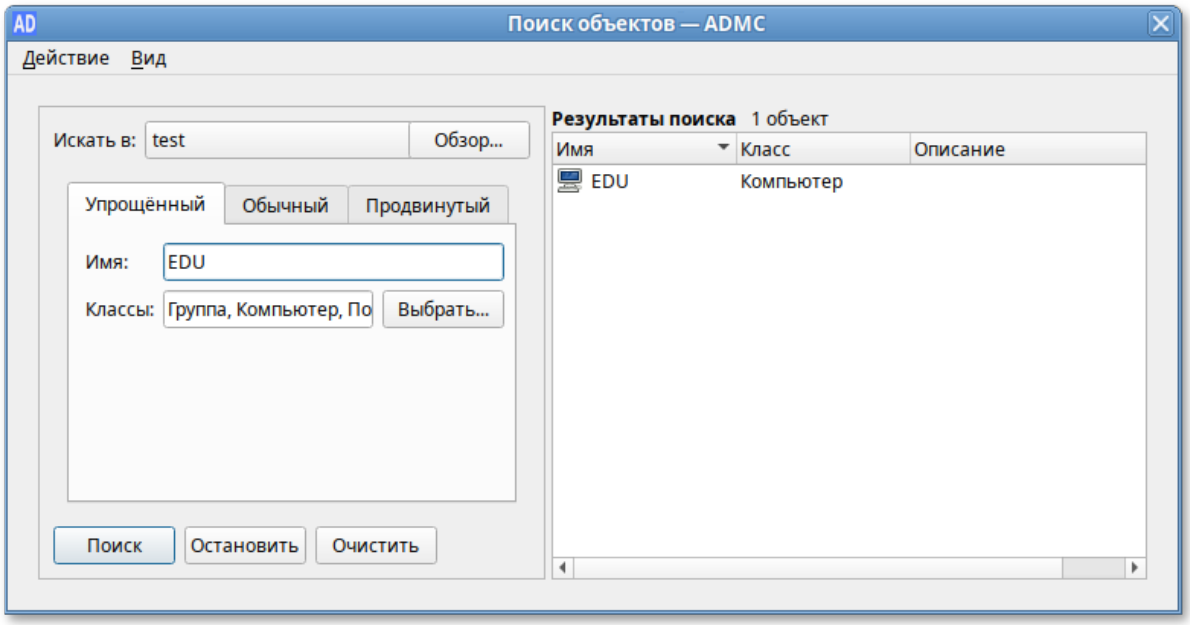


2. В поле **Классы**, нажав кнопку **Выбрать…**, выбрать классы объектов для поиска:



3. В поле **Имя** ввести имя объекта.

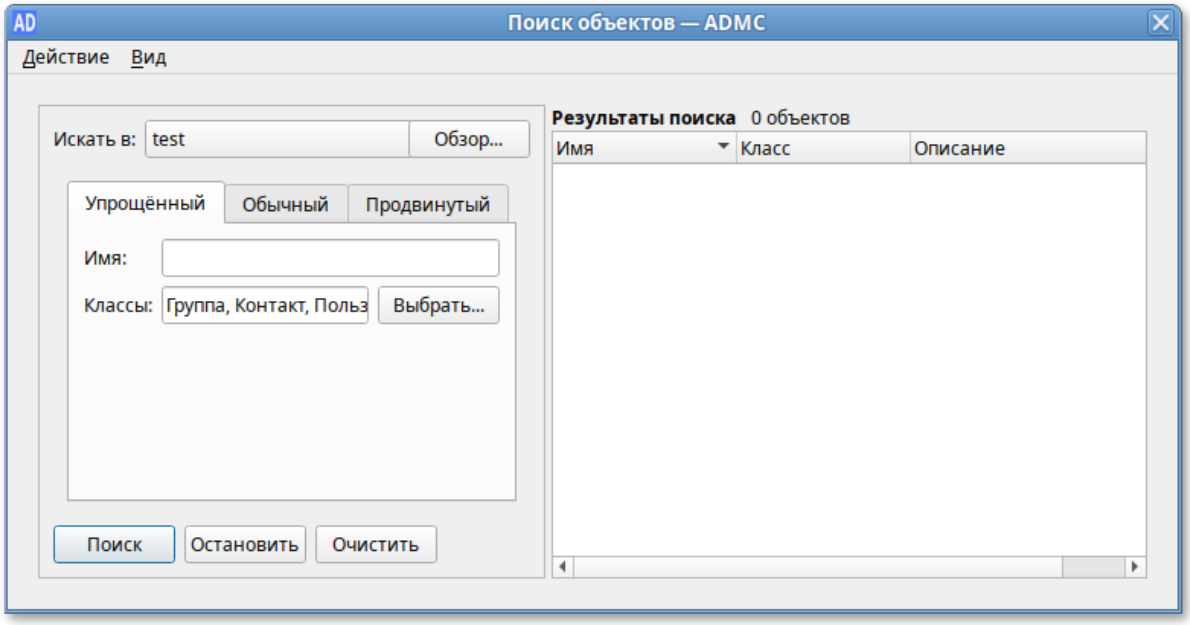
4. Нажать кнопку **Поиск**:



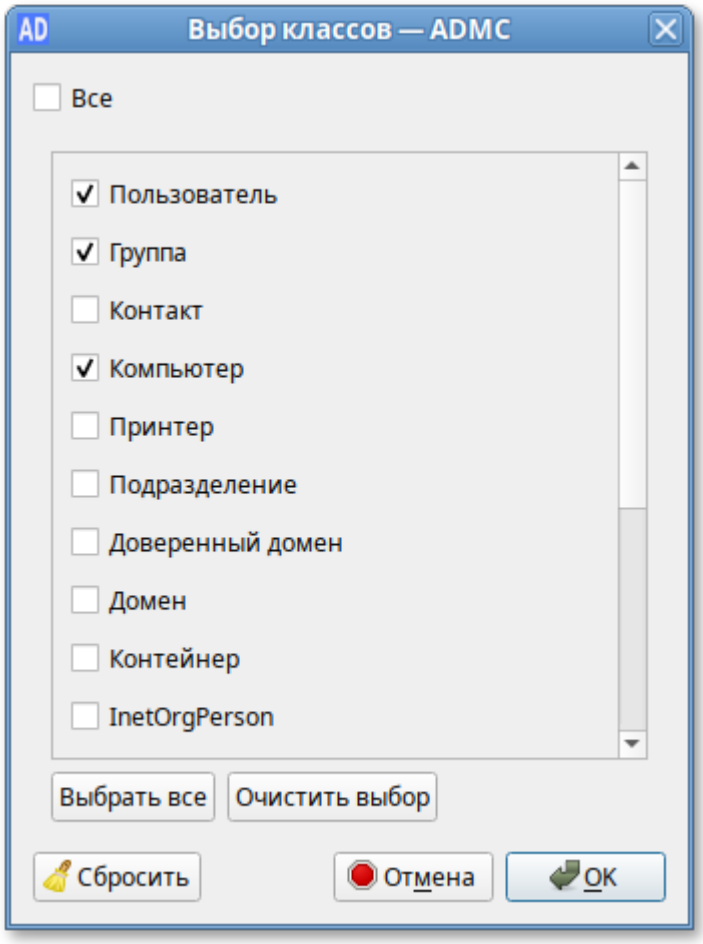
28.17.2. Обычный поиск

При использовании обычного поиска создаются фильтры, определяющие критерии поиска:

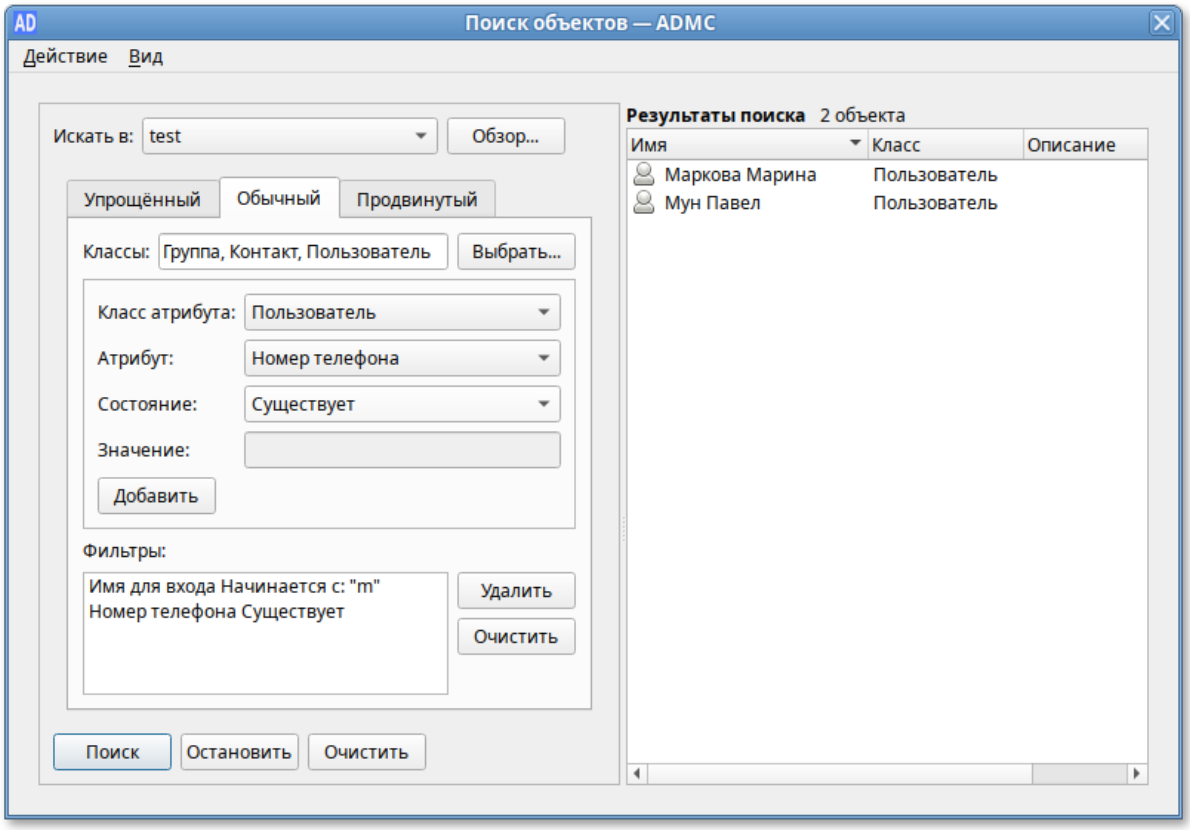
1. В диалоговом окне **Поиск объектов — ADMC** выбрать вкладку **Обычный**:



2. В поле **Классы**, нажав кнопку **Выбрать…**, выбрать классы объектов для поиска:



3. Создать фильтр:
   - в списке **Класс атрибута** выбрать класс атрибута;
   - в списке **Атрибут** выбрать атрибут (список атрибутов зависит от выбранного класса атрибутов);
   - в списке **Состояние** выбрать условие, которое будет использоваться для фильтра;
   - в поле **Значение** ввести значение условия (не для всех условий необходимо вводить значения).
4. Нажать кнопку **Добавить**.
5. Повторить пункты 2-3, чтобы добавить больше фильтров (фильтры для создания критериев поиска объединяются логическим И).
6. Нажать кнопку **Удалить**, если необходимо удалить фильтр из списка.
7. Нажать кнопку **Очистить**, если необходимо очистить список фильтров.
8. Нажать кнопку **Поиск**:



28.17.3. Продвинутый поиск

Продвинутый поиск предполагает использование LDAP-фильтров.

Использование LDAP-фильтров является наиболее эффективным способом поиска объектов в AD.

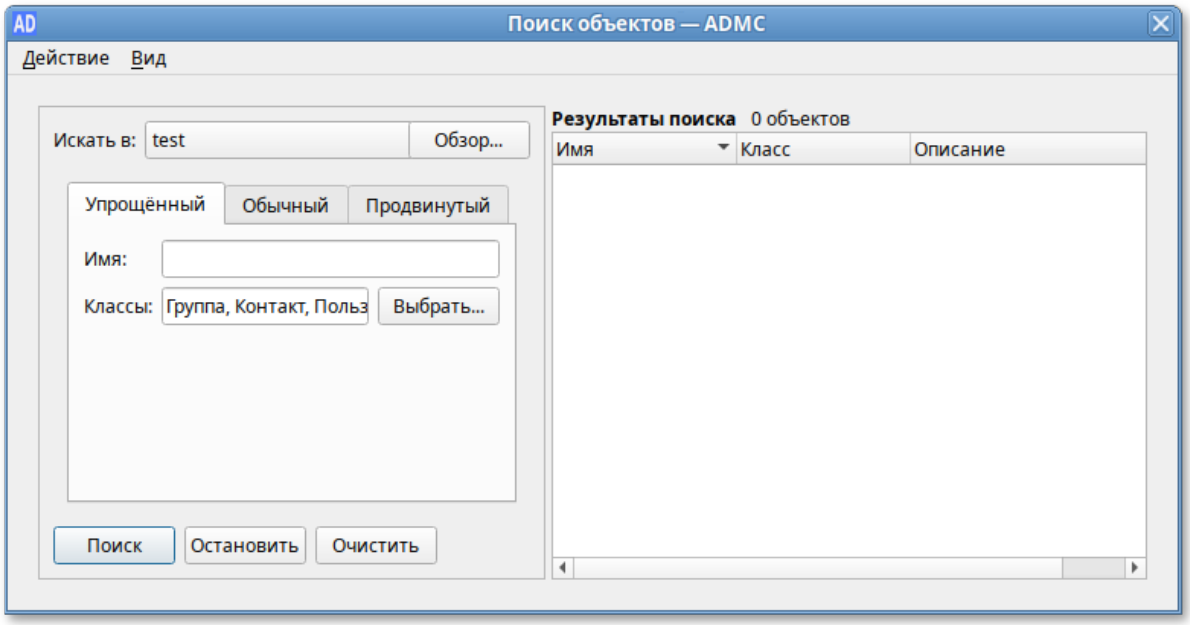
Синтаксис LDAP-фильтра имеет вид:

```
<Фильтр>=(<Атрибут><оператор сравнения><значение>)
```

При наличии нескольких условий поиска фильтры можно комбинировать с помощью логических операторов.

Процедура продвинутого поиска:

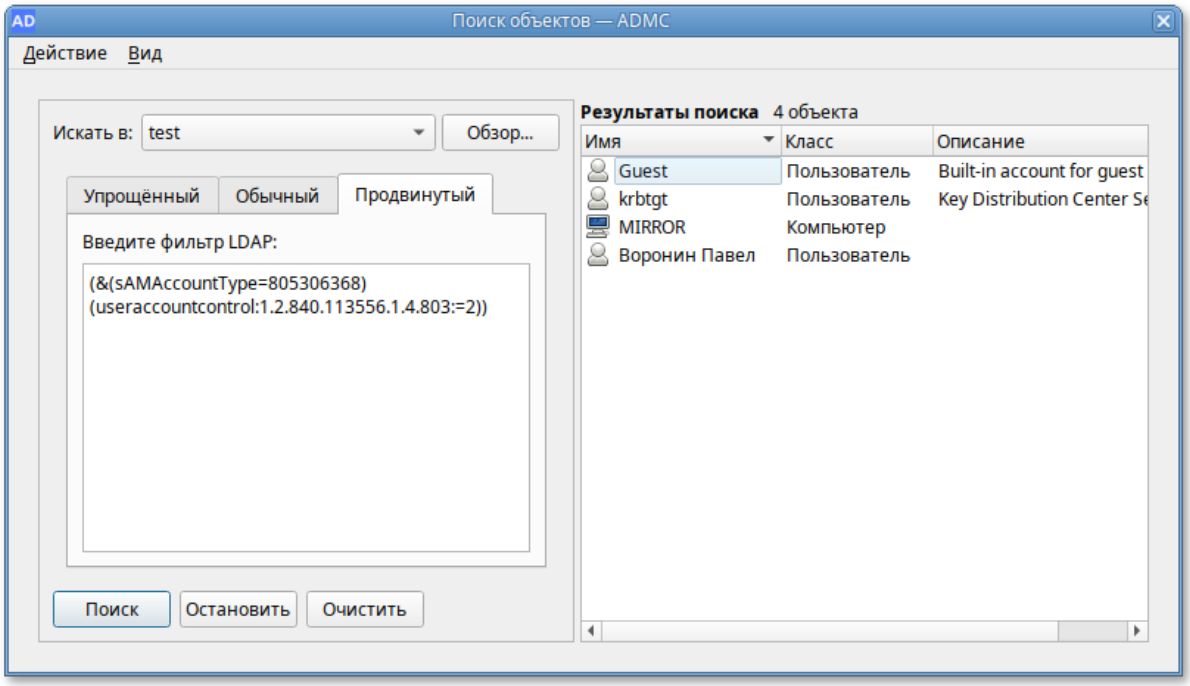
1. В диалоговом окне **Поиск объектов — ADMC** выбрать вкладку **Продвинутый**:



2. В поле **Искать в** выбрать область поиска (можно воспользоваться кнопкой **Обзор**).

3. Ввести LDAP-фильтр в поле **Введите фильтр LDAP**.

4. Нажать кнопку **Поиск**:

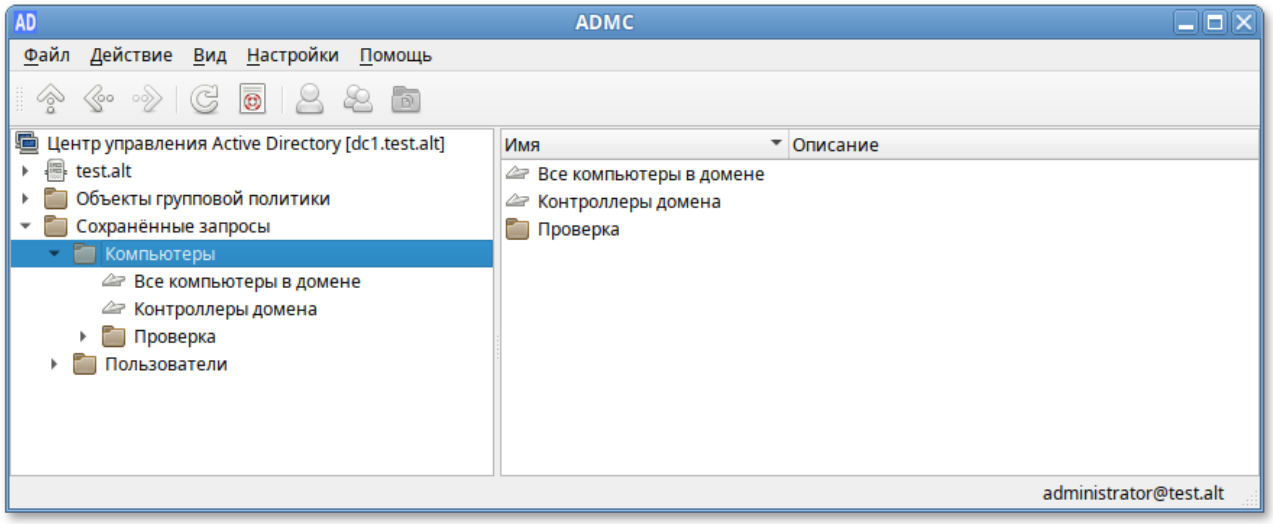


28.18. Использование сохранённых результатов поиска

Сохранение запросов (результатов поиска) — это удобный способ сохранять и воспроизводить поиск. Сохранённые запросы позволяют создавать различные LDAP-фильтры для выборки объектов домена. С помощью сохранённых запросов можно быстро и эффективно решать задачи поиска и выборки объектов в домене по различным критериям.

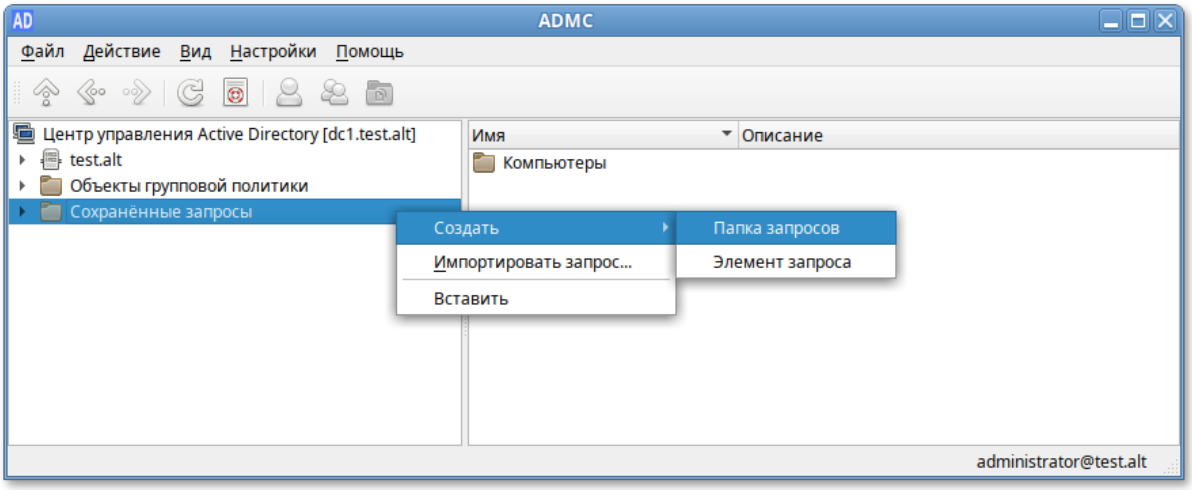
При использовании сохранённых запросов администратор может выполнять групповые операции с объектами из разных OU. Например, можно выполнить массовую блокировку/разблокировку, удаление учётных записей, переименование.

Сохранённые запросы можно организовать в древовидную структуру:

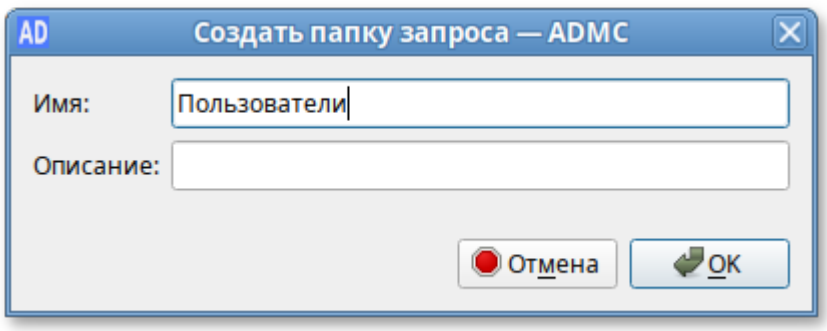


Создание папки запросов:

1. В контекстном меню папки **Сохранённые запросы** или её подпапки выбрать пункт **Создать → Папка запросов**:



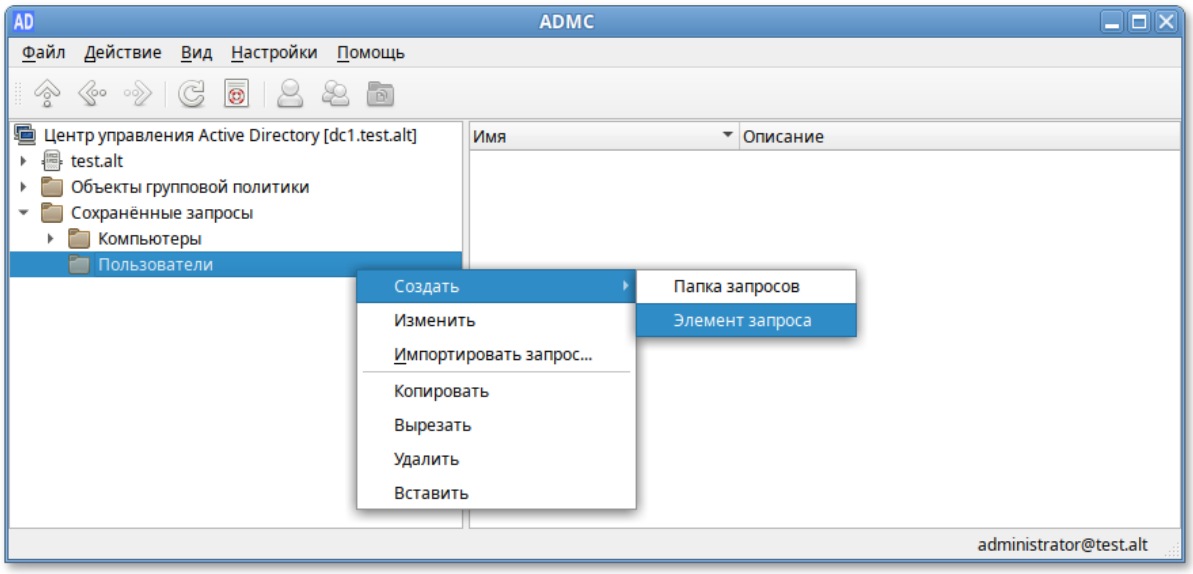
2. В диалоговом окне **Создать папку запросов — ADMC** в поле **Имя** вести название папки, в поле **Описание** можно добавить описание папки:



3. Нажать кнопку **OK**.

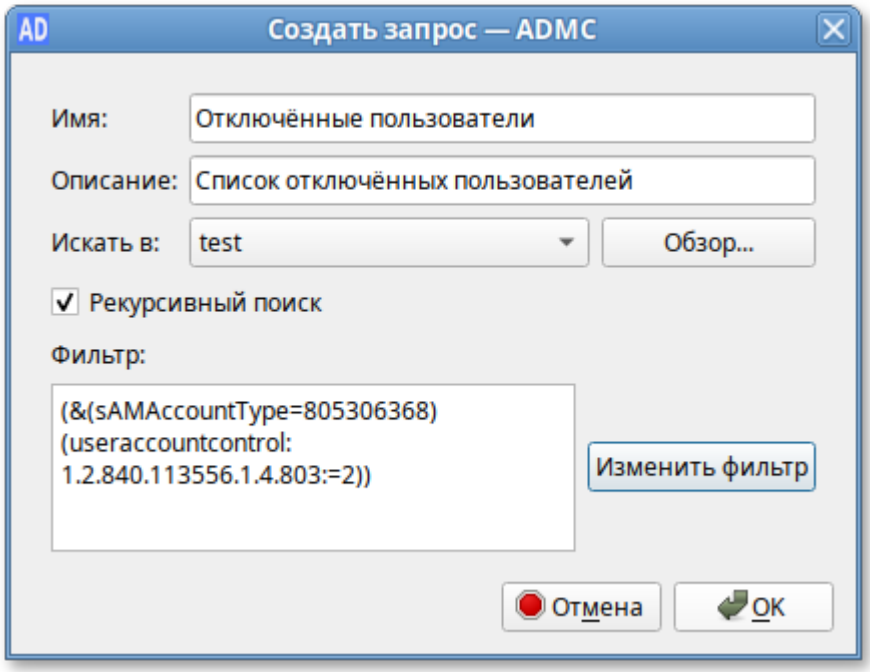
Создание запроса:

1. В контекстном меню папки запроса выбрать пункт **Создать → Элемент запроса**:



2. В диалоговом окне создания запроса необходимо указать:

   - **Имя** — название запроса;
   - **Описание** — описание запроса;
   - **Искать в** — объект, который будет использоваться в качестве основы для поиска. По умолчанию поиск выполняется по всему домену. Сузить область поиска можно, нажав кнопку **Обзор** и выбрав контейнер;
   - **Рекурсивный поиск** — поиск должен включать объекты более чем одного уровня;

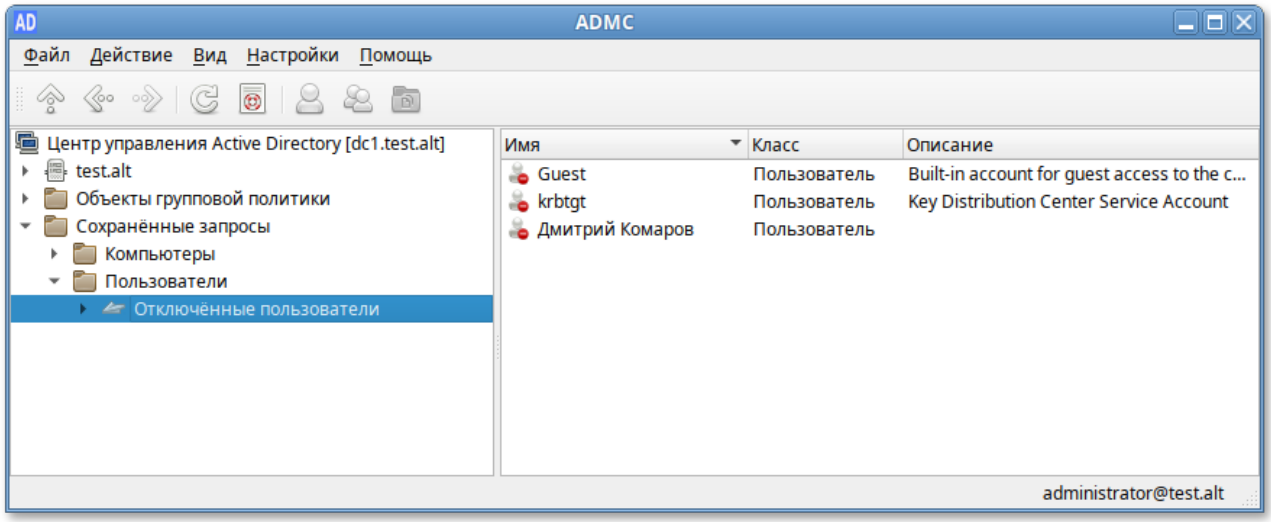


3. Нажать кнопку **Изменить фильтр**, чтобы создать фильтр поиска (для получения информации о том, как создавать фильтры, см. раздел Поиск объектов).

4. После создания фильтра он будет отображаться в поле **Фильтр** (в формате LDAP).

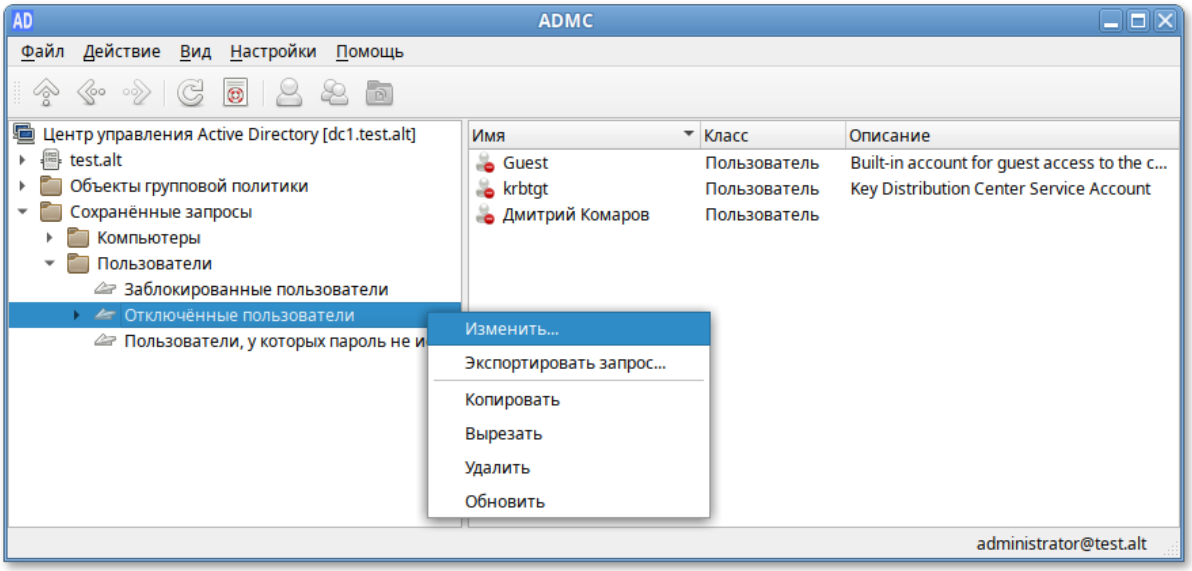
5. Нажать кнопку **OK**.

При выборе сохранённого запроса, в правом окне появится список объектов, который соответствует данному запросу:



Редактирование запроса:

1. В контекстном меню запроса выбрать пункт **Изменить…**:



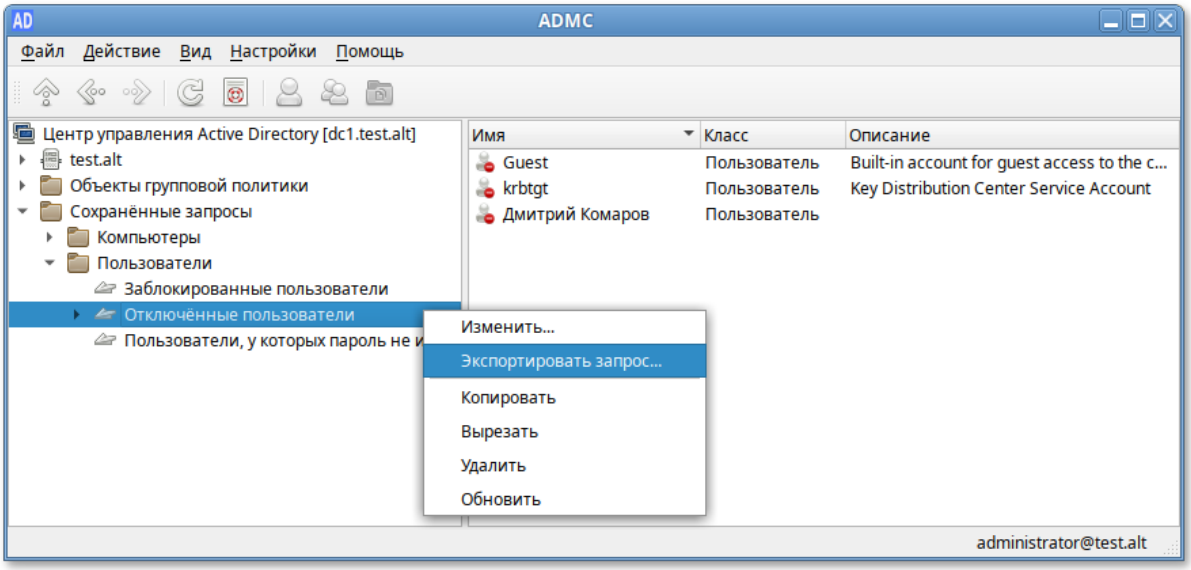
2. Внести необходимые изменения.

3. Нажать кнопку **OK**.

В ADMC существует возможность переноса поисковых запросов между компьютерами (экспорт и импорт поисковых запросов).

Экспорт запроса:

1. В контекстном меню запроса выбрать пункт **Экспортировать запрос…**.

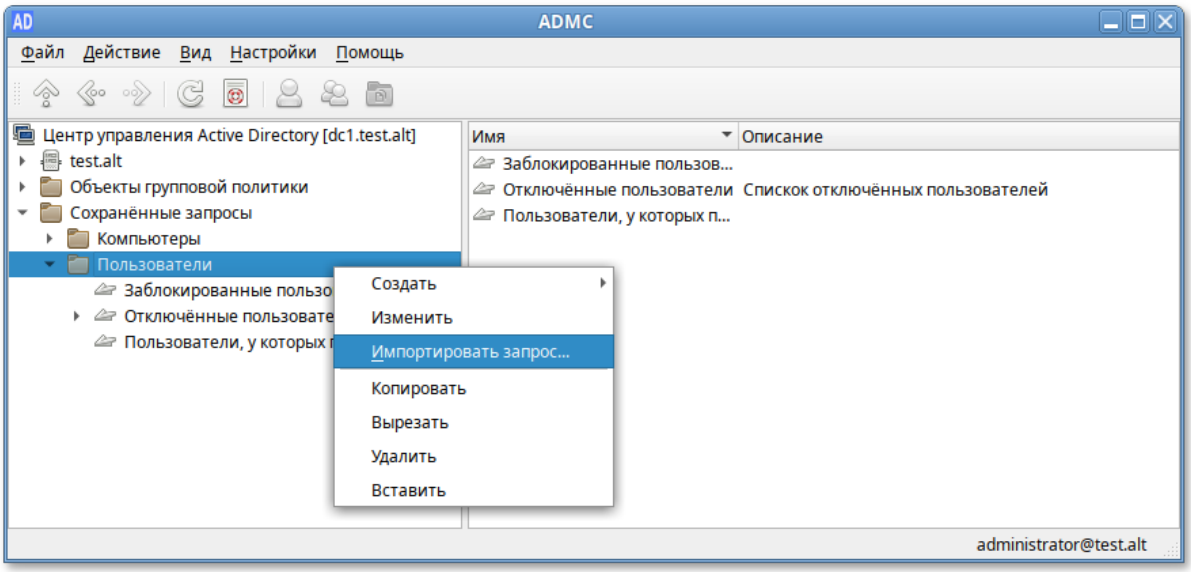


2. В открывшемся диалоговом окне указать название файла (<имя_файла>.json) и место назначения.

3. Нажать кнопку **Сохранить**.

Импорт запроса:

1. В контекстном меню папки, в которую будет импортирован запрос, выбрать пункт **Импортировать запрос…**:



2. В открывшемся диалоговом окне выбрать экспортированный файл поиска.

3. Нажать кнопку **Открыть**.

Для удаления запроса или папки запросов, необходимо в контекстном меню объекта выбрать пункт **Удалить**.

Глава 29. Модуль редактирования настроек клиентской конфигурации (GPUI)

29.1. Команда gpui-main

29.2. Запуск GPUI для редактирования доменных политик

29.3. Выбор набора шаблонов групповых политик

29.4. Интерфейс

29.5. Редактирование групповых политик

29.6. Редактирование предпочтений

29.7. Управление logon-скриптами

Модуль редактирования настроек клиентской конфигурации (далее — GPUI) предназначен для настройки и изменения параметров групповой политики в объектах групповой политики, которые могут ссылаться на организационные подразделения в AD.

GPUI предоставляет администраторам иерархическую древовидную структуру для настройки параметров групповой политики в объектах групповой политики. Эти объекты групповой политики могут быть связаны с организационными единицами (OU), содержащими компьютерные или пользовательские объекты. Связать объекты групповой политики с OU можно в модуле ADMC.

GPUI состоит из двух основных разделов: конфигурация компьютера и конфигурация пользователя. Раздел конфигурация компьютера содержит параметры всех политик, определяющих работу компьютера. Групповая политика применяется к компьютеру на этапе загрузки системы и в дальнейшем при выполнении циклов обновления. Раздел конфигурация пользователя содержит параметры всех политик, определяющих работу пользователя на компьютере. Групповая политика применяется к пользователю при его регистрации на компьютере и в дальнейшем при выполнении циклов обновления.

Каждая политика в объекте GPO может находится в одном из трех состояний: **Включено**, **Отключено**, **Не сконфигурировано**. В состоянии **Включено** в настройках можно указать параметры политики. В состоянии **Не сконфигурировано** — политика на объект не воздействует.

GPUI является расширяемым инструментом. Самый простой способ для разработчиков расширить редактор объектов групповой политики для своих приложений — это написать файлы настраиваемых административных шаблонов, которые «подключаются» к редактору объектов групповой политики.

29.1. Команда gpui-main

Синтаксис команды **gpui-main**:

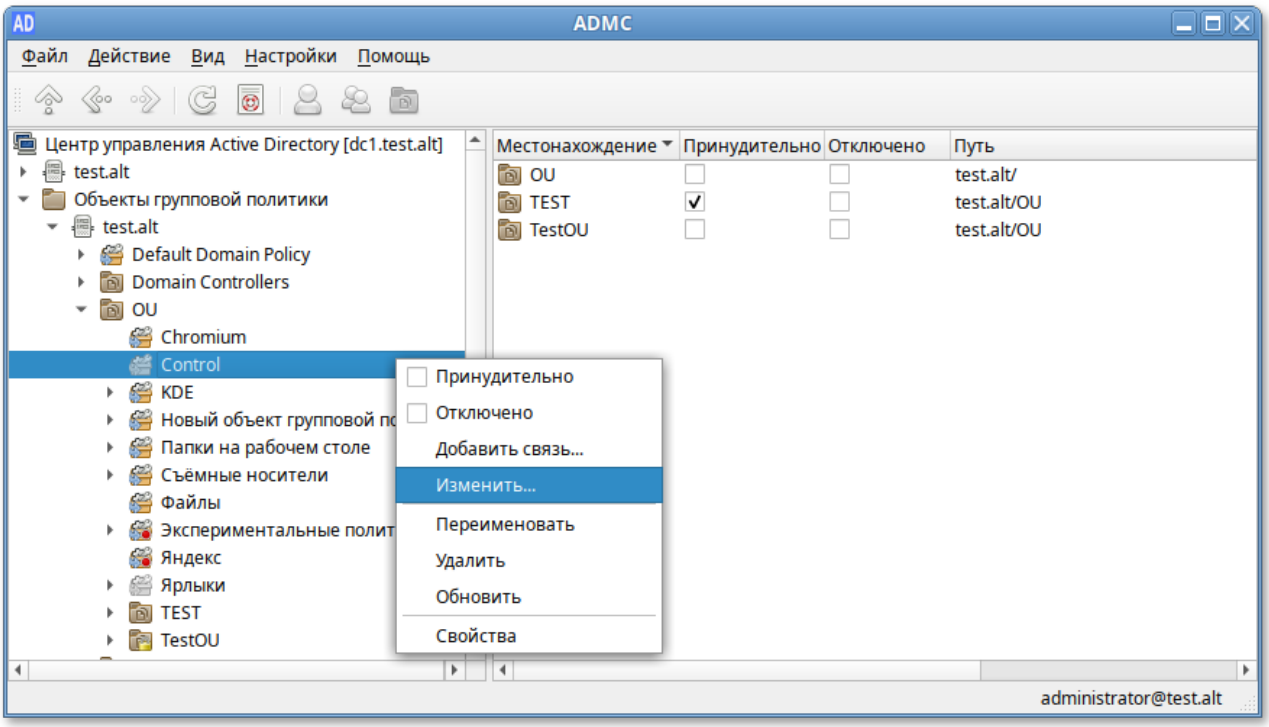
```
gpui-main [параметры]
```

Таблица 29.1. Опции команды gpui-main

Параметр	Описание
-p <путь>	Полный путь для редактируемой политики
-b <путь>	Полный путь к набору ADMX-файлов
-n <имя>	Опция оставлена для совместимости с ADMC. Она ничего не делает
--log-console <уровень>	Установить уровень логирования для консоли. По умолчанию: none
--log-syslog <уровень>	Установить уровень логирования для syslog. По умолчанию: none
--log-file <уровень>	Установить уровень логирования для файла в **~/.local/share/gpui/**. По умолчанию: warning
-v, --version	Вывести сведения о версии
-h, --help	Вывести справку о команде

29.2. Запуск GPUI для редактирования доменных политик

По умолчанию GPUI не редактирует никаких политик. Для того чтобы редактировать политику, GPUI нужно запустить либо из ADMC, выбрав в контекстном меню объекта групповой политики пункт **Изменить...**:



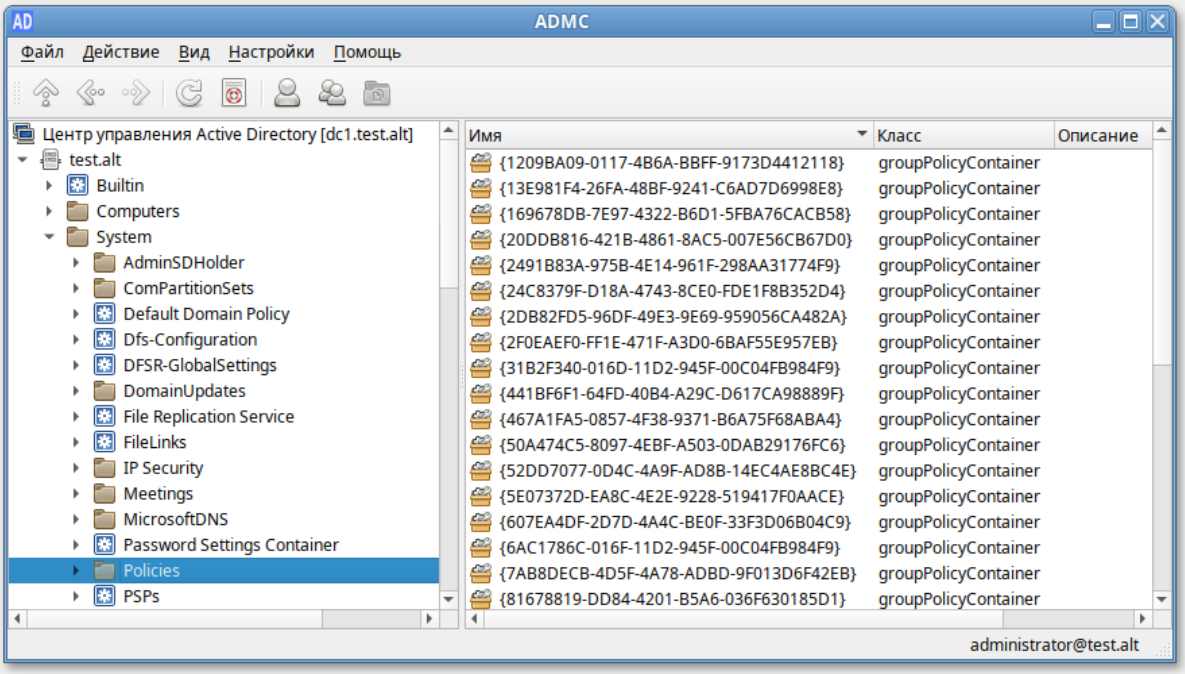
либо с указанием каталога групповой политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX}"
```

Ключ **-p** позволяет указать путь к шаблону групповой политики, который нужно редактировать, **dc1.test.alt** — имя контроллера домена, а **{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX}** — GUID шаблона групповой политики для редактирования. Можно указывать как каталоги smb, так и локальные каталоги.

Примечание

GUID шаблона групповой политики можно узнать в ADMC (это дочерний контейнер Policies контейнера System), в настройках должен быть отмечен пункт **Дополнительные возможности**:



Пример запуска GPUI для редактирования политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{2E80AFBE-BBDE-408B-B7E8-AF79E02839D6}"
```

29.3. Выбор набора шаблонов групповых политик

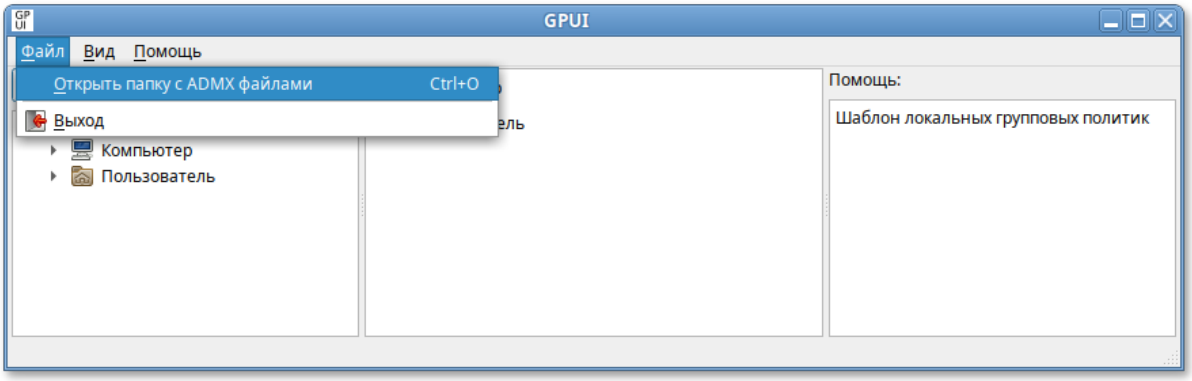
По умолчанию GPUI загружает ADMX-файлы, содержащие описание шаблонов групповых политик, из каталога **/usr/share/PolicyDefinitions**.

Для того чтобы указать другой набор шаблонов групповых политик, GPUI можно запустить с ключом **-b**:

```
$ gpui-main -b "/usr/share/PolicyDefinitions"
```

Каталог шаблонов групповых политик также можно выбрать в графическом интерфейсе:

1. Выбрать пункт меню **Файл** → **Открыть папку с ADMX файлами**:



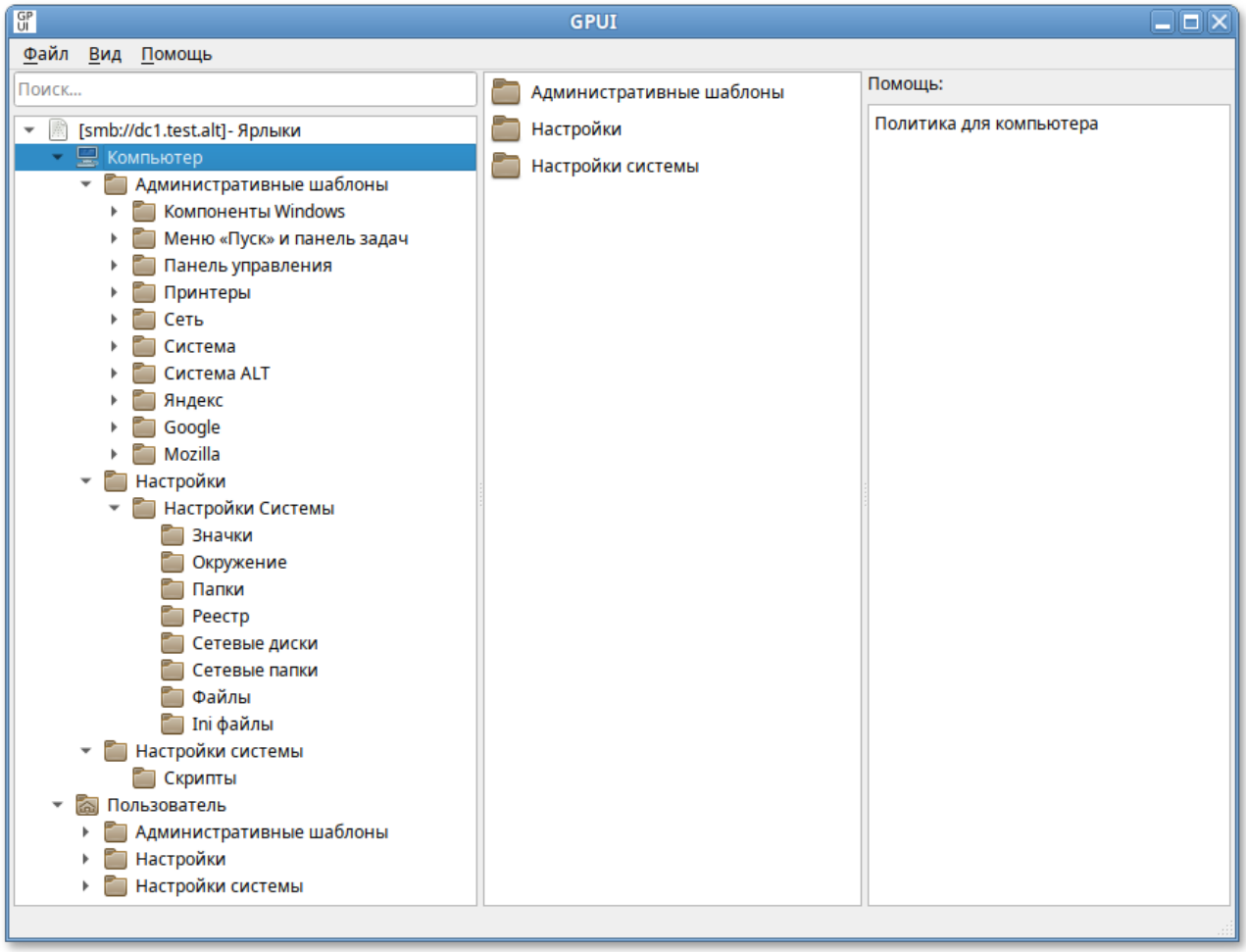
2. Открыть папку с шаблонами.

29.4. Интерфейс

Все настройки в GPUI разделены на два раздела:

- **Компьютер** (Machine) — раздел с настройками параметров компьютера;
- **Пользователь** (User) — раздел с настройками параметров пользователей домена.

Если параметр политики настраивается в секции **Компьютер**, групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном OU с компьютерами или пользователями.



В каждом разделе есть три подраздела:

- **Административные шаблоны** (Administrative Templates) — содержит параметры различных компонентов. Здесь доступны как административные шаблоны ОС «Альт» и Windows, так и дополнительные admx-шаблоны (например, admx-шаблоны для Mozilla Firefox или для Google Chrome);

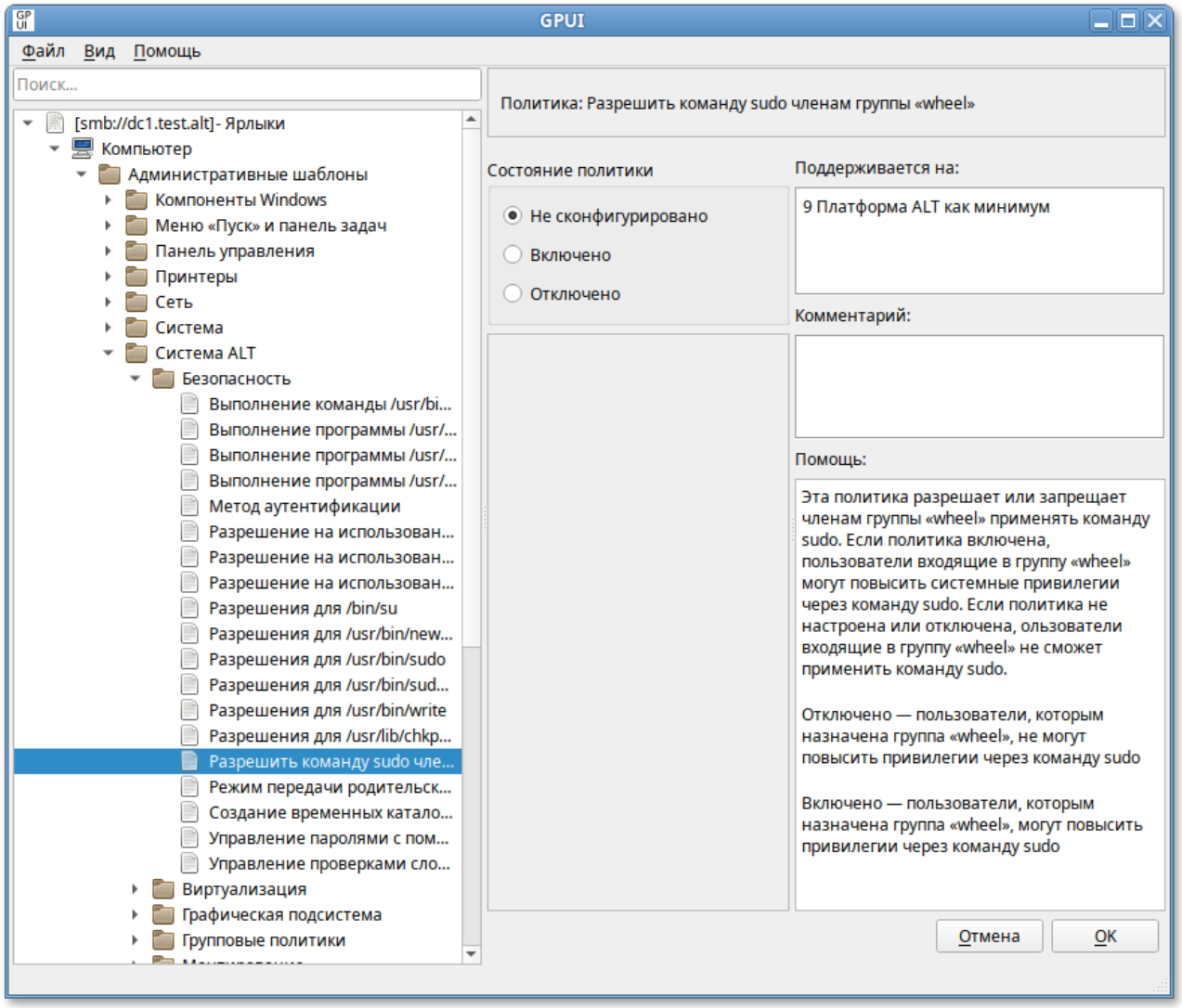
- **Настройки** (Preferences) — содержит дополнительный набор настроек (предпочтений). С помощью предпочтений можно настроить, в том числе такие параметры: создание ярлыков, подключение сетевых дисков, копирование файлов и папок на компьютеры;

- **Настройки системы** (System settings) — позволяет указать сценарии запуска и завершения работы компьютера, входа и выхода из системы пользователя.

Для быстрого доступа к политике можно воспользоваться поиском, для этого следует ввести в поле **Поиск…** ключевое слово.

29.4.1. Редактирование параметров в разделе Административные шаблоны

Чтобы изменить любой параметр групповой политики, нужно найти раздел, в котором он находится и открыть его настройки в правой панели:



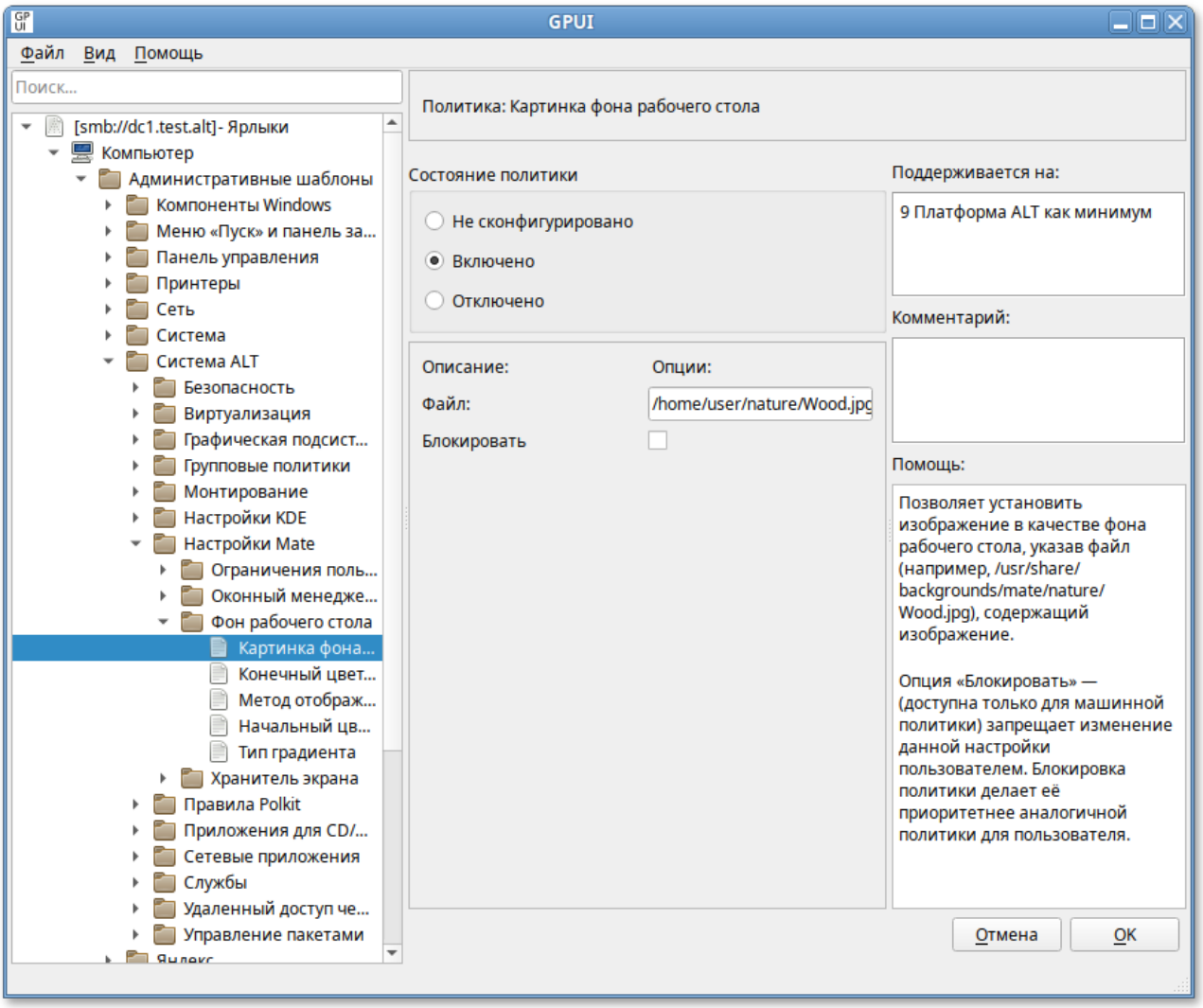
Параметры политики административных шаблонов могут иметь одно из трех состояний: **Не сконфигурировано**/**Включено**/**Отключено**. Параметры политики в состоянии **Не сконфигурировано** не влияют на пользователей или компьютеры. Если параметр политики находится в состоянии **Включено**, к пользователю или компьютеру применяется действие, описанное в заголовке параметра политики. Если параметр политики находится в состоянии **Отключено**, к пользователю или компьютеру применяется действие, противоположное описанному в заголовке параметра политики. Как правило, состояния параметров политики **Не сконфигурировано** и **Отключено** приводят к одинаковым результатам.

В каждом параметре политики административных шаблонов предоставлены подробные сведения о состояниях **Включено**, **Отключено** и **Не сконфигурировано**. Можно просмотреть эти сведения в поле **Помощь** для каждого параметра политики административных шаблонов.

В поле **Поддерживается на** указаны версии ОС, для которых данная политика применима. Например, **10 платформа ALT как минимум** означает, что политика применима только к дистрибутивным решениям ОС «Альт» десятой (p10) и одиннадцатой платформ (p11). Данный параметр не будет работать на девятой платформе (p9).

По умолчанию все параметры в разделе административных шаблонов не настроены (не сконфигурированы). Чтобы изменить настройку параметра групповой политики, достаточно выбрать новое состояние и нажать кнопку **OK**.

У некоторых настроек групповых политик можно задать дополнительные параметры, которые можно настроить в секции **Опции**. Например, чтобы установить изображение в качестве фона рабочего стола через ГП, нужно включить политику и указать путь к файлу с изображением в поле **Файл**:



В поле **Комментарий** можно указать примечание для ГП.

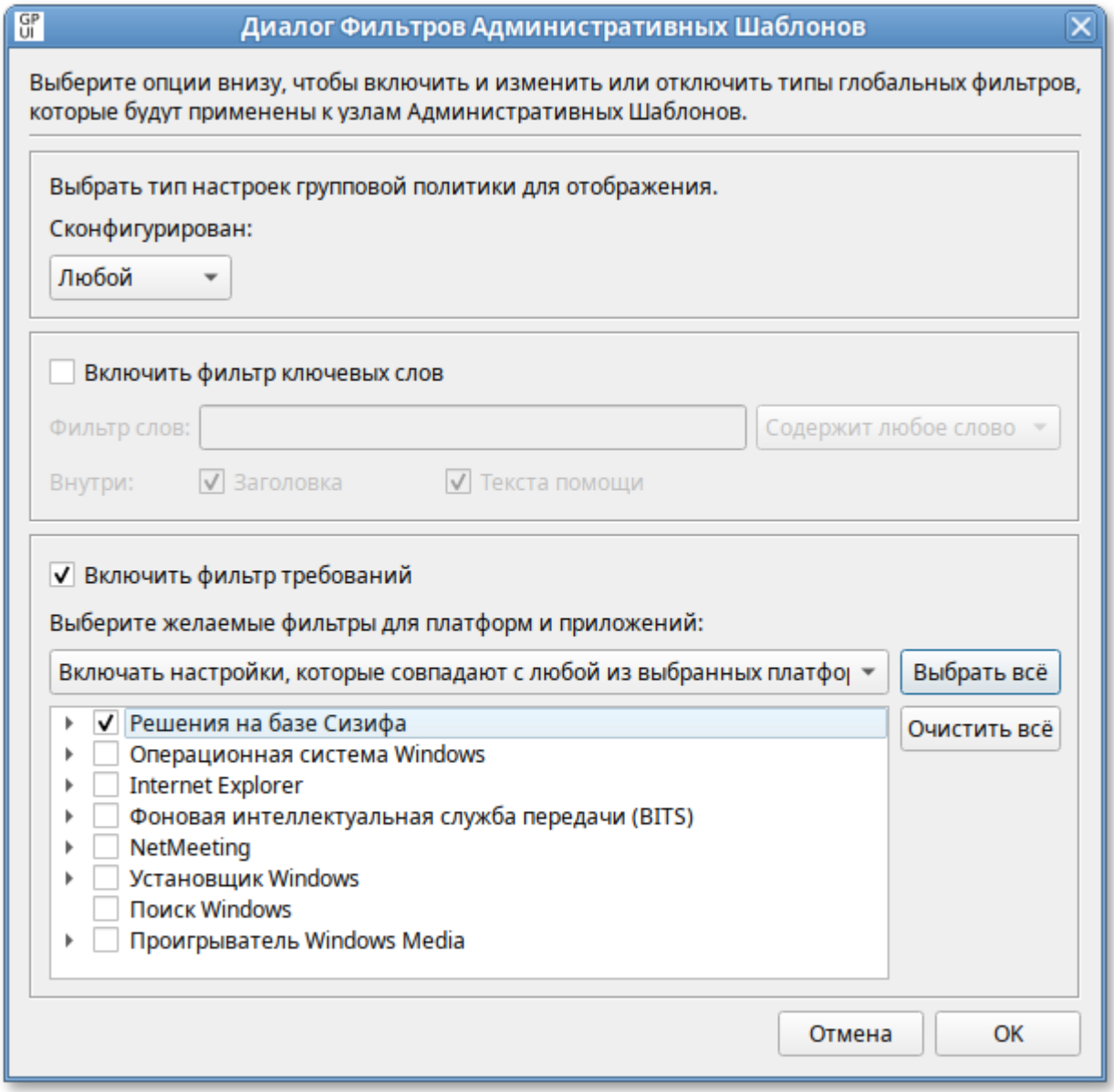
29.4.2. Фильтрация административных шаблонов

По умолчанию в GPUI отображаются все установленные административные шаблоны. Чтобы изменить отображение параметров политик административных шаблонов можно настроить фильтр административных шаблонов.

Фильтр административных шаблонов можно применять, если необходимо найти определенный параметр политики или ограничить количество параметров политики, отображаемых в GPUI.

Административные шаблоны можно отфильтровать на основе следующих факторов:

- настраиваемых параметров политики;
- ключевых слов в заголовке политики или тексте помощи к параметрам политики;
- требований параметров политики к платформам или приложениям.



Примечание

Фильтры являются включающими, поэтому необходимо выбирать элементы, которые следует отображать, а не исключаемые элементы.

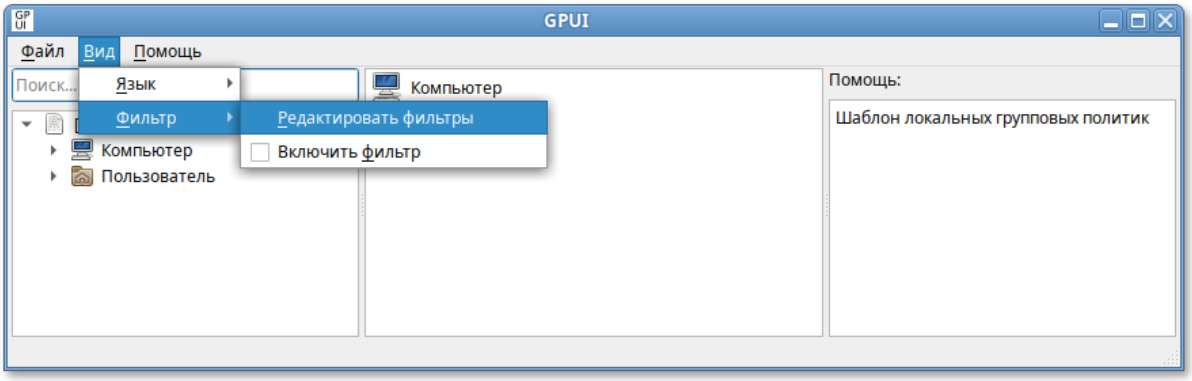
29.4.2.1. Фильтр по настроенным параметрам

Фильтр по настроенным параметрам имеет три состояния:

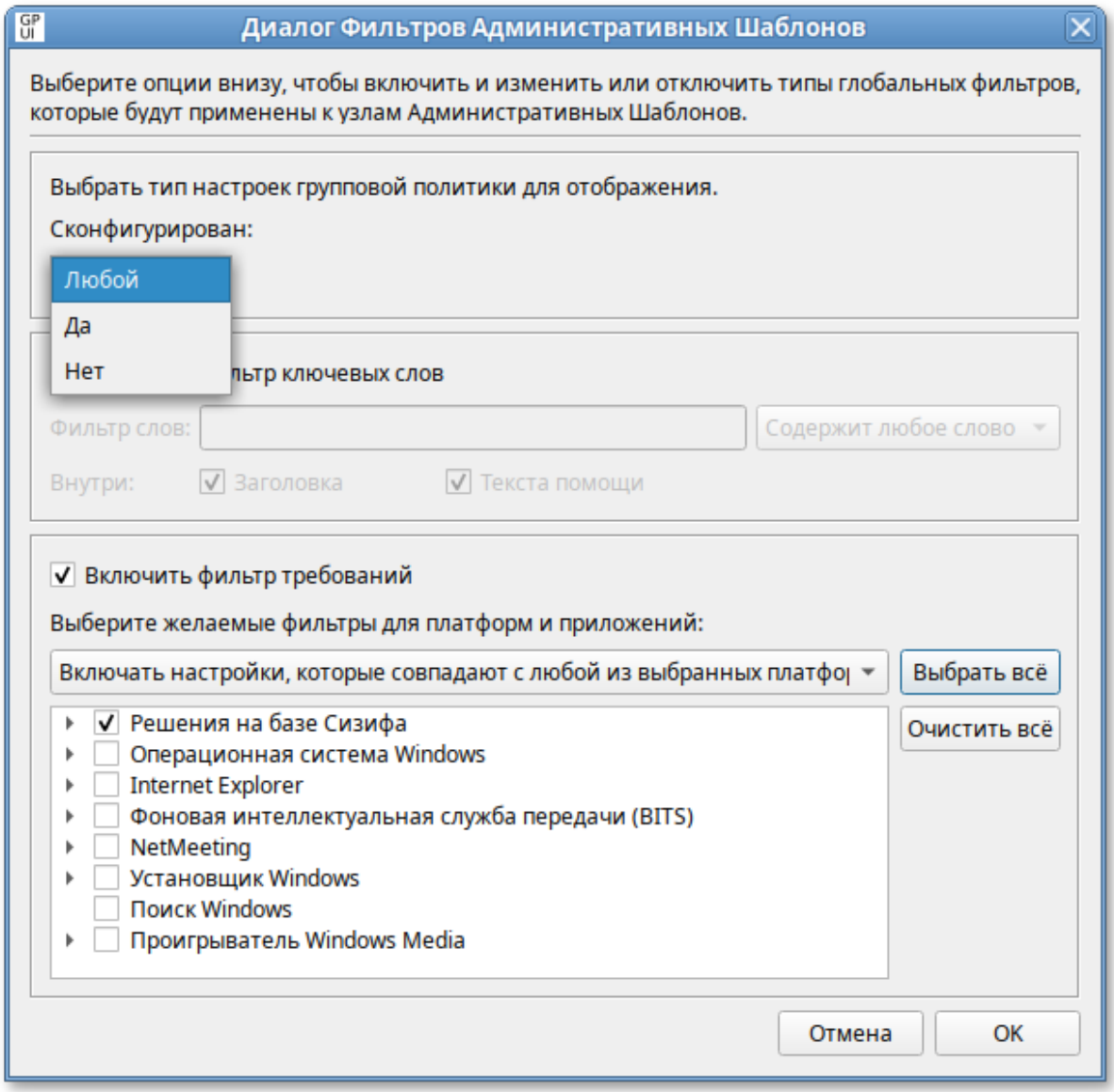
- **Любой** — отображать все параметры политики административных шаблонов (по умолчанию);
- **Да** — отображать только сконфигурированные параметры политики административных шаблонов;
- **Нет** — отображать только не сконфигурированные параметры политики административных шаблонов.

Для установки фильтра по настроенным параметрам необходимо:

1. В меню выбрать **Вид** → **Фильтр** → **Редактировать фильтры**:

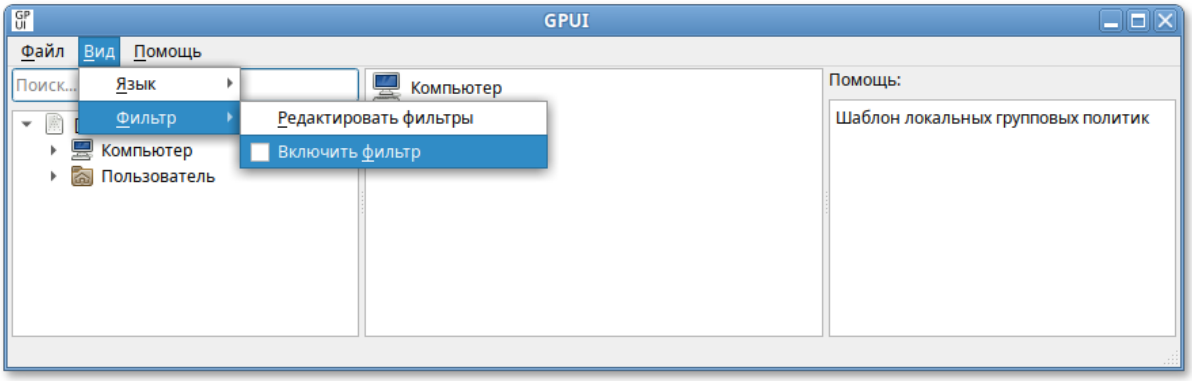


2. В открывшемся окне в списке **Сконфигурирован** выбрать необходимый фильтр:



3. Нажать кнопку **OK**, чтобы сохранить параметры фильтра.

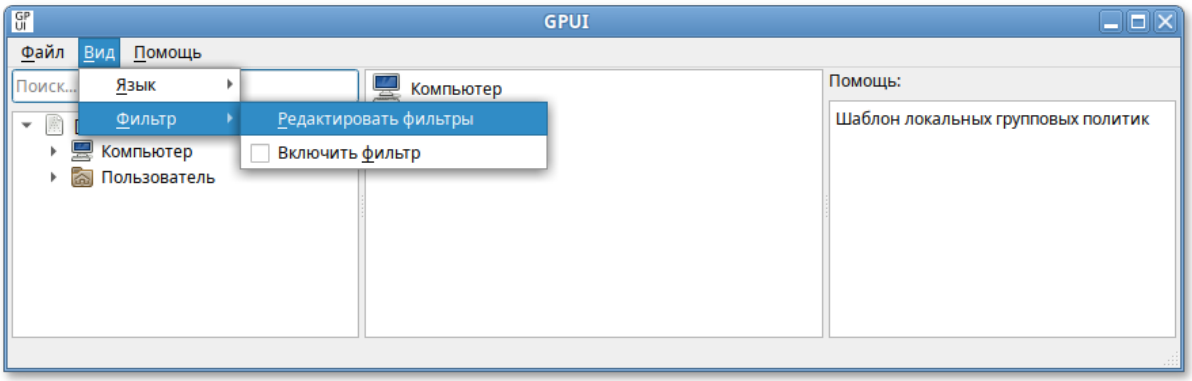
4. Чтобы применить фильтр в меню выбрать **Вид** → **Фильтр** → **Включить фильтр**:



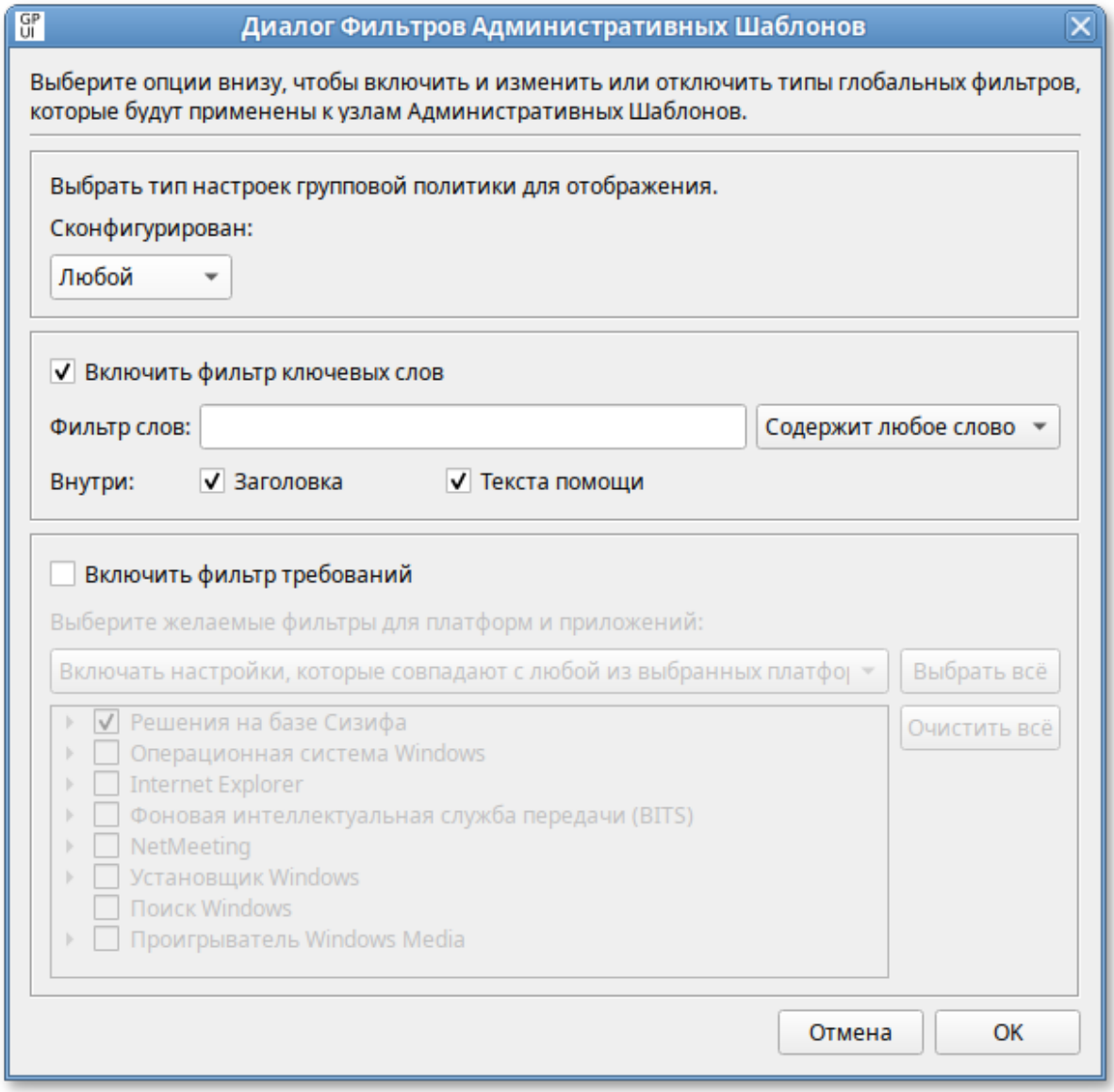
29.4.2.2. Фильтр по ключевым словам

Для установки фильтра по ключевым словам необходимо:

1. В меню выбрать **Вид** → **Фильтр** → **Редактировать фильтры**:



2. В открывшемся окне установить отметку **`Включить фильтр ключевых слов`**:



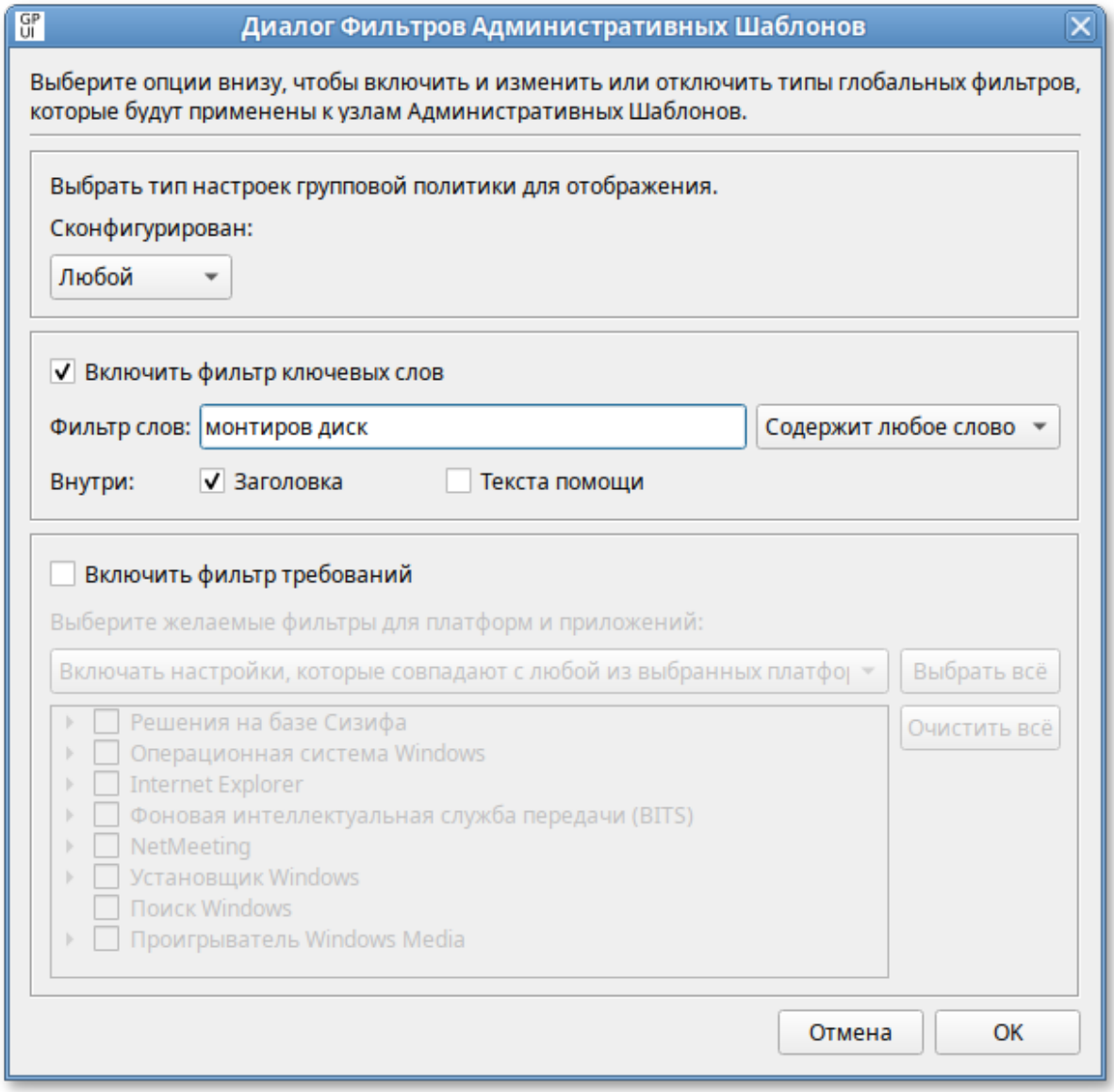
3. Ввести одно или несколько ключевых слов в поле **Фильтр слов** и выбрать необходимый фильтр:

    - **Содержит любое слово** — фильтр содержит любое слово из поля **Фильтр слов**;
    - **Содержит все слова** — фильтр содержит все слова из поля **Фильтр слов**;
    - **Полностью совпадает** — фильтр содержит точное соответствие словам **Фильтр слов**.

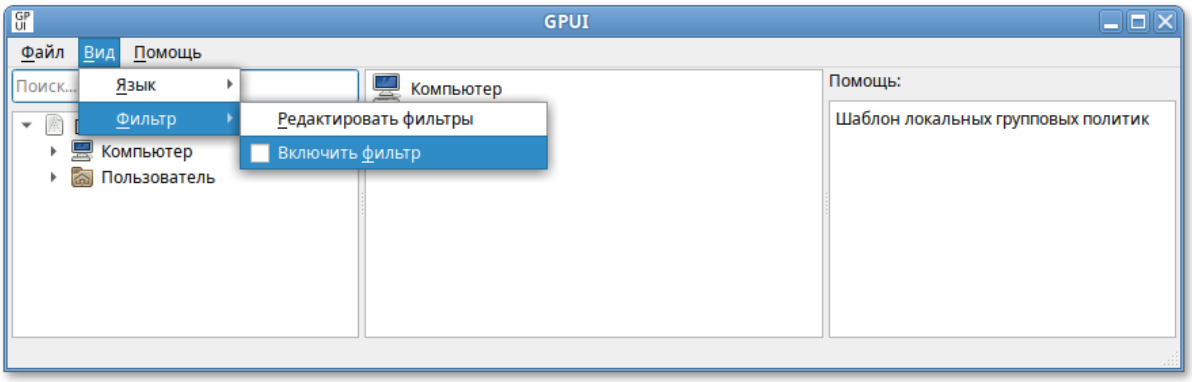
4. Установить соответствующие отметки в поле **Внутри**:

    - **Заголовка** — фильтр включает поиск в заголовке параметра политики;
    - **Текста помощи** — фильтр включает поиск в тексте помощи параметра политики.

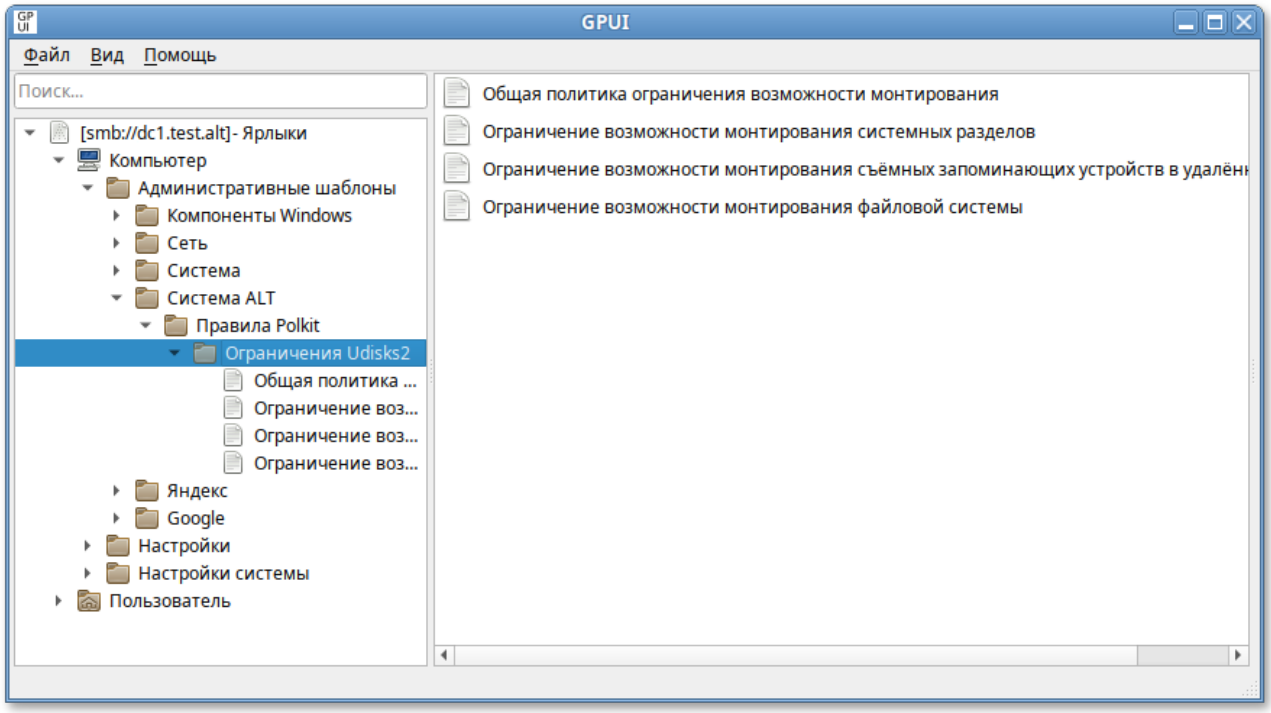
5. Нажать кнопку **OK**, чтобы сохранить параметры фильтра:



6. Чтобы применить фильтр в меню выбрать **Вид** → **Фильтр** → **Включить фильтр**:



Результат применения фильтра по ключевым словам:

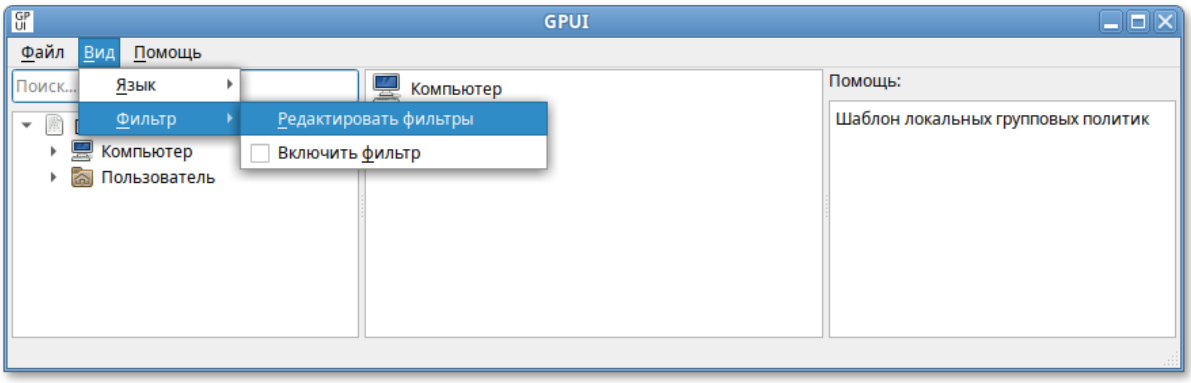


29.4.2.3. Фильтр по требованиям

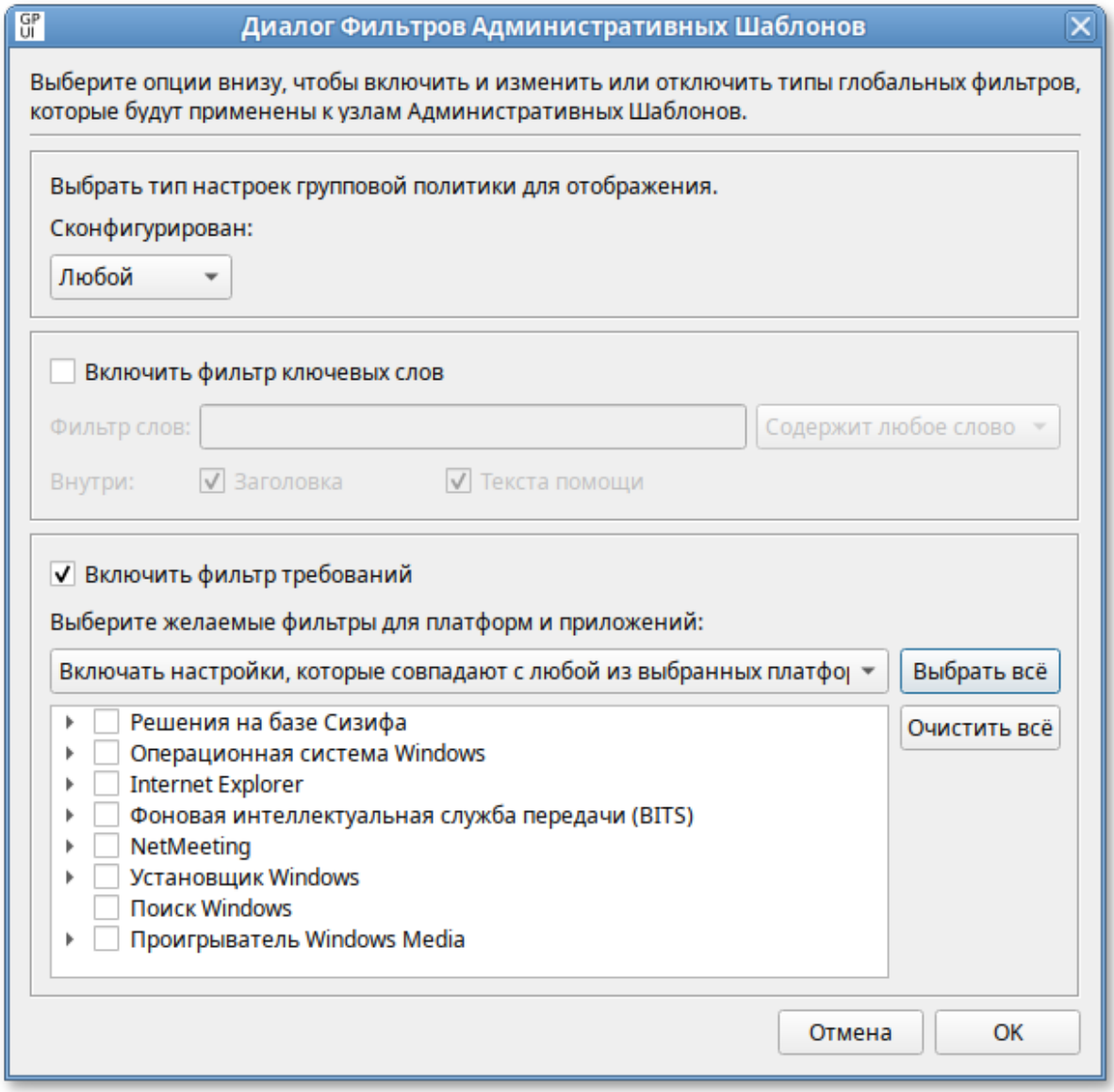
При помощи этого способа фильтрации, можно отобразить параметры, соответствующие всем выбранным платформам или отобразить параметры, соответствующие любой из выбранных платформ.

Для установки фильтра по требованиям необходимо:

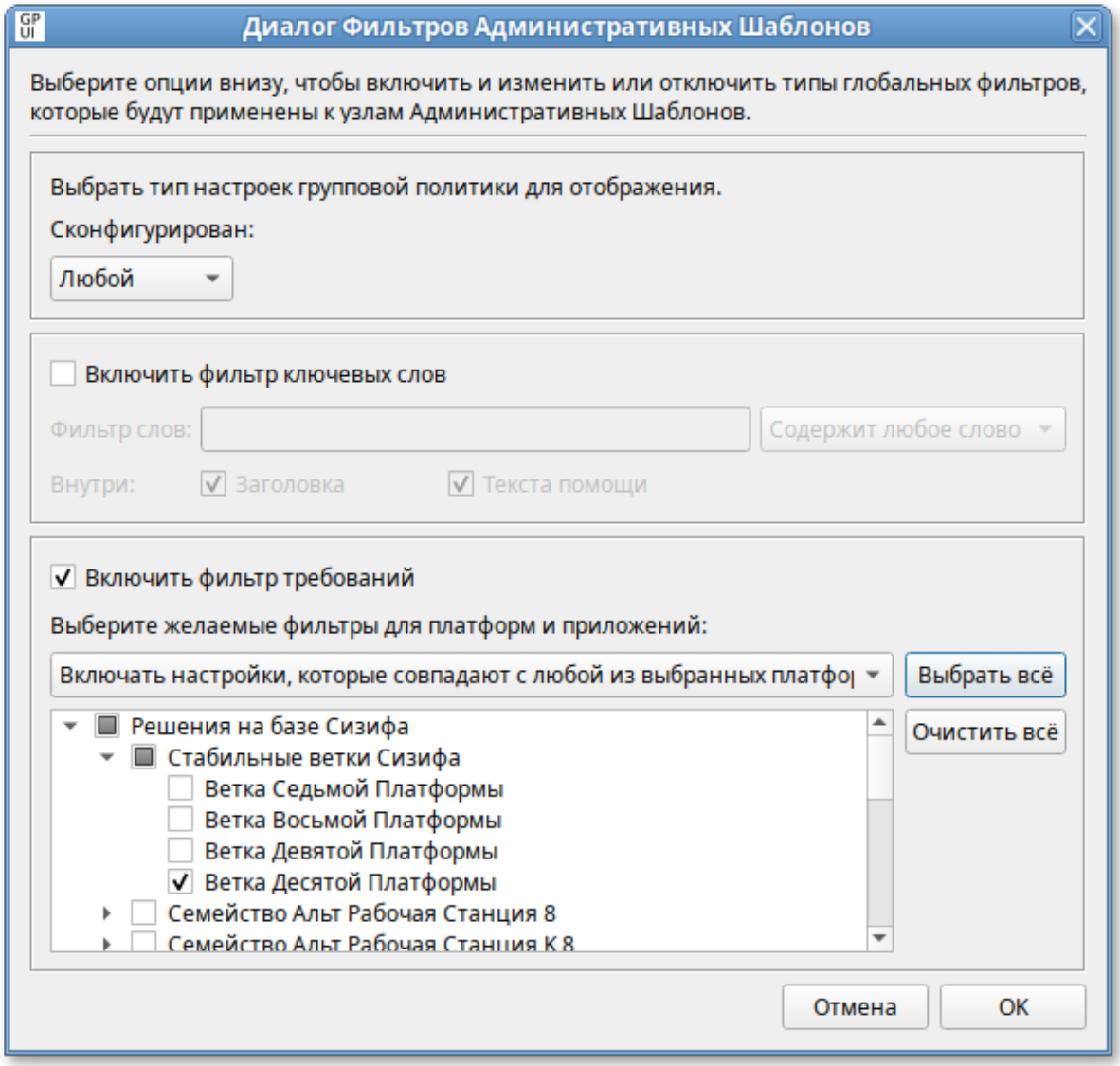
1. В меню выбрать **Вид** → **Фильтр** → **Редактировать фильтры**:



2. В открывшемся окне установить отметку **`Включить фильтр требований`**:



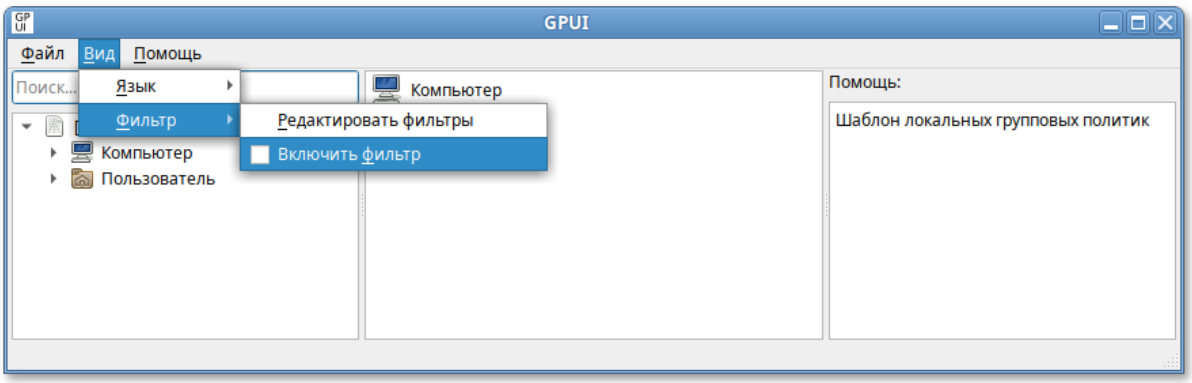
3. В списке **Выберите желаемые фильтры для платформы и приложений** выбрать необходимый фильтр:
   - **Включать настройки, которые совпадают с любой из выбранных платформ**;
   - **Включить настройки, которые совпадают со всеми выбранными платформами**.
4. Выбрать необходимые платформы:



Можно выбрать пункт **Решения на базе Сизифа** или нажать кнопку **Выбрать всё**, чтобы выбрать все элементы в списке, или нажать кнопку **Очистить всё**, чтобы снять выделение всех элементов списка.

5. Нажать кнопку **OK**, чтобы сохранить параметры фильтра.

6. Чтобы применить фильтр в меню выбрать **Вид** → **Фильтр** → **Включить фильтр**:

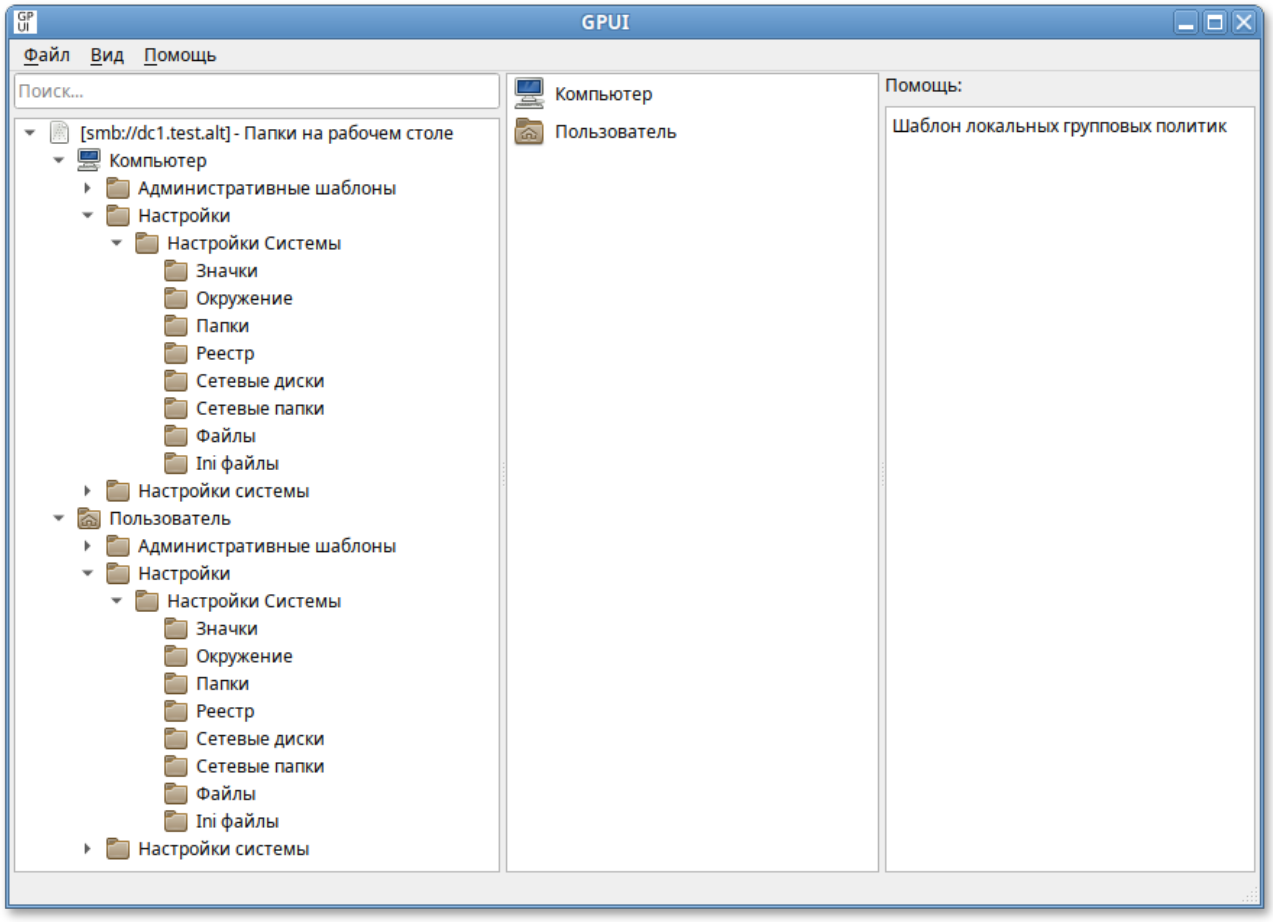


29.4.3. Работа с предпочтениями групповых политик

GPUI позволяет настраивать следующие предпочтения:

- **Значки** (управление ярлыками) — создание, редактирование или удаление ярлыков;
- **Окружение** (управление переменными среды) — создание, редактирование или удаление переменных среды;
- **Папки** (управление каталогами) — создание, редактирование или удаление каталогов;
- **Реестр** — копирование параметров реестра и их применение к другим компьютерам, создание, замена или удаление параметров реестра (для машин Windows);
- **Сетевые папки** (управление общими каталогами) — создание, удаление (скрытие из общего доступа) или редактирование общих ресурсов;
- **Сетевые диски** (подключение сетевых дисков) — создание, редактирование или удаление сопоставленных дисков и настройка видимости всех дисков;
- **Файлы** (управление файлами) — копирование, замена, удаление или изменение атрибутов файлов;
- **INI-файлы** (управление INI-файлами) — добавление, замена или удаление разделов/свойств файлов параметров настройки (INI) или информации об установке (INF).

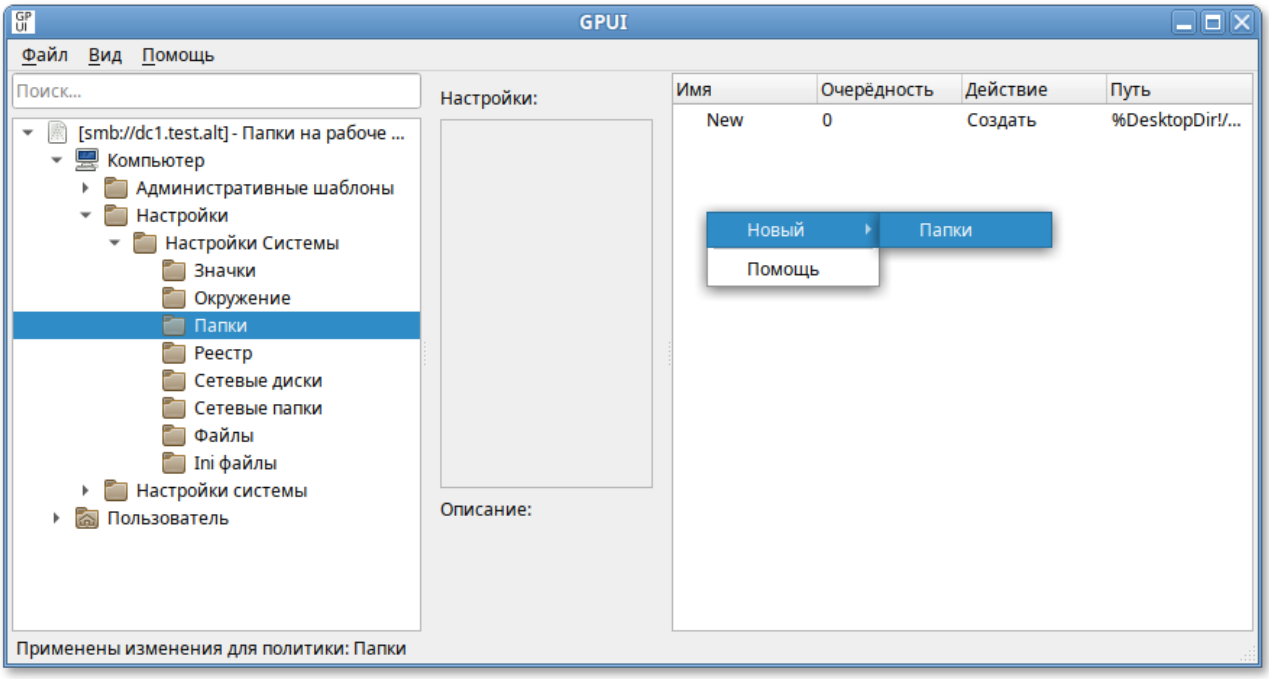
Предпочтения можно настроить для пользователей и компьютеров (пункт **Настройки** соответственно в элементах **Компьютер** и **Пользователь**):



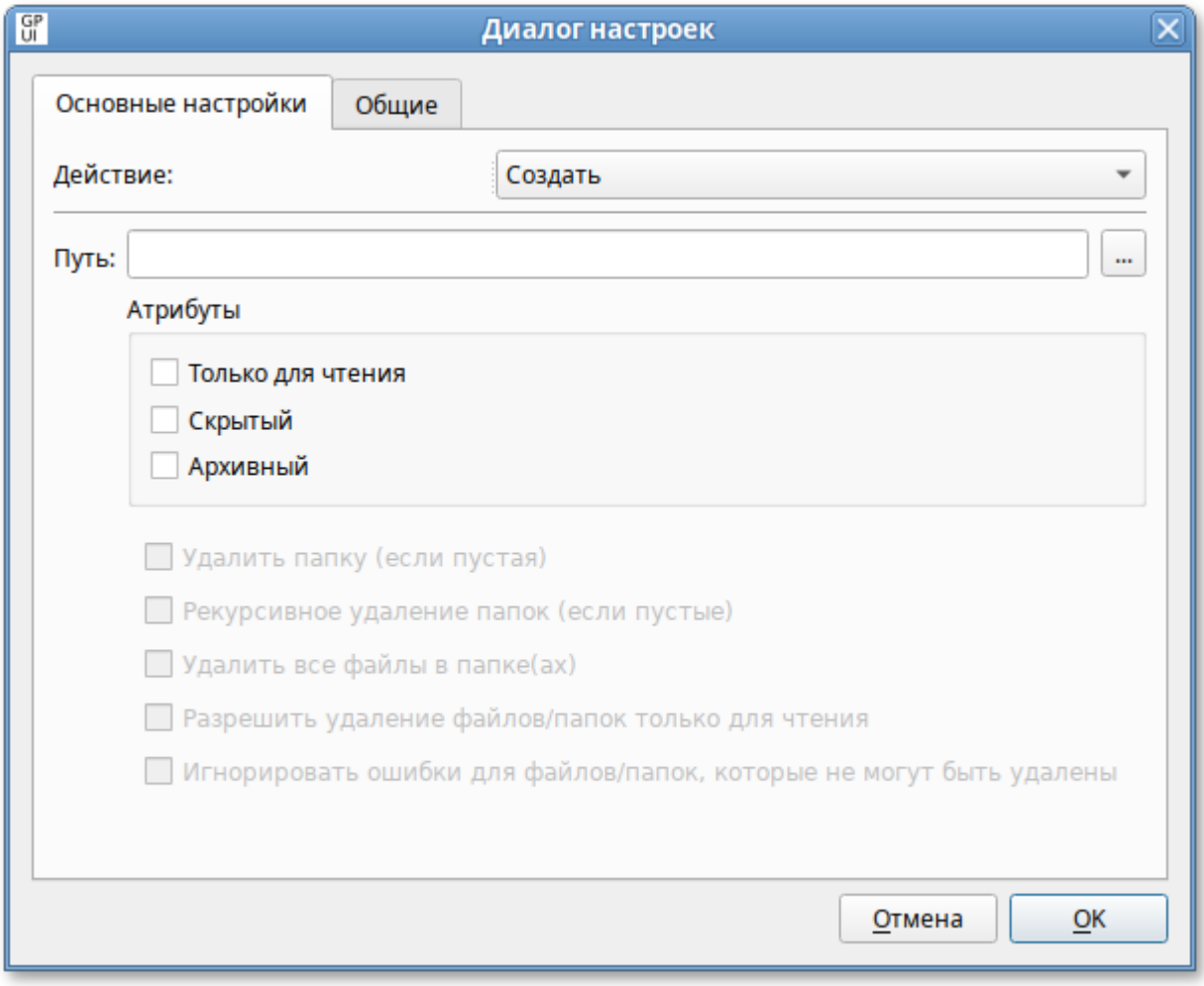
В каждом объекте групповой политики с каждым из расширений предпочтения можно создать несколько элементов предпочтения.

Для создания предпочтения необходимо перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы**, выбрать соответствующее предпочтение, затем в контекстном меню свободной области выбрать пункт **Новый** → **Название_предпочтения**.

Например, для создания нового предпочтения **Папки** необходимо перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы** → **Папки**. В контекстном меню свободной области выбрать пункт **Новый** → **Папки**.

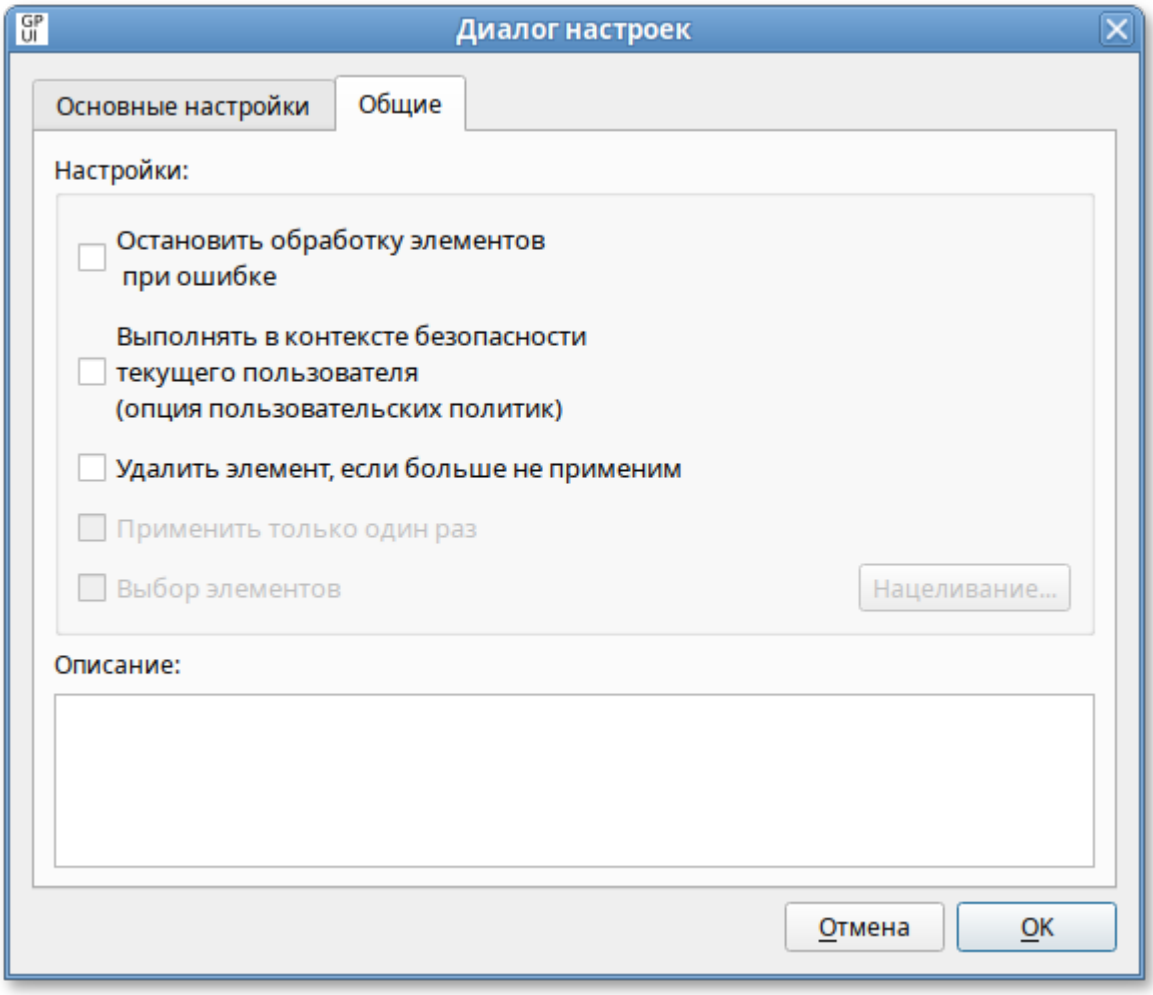


Откроется диалоговое окно **Диалог настроек**, где на вкладке **Основные настройки** можно задать параметры, характерные для соответствующего предпочтения (подробнее параметры настройки предпочтений рассмотрены в следующих разделах данного документа):

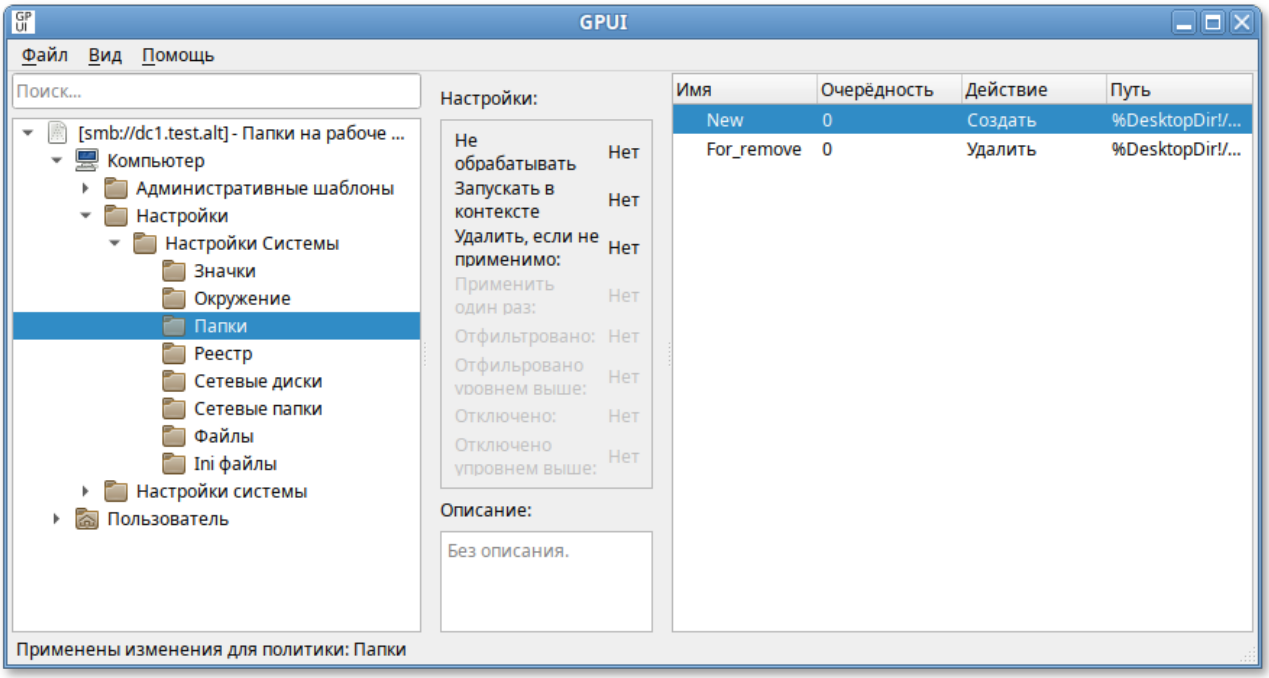


Вкладка **Общие** содержит настройки одинаковые для всех предпочтений:

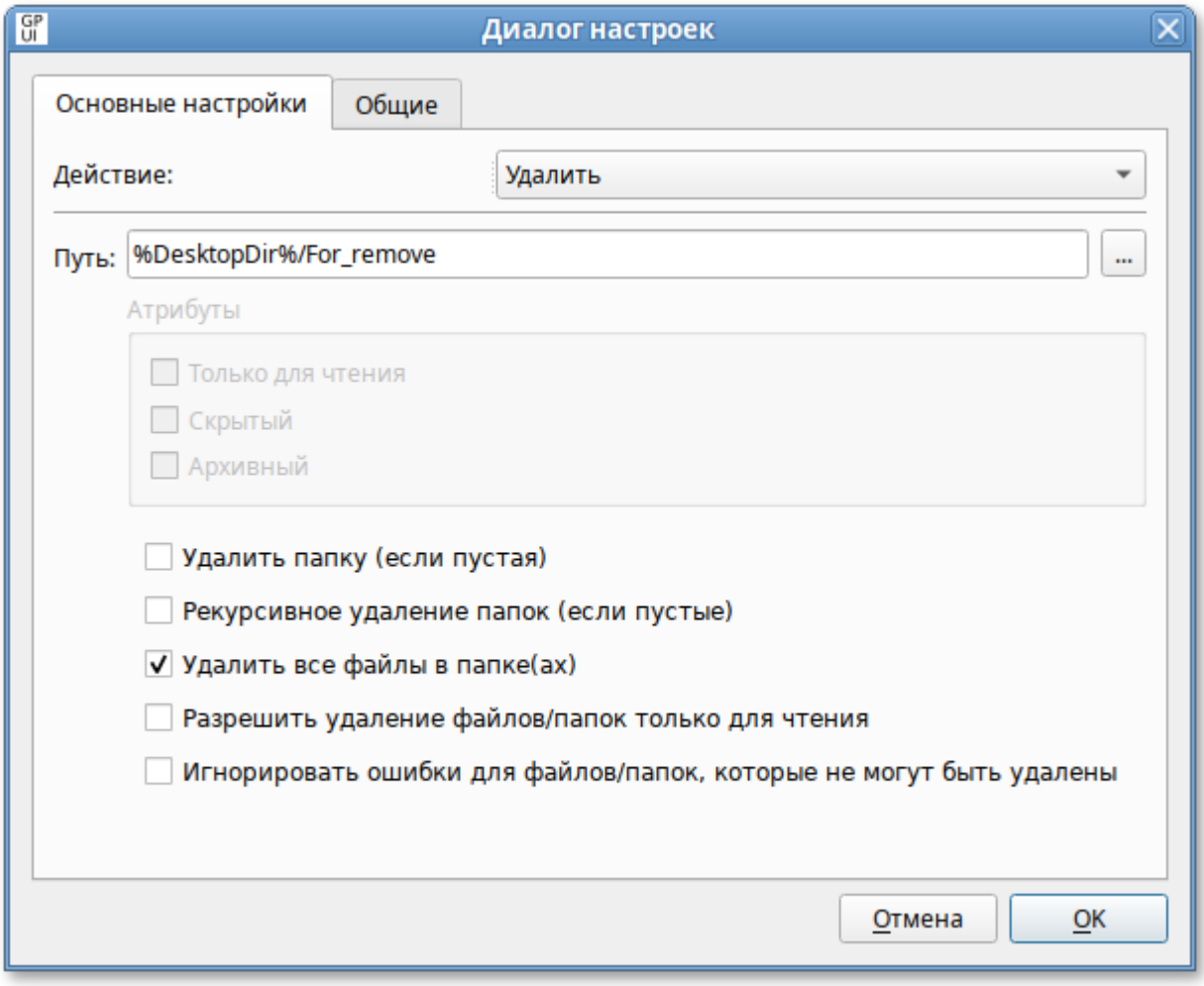
- **Остановить обработку элементов в этом расширении при возникновении ошибки** — при сбое элемента предпочтений обработка других элементов предпочтений в этом расширении останавливается;
- **Выполнять в контексте безопасности текущего пользователя (опция пользовательских политик)**;
- **Удалить элемент, если больше не применим**;
- **Описание**.



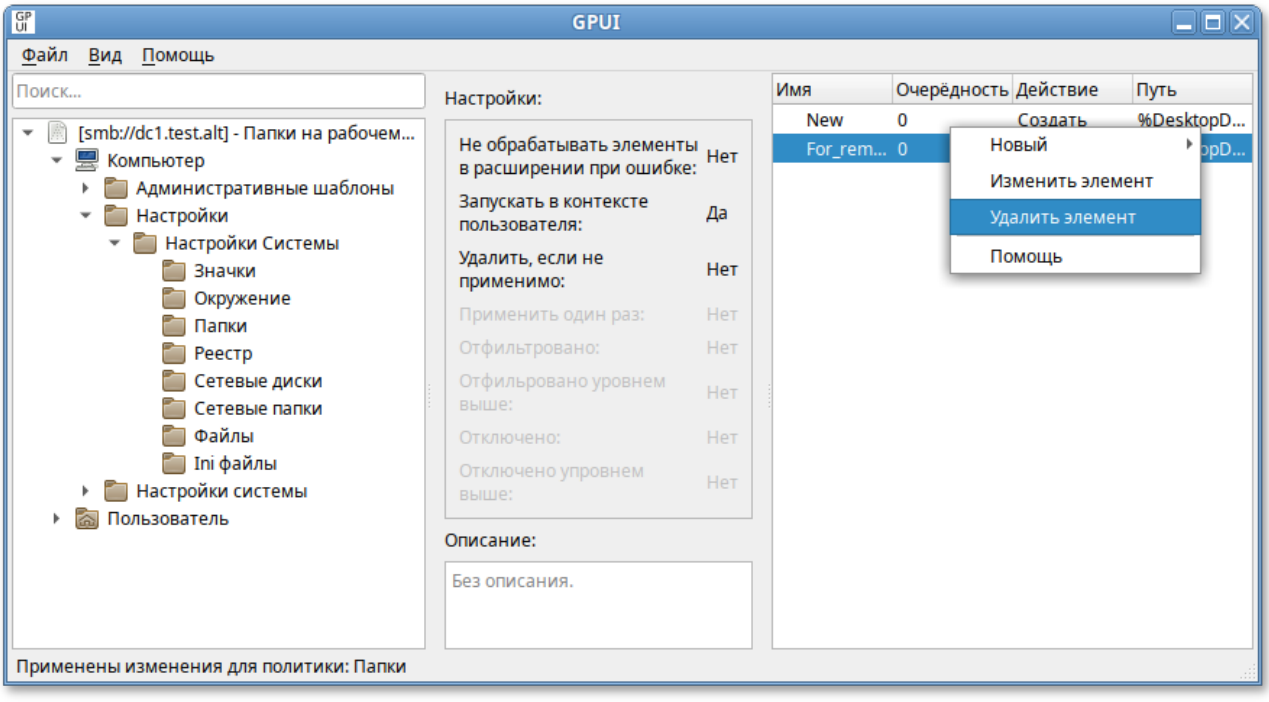
Для редактирования элемента предпочтения следует дважды щелкнуть мышью по элементу (или в контекстном меню предпочтения выбрать пункт **Изменить элемент**):



Откроется окно редактирования предпочтения:



Для удаления элемента следует в контекстном меню предпочтения выбрать пункт **Удалить элемент**:

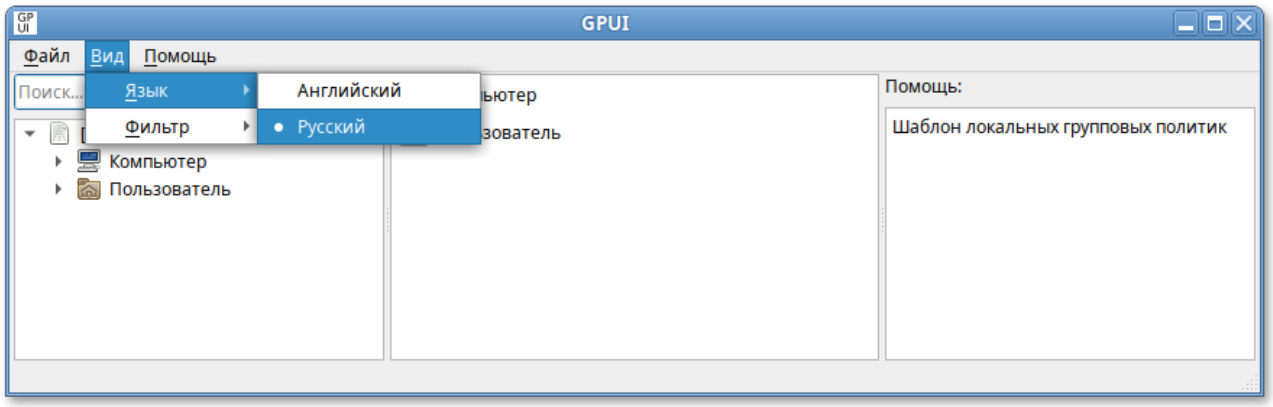


29.4.4. Работа со скриптами

Работа со скриптами подробно описана на странице: Управление logon-скриптами.

29.4.5. Смена языка

Для того чтобы изменить язык интерфейса, необходимо в меню выбрать **Вид** → **Язык**:

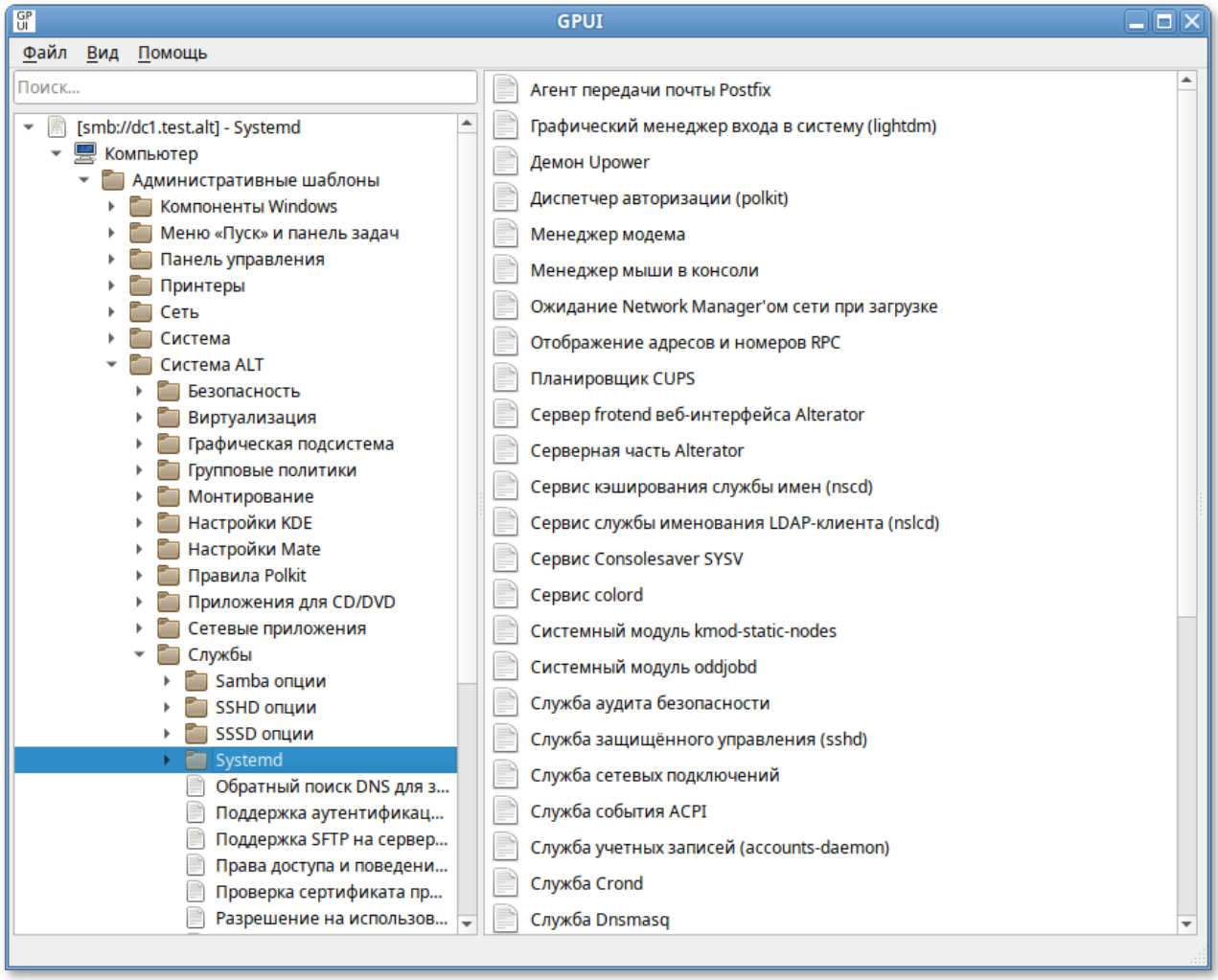


29.5. Редактирование групповых политик

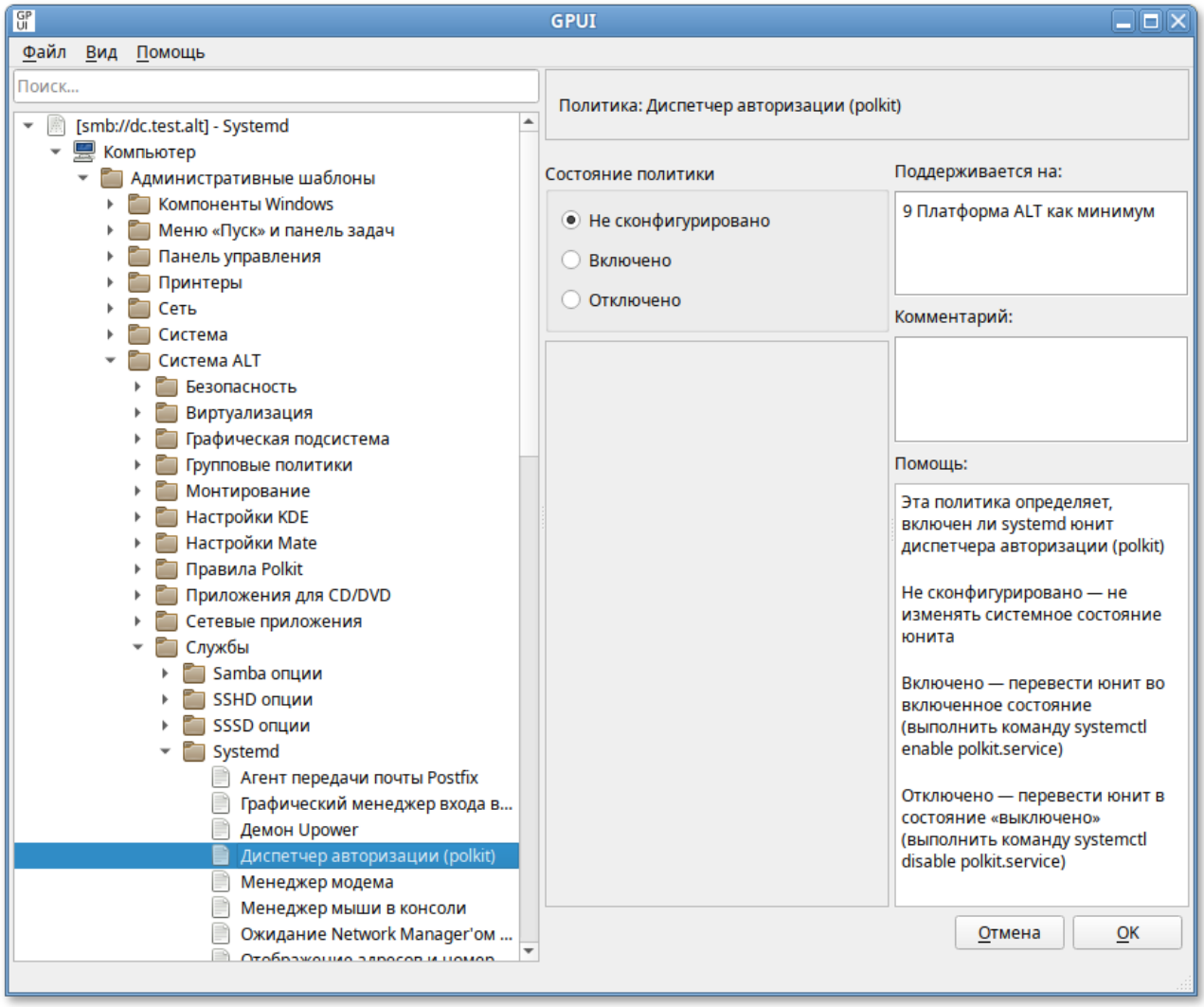
29.5.1. Включение или выключение различных служб (сервисов systemd)

Данные групповые политики позволяют управлять состоянием (включением или выключением) различных служб (сервисов systemd).

Для настройки политики следует перейти в **Компьютер** → **Административные шаблоны** → **Система ALT** → **Службы** → **Systemd**:



При выборе политики откроется диалоговое окно настройки политики:



Можно не задавать настройку политики, включить или отключить:

- **`Не сконфигурировано`** — не изменять системное состояние службы;
- **`Включено`** — перевести службу во включенное состояние (выполнить команду **`systemctl enable <служба>`**);
- **`Отключено`** — перевести службу в состояние выключено (выполнить команду **`systemctl disable <служба>`**).

Таблица 29.2. Список служб, состояние которых можно изменить, настроив соответствующую политику в GPUI

Служба	Описание	Сервис Systemd
Менеджер модема	Политика определяет, включен ли systemd юнит диспетчера модемов	ModemManager.service
Ожидание Network Manager'ом сети при загрузке	Политика определяет, включен ли systemd юнит «Network Manager Wait Online»	NetworkManager-wait-online.service
Управление службой Network Manager		NetworkManager.service

Служба	Описание	Сервис Systemd
	Политика определяет, включен ли systemd юнит «Network Manager»	
Служба учётных записей (accounts-daemon)	Политика определяет, включен ли systemd юнит службы учётных записей (accounts-daemon)	accounts-daemon.service
Служба события ACPI	Политика определяет, включен ли systemd юнит системной службы событий ACPI	acpid.service
Сервер frontend веб-интерфейса Alterator	Политика определяет, включен ли systemd юнит веб-сервера frotend WWW интерфейса Alterator	ahttpd.service
Серверная часть Alterator	Политика определяет, включен ли systemd юнит внутреннего сервера Alterator	alteratord.service
Служба аудита безопасности	Политика определяет, включен ли системный модуль службы аудита безопасности	auditd.service
Avahi mDNS/DNS-SD	Политика определяет, включен ли systemd юнит стека mDNS/DNS-SD Avahi	avahi-daemon.service
DNS-сервер BIND	Политика определяет, включен ли systemd юнит DNS-сервера (сервиса) BIND (Berkeley Internet Name Domain)	bind.service
Chronyd (служба NTP)	Политика определяет, включен ли systemd юнит NTP клиента/сервера Chronyd	chronyd.service
Сервис colord	Политика определяет, включен ли systemd юнит colord (сервис для управления, установки и создания цветовых профилей)	colord.service
Сервис Consolesaver SYSV	Политика определяет, включен ли systemd юнит Consolesaver (SYSV: этот пакет загружает конфигурацию энергосбережения консоли)	consolesaver.service
Cpufreq-simple сервис		cpufreq-simple.service

Служба	Описание	Сервис Systemd
	Политика определяет, включен ли systemd юнит службы Cpufreq-simple (загружает модули ядра, необходимые для масштабирования cpufreq)	
Служба Crond	Политика определяет, включен ли systemd юнит службы Cron	crond.service
Шина системных сообщений D-Bus	Политика определяет, включен ли systemd юнит шины системных сообщений D-Bus	dbus.service
Служба Dnsmasq	Политика определяет, включен ли systemd юнит службы Dnsmasq (облегченный DHCP и кеширующий DNS-сервер, а также TFTP-сервер для поддержки загрузки по сети)	dnsmasq.service
Менеджер мыши в консоли	Политика определяет, включен ли sytemd юнит диспетчера мыши консоли	gpm.service
Системный модуль kmod-static-nodes	Политика определяет, включен ли systemd юнит kmod-static-nodes (создаёт список необходимых статических узлов устройства для текущего ядра)	kmod-static-nodes.service
Kerberos 5 KDC	Политика определяет, включен ли systemd юнит Kerberos 5 KDC	krb5kdc.service
Графический менеджер входа в систему (lightdm)	Политика определяет, включен ли systemd юнит службы графического менеджера входа в систему	lightdm.service
Служба сетевых подключений	Политика определяет, включен ли systemd юнит службы сетевых подключений	network.service
Samba NMB сервис	Политика определяет, включен ли systemd юнит сервиса Samba NMB	nmb.service
Сервис кеширования службы имен (nscd)	Политика определяет, включён ли systemd юнит сервиса кеширования службы имен	nscd.service
Сервис службы именования LDAP-клиента (nslcd)		nslcd.service

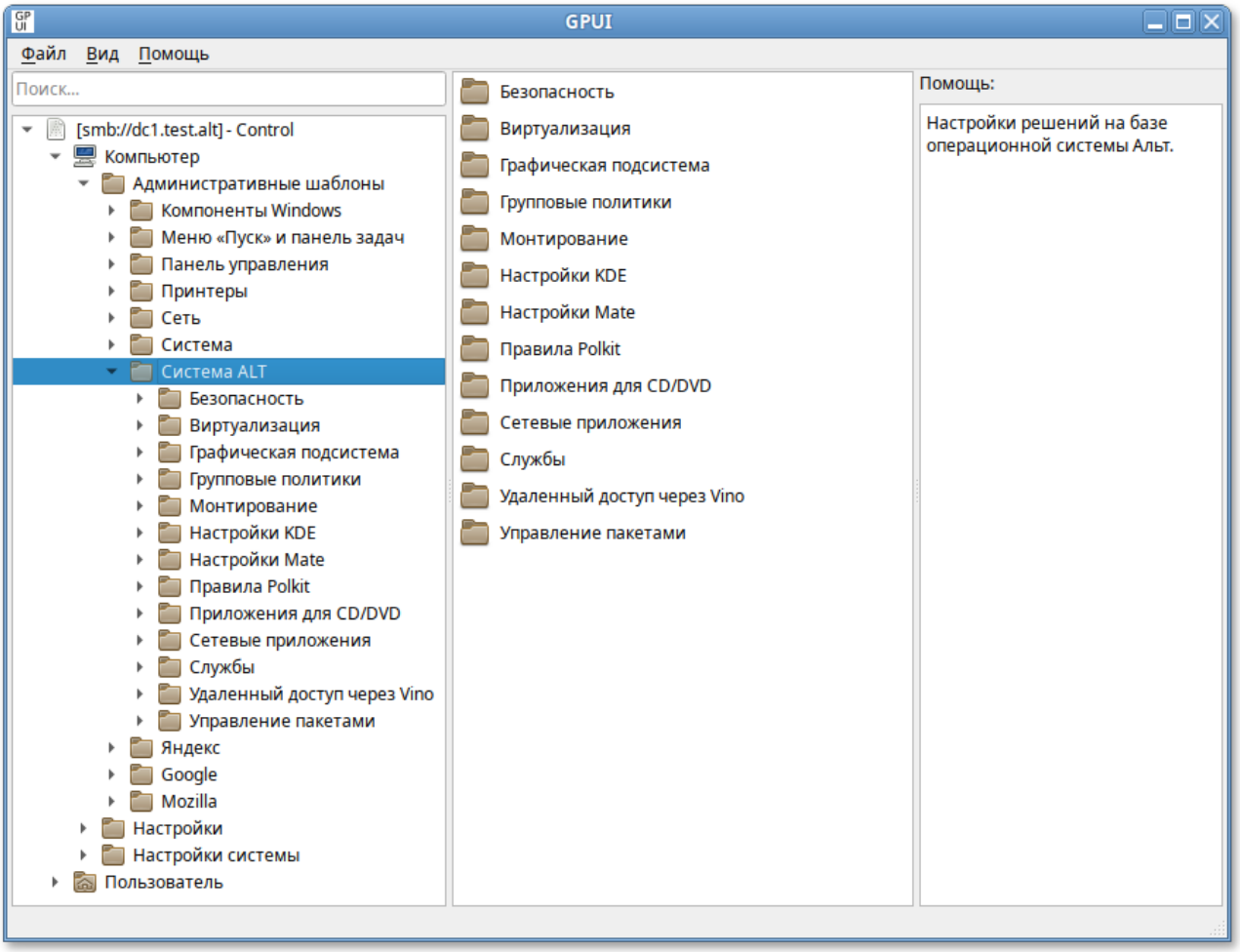
Служба	Описание	Сервис Systemd
	Политика определяет, включен ли systemd юнит сервиса служб именования клиента LDAP	
Системный модуль oddjobd	Политика определяет, включен ли systemd юнит oddjobd (используется для запуска привилегированных операций для непривилегированных процессов)	oddjobd.service
SYSV: интерфейс терминала смарт-карт	Политика определяет, включен ли systemd юнит Openct (SYSV: терминал смарт-карт)	openct.service
Планировщик CUPS	Политика определяет, включен ли systemd юнит Service CUPS (планировщик)	org.cups.cupsd.service
Служба PC/SC Smart Card	Политика определяет, включен ли systemd юнит службы поддержки PC/SC Smart Card	pcscd.service
Диспетчер авторизации (polkit)	Политика определяет, включен ли systemd юнит диспетчера авторизации (polkit)	polkit.service
Агент передачи почты Postfix	Политика определяет, включен ли systemd юнит агента передачи почты Postfix	postfix.service
Сервис отображения универсальных адресов и номеров программ RPC	Политика определяет, включен ли systemd юнит RPC bind	rpcbind.service
Samba SMB сервис	Политика определяет, включен ли systemd юнит сервис Samba SMB	smb.service
Служба защищенного управления (sshd)	Политика определяет, включен ли systemd юнит демона сервера OpenSSH	sshd.service
Демон Upower	Политика определяет, включен ли systemd юнит Daemon Upower (управление питанием)	upower.service
Samba Winbind сервис	Политика определяет, включен ли systemd юнит Samba Winbind	winbind.service

29.5.2. Управление control framework

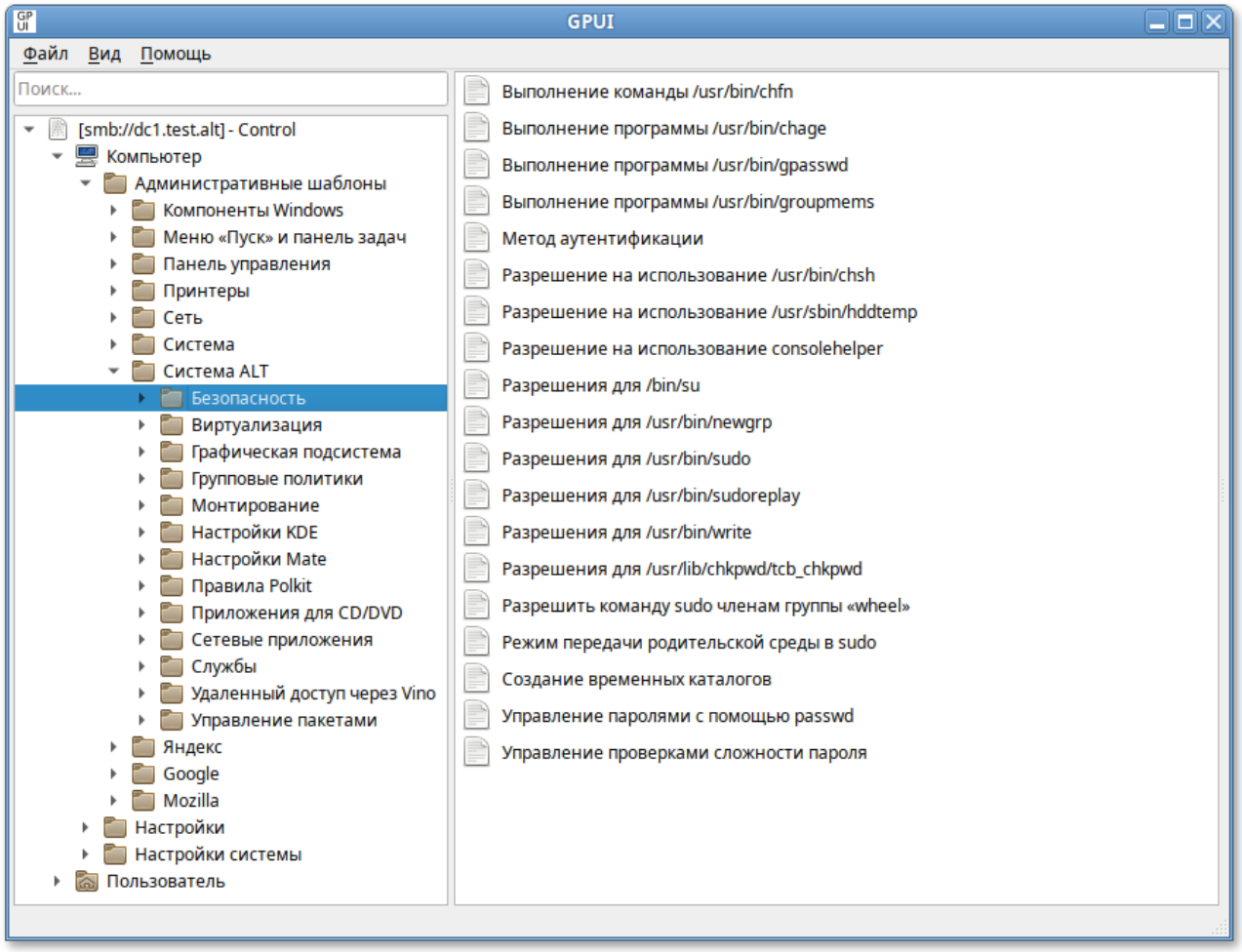
Через групповые политики реализовано управление настройками control.

control — использующийся в ОС «Альт» механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор. Подсистема control используется для управления доступом к службам и позволяет переключать многие системные службы между заранее определенными состояниями.

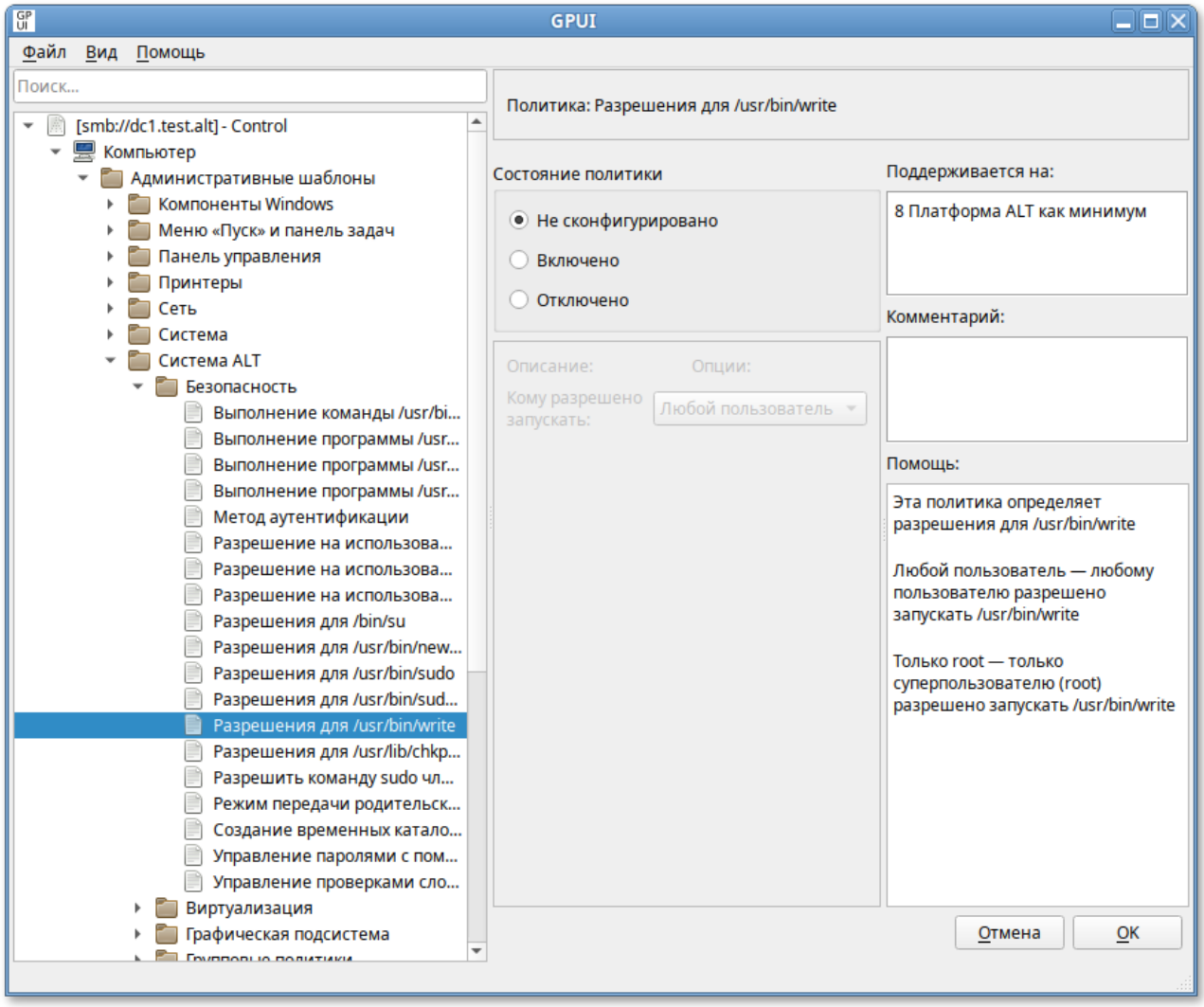
Для настройки политики следует перейти в **Компьютер** → **Административные шаблоны** → **Система ALT**. В этом разделе есть несколько подразделов, соответствующих категориям control:



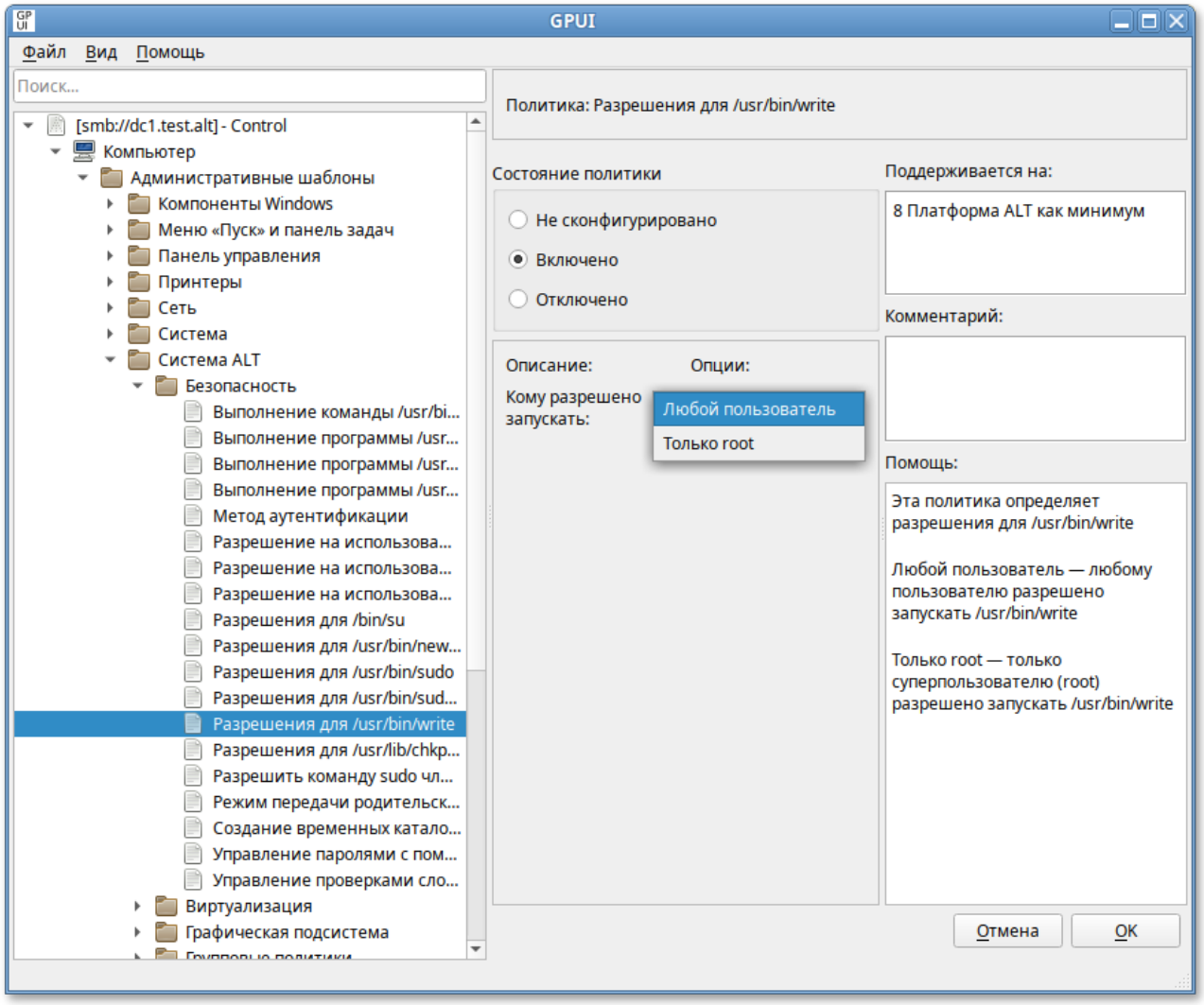
После выбора категории в правом окне редактора отобразится список политик:



При выборе политики откроется диалоговое окно настройки политики:



Можно не задавать настройку политики, включить или отключить. Если выбрать параметр **Включено**, в разделе **Параметры** в выпадающем списке можно выбрать режим доступа для данного control:



Все control в GPUI разделены на категории:

- Безопасность;
- Службы;
- Сетевые приложения;
- Приложения для CD/DVD;
- Монтирование;
- Виртуализация;
- Графическая подсистема.

Таблица 29.3. Категория «Безопасность»

Политика	Control	Описание	Режимы
Выполнение программы **/usr/bin/chage**	chage	Политика позволяет контролировать доступ для выполнения программы **/usr/bin/chage**	

Политика	Control	Описание	Режимы
			• **Только root** — только суперпользователь (root) может выполнить **/usr/bin/chage** • **Любой пользователь** — любой пользователь может просмотреть, когда ему следует сменить свой пароль, используя команду **chage -l имя_пользователя**
Выполнение программы **/usr/bin/chfn**	chfn	Политика позволяет контролировать поведение и права доступа к команде **chfn** (**/usr/bin/chfn**). Команда **chfn** может изменить полное имя пользователя, номер кабинета, номера офисного и домашнего телефона для учётной записи пользователя. Обычный пользователь может изменять поля только для своей учётной записи, с учётом ограничений в **/etc/login.defs** (конфигурация по умолчанию не позволяет пользователям менять свое полное имя)	• **Только root** — только суперпользователь (root) может выполнить **/usr/bin/chfn** • **Любой пользователь** — любой пользователь может использовать команду **/usr/bin/chfn**
Выполнение программы **/usr/bin/chsh**	chsh	Политика позволяет управлять правами доступа к команде **chsh** (**/usr/bin/chsh**). Команда **chsh** позволяет изменить командную оболочку (или интерпретатор командной строки), запускаемую по умолчанию при регистрации пользователя в текстовой консоли (по умолчанию используется **/bin/bash**). Обычный пользователь может изменить командную оболочку только для своей учётной записи (командная оболочка должна быть перечислена в файле **/etc/**	• **Только root** — только суперпользователь (root) может выполнить **/usr/bin/chsh** • **Все пользователи** — любой пользователь может использовать команду **/usr/bin/chsh**

Политика	Control	Описание	Режимы
		shells). Суперпользователь может изменить настройки для любой учётной записи (могут быть указаны любые значения)	
Разрешение на использование **consolehelper**	consolehelper	Определяет права доступа к инструменту **consolehelper** (**/usr/lib/consolehelper/priv/auth**), который позволяет пользователям консоли запускать системные программы, выполняя аутентификацию через PAM. Когда это возможно, аутентификация выполняется графически; в противном случае выполняется в текстовой консоли, с которой был запущен **consolehelper**	**Любой пользователь** — любой пользователь может использовать **consolehelper** **Только wheel** — только члены группы «wheel» могут использовать команду **consolehelper** **Только root** — только суперпользователь (root) может использовать **consolehelper**
Выполнение программы **/usr/bin/gpasswd**	gpasswd	Определяет права на запуск инструмента **/usr/bin/gpasswd**	**Любой пользователь** — любой пользователь может выполнить **/usr/bin/gpasswd** **Только wheel** — только члены группы «wheel» могут выполнять **/usr/bin/gpasswd** **Только root** — только суперпользователь (root) может выполнить **/usr/bin/gpasswd**
Выполнение программы **/usr/bin/groupmems**	groupmems	Определяет права на выполнение программы **/usr/bin/groupmems**	**Любой пользователь** — любой пользователь может выполнить **/usr/bin/groupmems** **Только wheel** — только члены группы «wheel» могут выполнять команду **/usr/bin/groupmems** **Только root** — только суперпользователь (root) может выполнить **/usr/bin/groupmems**

Политика	Control	Описание	Режимы
Выполнение программы **/usr/sbin/hddtemp**	groupmems	Разрешение на использование инструмента **/usr/sbin/hddtemp** — отслеживание температуры жёсткого диска	**Любой пользователь** — любой пользователь может выполнить **/usr/sbin/hddtemp** **Только wheel** — только члены группы «wheel» могут выполнять **/usr/sbin/hddtemp** **Только root** — только суперпользователь (root) может выполнить **/usr/sbin/hddtemp**
Разрешения для **/usr/bin/newgrp**	newgrp	Разрешение на использование инструмента **/usr/bin/newgrp**	**Любой пользователь** — любой пользователь может выполнить **/usr/bin/newgrp** **Только wheel** — только члены группы «wheel» могут выполнять **/usr/bin/newgrp** **Только root** — только суперпользователь (root) может выполнить **/usr/bin/newgrp**
Создание временных каталогов	pam_mktemp	Определяет, следует ли создавать отдельные временные каталоги для пользователей	**Отключено** — отключить создание отдельных временных каталогов для пользователей **Включено** — включить создание отдельных временных каталогов для пользователей
Управление паролями с помощью **passwd**	passwd	Определяет политику управления паролями с помощью команды **/usr/bin/passwd**	

Политика	Control	Описание	Режимы
			TCB — любой пользователь может изменить свой пароль, используя **/usr/bin/passwd**, когда включена схема tcb **Традиционный (схема tcb отключена)** — любой пользователь может изменить свой пароль, используя **/usr/bin/passwd**, когда схема tcb отключена **Только root** — только суперпользователь (root) имеет право изменять пароли пользователей
Управление проверками сложности пароля	passwdqc-enforce	Политика управляет паролями для достаточной надежности пароля	**Все** — включить проверку сложности пароля для всех пользователей **Только для пользователей** — включить проверку сложности пароля для всех пользователей, кроме суперпользователей
Разрешения для **/bin/su**	su	Определяет разрешения для **/bin/su**	**Любой пользователь** — любой пользователь может запускать **/bin/su** **Все пользователи, кроме root** — любой пользователь может запускать **/bin/su**, но только пользователи группы «wheel» могут повышать привилегии суперпользователя **Только wheel** — только пользователи из группы «wheel» могут запускать **/bin/su**

Политика	Control	Описание	Режимы
			Только root — только суперпользователь (root) может запускать **/bin/su**
Разрешения для **/usr/bin/sudo**	sudo	Определяет разрешения для **/usr/bin/sudo**	**Любой пользователь** — любой пользователь может запускать **/usr/bin/sudo** **Только wheel** — только пользователи из группы «wheel» могут запускать **/usr/bin/sudo** **Только root** — только суперпользователь (root) может запускать **/usr/bin/sudo**
Режим передачи родительской среды в sudo	sudoers	Определяет, передаются ли переменные среды в sudo	**Строгий** — не передавать переменные окружения дочернему процессу **Слабый** — передать переменные окружения дочернему процессу
Разрешения для **/usr/bin/sudoreplay**	sudoreplay	Определяет разрешения для **/usr/bin/sudoreplay**	**Любой пользователь** — любой пользователь может запускать **/usr/bin/sudoreplay** **Только wheel** — только пользователи из группы «wheel» могут запускать **/usr/bin/sudoreplay** **Только root** — только суперпользователь (root) может запускать **/usr/bin/sudoreplay**
Разрешить команду **sudo** членам группы «wheel»	sudowheel	Эта политика разрешает или запрещает членам группы «wheel» применять команду **sudo**. Если политика	

Политика	Control	Описание	Режимы
		включена, пользователи, входящие в группу «wheel», могут повысить системные привилегии через команду **sudo**. Если политика не сконфигурирована или отключена, пользователи, входящие в группу «wheel», не смогут применить команду **sudo**	**Отключено** — пользователи группы «wheel» не могут повысить привилегии через команду **sudo** **Включено** — пользователи группы «wheel» могут повысить привилегии через команду **sudo**
Метод аутентификации	system-auth	Определяет метод аутентификации пользователя	**Winbind** — использовать Winbind для аутентификации **SSSD** — использовать метод проверки подлинности демона System Security Services
Разрешения для **/usr/lib/chkpwd/tcb_chkpwd**	tcb_chkpwd	Определяет разрешения для привилегированного помощника **/usr/lib/chkpwd/tcb_chkpwd**	**Любой пользователь с отключенным tcb** — любой пользователь может быть аутентифицирован с использованием привилегированного помощника **/usr/lib/chkpwd/tcb_chkpwd** когда отключена схема tcb **Любой пользователь с включенным tcb** — любой пользователь может аутентифицироваться с помощью привилегированного помощника **/usr/lib/chkpwd/tcb_chkpwd** если включена схема tcb

Политика	Control	Описание	Режимы
			Только root — только суперпользователь (root) может быть аутентифицирован с помощью **/usr/lib/chkpwd/tcb_chkpwd**
Разрешения для **/usr/bin/write**	write	Определяет разрешения для **/usr/bin/write**	**Любой пользователь** — любой пользователь может запускать **/usr/bin/write** **Только root** — только суперпользователь (root) может запускать **/usr/bin/write**

Примечание

Для поддержки общих сетевых ресурсов с помощью политик на клиенте должны быть выполнены следующие условия:

- установлен пакет *samba-usershares*;
- в файле **/etc/samba/smb.conf** в секции [global] подключен файл **/etc/samba/usershares.conf** (include = /etc/samba/usershares.conf).

Таблица 29.4. Категория «Службы»

Политика	Control	Описание	Режимы
Права доступа и поведение очереди заданий **/usr/bin/at**	at	Политика позволяет контролировать поведение и права доступа для запуска очереди заданий (права доступа для запуска **/usr/bin/at**)	**Все пользователи** — всем пользователям разрешено запускать **/usr/bin/at** **Только root** — только суперпользователь (root) может запускать **/usr/bin/at** **Режим совместимости** — режим «atdaemon» (не должен использоваться)
Режим демона NTP Chrony	chrony		

Политика	Control	Описание	Режимы
		Политика определяет режим работы (конфигурацию) демона Chrony, который реализует функции сетевого протокола времени	**Сервер** — в файл конфигурации будет добавлена директива «allow all» **Клиент** — директива «allow» в файле конфигурации демона будет закомментирована
Разрешение на использование **crontab**	crontab	Политика определяет права доступа к инструменту **crontab** (**/usr/bin/crontab**)	**Любой пользователь** — любой пользователь может использовать **/usr/bin/crontab** **Только root** — только суперпользователь (root) может использовать **/usr/bin/crontab**
Режим CUPS	cups	Политика определяет поведение CUPS	**Внешний интерфейс IPP** — внешний интерфейс IPP доступен для пользователя **Только локальные утилиты** — только локальные утилиты могут работать с CUPS
Обратный поиск DNS для запросов OpenLDAP	ldap-reverse-dns-lookup	Политика определяет, разрешен ли обратный поиск DNS для запросов OpenLDAP	**Разрешено** — выполнять обратный поиск DNS для запросов OpenLDAP **Не разрешено** — не выполнять обратный поиск DNS для запросов OpenLDAP **По умолчанию** — выполнять обратный поиск DNS для запросов OpenLDAP
	ldap-tls-cert-check		

Политика	Control	Описание	Режимы
Проверка сертификата при установлении соединений TLS OpenLDAP		Политика определяет режим проверки сертификата при установке TLS соединений OpenLDAP	**По умолчанию** — установить соединение только с правильным сертификатом **Никогда** — не выполнять никаких проверок **Разрешить** — установить соединение, даже если сертификат отсутствует или неверный **Пробовать** — установить соединение, если нет сертификата или с действующим сертификатом **Требовать** — установить соединение только с правильным сертификатом
Режим работы Postfix MTA	postfix	Политика определяет режим работы MTA Postfix (почтовый транспортный агент)	**Локальный (отключен)** — Postfix MTA отключен **Сервер (фильтры отключены)** — Postfix MTA включен без почтовых фильтров **Фильтр** — Postfix MTA включен с почтовыми фильтрами
Разрешения для **/usr/sbin/postqueue**	postqueue	Определяет разрешения для **/usr/sbin/postqueue**	**Любой пользователь** — любому пользователю разрешено запускать **/usr/sbin/postqueue** **Группа mailadm** — пользователям из группы «mailadm» разрешено запускать **/usr/sbin/postqueue** **Только root** — только суперпользователю (root) разрешено запускать **/usr/sbin/postqueue**

Политика	Control	Описание	Режимы
Режим работы Rpcbind	rpcbind	Политика определяет режим работы **rpcbind** (**/sbin/rpcbind**)	**Сервер** — rpcbind будет прослушивать входящие соединения из сети **Локальный** — rpcbind будет принимать только локальные запросы
Поддержка SFTP на сервере OpenSSH	sftp	Политика определяет поддержку SFTP на сервере OpenSSH	**Включено** — включить поддержку SFTP на сервере OpenSSH **Отключено** — отключить поддержку SFTP на сервере OpenSSH
Поддержка аутентификации OpenSSH-клиентов через GSSAPI	ssh-gssapi-auth	Эта политика определяет функциональные возможности поддержки аутентификации OpenSSH-клиентов через GSSAPI	**Включено** — поддержка аутентификации через GSSAPI для OpenSSH-клиентов включена **Отключено** — поддержка аутентификации через GSSAPI для OpenSSH-клиентов отключена
Samba опции			
Гостевой доступ к общим каталогам	smb-conf-usershare-allow-guests	Политика управляет возможностью предоставления гостевого доступа общему ресурсу. Данная политика управляет параметром **usershare allow guests** в файле **/etc/samba/usershares.conf**.	**Включено** — разрешить предоставление гостевого доступа к общему ресурсу; разрешить создание общих каталогов с параметром доступа без авторизации (**usershare allow guests = yes**) **Отключено** — запретить предоставление гостевого доступа к общему ресурсу; запретить создание общих каталогов с

Политика	Control	Описание	Режимы
			параметром доступа без авторизации (**`usershare allow guests = no`**)
Доступ к общим каталогам других пользователей	smb-conf-usershare-owner-only	Политика управляет правом пользователя на предоставление общего доступа или доступ к каталогу, если пользователь не является владельцем этого каталога. Данная политика управляет параметром **`usershare owner only`** в файле **`/etc/samba/usershares.conf`**.	**Включено** — запретить предоставление общего доступа не владельцу каталога; запретить доступ к общим каталогам пользователей, без проверки владельца каталога (**`usershare owner only = yes`**) **Отключено** — разрешить предоставление общего доступа не владельцу каталога; разрешить доступ к общим каталогам пользователей, без проверки владельца каталога (**`usershare owner only = no`**)
Доступ членам группы «sambashare» к управлению общими каталогами	role-sambashare	Политика управляет разрешением членам группы «sambashare» управлять общими каталогами. Конфигурации пользовательских общих ресурсов расположены в каталоге **`/var/lib/samba/usershares`**, права на запись в котором имеют члены группы «usershares». Данная политика позволяет расширить привилегии членов группы «sambashare», добавляя их в группу «usershares».	**Включено** — разрешить членам группы «sambashare» управлять общими каталогами **Отключено** — запретить членам группы «sambashare» управлять общими каталогами
	role-usershares	Политика управляет разрешением членам группы «users» управлять общими каталогами.	

Политика	Control	Описание	Режимы
Доступ членам группы «users» к управлению общими каталогами		Конфигурации пользовательских общих ресурсов расположены в каталоге **/var/lib/samba/usershares**, права на запись в котором имеют члены группы «usershares». Данная политика позволяет расширить привилегии членов группы «users», добавляя их в группу «usershares».	**Включено** — разрешить членам группы «users» управлять общими каталогами **Отключено** — запретить членам группы «users» управлять общими каталогами. Данный параметр также влияет на разрешение управления общими каталогами через настройку предпочтений
Запрет на создание общих каталогов в системных каталогах	smb-conf-usershare-deny-list	Данная политика управляет параметром **usershare prefix deny list** в файле **/etc/samba/usershares.conf** — открывая или закрывая комментарием этот параметр. Параметр **usershare prefix deny list** определяет каталоги в корневом каталоге (/), в которых пользователю запрещено создавать общие каталоги. Если абсолютный путь к общему каталогу пользователя начинается с одного из перечисленных каталогов, то доступ к нему будет запрещен. Таким образом ограничивается список каталогов, в которых возможно создавать общие пользовательские каталоги. По умолчанию в параметре **usershare prefix deny list** заданы каталоги: **/etc**, **/dev**, **/sys**, **/proc**. Если настроен список запрещенных каталогов **usershare prefix deny list**, и список разрешенных каталогов **usershare**	**Включено** — включить список запрещенных каталогов (параметр **usershare prefix deny list** будет раскомментирован) **Отключено** — отключить список запрещенных каталогов (параметр **usershare prefix deny list** будет закомментирован)

Политика	Control	Описание	Режимы
		prefix allow list, сначала обрабатывается список запрета, а затем уже список разрешений.	
Разрешение на создание общих каталогов в системных каталогах	smb-conf-usershare-allow-list	Данная политика управляет параметром **usershare prefix allow list** в файле **/etc/samba/usershares.conf** — открывая или закрывая комментарием этот параметр. Параметр **usershare prefix allow list** определяет каталоги в корневом каталоге (/), в которых пользователю разрешено создавать общие каталоги. Если абсолютный путь к общему каталогу пользователя не начинается с одного из перечисленных каталогов, то доступ к нему будет запрещен. Таким образом ограничивается список каталогов, в которых возможно создавать общие пользовательские каталоги. По умолчанию в параметре **usershare prefix allow list** заданы каталоги: **/home**, **/srv**, **/mnt**, **/media**, **/var**. Если настроен список запрещенных каталогов **usershare prefix deny list**, и список разрешенных каталогов **usershare prefix allow list**, сначала обрабатывается список запрета, а затем уже список разрешений.	- **Включено** — включить список разрешенных каталогов (параметр **usershare prefix allow list** будет раскомментирован) - **Отключено** — отключить список разрешенных каталогов (параметр **usershare prefix allow list** будет закомментирован)
Разрешение на создание пользовательских общих каталогов	smb-conf-usershare	Политика управляет возможностью создания пользовательских общих каталогов на компьютере.	

Политика	Control	Описание	Режимы
		Дананя политика управляет параметром **`usershare max shares`** в файле **`/etc/samba/usershares.conf`**, который устанавливает предельное число общих каталогов.	**`Включено`** — включить возможность создания и использования общих каталогов пользователей (**`usershare max shares = 100`**) **`Отключено`** — отключить возможность создания и использования общих каталогов пользователей (**`usershare max shares = 0`**)
SSHD опции			
Контроль доступа по группам к серверу OpenSSH	ssh-gssapi-auth	Эта политика включает в службе удаленного доступа OpenSSH контроль доступа по списку разрешенных групп	**`Включено`** — контроль доступа по группам для службы удаленного доступа OpenSSH включен **`Отключено`** — контроль доступа по группам для службы удаленного доступа OpenSSH отключен
Группы для контроля доступа к серверу OpenSSH	sshd-allow-groups-list	Эта политика определяет, какие группы входят в список разрешенных для службы удаленного доступа к серверу OpenSSH	**`Все пользователи`** — разрешить доступ к серверу OpenSSH для групп «wheel» и «users» **`Группы wheel и remote`** — разрешить доступ к серверу OpenSSH для групп администраторов и пользователей удалённого доступа («wheel» и «remote») **`Только wheel`** — разрешить доступ к серверу OpenSSH только для группы администраторов («wheel»)

Политика	Control	Описание	Режимы
			Только remote — разрешить доступ к серверу OpenSSH только для группы «remote»
Поддержка GSSAPI-аутентификации на сервере OpenSSH	sshd-gssapi-auth	Эта политика включает поддержку аутентификации с использованием GSSAPI на сервере OpenSSH	**Включено** — поддержка GSSAPI на сервере OpenSSH включена **Отключено** — поддержка GSSAPI на сервере OpenSSH отключена
Аутентификация по паролю на сервере OpenSSH	sshd-password-auth	Эта политика включает поддержку аутентификации по паролю на сервере OpenSSH	**Включено** — поддержка аутентификации по паролю на сервере OpenSSH включена **Отключено** — поддержка аутентификации по паролю на сервере OpenSSH отключена
Аутентификация суперпользователя на сервере OpenSSH	sshd-permit-root-login	Эта политика определяет режимы аутентификации для суперпользователя (root) на сервере OpenSSH	**Только без пароля** — суперпользователю разрешена только беспарольная аутентификация на сервере OpenSSH **Разрешено** — суперпользователю разрешена аутентификация на сервере OpenSSH **Не разрешено** — суперпользователю запрещена аутентификация на сервере OpenSSH **По умолчанию** — сбросить режим аутентификации для суперпользователя на значение по умолчанию в пакете

Политика	Control	Описание	Режимы
SSSD опции			
Контроль доступа в SSSD через групповые политики	sssd-ad-gpo-access-control	Эта политика определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках Active Directory (GPO)	**Принудительный режим** — правила управления доступом в SSSD основанные на GPO выполняются, ведётся логирование **Разрешающий режим** — правила управления доступом в SSSD основанные на GPO не выполняются, ведётся только логирование. Такой режим необходим администратору, чтобы оценить как срабатывают новые правила **Отключить** — правила управления доступом в SSSD основанные на GPO не логируются и не выполняются **По умолчанию** — настройка контроля доступом в SSSD основанное на GPO сброшена на значение по умолчанию в пакете
Игнорирование политик при недоступности GPT	sssd-ad-gpo-ignore-unreadable	Эта настройка определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен какой-либо шаблон (GPT) объекта групповой политики (GPO)	**Включить** — игнорировать правила управления доступом через групповые политики, если шаблоны групповых политик не доступны для SSSD **Отключить** — запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны

Политика	Control	Описание	Режимы
			По умолчанию — настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете
Кеширование учётных данных пользователей	sssd-cache-credentials	Эта политика определяет, будут ли учётные данные удалённых пользователей сохраняться в локальном кеше SSSD	**Включить** — сохранение в локальном кеше SSSD учётных данных пользователей включено **Отключить** — сохранение в локальном кеше SSSD учётных данных пользователей отключено **По умолчанию** — настройка сохранения в локальном кеше SSSD учётных данных пользователей сброшена на значение по умолчанию в пакете
Режим привилегий службы SSSD	sssd-drop-privileges	Эта политика позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	**Привилегированный** — служба SSSD запущена от имени привилегированного суперпользователя (root) **Непривилегированный** — служба SSSD запущена от имени непривилегированного пользователя (_sssd) **По умолчанию** — режим привилегий службы SSSD задан по умолчанию в пакете
Обновление DNS-записей прямой зоны	sssd-dyndns-update		

Политика	Control	Описание	Режимы
		Эта политика позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD	**Включить** — автоматическое обновление DNS-записи клиента через SSSD включено **Отключить** — автоматическое обновление DNS-записи клиента через SSSD отключено **По умолчанию** — настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете
Обновление DNS-записей обратной зоны	sssd-dyndns-update-ptr	Данная политика определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG). Эта политика работает только если включено «Обновление DNS-записей прямой зоны»	**Включить** — автоматическое обновление DNS-записи обратной зоны через SSSD включено **Отключить** — автоматическое обновление DNS-записи обратной зоны через SSSD отключено **По умолчанию** — настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете

Таблица 29.5. Категория «Сетевые приложения»

Политика	Control	Описание	Режимы
Разрешение на использование **/usr/bin/mtr**	mtr	Разрешение на использование сетевого инструмента **/usr/bin/mtr**	**Любой пользователь** — любой пользователь может выполнить **/usr/bin/mtr**

Политика	Control	Описание	Режимы
			Группа netadmin — только члены группы «netadmin» могут выполнять **/usr/bin/mtr** **Только root** — только суперпользователь (root) может выполнить **/usr/bin/mtr**
Разрешения для **/usr/bin/ping**	ping	Эта политика определяет разрешения для **/usr/bin/ping**	**Любой пользователь** — любой пользователь может запускать **/usr/bin/ping** **Группа netadmin** — пользователям из группы «netadmin» разрешено запускать **/usr/bin/ping** **Только root** — только суперпользователь (root) может запускать **/usr/bin/ping** **Любой пользователь (в контейнерах)** — любой пользователь может запускать **/usr/bin/ping** (в контейнерах) **Группа netadmin (в контейнерах)** — пользователям из группы «netadmin» разрешено запускать **/usr/bin/ping** (в контейнерах)
Разрешения для **/usr/sbin/pppd**	ppp	Эта политика определяет разрешения для **/usr/sbin/pppd**	**Только root** — только суперпользователю (root) разрешено запускать **/usr/sbin/pppd** **Традиционный** — любой пользователь имеет право запустить **/usr/sbin/pppd** без повышения привилегий

Политика	Control	Описание	Режимы
			Группа uucp — пользователям из группы «uucp» имеют право запускать **/usr/sbin/pppd** с правами суперпользователя **Любой пользователь** — любой пользователь имеет право запускать **/usr/sbin/pppd** с правами суперпользователя
Разрешения для wireshark-capture (**dumpcap**)	wireshark-capture	Эта политика определяет функциональные возможности (режимы) разрешения для захвата wireshark (**/usr/bin/dumpcap**)	**Любой пользователь** — любой пользователь имеет право запустить **/usr/bin/dumpcap**, захват трафика включен **Любой пользователь, без захвата трафика** — любой пользователь имеет право запустить **/usr/bin/dumpcap**, захват трафика отключен **Группа netadmin** — пользователям из группы «netadmin» имеют право запускать **/usr/bin/dumpcap** **Только root** — только суперпользователь (root) может запускать **/usr/bin/dumpcap**

Таблица 29.6. Категория «Приложения для CD/DVD»

Политика	Control	Описание	Режимы
Разрешение на использование **/usr/bin/dvd-ram-control**	dvd-ram-control	Эта политика определяет права доступа к **/usr/bin/dvd-ram-control**	**Только cdwriter** — только члены группы «cdwriter» могут выполнять **/usr/bin/dvd-ram-control**

Политика	Control	Описание	Режимы
			Только root — только суперпользователь (root) может выполнять **/usr/bin/dvd-ram-control** **Режим совместимости** — режим совместимости, не должен использоваться
Разрешения на использование **/usr/bin/dvd+rw-booktype**	dvd+rw-booktype	Эта политика определяет права доступа к **/usr/bin/dvd+rw-booktype**	**Только cdwriter** — только члены группы «cdwriter» могут выполнять **/usr/bin/dvd+rw-booktype** **Только root** — только суперпользователь (root) может выполнять **/usr/bin/dvd+rw-booktype** **Режим совместимости** — режим совместимости, не должен использоваться
Разрешения на использование **/usr/bin/dvd+rw-format**	dvd+rw-format	Эта политика определяет права доступа к **/usr/bin/dvd+rw-format**	**Только cdwriter** — только члены группы «cdwriter» могут выполнять **/usr/bin/dvd+rw-format** **Только root** — только суперпользователь (root) может выполнять **/usr/bin/dvd+rw-format** **Режим совместимости** — режим совместимости, не должен использоваться
Разрешения на использование **/usr/bin/dvd+rw-mediainfo**	dvd+rw-mediainfo	Эта политика определяет права доступа к **/usr/bin/dvd+rw-mediainfo**	**Только cdwriter** — только члены группы «cdwriter» могут выполнять **/usr/bin/dvd+rw-mediainfo**

Политика	Control	Описание	Режимы
			Только root — только суперпользователь (root) может выполнять **/usr/bin/dvd+rw-mediainfo** **Режим совместимости** — режим совместимости, не должен использоваться
Разрешения на использование **/usr/bin/growisofs**	growisofs	Эта политика определяет права на использование инструмента **/usr/bin/growisofs**	**Только cdwriter** — только члены группы «cdwriter» могут выполнять **/usr/bin/growisofs** **Только root** — только суперпользователь (root) может выполнять **/usr/bin/growisofs** **Режим совместимости** — режим совместимости, не должен использоваться

Таблица 29.7. Категория «Монтирование»

Политика	Control	Описание	Режимы
Доступ к инструментам FUSE	fusermount	Эта политика определяет права доступа для монтирования файловой системы FUSE (выполнение программ **/usr/bin/fusermount** и **/usr/bin/fusermount3**)	**Любой пользователь** — любой пользователь может выполнить **/usr/bin/fusermount** и **/usr/bin/fusermount3** **Только fuse** — только члены группы «fuse» могут выполнять **/usr/bin/fusermount** и **/usr/bin/fusermount3** **Только wheel** — только члены группы «wheel» могут выполнять **/usr/bin/fusermount** и **/usr/bin/fusermount3**

Политика	Control	Описание	Режимы
			Только root — только суперпользователь (root) может выполнить **/usr/bin/fusermount** и **/usr/bin/fusermount3**
Разрешения для **/bin/mount** и **/bin/umount**	mount	Эта политика определяет разрешения для **/bin/mount** и **/bin/umount**	**Любой пользователь** — любому пользователю разрешено запускать **/bin/mount** и **/bin/umount** **Группа wheel** — пользователям из группы «wheel» разрешено запускать **/bin/mount** и **/bin/umount** **Непривилегированный пользователь** — любой пользователь может запускать **/bin/mount** и **/bin/umount** для непривилегированных действий (не от имени root) **Только root** — только суперпользователь (root) может запускать **/bin/mount** и **/bin/umount**
Разрешения для **/sbin/mount.nfs**	nfsmount	Эта политика определяет разрешения для **/sbin/mount.nfs**	**Любой пользователь** — любому пользователю разрешено запускать **/sbin/mount.nfs** **Только wheel** — пользователям из группы «wheel» разрешено запускать **/sbin/mount.nfs** **Только root** — только суперпользователю (root) может запускать **/sbin/mount.nfs**
	udisks2		

Политика	Control	Описание	Режимы
Правила подключения USB-накопителей		Эта политика определяет правила подключения USB-накопителей	**По умолчанию** — подключить накопитель индивидуально (**/run/media/$user/**) для каждого пользователя **Общий** — подключить накопитель к общедоступной точке (**/media/**)

Таблица 29.8. Категория «Виртуализация»

Политика	Control	Описание	Режимы
Разрешения для VirtualBox	virtualbox	Эта политика определяет разрешения для VirtualBox	**Любой пользователь** — любому пользователю разрешено использовать VirtualBox **Группа vboxusers** — пользователям из группы «vboxusers» разрешено использовать VirtualBox **Только root** — только суперпользователю (root) разрешено использовать VirtualBox

Таблица 29.9. Категория «Графическая подсистема»

Политика	Control	Описание	Режимы
Список пользователей в greeter (LightDM)	lightdm-greeter-hide-users	Эта политика определяет, будет ли показан список всех пользователей при входе в систему с помощью LightDM (в greeter — на экране приветствия/входа в систему LightDM) или нет	**Показать** — показать список доступных пользователей в greeter **Скрыть** — не перечислять всех пользователей в greeter
Стандартные каталоги в home	xdg-user-dirs		

Политика	Control	Описание	Режимы
		Эта политика определяет, работает ли функция стандартных каталогов (Документы, Загрузки, Изображения и т.д.) xdg-user-dirs в домашнем каталоге (home) пользователя	**Отключено** — функция сохранения списка пользовательских каталогов отключена **Группа vboxusers** — функция сохранения списка пользовательских каталогов включена
Разрешения для Xorg	xorg-server	Эта политика определяет разрешения для Xorg (**/usr/bin/Xorg**)	**Любой пользователь** — любому пользователю разрешено запускать **/usr/bin/Xorg** **Группа xgrp** — пользователям группы «xgrp» разрешено запускать **/usr/bin/Xorg** **Только root** — только суперпользователь (root) может запускать **/usr/bin/Xorg**

29.5.3. Управление настройками службы Polkit

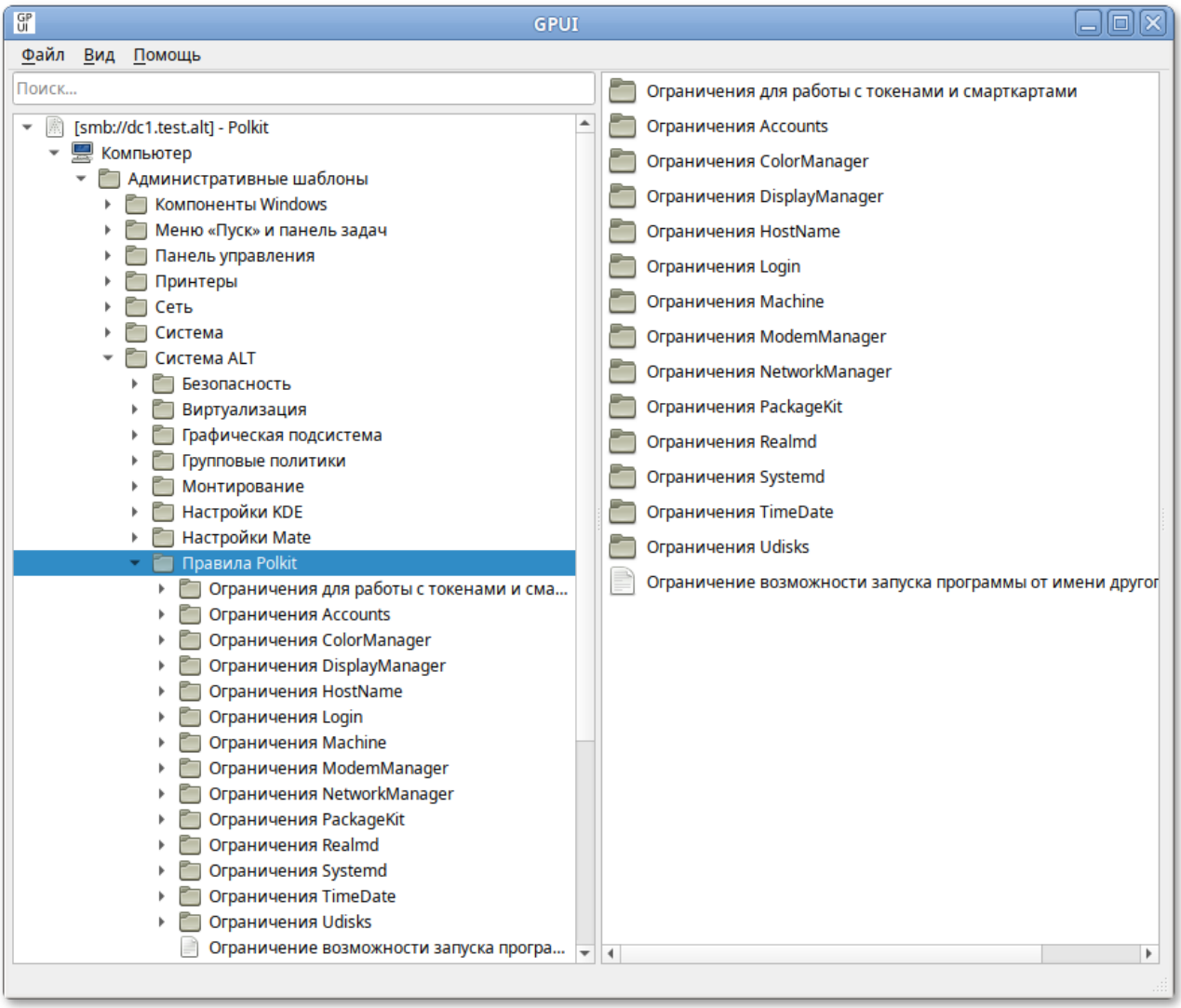
Через групповые политики реализовано управление настройками службы Polkit (PolicyKit).

В настоящий момент реализованы следующие настройки:

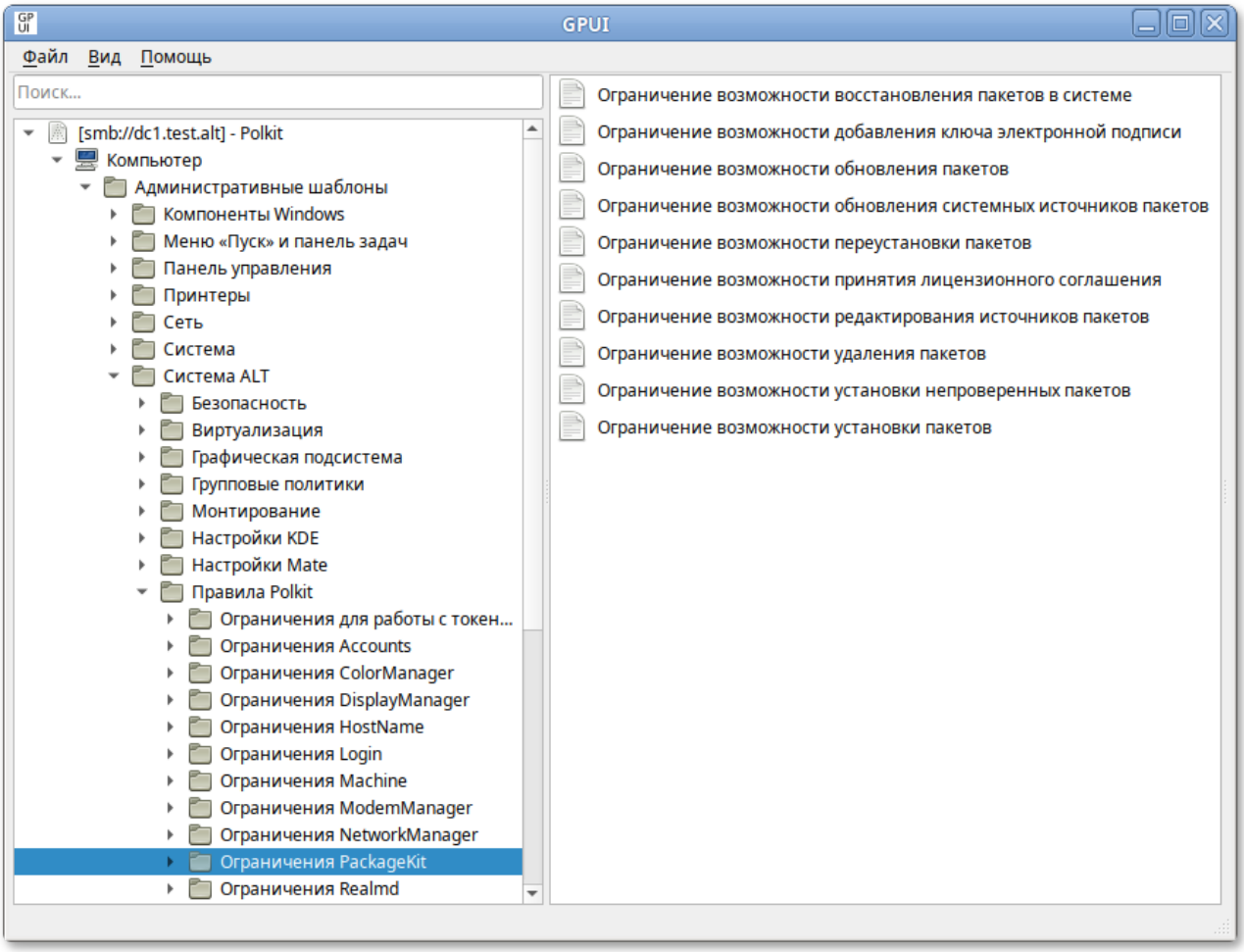
- Ограничения Accounts — формирование правил PolKit для управления службой Accounts;
- Ограничения ColorManager — формирование правил PolKit для управления службой Color Manager;
- Ограничения DisplayManager — формирование правил PolKit для управления службой HostName;
- Ограничения HostName — формирование правил PolKit для управления службой Login;
- Ограничения службы Login — формирование правил PolKit для управления службой Login;
- Ограничения службы Machine — формирование правил PolKit для управления службой Machine;
- Ограничения ModemManager — формирование правил PolKit для операций с ModemManager (взаимодействие с модемом или мобильным телефоном);

- Ограничения NetworkManager — формирование правил PolKit для операций с сетевыми подключениями и настройкой сетевых интерфейсов;
- Ограничения PackageKit — формирование правил PolKit для установки, удаления, обновления пакетов;
- Ограничения Realmd — формирование правил PolKit для управления службой Realmd;
- Ограничения Systemd — формирование правил PolKit для управления службой Systemd;
- Ограничения TimeDate — формирование правил PolKit для управления службой TimeDate;
- Ограничения Udisks — формирование правил PolKit для монтирования файловых систем (демон udisk2);
- Ограничения для работы с токенами и смарт-картами — формирование правил PolKit для работы с токенами и смарт-картами.

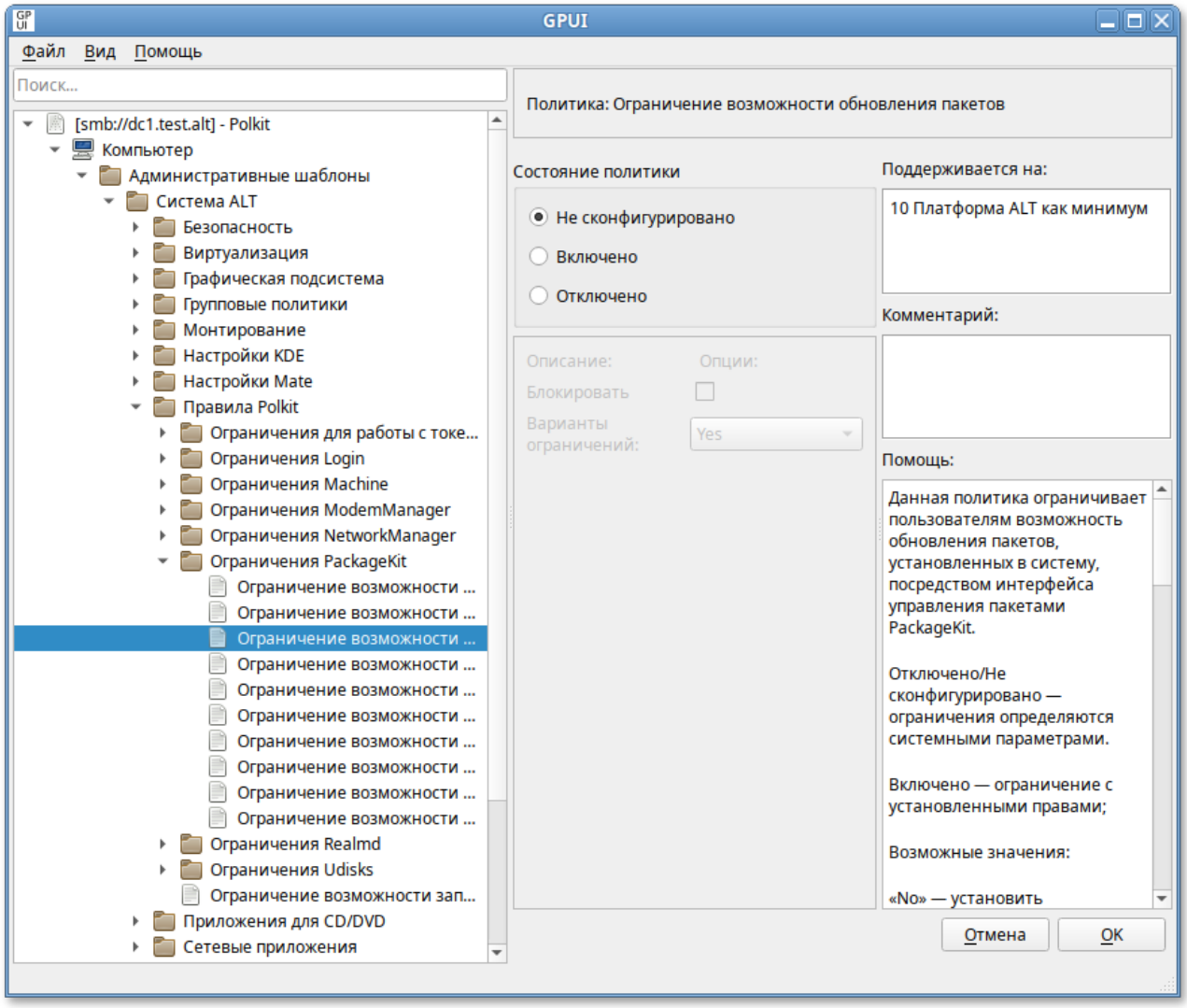
Для настройки политики следует перейти в **Компьютер/Пользователь → Административные шаблоны → Система ALT → Правила Polkit**. В этом разделе есть несколько подразделов:



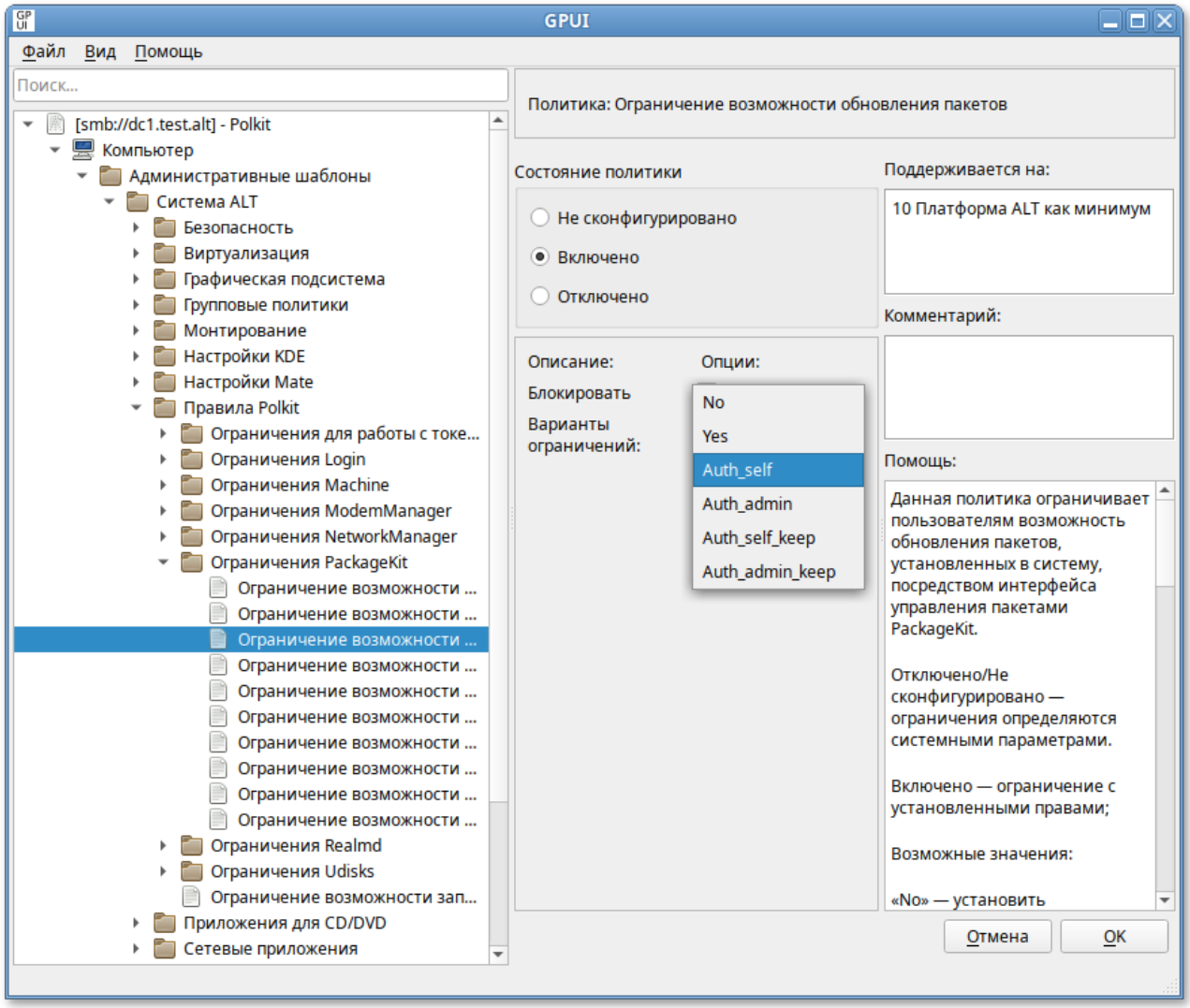
При выборе раздела в правом окне редактора отобразится список политик:



При выборе политики откроется диалоговое окно настройки политики:



Можно не задавать настройку политики, включить или отключить. Если политика находится в состоянии **Отключено/Не сконфигурировано** ограничения определяются системными параметрами. Если выбрать параметр **Включено**, в разделе **Опции** в выпадающем списке можно будет выбрать вариант ограничения:



Если выбран параметр **Включено**, для каждой из политик Polkit доступны следующие ограничения:

- **No** — установить ограничение с запретом действия (пользователю не разрешено выполнять действие);
- **Yes** — снять ограничение (пользователь может выполнять действие без какой-либо аутентификации);
- **Auth_self** — пользователь должен ввести свой пароль для аутентификации. Следует обратить внимание, что этого уровня ограничения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется ограничение **Auth_admin**;
- **Auth_admin** — пользователь должен ввести пароль администратора при каждом запросе. Требуется аутентификация пользователя с правами администратора;
- **Auth_self_keep** — подобно **Auth_self**, но авторизация сохраняется в течение короткого периода времени (например, пять минут). Следует обратить внимание, что этого уровня ограничения недостаточно для большинства применений в многопользовательских системах, обычно рекомендуется ограничение **Auth_admin_keep**;
- **Auth_admin_keep** — аналогично **Auth_admin**, но авторизация сохраняется в течение короткого периода времени (например, пять минут).

Примечание

Администратор — в ОС «Альт» определён в правиле **/etc/polkit-1/rules.d/50-default.rules**:

```
polkit.addAdminRule(function(action, subject) {
        return ["unix-group:wheel"];
});
```

По умолчанию запрашивается пароль пользователя, находящегося в группе wheel.

Для машинной политики создается файл правил **49-alt_group_policy_permissions.rules**, для пользовательской политики — **48-alt_group_policy_permissions_user.<USERNAME>.rules**. Правила для пользовательской политики обрабатываются до правил для машинной политики. У машинных политик имеются блокировки (параметр **Блокировать**), при установке которых машинные политики становятся приоритетнее пользовательских (создается файл правил **47-alt_group_policy_permissions.rules**).

Таблица 29.10. Ограничения Accounts

Политика	Описание	Правило Polkitd для службы Accounts (org.freedesktop.accounts)
Ограничение возможности изменения конфигурации экрана входа в систему	Данная политика управляет ограничением возможности изменения конфигурации экрана входа в систему	set-login-option
Ограничение возможности изменения собственного пароля пользователя	Данная политика управляет ограничением возможности изменения собственного пароля пользователя	change-own-password
Ограничение возможности изменения собственных пользовательских данных	Данная политика управляет ограничением возможности изменения собственных пользовательских данных	change-own-user-data
Ограничение возможности управления учетными записями пользователей	Данная политика управляет ограничением возможности управления учетными записями пользователей	user-administration

Таблица 29.11. Ограничения ColorManager

Политика	Описание	Правило Polkitd
Ограничение возможности изменения цветового профиля	Политика ограничивает возможность изменения цветового профиля	org.freedesktop.color-manager.modify-profile
Ограничение возможности изменения цветовых параметров для устройства	Политика ограничивает возможность изменения цветовых параметров для устройства	org.freedesktop.color-manager.modify-device
Ограничение возможности использования цветового датчика	Политика ограничивает возможность использования цветового датчика	org.freedesktop.color-manager.sensor-lock
Ограничение возможности создания цветового профиля	Политика ограничивает возможность создания цветового профиля	org.freedesktop.color-manager.create-profile
Ограничение возможности создания цветоуправляемого устройства	Политика управляет ограничением возможности создания цветоуправляемого устройства	org.freedesktop.color-manager.create-device
Ограничение возможности удаления цветового профиля	Политика ограничивает возможность удаления цветового профиля	org.freedesktop.color-manager.delete-profile
Ограничение возможности удаления цветоуправляемого устройства	Политика ограничивает возможность удаления цветоуправляемого устройства	org.freedesktop.color-manager.delete-device
Ограничение возможности установки цветовых профилей в системный каталог	Политика ограничивает возможность установки цветовых профилей в системный каталог	org.freedesktop.color-manager.install-system-wide
Ограничение возможности временной блокировки цветового профиля устройства	Политика управляет ограничением возможности временной блокировки цветового профиля устройства. Метод device-inhibit утилиты colormgr блокирует цветовой профиль для применения к устройству. Блокировка устанавливается на время (в секундах). При параметре timeout равным «0», применение цветового профиля к устройству будет заблокировано «навсегда», до прекращения работы утилиты colormgr. Polkit позволяет ограничить доступ пользователя к данному методу.	org.freedesktop.color-manager.device-inhibit

Таблица 29.12. Ограничения DisplayManager

Политика	Описание	Правило Polkitd для службы DisplayManager
Ограничение доступа к своей учетной записи	Данная политика управляет ограничением возможности доступа к своей учетной записи	org.freedesktop.DisplayManager.AccountsService.ModifyOwn
Ограничение доступа к списку учетных записей пользователей	Данная политика управляет ограничением возможности доступа к списку учетных записей пользователей	org.freedesktop.DisplayManager.AccountsService.ModifyAny
Ограничение чтения списка учетных записей пользователей	Данная политика управляет ограничением возможности чтения списка учетных записей пользователей	org.freedesktop.DisplayManager.AccountsService.ReadAny

Таблица 29.13. Ограничения HostName

Политика	Описание	Правило Polkitd для HostName
Ограничение возможности установки имени хоста	Данная политика управляет ограничением возможности установки имени хоста	org.freedesktop.hostname1.set-hostname
Ограничение возможности установки информации о машине	Данная политика управляет ограничением возможности установки информации о машине	org.freedesktop.hostname1.set-machine-info
Ограничение возможности установки статического имени хоста	Данная политика управляет ограничением возможности установки статического имени хоста	org.freedesktop.hostname1.set-static-hostname

Таблица 29.14. Ограничения для работы с токенами и смарт-картами

Политика	Описание	Правило Polkitd
Ограничение возможности доступа к демону PC/SC	Данная политика управляет ограничением возможности доступа к демону PC/SC и регулирует работу с токенами	org.debian.pcsc-lite.access_pcsc
Ограничение возможности доступа к смарт-картам	Данная политика управляет ограничением возможности доступа к смарт-картам	org.debian.pcsc-lite.access_card

Таблица 29.15. Ограничения службы Login

Политика	Описание	Правило Polkitd
Ограничение возможности блокировки или разблокировки экрана активных сеансов	Политика ограничивает возможность блокировки или разблокировки экрана активных сеансов	org.freedesktop.login1.lock-sessions
Ограничение возможности выключения питания системы	Политика ограничивает возможность выключения питания системы	org.freedesktop.login1.power-off
Ограничение возможности выключения системы, когда приложение запрещает это действие	Политика ограничивает возможность выключения системы, когда приложение запрещает это действие	org.freedesktop.login1.power-off-ignore-inhibit
Ограничение возможности выключения системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность выключения системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.power-off-multiple-sessions
Ограничение возможности изменения сеанса виртуального терминала	Политика управляет ограничением возможности изменить сеанс виртуального терминала	org.freedesktop.login1.chvt
Ограничение возможности остановки системы	Политика ограничивает возможность остановки системы	org.freedesktop.login1.halt
Ограничение возможности остановки системы, пока приложение запрещает это действие	Политика ограничивает возможность остановки системы, пока приложение запрещает это действие	org.freedesktop.login1.halt-ignore-inhibit
Ограничение возможности остановки системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность остановки системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.halt-multiple-sessions
Ограничение возможности очистки устройства в месте привязки (изменение	Политика управляет ограничением возможности очистки устройства в месте привязки (изменение способа подключения устройств к рабочим местам)	org.freedesktop.login1.flush-devices

Политика	Описание	Правило Polkitd
способа подключения устройств к рабочим местам)		
Ограничение возможности перевода системы в спящий режим	Политика ограничивает возможность перевода системы в спящий режим	org.freedesktop.login1.hibernate
Ограничение возможности перевода системы в спящий режим, пока приложение препятствует этому	Политика ограничивает возможность перевода системы в спящий режим, пока приложение препятствует этому	org.freedesktop.login1.hibernate-ignore-inhibit
Ограничение возможности перевода системы в спящий режим, при наличии активных сеансов других пользователей	Политика ограничивает возможность перевода системы в спящий режим, при наличии активных сеансов других пользователей	org.freedesktop.login1.hibernate-multiple-sessions
Ограничение возможности перезагрузки системы	Политика ограничивает возможность перезагрузки системы	org.freedesktop.login1.reboot
Ограничение возможности перезагрузки системы, когда приложение препятствует этому действию	Политика ограничивает возможность перезагрузки системы, когда приложение препятствует этому действию	org.freedesktop.login1.reboot-ignore-inhibit
Ограничение возможности перезагрузки системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность перезагрузки системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.reboot-multiple-sessions
Ограничение возможности приложениям блокировать выключение системы	Политика ограничивает возможность приложениям блокировать выключение системы	org.freedesktop.login1.inhibit-block-shutdown
	Политика ограничивает возможность приложениям запрещать автоматическое приостановление работы системы	org.freedesktop.login1.inhibit-block-idle

Политика	Описание	Правило Polkitd
Ограничение возможности приложениям запрещать автоматическое приостановление работы системы		
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратного ключа гибернации (энергосбережения) системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратного ключа гибернации (энергосбережения) системы	org.freedesktop.login1.inhibit-handle-hibernate-key
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратного переключателя крышки (устройства)	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратного переключателя крышки (устройства)	org.freedesktop.login1.inhibit-handle-lid-switch
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратной клавиши перезагрузки системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши перезагрузки системы	org.freedesktop.login1.inhibit-handle-reboot-key
Ограничение возможности приложениям запрещать низкоуровневую обработку аппаратной клавиши питания системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши питания системы	org.freedesktop.login1.inhibit-handle-power-key
Ограничение возможности приложениям запрещать низкоуровневую	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши приостановки системы	org.freedesktop.login1.inhibit-handle-suspend-key

Политика	Описание	Правило Polkitd
обработку аппаратной клавиши приостановки системы		
Ограничение возможности приложениям запрещать системный сон	Политика ограничивает возможность приложениям запрещать системный сон	org.freedesktop.login1.inhibit-block-sleep
Ограничение возможности приложениям откладывать выключение системы	Политика ограничивает возможность приложениям откладывать выключение системы	org.freedesktop.login1.inhibit-delay-shutdown
Ограничение возможности приложениям откладывать переход в спящий режим	Политика ограничивает возможность приложениям откладывать переход в спящий режим	org.freedesktop.login1.inhibit-delay-sleep
Ограничение возможности приостановки работы системы	Политика ограничивает возможность приостановки работы системы	org.freedesktop.login1.suspend
Ограничение возможности приостановки работы системы, пока приложение препятствует этому действию	Политика ограничивает возможность приостановки работы системы, пока приложение препятствует этому действию	org.freedesktop.login1.suspend-ignore-inhibit
Ограничение возможности приостановки работы системы, при наличии активных сеансов других пользователей	Политика ограничивает возможность приостановки работы системы, при наличии активных сеансов других пользователей	org.freedesktop.login1.suspend-multiple-sessions
Ограничение возможности присоединения устройств к рабочим местам	Политика управляет ограничением возможности присоединить устройства к рабочим местам	org.freedesktop.login1.attach-device
	Политика ограничивает возможность разрешения незалогиненному пользователю запускать программы	org.freedesktop.login1.set-self-linger

Политика	Описание	Правило Polkitd
Ограничение возможности разрешения незалогиненному пользователю запускать программы		
Ограничение возможности разрешения незалогиненным пользователям запускать программы	Политика ограничивает возможность разрешения незалогиненным пользователям запускать программы	org.freedesktop.login1.set-user-linger
Ограничение возможности указания загрузчику системы на загрузку в определенную запись загрузчика	Политика ограничивает возможность указания загрузчику системы на загрузку в определенную запись загрузчика	org.freedesktop.login1.set-reboot-to-boot-loader-entry
Ограничение возможности указания загрузчику системы на необходимость загрузки в меню загрузчика	Политика ограничивает возможность указания загрузчику системы на необходимость загрузки в меню загрузчика	org.freedesktop.login1.set-reboot-to-boot-loader-menu
Ограничение возможности указания микропрограмме системы на необходимость перезагрузки в интерфейс настройки микропрограммы	Политика ограничивает возможность указания микропрограмме системы на необходимость перезагрузки в интерфейс настройки микропрограммы	org.freedesktop.login1.set-reboot-to-firmware-setup
Ограничение возможности управления активными сеансами, пользователями и местами	Политика ограничивает возможность управления активными сеансами, пользователями и местами	org.freedesktop.login1.manage
Ограничение возможности установки «причины» перезагрузки в ядре	Политика ограничивает возможность установить «причины» перезагрузки в ядре	org.freedesktop.login1.set-reboot-parameter

Политика	Описание	Правило Polkitd
Ограничение возможности установки сообщения на стене (сообщение, которое будет отправлено на все терминалы)	Политика ограничивает возможность установки сообщения на стене (сообщение, которое будет отправлено на все терминалы)	org.freedesktop.login1.set-wall-message

Таблица 29.16. Ограничения службы Machine

Политика	Описание	Правило Polkitd
Ограничение возможности авторизации в локальном контейнере	Политика управляет ограничением возможности авторизации в локальном контейнере	org.freedesktop.machine1.login
Ограничение возможности авторизации на локальном хосте	Политика управляет ограничением возможности авторизации на локальном хосте	org.freedesktop.machine1.host-login
Ограничение возможности получения интерпретатора командной строки (командной оболочки) в локальном контейнере	Политика управляет ограничением возможности получения интерпретатора командной строки (командной оболочки) в локальном контейнере	org.freedesktop.machine1.shell
Ограничение возможности получения интерпретатора командной строки (командной оболочки) на локальном хосте	Политика управляет ограничением возможности получения интерпретатора командной строки (командной оболочки) на локальном хосте	org.freedesktop.machine1.host-shell
Ограничение возможности получения псевдотелетайпа (TTY) в локальном контейнере	Политика управляет ограничением возможности получения псевдотелетайпа (TTY) в локальном контейнере	org.freedesktop.machine1.open-pty
Ограничение возможности получения псевдотелетайпа (TTY) на локальном хосте	Политика управляет ограничением возможности получения псевдотелетайпа (TTY) на локальном хосте	org.freedesktop.machine1.host-open-pty

Политика	Описание	Правило Polkitd
Ограничение возможности управления локальными виртуальными машинами и контейнерами	Политика управляет ограничением возможности управления локальными виртуальными машинами и контейнерами	org.freedesktop.machine1.manage-machines
Ограничение возможности управления локальными виртуальными машинами и образами контейнеров	Политика управляет ограничением возможности управления локальными виртуальными машинами и образами контейнеров	org.freedesktop.machine1.manage-images

Таблица 29.17. Ограничения ModemManager

Политика	Описание	Правило Polkitd
Ограничение возможности блокировки и управления мобильным широкополосным устройством	Политика ограничивает возможность изменения конфигурации мобильного широкополосного устройства	org.freedesktop.ModemManager1.Device.Control
Ограничение возможности добавления, изменения или удаления контактов устройства	Политика управляет ограничением возможности добавления, изменения и удаления контактов мобильного широкополосного доступа	org.freedesktop.ModemManager1.Contacts
Ограничение возможности запросов и использования сетевой информации и услуг	Политика ограничивает возможность запрашивать или использовать сетевую информацию и службы	org.freedesktop.ModemManager1.USSD
Ограничение возможности запросов информации о сетевом времени и часовом поясе	Политика ограничивает возможность запрашивать информацию о сетевом времени	org.freedesktop.ModemManager1.Time
	Политика ограничивает возможность отправки или манипулирования текстовыми сообщениями устройства	org.freedesktop.ModemManager1.Messaging

Политика	Описание	Правило Polkitd
Ограничение возможности отправки, сохранения, изменения и удаления текстовых сообщений		
Ограничение возможности приема входящих голосовых вызовов или начала исходящего голосового вызова	Политика ограничивает возможность голосовых вызовов	org.freedesktop.ModemManager1.Voice
Ограничение возможности просмотра информации о географическом положении и позиционировании	Политика ограничивает возможность просмотра информации о географическом положении	org.freedesktop.ModemManager1.Location
Ограничение возможности управления демоном Modem Manager	Политика ограничивает возможность управления диспетчером модемов	org.freedesktop.ModemManager1.Control
Ограничение возможности управления прошивкой мобильного широкополосного устройства	Политика ограничивает возможность управления микропрограммой мобильного широкополосного устройства	org.freedesktop.ModemManager1.Firmware

Таблица 29.18. Ограничения NetworkManager

Политика	Описание	Правило Polkitd
Ограничение возможности включения или отключения сети	Политика управляет ограничением возможности включения или отключения сетевого взаимодействия системы. Если сетевое взаимодействие отключено, все управляемые интерфейсы отсоединяются и деактивируются. Если сетевое взаимодействие включено, все управляемые интерфейсы доступны для активации	org.freedesktop.NetworkManager.enable-disable-network
Ограничение возможности включения или отключения статистики	Политика управляет ограничением возможности включения или отключения счётчика статистики устройства	org.freedesktop.NetworkManager.enable-disable-statistics

Политика	Описание	Правило Polkitd
Ограничение возможности включения или отключения устройств Wi-Fi	Данная политика управляет ограничением возможности включения или отключения устройств Wi-Fi	org.freedesktop.NetworkManager.enable-disable-wifi
Ограничение возможности включения или отключения устройств WiMAX	Данная политика управляет ограничением возможности включения или отключения мобильных широкополосных устройств WiMAX	org.freedesktop.NetworkManager.enable-disable-wimax
Ограничение возможности включения или отключения WWAN-устройств	Политика управляет ограничением возможности включения или отключения WWAN-устройств	org.freedesktop.NetworkManager.enable-disable-wwan
Ограничение возможности изменения общих настроек DNS	Политика управляет ограничением возможности изменений общей конфигурации DNS	org.freedesktop.NetworkManager.settings.modify.global-dns
Ограничение возможности изменения персональных сетевых настроек	Данная политика управляет ограничением возможности изменений личных сетевых соединений	org.freedesktop.NetworkManager.settings.modify.own
Ограничение возможности изменения постоянного имени хоста	Данная политика управляет ограничением возможности изменения постоянного имени (hostname) системы	org.freedesktop.NetworkManager.settings.modify.hostname
Ограничение возможности изменения сетевых подключений для всех пользователей	Политика управляет ограничением возможности изменения системных сетевых настроек для всех пользователей	org.freedesktop.NetworkManager.settings.modify.system
Ограничение возможности изменения системных настроек для сети	Политика управляет ограничением возможности изменения системных сетевых настроек	org.freedesktop.NetworkManager.network-control
Ограничение возможности изменения состояния сна NetworkManager	Данная политика управляет ограничением возможности перевода NetworkManager в спящий режим или пробуждения из спящего режима (должна использоваться только для управления питанием системы). В спящем состоянии все интерфейсы, которыми управляет NetworkManager, деактивированы. В бодрствующем состоянии устройства доступны для активации. Обращение к состоянию сна	org.freedesktop.NetworkManager.sleep-wake

Политика	Описание	Правило Polkitd
	NetworkManager не вызывается пользователем напрямую; функция предназначена для отслеживания приостановки/возобновления работы системы.	
Ограничение возможности отката конфигурации сетевых интерфейсов к контрольной точке	Политика управляет ограничением возможности создания контрольной точки сетевых интерфейсов или отката к ней	org.freedesktop.NetworkManager.checkpoint-rollback
Ограничение возможности перезагрузки NetworkManager	Политика управляет ограничением возможности перезагрузки конфигурации NetworkManager	org.freedesktop.NetworkManager.reload
Ограничение возможности проверки подключения сети	Политика управляет ограничением возможности включения или отключения проверки подключения к сети	org.freedesktop.NetworkManager.enable-disable-connectivity-check
Ограничение возможности сканирования Wi-Fi сетей	Данная политика управляет ограничением возможности сканирования Wi-Fi сетей	org.freedesktop.NetworkManager.wifi.scan
Ограничение возможности совместных подключений через защищённую сеть Wi-Fi	Политика управляет ограничением возможности совместного подключения через защищенную сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.protected
Ограничение возможности совместных подключений через открытую сеть Wi-Fi	Политика управляет ограничением возможности совместного подключения ерез открытую сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.open

Ограничения NetworkManager для текущего пользователя можно просмотреть, выполнив команду:

```
$ nmcli general permissions
PERMISSION                                                VALUE
org.freedesktop.NetworkManager.checkpoint-rollback        auth
org.freedesktop.NetworkManager.enable-disable-connectivity-check  нет
org.freedesktop.NetworkManager.enable-disable-network     auth
org.freedesktop.NetworkManager.enable-disable-statistics  auth
org.freedesktop.NetworkManager.enable-disable-wifi        да
org.freedesktop.NetworkManager.enable-disable-wimax       да
org.freedesktop.NetworkManager.enable-disable-wwan        да
org.freedesktop.NetworkManager.network-control            да
org.freedesktop.NetworkManager.reload                     auth
org.freedesktop.NetworkManager.settings.modify.global-dns  нет
org.freedesktop.NetworkManager.settings.modify.hostname   auth
org.freedesktop.NetworkManager.settings.modify.own        auth
```

```
org.freedesktop.NetworkManager.settings.modify.system              да
org.freedesktop.NetworkManager.sleep-wake                          да
org.freedesktop.NetworkManager.wifi.scan                           да
org.freedesktop.NetworkManager.wifi.share.open                     да
org.freedesktop.NetworkManager.wifi.share.protected                да
```

Таблица 29.19. Ограничения PackageKit

Политика	Описание	Правило Polkitd
Ограничение возможности восстановления пакетов в системе	Данная политика ограничивает пользователям возможность восстановления системы пакетов, если в ней возникли проблемы, например, пропали зависимости, посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.repair-system
Ограничение возможности добавления ключа электронной подписи	Данная политика ограничивает пользователям возможность добавления ключа подписи в список доверенных ключей системы посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-trust-signing-key
Ограничение возможности обновления пакетов	Данная политика ограничивает пользователям возможность обновления пакетов, установленных в систему, посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-update
Ограничение возможности обновления системных источников пакетов	Данная политика ограничивает пользователям возможность обновления системных источников пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-refresh
Ограничение возможности переустановки пакетов	Данная политика ограничивает пользователям возможность переустановки пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-reinstall
Ограничение возможности принятия лицензионного соглашения	Данная политика ограничивает пользователям возможность принятия пользовательского соглашения программ посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-eula-accept
Ограничение возможности редактирования источников пакетов	Данная политика ограничивает пользователям возможность редактирования источников пакетов в системе посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-configure
Ограничение возможности удаления пакетов	Данная политика ограничивает пользователям возможность удаления пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-remove
Ограничение возможности установки пакетов	Данная политика ограничивает пользователям возможность установки пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install
	Данная политика ограничивает пользователям возможность установки ненадёжных или непроверенных пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install-untrusted

Политика	Описание	Правило Polkitd
Ограничение возможности установки непроверенных пакетов		

Таблица 29.20. Ограничения Realmd

Политика	Описание	Правило Polkitd
Ограничение возможности возможности запустить обнаружение области Kerberos REALM	Данная политика управляет ограничением возможности запустить обнаружение области Kerberos REALM	org.freedesktop.realmd.discover-realm
Ограничение возможности изменения политики входа в систему	Данная политика управляет ограничением возможности изменения политики входа в систему	org.freedesktop.realmd.login-policy
Ограничение возможности присоединения машины к домену или Kerberos REALM	Данная политика управляет ограничением возможности присоединения машины к домену или Kerberos REALM	org.freedesktop.realmd.configure-realm
Ограничение возможности отключения машины из домена или Kerberos REALM	Данная политика управляет ограничением возможности удаления машины из домена или Kerberos REALM	org.freedesktop.realmd.deconfigure-realm

Таблица 29.21. Ограничения Systemd

Политика	Описание	Правило Polkitd для службы Systemd (org.freedesktop.systemd1)
Ограничение возможности отправки пароля системе	Данная политика управляет ограничением возможности отправки пароля системе	reply-password
Ограничение возможности перезагрузки состояния systemd	Данная политика управляет ограничением возможности перезагрузки состояния systemd	reload-daemon
	Данная политика управляет ограничением возможности управления системными службами или другими устройствами	manage-units

Политика	Описание	Правило Polkitd для службы Systemd (org.freedesktop.systemd1)
Ограничение возможности управления системными службами или другими устройствами		
Ограничение возможности управления файлами системных служб или модулей	Данная политика управляет ограничением возможности управления файлами системных служб или модулей	manage-unit-files
Ограничение возможности установки или удаления переменных окружения менеджера систем и служб	Данная политика управляет ограничением возможности установки или удаления переменных окружения менеджера систем и служб	set-environment

Таблица 29.22. Ограничения TimeDate

Политика	Описание	Правило Polkitd для службы TimeDate (org.freedesktop.timedate1)
Ограничение возможности включения или выключения синхронизации сетевого времени	Данная политика управляет ограничением возможности включения или выключения синхронизации сетевого времени	set-ntp
Ограничение возможности установки системного времени	Данная политика управляет ограничением возможности установки системного времени	set-time
Ограничение возможности установки системного часового пояса	Данная политика управляет ограничением возможности установки системного часового пояса	set-timezone
	Данная политика управляет ограничением возможности установки RTC в местный часовой пояс или UTC	set-local-rtc

Политика	Описание	Правило Polkitd для службы TimeDate (org.freedesktop.timedate1)
Ограничение возможности установки RTC в местный часовой пояс или UTC		

Таблица 29.23. Ограничения Udisks

Политика	Описание	Правило Polkitd
Общая политика ограничения возможности монтирования	Данная политика ограничивает возможность монтирования съёмных запоминающих устройств, монтирования системных разделов, монтирования съёмных запоминающих устройств в удалённых сеансах	org.freedesktop.udisks2.filesystem-mount org.freedesktop.udisks2.filesystem-mount-other-seat org.freedesktop.udisks2.filesystem-mount-system
Ограничение возможности включения/ отключения SMART	Данная политика управляет ограничением возможности включения/отключения SMART	org.freedesktop.udisks2.ata-smart-enable-disable
Ограничение возможности демонтировать устройство, смонтированное другим пользователем	Данная политика управляет ограничением возможности демонтировать устройство, смонтированное другим пользователем	org.freedesktop.udisks2.filesystem-unmount-others
Ограничение возможности заблокировать зашифрованное устройство, разблокированное другим пользователем	Данная политика управляет ограничением возможности заблокировать зашифрованное устройство, разблокированное другим пользователем	org.freedesktop.udisks2.encrypted-lock-others
Ограничение возможности запуска самопроверки SMART	Данная политика управляет ограничением возможности запуска самопроверки SMART	org.freedesktop.udisks2.ata-smart-selftest
Ограничение возможности извлечь носитель	Данная политика управляет ограничением возможности извлечь носитель	org.freedesktop.udisks2.eject-media

Политика	Описание	Правило Polkitd
Ограничение возможности извлечь носитель из дисковода, подключенного к другому рабочему месту	Данная политика управляет ограничением возможности извлечь носитель из дисковода, подключенного к другому рабочему месту	org.freedesktop.udisks2.eject-media-other-seat
Ограничение возможности извлечь носитель из системного диска	Данная политика управляет ограничением возможности извлечь носитель из системного диска	org.freedesktop.udisks2.eject-media-system
Ограничение возможности изменения настроек привода	Данная политика управляет ограничением возможности изменения настроек привода	org.freedesktop.udisks2.modify-drive-settings
Ограничение возможности изменения общесистемной конфигурации	Данная политика управляет ограничением возможности изменения общесистемной конфигурации	org.freedesktop.udisks2.modify-system-configuration
Ограничение возможности изменения петлевых (loop) устройств	Данная политика управляет ограничением возможности изменения петлевых (loop) устройств	org.freedesktop.udisks2.loop-modify-others
Ограничение возможности изменения системного устройства	Данная политика управляет ограничением возможности изменения системного устройства	org.freedesktop.udisks2.modify-device-system
Ограничение возможности изменения устройства	Данная политика управляет ограничением возможности изменения устройства	org.freedesktop.udisks2.modify-device
Ограничение возможности изменения устройства, подключенного к другому рабочему месту	Данная политика управляет ограничением возможности изменения устройства, подключенного к другому рабочему месту	org.freedesktop.udisks2.modify-device-other-seat
Ограничение возможности изменить пароль для зашифрованного устройства	Данная политика управляет ограничением возможности изменения пароля для зашифрованного устройства	org.freedesktop.udisks2.encrypted-change-passphrase
	Данная политика управляет ограничением возможности изменения системного пароля для зашифрованного устройства	org.freedesktop.udisks2.encrypted-change-passphrase-system

Политика	Описание	Правило Polkitd
Ограничение возможности изменения системного пароля для зашифрованного устройства		
Ограничение возможности монтирования системных разделов	Данная политика ограничивает возможность монтирования системных разделов. Системное устройство хранения информации — это неизвлекаемое устройство. Для таких устройств переменная **`HintSystem`** установлена в значение **`True`**. Жёсткий диск с установленной ОС относится к системным устройствам	org.freedesktop.udisks2.filesystem-mount-system
Ограничение возможности монтирования съёмных запоминающих устройств в удалённых сеансах	Данная политика ограничивает возможность монтирования съёмных запоминающих устройств с устройства, подключенного к удалённому рабочему месту (например, на другом компьютере или удаленной сессии)	org.freedesktop.udisks2.filesystem-mount-other-seat
Ограничение возможности монтирования файловой системы	Данная политика управляет ограничением возможности монтирования файловой системы устройства	org.freedesktop.udisks2.filesystem-mount
Ограничение возможности монтирования файловой системы от имени другого пользователя	Данная политика управляет ограничением возможности монтирования файловой системы от имени другого пользователя	org.freedesktop.udisks2.filesystem-mount-other-user
Ограничение возможности монтировать/ демонтировать файловые системы, указанные в файле fstab с параметром x-udisks-auth	Данная политика управляет ограничением возможности монтирования/демонтирования файловых систем, указанных в файле fstab с параметром x-udisks-auth	org.freedesktop.udisks2.filesystem-fstab
Ограничение возможности надежно стереть жёсткий диск	Данная политика управляет ограничением возможности надежно стереть жёсткий диск	org.freedesktop.udisks2.ata-secure-erase
Ограничение возможности обновить данные SMART	Данная политика управляет ограничением возможности обновить данные SMART	org.freedesktop.udisks2.ata-smart-update
Ограничение возможности отменить задание	Данная политика управляет ограничением возможности отменить задание	org.freedesktop.udisks2.cancel-job

Политика	Описание	Правило Polkitd
Ограничение возможности отменить задание, начатое другим пользователем	Данная политика управляет ограничением возможности отменить задание, начатое другим пользователем	org.freedesktop.udisks2.cancel-job-other-user
Ограничение возможности отправить команду ожидания для диска с удаленного места	Данная политика управляет ограничением возможности отправить команду ожидания для диска с удаленного места	org.freedesktop.udisks2.ata-standby-other-seat
Ограничение возможности разблокировать зашифрованное системное устройство	Данная политика управляет ограничением возможности разблокировать зашифрованное системное устройство	org.freedesktop.udisks2.encrypted-unlock-system
Ограничение возможности разблокировать зашифрованное устройство	Данная политика управляет ограничением возможности разблокировать зашифрованное устройство	org.freedesktop.udisks2.encrypted-unlock
Ограничение возможности разблокировать зашифрованное устройство, подключенное к другому рабочему месту	Данная политика управляет ограничением возможности разблокировать зашифрованное устройство, подключенное к другому рабочему месту	org.freedesktop.udisks2.encrypted-unlock-other-seat
Ограничение возможности разблокировать зашифрованное устройство, указанное в файле crypttab, с опцией x-udisks-auth	Данная политика управляет ограничением возможности разблокировать зашифрованное устройство, указанное в файле crypttab, с опцией x-udisks-auth	org.freedesktop.udisks2.encrypted-unlock-crypttab
Ограничение возможности отправить команду режима ожидания на системный диск	Данная политика управляет ограничением возможности отправить команду режима ожидания на системный диск	org.freedesktop.udisks2.ata-standby-system
Ограничение возможности отправить резервную команду	Данная политика управляет ограничением возможности отправить резервную команду	org.freedesktop.udisks2.ata-standby
	Данная политика управляет ограничением возможности разрешения на проверку состояния питания жесткого диска	org.freedesktop.udisks2.ata-check-power

Политика	Описание	Правило Polkitd
Ограничение возможности разрешения на проверку состояния питания жесткого диска		
Ограничение возможности смены владельца файловой системы	Данная политика управляет ограничением возможности смены владельца файловой системы	org.freedesktop.udisks2.filesystem-take-ownership
Ограничение возможности удаления петлевых (loop) устройств	Данная политика управляет ограничением возможности удаления петлевых (loop) устройств	org.freedesktop.udisks2.loop-delete-others
Ограничение возможности разрешения управления массивами RAID	Данная политика управляет ограничением возможности разрешения управления массивами RAID	org.freedesktop.udisks2.manage-md-raid
Ограничение возможности управления петлевыми (loop) устройствами	Данная политика управляет ограничением возможности управления петлевыми (loop) устройствами	org.freedesktop.udisks2.loop-setup
Ограничение возможности управления пространством подкачки	Данная политика управляет ограничением возможности управления пространством подкачки	org.freedesktop.udisks2.manage-swapspace
Ограничение возможности установить данные SMART из большого двоичного объект	Данная политика управляет ограничением возможности установить данные SMART из большого двоичного объекта	org.freedesktop.udisks2.ata-smart-simulate

Таблица 29.24. Другие политики

Политика	Описание	Правило Polkitd
Ограничение возможности запуска программы от имени другого пользователя	Данная политика управляет ограничением возможности запуска программы от имени другого пользователя	org.freedesktop.policykit.exec

Все настройки политики управления политиками Polkit хранятся в файлах **`{GUID GPT}/Machine/Registry.pol`** и **`{GUID GPT}/User/Registry.pol`**.

Пример файла **`Registry.pol`**:

```
PReg
[Software\BaseALT\Policies\PolkitLocks;org.freedesktop.udisks2.filesystem-
mount;;;]
[Software\BaseALT\Policies\Polkit;org.freedesktop.udisks2.filesystem-mount;;;No]
[Software\BaseALT\Policies\Polkit;org.freedesktop.packagekit.system-
update;;;Auth_self]
[Software\BaseALT\Policies\PolkitLocks;org.freedesktop.NetworkManager.network-
control;;;]
[Software\BaseALT\Policies\Polkit;org.freedesktop.NetworkManager.network-
control;;Yes]
```

29.5.4. Политика доступа к съемным носителям

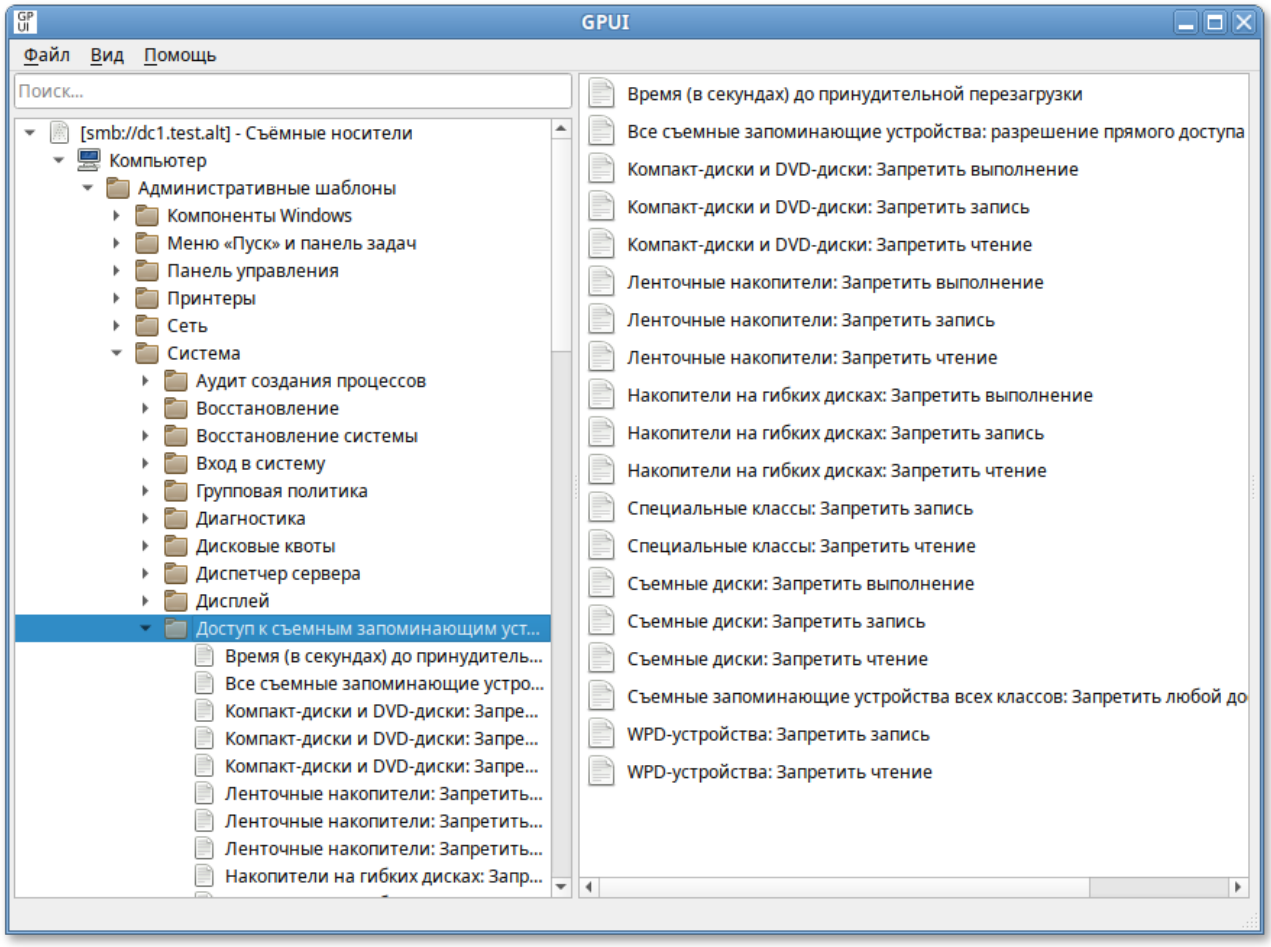
Эта групповая политика позволяет централизованно для компьютеров или пользователей настраивать доступ к съемным запоминающим устройствам (CD, DVD, USB и др.).

Примечание

Политика полного запрета на доступ к съемным носителям реализована через правила в Polkit (**`/etc/polkit-1/rules.d/`**).

Правила для пользовательской политики обрабатываются до правил для машинной политики. Для машинной политики создается файл правил **`49-gpoa_disk_permissions.rules`**, для пользовательской политики — **`48-gpoa_disk_permissions_user.<USERNAME>.rules`**.

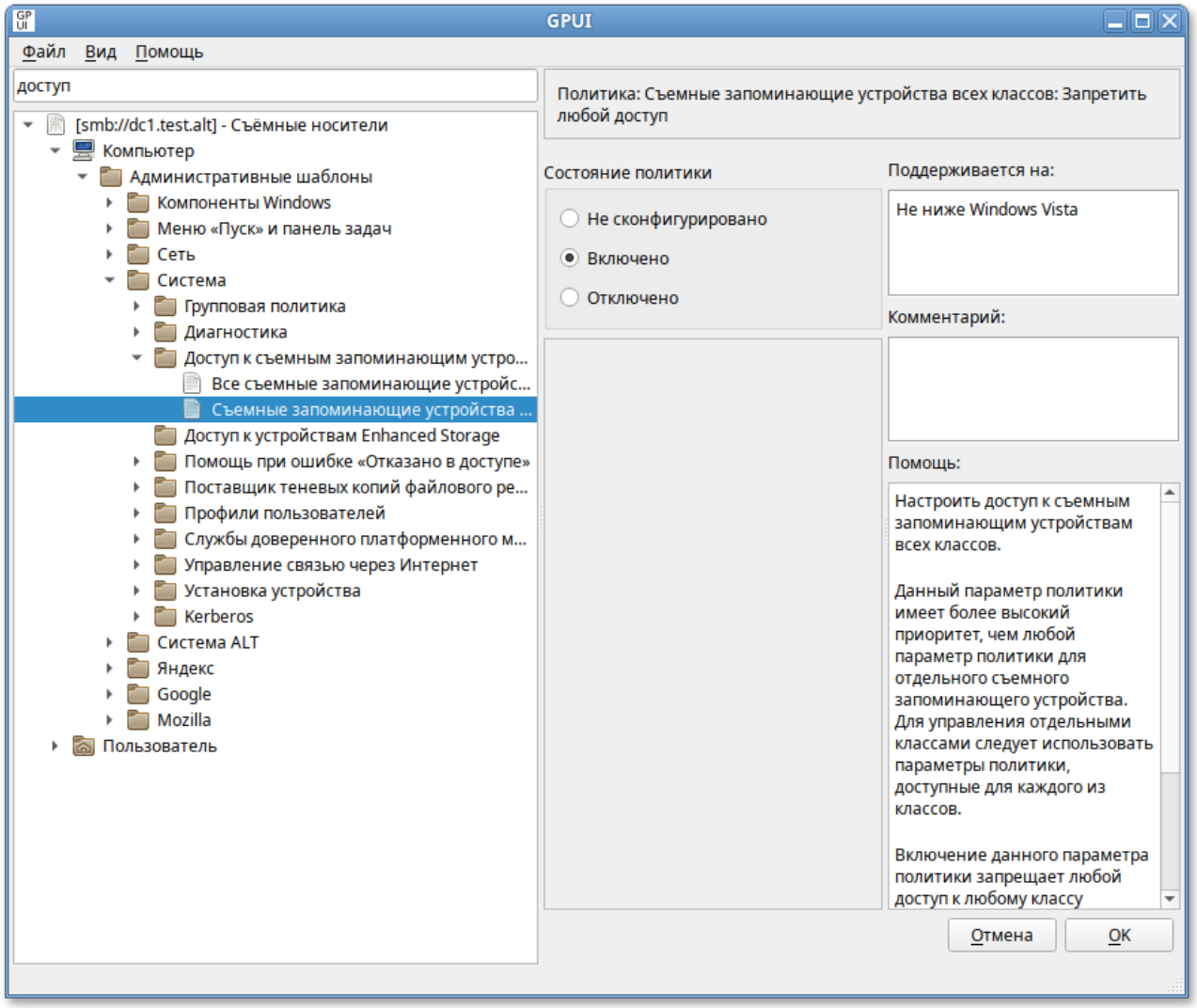
Для настройки этой политики следует перейти в **Компьютер/Пользователь** → **Административные шаблоны** → **Система** → **Доступ к съемным запоминающим устройствам**:



Примечание

На данный момент реализована только политика **Съемные запоминающие устройства всех классов: Запретить любой доступ** (машинная и пользовательская).

Щелкнуть левой кнопкой мыши на политике **Съемные запоминающие устройства всех классов: Запретить любой доступ**, откроется диалоговое окно настройки политики. Можно не задавать настройку политики, включить или отключить:



Для включения запрета на доступ следует выбрать параметр **Включено**, для отключения — **Отключено** или **Не сконфигурировано**.

Настройки политики управления съемными носителями хранятся в файлах **{GUID GPT}/Machine/Registry.pol** и **{GUID GPT}/User/Registry.pol**.

Пример файла **Registry.pol**:

```
PReg
[Software\Policies\Microsoft\Windows\RemovableStorageDevices;Deny_All;;;]
```

29.5.5. Управление gsettings

Данные групповые политики позволяют управлять ключами gsettings. В свою очередь gsettings управляет ключами dconf.

В настоящий момент реализованы настройки удаленного доступа к рабочему столу (VNC) через Vino и настройки графической среды Mate, а именно:

- настройки фона рабочего стола;
- настройки хранителя экрана;
- настройки сеанса;

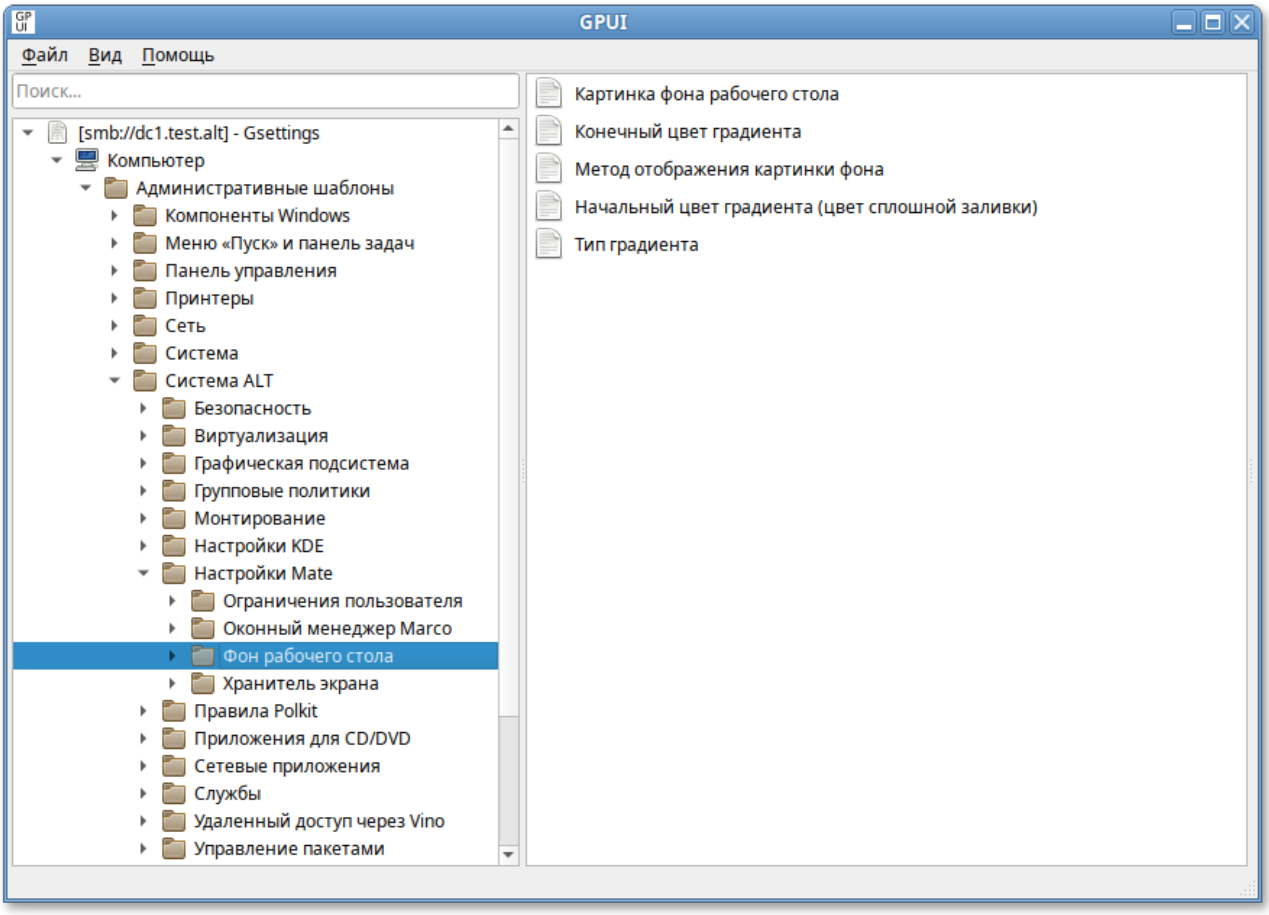
- настройки ограничений пользователя;
- настройки оконного менеджера Marco;
- настройки клавиатуры.

Машинные политики являются действующими по умолчанию, а пользовательские, при установке, замещают машинные. У машинных политик имеются блокировки, при установке которых пользовательские настройки игнорируются, а для применения используются значения, установленные машинными политиками.

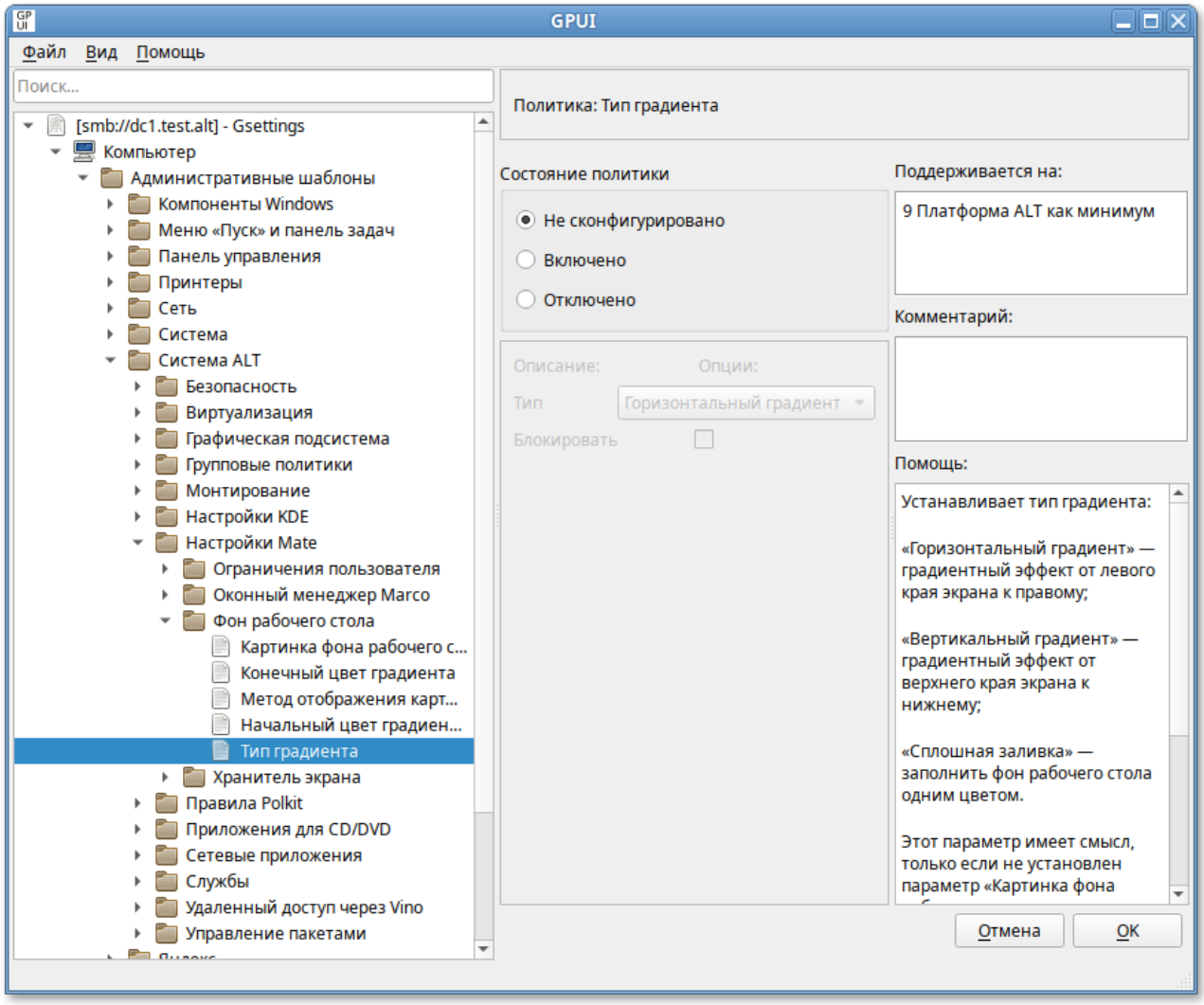
Порядок применения политик:

1. Машинные политики применяются при загрузке компьютера.
2. Машинные политики без блокирования могут применяться, но только в том случае, если пользователь ни разу не изменял эти политики.
3. Машинные политики с блокировкой применяются независимо от пользовательских настроек.
4. Пользовательские политики применяются при логине пользователя и только в случае, если нет таких же машинных политик с блокировкой.

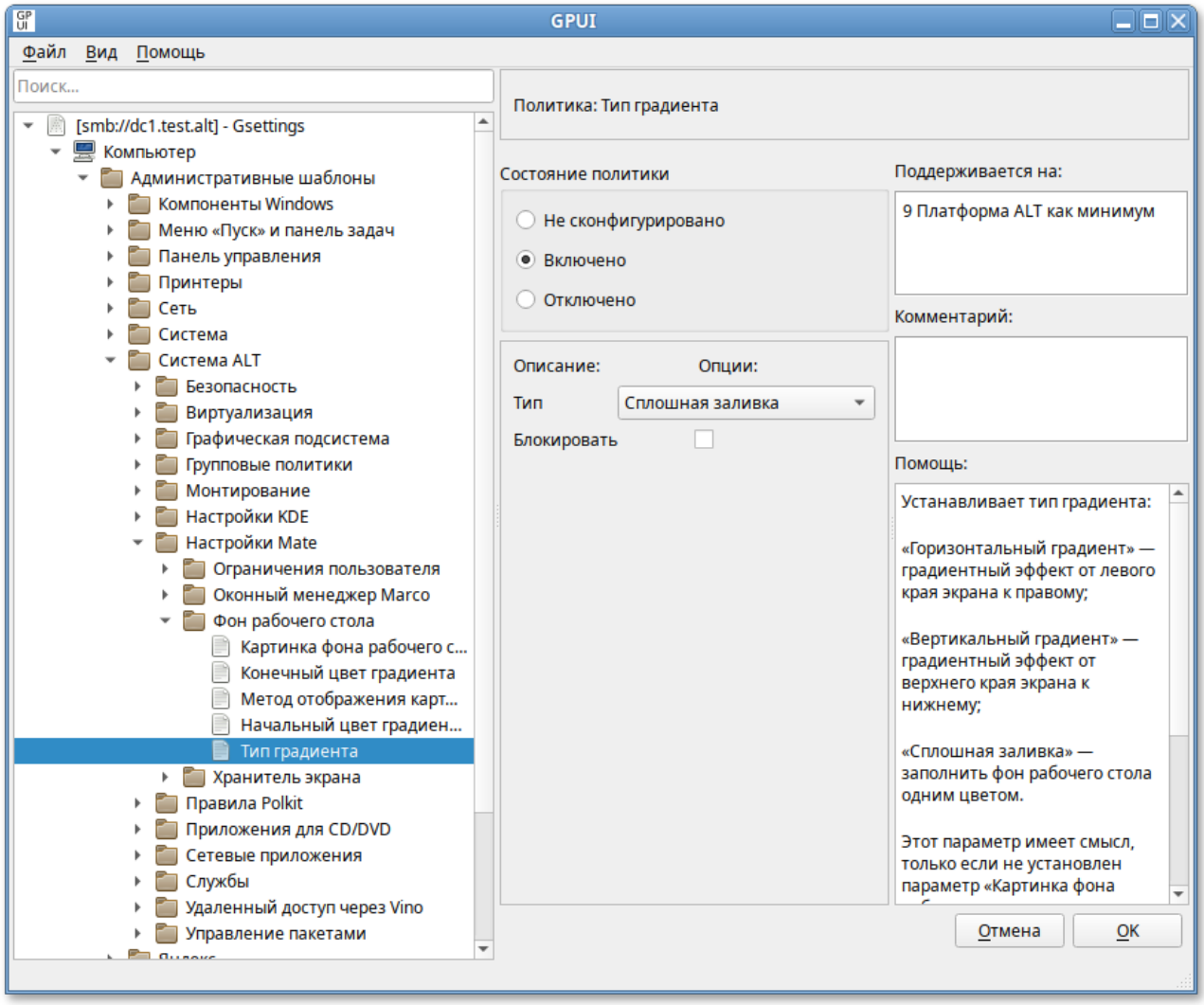
Для настройки политики следует перейти в **Компьютер/Пользователь → Административные шаблоны → Система ALT → Настройки Mate/Удаленный доступ через Vino**. Выбрать раздел, в правом окне редактора отобразится список политик:



При выборе политики откроется диалоговое окно настройки политики:



Можно не задавать настройку политики, включить или отключить. Если выбрать параметр **Включено**, в разделе **Параметры** в выпадающем списке можно указать настройки политики:



Политика, управляющая настройкой фона рабочего стола, изменяет ключ KEY в схеме org.mate.background. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.background.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.mate.background.KEY.

Таблица 29.25. Настройки фона рабочего стола

Политика	Ключ	Описание	Значение
Картинка фона рабочего стола	picture-filename	Позволяет установить изображение в качестве фона рабочего стола, указав файл, содержащий изображение	Строка, содержащая путь (с точки зрения клиента) к файлу изображения (например, **`/usr/share/backgrounds/mate/nature/Wood.jpg`**)
Метод отображения картинки фона	picture-options	Устанавливает метод отображения изображения, заданного параметром **`Картинка фона рабочего стола`**	**None** (нет) — нет изображения

Политика	Ключ	Описание	Значение
			`Wallpaper` (мозаика) — дублирует изображение в оригинальном размере таким образом, что изображение полностью покрывает рабочий стол **`Centered`** (по центру) — отображает изображение в центре рабочего стола в соответствии с оригинальным размером изображения **`Scaled`** (масштаб) — увеличивает изображение, сохраняя пропорции, до тех пор, пока величина одной из границ изображения не совпадет с величиной одной из границ экрана **`Stretched`** (растянуть) — увеличивает изображение для соответствия размеру рабочего стола, изменяя пропорции при необходимости **`Zoom`** (приближение) — увеличивает наименьшую из сторон изображения до тех пор, пока ее величина не совпадет с величиной соответствующей границы экрана; изображение может быть обрезано по другой стороне **`Spanned`** (заполнение) — увеличивает изображение, сохраняя пропорции, до тех пор, пока величина одной из границ изображения не совпадет с величиной одной из границ экрана
Тип градиента	color-shading-type		

Политика	Ключ	Описание	Значение
		Устанавливает тип градиента фона рабочего стола. Этот параметр имеет смысл, только если не установлен параметр **Картинка фона рабочего стола**	**Вертикальный градиент** — градиентный эффект от верхнего края экрана к нижнему **Горизонтальный градиент** — градиентный эффект от левого края экрана к правому **Сплошная заливка** — заполнить фон рабочего стола одним цветом
Конечный цвет градиента	secondary-color	Устанавливает «конечный» цвет градиента фона рабочего стола. Данным цветом заканчивается градиент и, в зависимости от типа градиента, параметр определяет цвет правого или нижнего края рабочего стола. Данный параметр не используется, если в параметре **Тип градиента** выбрана **Сплошная заливка**	Ключевое слово цвета (red, aqua, navy и т.д.) Строка типа #RRGGBB Строка типа rgb(0,0,0)
Начальный цвет градиента	primary-color	Устанавливает начальный цвет градиента фона рабочего стола. Данным цветом начинается градиент и, в зависимости от типа градиента, параметр определяет цвет левого или верхнего края рабочего стола, или цвет сплошной заливки	Ключевое слово цвета (red, aqua, navy и т.д.) Строка типа #RRGGBB Строка типа rgb(0,0,0)

Политика, управляющая настройкой хранителя экрана, изменяет ключ KEY в схеме org.mate.screensaver. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.screensaver.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.mate.screensaver.KEY.

Таблица 29.26. Настройки хранителя экрана

Политика	Ключ	Описание	Значение
Время смены тем	cycle-delay	Устанавливает интервал (в минутах) между сменами тем хранителя экрана.	Время в минутах

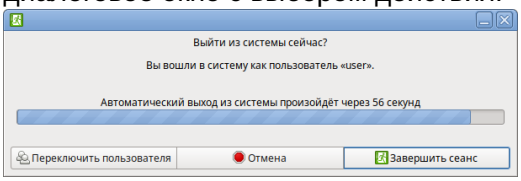
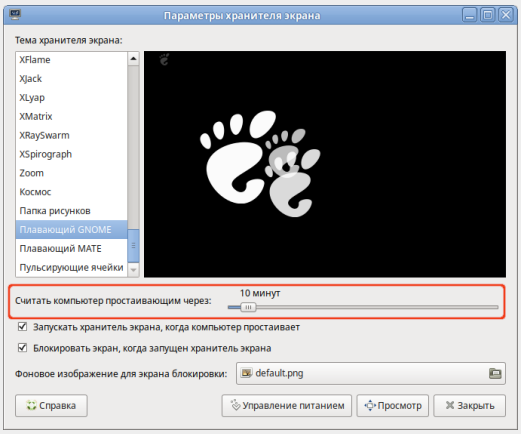
Политика	Ключ	Описание	Значение
		Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана** и если для параметра **Режим работы** установлено значение **Случайные темы**.	
Время до блокировки паролем	lock-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, компьютер будет заблокирован. Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана** и **Блокировка компьютера**	Время в минутах
Блокировка компьютера	lock-enabled	Включает блокировку компьютера при активации хранителя экрана. Блокировка будет включена через интервал времени, установленный настройкой **Время до блокировки паролем**. Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана**	-
Время до выхода из сеанса	logout-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, при разблокировании пользователю будет предоставлена возможность выхода из сеанса. Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана** и **Выход из сеанса после блокировки**	Время в минутах
Выход из сеанса после блокировки	logout-enabled		-

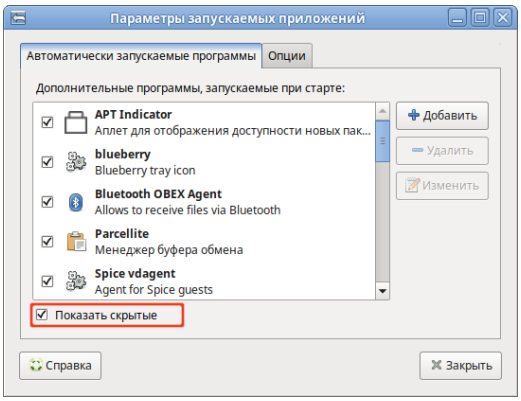
Политика	Ключ	Описание	Значение
		После некоторой задержки добавляет кнопку выхода из сеанса (**Завершить сеанс**) к диалогу разблокирования экрана. Время задержки указывается в настройке **Время выхода из сеанса**. Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана** и **Блокировка компьютера** (так как без блокировки не появляется диалог с кнопкой)	
Режим работы	mode	Устанавливает режим работы хранителя экрана. Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана**	Доступны следующие режимы: - **Отключён** — режим отключён - **Пустой экран** — не показывать никаких изображений, только чёрный экран - **Выбранная тема** — показывать одну (указанную) тему хранителя экрана - **Случайные темы** — выбрать тему хранителя экрана случайным образом
Переключить пользователя после блокировки	user-switch-enabled	Добавляет кнопку **Переключить пользователя** к диалогу разблокирования экрана. Этот параметр имеет смысл только при активированном параметре **Включение хранителя экрана** и **Блокировка компьютера** (так как без блокировки не появляется диалог с кнопкой)	-
	idle-activation-enabled		-

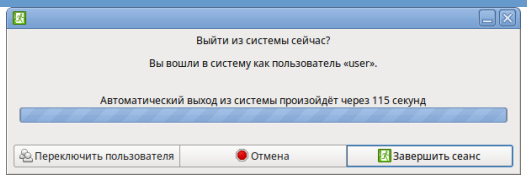
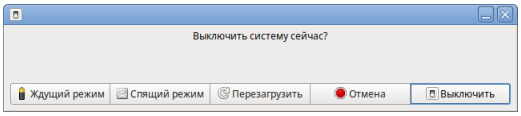
Политика	Ключ	Описание	Значение
Включение хранителя экрана		Обеспечивает включение хранителя экрана при бездействии системы	

Политика, управляющая настройкой ограничений сессии, изменяет ключ KEY в схеме org.mate.session. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.session.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.mate.session.KEY.

Таблица 29.27. Настройки сеанса

Политика	Ключ	Описание	Значение
Запрос при выходе из сеанса	logout-prompt	Если политика включена и для поля **Запрос при выходе из сеанса** выбрано значение **Включено**, при завершении сеанса будет выведено диалоговое окно с выбором действия:  Если политика включена и для поля **Запрос при выходе из сеанса** выбрано значение **Отключено**, завершение сеанса будет происходить автоматически, без появления диалогового окна.	-
Интервал бездействия, по истечении которого сеанс считается простаивающим	idle-delay	Устанавливает время в минутах, по истечении которого, сеанс будет считаться простаивающим. Данная политика позволяет управлять настройкой **Считать компьютер простаивающим через**: 	Время в минутах

Политика	Ключ	Описание	Значение
		Этот параметр имеет смысл только при активированных параметрах **Включение хранителя экрана** и **Блокировка компьютера**.	
Отображение скрытых автоматически запускаемых приложений	show-hidden-apps	Включает отображение скрытых автоматически запускаемых приложений в меню **Параметры запускаемых приложений**. Если политика включена и для неё выбрано состояние **Включено**, в окне **Параметры запускаемых приложений** будут показаны скрытые автоматически запускаемые приложения: 	-
Сохранение сеансов	auto-save-session	Позволяет автоматически сохранять рабочий сеанс для восстановления при следующем запуске. Если политика включена и для неё выбрано состояние **Включено**, система будет автоматически сохранять рабочий сеанс (система запомнит какие приложения были запущены при выходе из системы и автоматически запустит их при входе в систему).	-
Таймаут выхода из сеанса	logout-timeout	Позволяет установить время в секундах, по истечении которого произойдет выход из системы. Если политика включена, при завершении сеанса и выключении компьютера, в диалоговом окне с выбором действия будет выставлен тайм-аут со значением, указанным в поле **В секундах**:	Время в секундах

Политика	Ключ	Описание	Значение
		 Если в поле **В секундах** указан 0, то тайм-аут будет отключен:  Если политика не сконфигурирована или отключена, значение тайм-аута будет равно 60 секундам.	

Политика, управляющая настройкой ограничений пользователя, изменяет ключ KEY в схеме org.mate.lockdown. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.lockdown.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.mate.lockdown.KEY.

Таблица 29.28. Настройки ограничений пользователя

Политика	Ключ	Описание	Значение
Запрет блокировки экрана	picture-filename	Запрещает пользователю блокировать экран паролем. При установке данной настройки, значение параметра **Блокировка компьютера** игнорируется	-
Запрет пользователю завершать сеанс	disable-log-out	Запрещает пользователю завершать свой сеанс	-
Запрет выбора тем рабочего стола	picture-filename	Запрещает пользователю изменять тему оформления графической среды Mate	-
Запрет переключения пользователей	disable-user-switching	Запрещает пользователю переключение на другую учётную запись, пока активен его сеанс. Отключает кнопку **Переключить пользователя** в диалоговом окне, вызываемом при выборе в главном меню пункта **Завершить сеанс**	-

Политика, управляющая настройкой удаленного доступа VNC, изменяет ключ KEY в схеме org.gnome.Vino. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.gnome.Vino.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.gnome.Vino.KEY.

Таблица 29.29. Настройки удаленного доступа VNC

Политика	Ключ	Описание	Значение
Альтернативный порт	alternative-port	Устанавливает альтернативный порт для удаленного подключения к рабочему столу. Используется только при установленном параметре **Включить альтернативный порт**	Значение номера порта в пределах от 5 000 до 50 000. По умолчанию используется порт 5900
Методы аутентификации	authentication-methods	Устанавливает методы аутентификации пользователей, подключающихся к рабочему столу. Используется только при установленном параметре **Пароль для подключения**	- **None** — пароль для подключения не требуется - **Vnc** — для подключения необходим пароль
Удаленный доступ	enabled	Разрешает удаленный доступ к рабочему столу с использованием протокола RFB и VNC	- **Включено** — удаленный доступ разрешен - **Отключено** — удаленный доступ запрещён
Иконка подключения	icon-visibility	Управляет отображением значка подключения в области уведомления	- **Никогда** — значок не отображается - **Всегда** — значок отображается всегда - **Только при подключении клиента** — значок отображается при подключении удалённого пользователя
Подтверждение при подключении	prompt-enabled	Включает запрос подтверждения при любой попытке доступа к рабочему столу. Рекомендуется при отсутствии защиты подключения паролем	- **Включено** — запрашивается подтверждение доступа - **Отключено** — подтверждение доступа не запрашивается
Включить альтернативный порт	prompt-enabled		- **Включено** — включить прослушивание альтернативного порта

Политика	Ключ	Описание	Значение
		Включить прослушивание альтернативного порта для удалённых подключений (вместо порта по умолчанию 5 900). Порт указывается в параметре **Альтернативный порт**	**Отключено** — не включать прослушивание альтернативного порта
Удалённое управление	view-only	Запрещает удалённое управление рабочим столом. Удалённым пользователям, разрешается только просматривать рабочий стол, но не управлять мышью и клавиатурой	**Включено** — удаленное управление разрешено **Отключено** — удаленное управление запрещёно

Политика, управляющая настройкой оконного менеджера Marco, изменяет ключ KEY в схеме org.mate.Marco.general. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.pMarco.general.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.mate.Marco.general.KEY.

Таблица 29.30. Настройки оконного менеджера Marco

Политика	Ключ	Описание	Значение
Иконки заголовка окна	button-layout	Настройки расположения кнопок в заголовке окна	Строка вида: menu:minimize,maximize,spacer,close Разделителем правой и левой половин является двоеточие. Имена кнопок разделяются запятыми. Например, строка *'menu:minimize,maximize,spacer,close'* — расположить кнопку меню окна слева, а справа кнопки свернуть, распахнуть, закрыть окно. Дублирование кнопок не допускается. Неизвестные имена кнопок игнорируются без уведомления. Специальный элемент spacer может использоваться для вставки пробела между двумя кнопками.
	action-middle-click-titlebar		

Политика	Ключ	Описание	Значение
Действие по нажатию средней кнопки		Установливает действие, выполняемое по нажатию средней кнопки мыши по заголовку окна	**Свернуть в заголовок** (toggle_shade) — свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно **На весь экран** (toggle_maximize) — распахнуть окно на весь экран или восстановить исходный размер **Растянуть по вертикали** (toggle_maximize_verticall y) — развернуть окно вертикально без изменения его ширины **Растянуть по горизонтали** (toggle_maximize_horizont ally) — развернуть окно горизонтально без изменения его высоты **Свернуть** (minimize) — свернуть окно **Показать меню** (menu) — показать меню окна **Задвинуть** (lower) — поместить окно под другими **Ничего не делать** (none) — никакого действия не производить **Последнее действие** (last) — повторить предыдущее действие
Действие по нажатию правой кнопки	action-right-click-titlebar	Устанавливает действие, выполняемое по нажатию правой кнопки мыши по заголовку окна	**Свернуть в заголовок** (toggle_shade) — свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно

Политика	Ключ	Описание	Значение
			На весь экран (toggle_maximize) — распахнуть окно на весь экран или восстановить исходный размер **Растянуть по вертикали** (toggle_maximize_vertically) — развернуть окно вертикально без изменения его ширины **Растянуть по горизонтали** (toggle_maximize_horizontally) — развернуть окно горизонтально без изменения его высоты **Свернуть** (minimize) — свернуть окно **Показать меню** (menu) — показать меню окна **Задвинуть** (lower) — поместить окно под другими **Ничего не делать** (none) — никакого действия не производить **Последнее действие** (last) — повторить предыдущее действие
Действие по двойному щелчку	action-double-click-titlebar	Устанавливает действие, выполняемое по двойному щелчку левой кнопкой мыши по заголовку окна	**Свернуть в заголовок** (toggle_shade) — свернуть окно в заголовок. По двойному щелчку окно разворачивается обратно **На весь экран** (toggle_maximize) — распахнуть окно на весь экран или восстановить исходный размер **Растянуть по вертикали** (toggle_maximize_vertically) — развернуть окно вертикально без изменения его ширины

Политика	Ключ	Описание	Значение
			Растянуть по горизонтали (toggle_maximize_horizontally) — развернуть окно горизонтально без изменения его высоты **Свернуть** (minimize) — свернуть окно **Показать меню** (menu) — показать меню окна **Задвинуть** (lower) — поместить окно под другими **Ничего не делать** (none) — никакого действия не производить **Последнее действие** (last) — повторить предыдущее действие
Изменение размеров окна при перетаскивании	primary-color	Включает изменение размеров окна при перетаскивании его в различные области экрана. Если включено, перетаскивание окна на границу экрана распахивает окно вертикально и изменяет горизонтальный размер до половины доступного пространства. Если активирован параметр **Распахнуть окно при перетаскивании к верхнему краю экрана**, перетаскивание окна наверх разворачивает окно.	-
Разворачивание при перетаскивании (Распахнуть окно при перетаскивании к верхнему краю экрана)	allow-top-tiling	Включает разворачивание окна во весь экран при перетаскивании его к верхнему краю экрана. Этот параметр имеет смысл только при активированном параметре **Изменение размеров окна при перетаскивании**	-
	alt-tab-max-columns		Количество колонок

Политика	Ключ	Описание	Значение
Размер окна переключения Alt+Tab		Устанавливает количество колонок в окне переключения приложений Alt+Tab	
Задержка при восстановлении	alt-tab-max-columns	Временной интервал в миллисекундах, по истечении которого окно в фокусе будет поднято поверх остальных. Этот параметр имеет смысл только при активированном параметре **Автоматически поднимать окно, получившее фокус**	Время в миллисекундах
Автоматически поднимать окно, получившее фокус	auto-raise	При включении этой политики, окно, получившее фокус, автоматически отображается поверх остальных. Параметр **Переключение фокуса окон** должен быть установлен в **Sloppy** или **Mouse**. Интервал, по истечении которого, окно поднимается, устанавливается в параметре **Задержка при восстановлении**	-
Новые окна по центру	center-new-windows	Если включено, то новые окна будут открываться по центру экрана. В противном случае они будут открыты в левом верхнем углу экрана	-
Миниатюры при переключении окон	compositing-fast-alt-tab	Если включено, то вместо миниатюр предварительного просмотра в окне переключения Alt+Tab будут отображаться значки приложений	-
Режим активации окна	focus-mode	Режим переключения фокуса в окно определяет, как активируются окна	• **Click** — для активации окна на нём надо щелкнуть • **Sloppy** — окно активируется, когда на него перемещается указатель мыши • **Mouse** — окно активируется, когда в него перемещается указатель мыши, и

Политика	Ключ	Описание	Значение
			перестает быть активным, когда указатель мыши уходит из него
Переключение фокуса на новое окно	focus-new-windows	Определяет, как новое окно получает фокус	**`Smart`** — новое окно получает фокус при создании **`Strict`** — окна, запущенные из терминала, не получают фокус
Размер иконок в окне Alt+Tab	icon-size	Устанавливает размер значков, отображаемых в окне переключения приложений Alt+Tab	Интервал допустимых значений: 8-256
Количество рабочих областей (мест)	num-workspaces	Установка количества рабочих мест	Интервал допустимых значений 1-36
Расположение новых окон	placement-mode	Указывает как будут позиционироваться новые окна	**`Автоматически`** (automatic) — система выбирает местоположение на основе доступного пространства на рабочем столе, или располагает каскадом, если нет места **`Указатель`** (pointer) — новые окна размещаются в соответствии с положением указателя мыши **`Ручной`** (manual) — пользователь должен вручную расположить новое окно с помощью мыши или клавиатуры
Граница окна при переключении с помощью Alt+Tab	show-tab-border	Выделять границу выбранного окна при переключении с помощью Alt+Tab	-

Политика	Ключ	Описание	Значение
Тема оформления	theme	Устанавливает тему, отвечающую за отображение границ окон, заголовка и т.д.	Строка, содержащая название темы (например, Dopple)
Шрифт заголовка окна	titlebar-font	Устанавливает шрифт заголовков окон. Этот параметр игнорируется, если активирован параметр **Системный шрифт в заголовке окна**	Строка, содержащая название шрифта и через пробел, размер шрифта (например, Noto Sans Bold 10)
Системный шрифт в заголовке окна	titlebar-uses-system-font	Если включено, в заголовках окон используется стандартный системный шрифт. Параметр **Шрифт заголовка окна** при этом игнорируется	-
Переключение рабочих областей (столов)	wrap-style	Определяет, каким образом пролистывать от одного рабочего стола к другому на границе переключателя рабочих мест	- **No wrap** — при попытке пролистать рабочее место за границу переключателя ничего не произойдет - **Classic** — конец одной строки ведет на начало следующей и конец одной колонки ведет к началу следующей - **Toroidal** — конец каждой строки ведет к её же началу и конец каждой колонки ведёт к её же началу

Политика, управляющая настройкой клавиатуры, изменяет ключ KEY в схеме org.mate.peripherals-keyboard. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.mate.peripherals-keyboard.KEY. Блокировка устанавливается в ветке реестра Software\BaseALT\Policies\GSettingsLocks ключ org.mate.peripherals-keyboard.KEY.

Таблица 29.31. Настройки клавиатуры

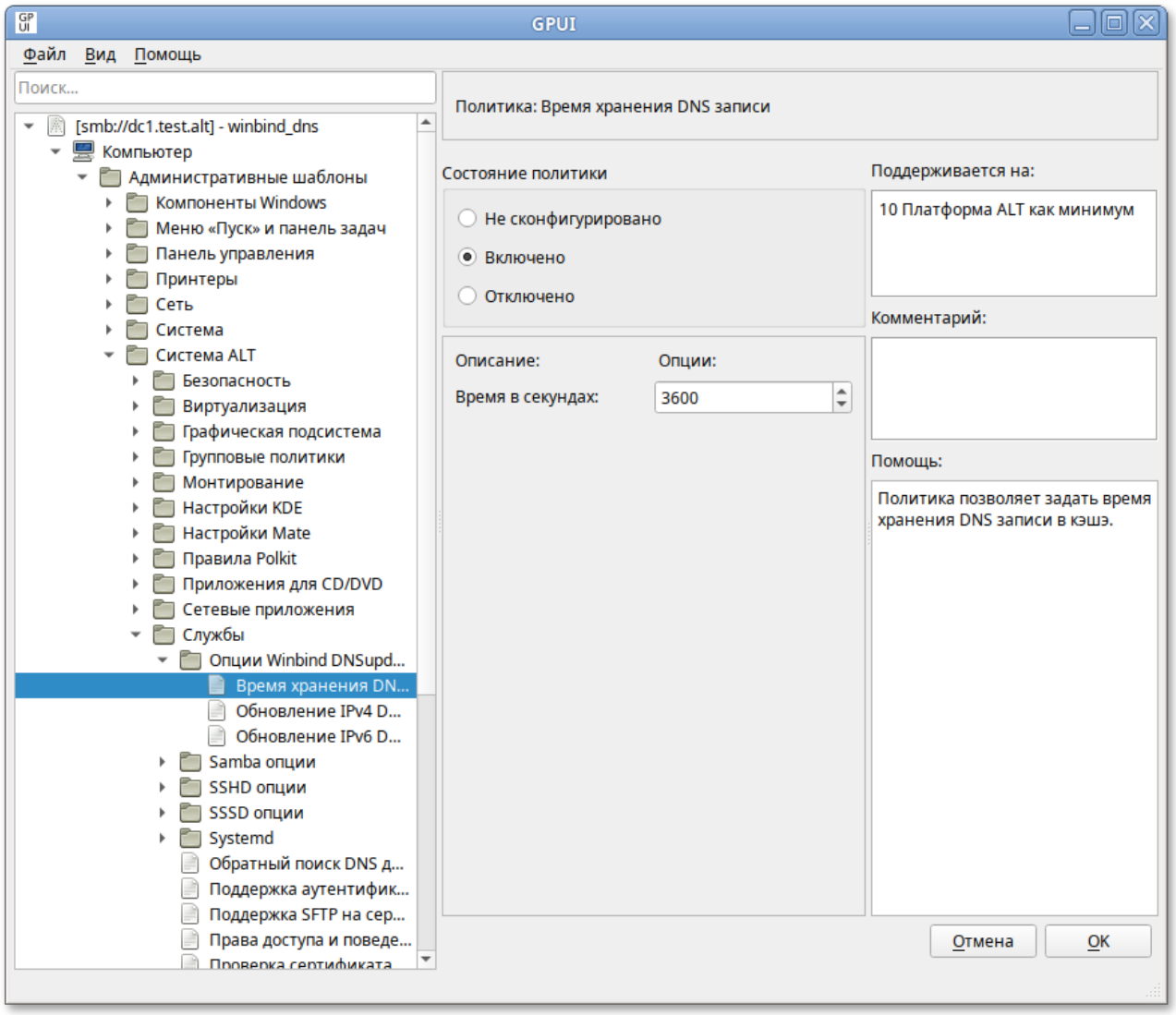
Политика	Ключ	Описание	Значение
Задержка перед повтором	delay	Задержка перед повтором нажатой и удерживаемой клавиши	Время в миллисекундах
Скорость повтора	rate	Устанавливает скорость повтора нажатой и удерживаемой клавиши	Количество повторов в секунду
	repeat		-

Политика	Ключ	Описание	Значение
Повторять удерживаемую нажатой клавишу		Включить повтор нажатой и удерживаемой клавиши. Если нажать и удерживать клавишу при включённом повторе ввода, действие, соответствующее клавише, будет повторяться. Например, если нажать и удерживать клавишу с буквой, то эта буква будет многократно повторена.	

29.5.5.1. Опции Winbind DNSupdate

С помощью групповых политик в Альт Домен можно централизованно управлять параметрами winbind-dnsupdate.

Для настройки данных политик следует перейти в **Компьютер → Административные шаблоны → Система ALT → Службы → Опции Winbind DNSupdate**:



Политика, управляющая опцией Winbind DNSupdate, изменяет ключ KEY в схеме org.altlinux.winbind.dnsupdate. В реестре Windows данная политика изменяет в Software\BaseALT\Policies\gsettings ключ org.altlinux.winbind.dnsupdate.KEY.

Таблица 29.32. Опции Winbind DNSupdate

Политика	Ключ	Описание	Значение
Время хранения DNS записи	ttl	Позволяет позволяет задать время хранения DNS записи в кеше	Время в секундах
Обновление IPv4 DNS записей	enable-update-ipv4, ipv4_ptr_update	Позволяет включить обновление прямой и обратной IPv4 DNS записи компьютера. Включение параметра **Обновление обратной IPv4 DNS записи** имеет смысл только при включённом параметре **Обновление прямой IPv4 DNS записи**	-
Обновление IPv6 DNS записей	enable-update-ipv6, ipv6_ptr_update	Позволяет включить обновление прямой и обратной IPv6 DNS записи компьютера. Включение параметра **Обновление обратной IPv6 DNS записи** имеет смысл только при включённом параметре **Обновление прямой IPv6 DNS записи**	-

29.5.6. Управление настройками среды рабочего стола KDE

Данные групповые политики позволяют управлять настройками среды рабочего стола KDE.

Для реализации применения групповых политик управления настройками среды рабочего стола KDE используется механизм, основанный на редактировании конфигурационных файлов.

Файл конфигурации состоит из пар «ключ=значение», которые размещены в группах. Начало группы обозначается именем группы, заключенным в квадратные скобки. Все последующие записи «ключ=значение» принадлежат этой группе. Группа заканчивается, когда начинается другая группа или когда достигается конец файла. Записи в верхней части файла, которым не предшествует имя группы, относятся к группе по умолчанию. Пустые строки, как и строки, начинающиеся с решетки («#»), в файлах конфигурации игнорируются.

Пример файла конфигурации:

```
[General]
FilterBar=0
Version=202
ViewPropsTimestamp=2023,10,5,18,6,33.478
```

```
[MainWindow]
MenuBar=Disabled
ToolBarsMovable=Disabled
```

Если в дереве каталогов обнаружено несколько файлов конфигурации с одинаковым именем, их содержимое объединяется. Здесь играет роль порядок приоритета каталогов: когда два файла определяют один и тот же ключ конфигурации, файл с наивысшим приоритетом определяет, какое значение используется для ключа. Конфигурационные файлы из $KDEHOME всегда обладают наивысшим приоритетом. В случае, если в одном конфигурационном файле один ключ указан несколько раз, будет использовано последнее его значение.

Машинные политики являются действующими по умолчанию, а пользовательские, при установке, замещают машинные. У политик имеются блокировки. При установке машинных блокировок пользовательские настройки игнорируются, а для применения используются значения, установленные машинными политиками.

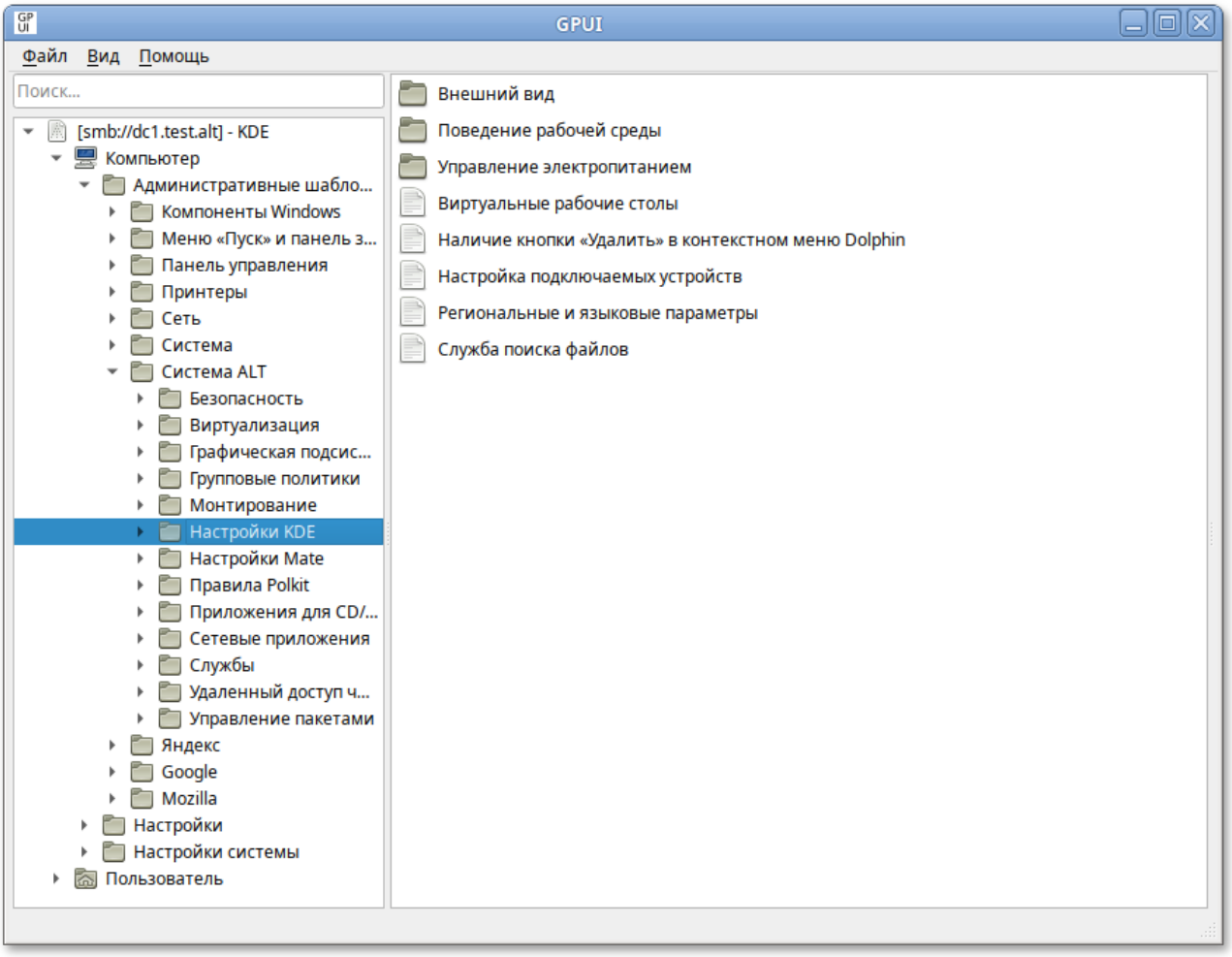
Примечание

Поведение разных приложений на блокировку может отличаться. Одни приложения могут распознавать блокировку, другие использовать пользовательские настройки, несмотря на наличие блокировки.

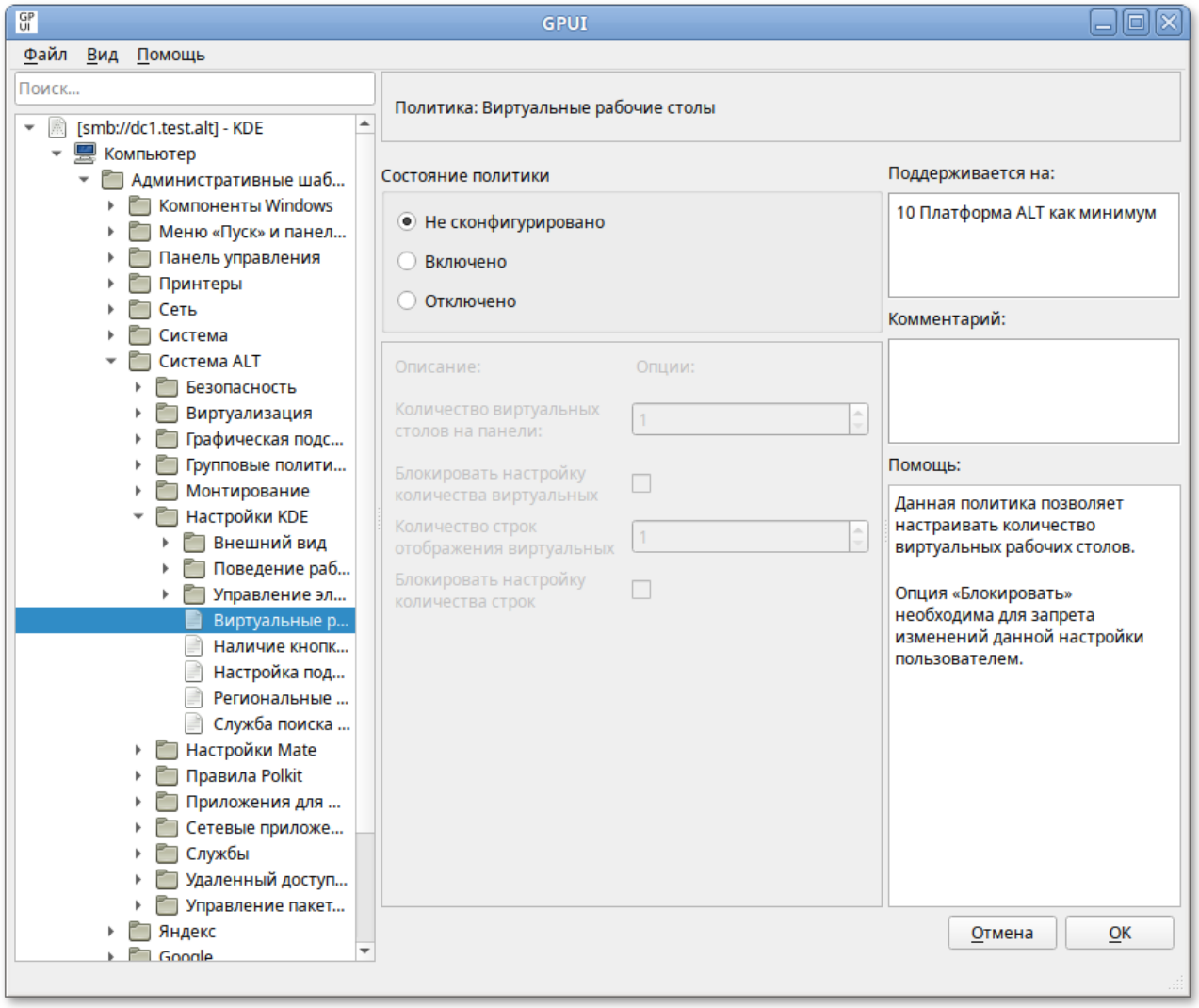
Порядок применения политик:

1. Машинные политики применяются при загрузке компьютера.
2. Машинные политики без блокирования могут применяться, но только в том случае, если пользователь ни разу не изменял эти политики.
3. Машинные политики с блокировкой применяются независимо от пользовательских настроек.
4. Пользовательские политики применяются при логине пользователя и только в случае, если нет таких же машинных политик с блокировкой.

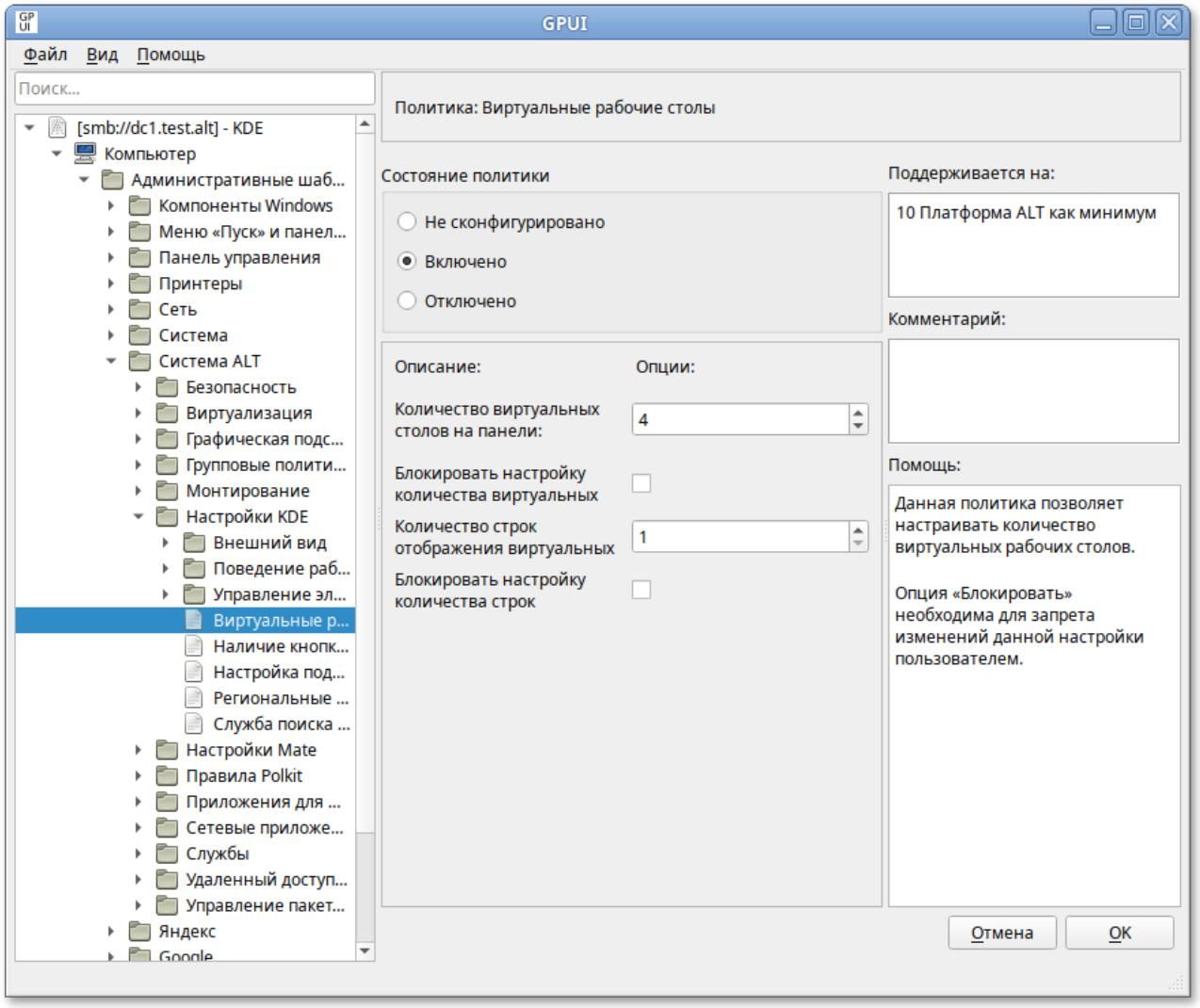
Для настройки политики следует перейти в **Компьютер/Пользователь → Административные шаблоны → Система ALT → Настройки KDE**. Выбрать раздел, в правом окне редактора отобразится список политик:



При выборе политики откроется диалоговое окно настройки политики:



Можно не задавать настройку политики, включить или отключить. Если выбрать параметр **Включено**, в разделе **Параметры** в выпадающем списке можно указать настройки политики:



Политики, управления настройками среды рабочего стола KDE, относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. раздел Экспериментальные групповые политики).

Значения параметров данных политик прописываются в файлы конфигурации:

- **`/etc/xdg/<имя_файла>`** — машинная политика;
- **`~/.config/<имя_файла>`** — пользовательская политика.

Таблица 29.33. Настройки среды рабочего стола KDE

Политика	Описание	Примечание
Виртуальные рабочие столы	Позволяет настроить количество виртуальных рабочих столов.	Файлы конфигурации: - **`/etc/xdg/kwinrc`** — машинная политика - **`~/.config/kwinrc`** — пользовательская политика Пример файла конфигурации:

Политика	Описание	Примечание
		``` [Desktops] Number=4 Rows=1 ``` Где: - **Rows=1** — количество строк отображения виртуальных окон на панели; - **Number=4** — количество виртуальных окон на панели.
Наличие кнопки «Удалить» в контекстном меню Dolphin	Позволяет управлять отображением кнопки **Удалить** в контекстном меню Dolphin	Файлы конфигурации: - **/etc/xdg/kdeglobals** — машинная политика - **~/.config/kdeglobals** — пользовательская политика Пример файла конфигурации: ``` [KDE] ShowDeleteCommand[$i]=1 ``` Возможные значения: - **ShowDeleteCommand=1** — показывать кнопку **Удалить** в контекстном меню Dolphin; - **ShowDeleteCommand=0** — не показывать кнопку **Удалить** в контекстном меню Dolphin; - **ShowDeleteCommand[$i]=1** — показывать кнопку **Удалить** в контекстном меню Dolphin и заблокировать возможность изменения данной настройки пользователем.
Настройка подключаемых устройств	Позволяет настроить автоматическое монтирование подключаемых устройств.	Возможные значения: - **Автоматически монтировать устройства** — если этот параметр отключён (**AutomountEnabled=0**), никакие носители информации не будут монтироваться автоматически; - **При входе в систему** — если этот параметр включён (**AutomountOnLogin=1**) и при входе пользователя в систему к ней были подключены внешние носители информации, Plasma автоматически сделает их содержимое доступным для других программ;

Политика	Описание	Примечание

		▸**При подключении** — если этот параметр включён (**AutomountOnPlugin=1**), устройства будут монтироваться при подключении их к системе;
		▸**Автоматически монтировать те носители, которые никогда ранее не были примонтированы вручную** — если этот параметр отключён (**AutomountUnknownDevices=0**), автоматически будут монтироваться только те носители, информацию о которых помнит система (носитель «запоминается», если он был хотя бы один раз был смонтирован).
		
		Файлы конфигурации:
		
		▸**/etc/xdg/kded_device_automounterrc** — машинная политика
		▸**~/.config/kded_device_automounterrc** — пользовательская политика
		
		Пример файла конфигурации:
		
		`[General]`
		`AutomountEnabled=1`
		`AutomountOnLogin=1`
		`AutomountOnPlugin=0`
		`AutomountUnknownDevices=0`

Региональные и языковые параметры	Позволяет установить региональные и языковые параметры. Эти параметры меняют настройки не только самого языка системы, но и задают настройки валюты, стандарт времени, числовые значения, стиль написания имени, телефонный код и стандарт телефонного номера страны. Параметры вписываются в поля **Стандарт** и **Язык**.
	
	Примеры:
	
	▸«Русский язык»: **Стандарт** — ru_RU.UTF-8; **Язык** — ru;
		Файлы конфигурации:
		
		▸**/etc/xdg/plasma-localerc** — машинная политика
		▸**~/.config/plasma-localerc** — пользовательская политика
		
		Пример файла конфигурации:
		
		`[Formats]`
		`LANG[$i]=ru_RU.UTF-8`
		
		`[Translation]`
		`LANGUAGE=ru`

Политика	Описание	Примечание
	Французский язык»: **Стандарт** — fr_FR.UTF-8; **Язык** — fr; Немецкий язык»: **Стандарт** — de_DE.UTF-8; **Язык** — de; «Английский язык (Американский)»: **Стандарт** — en_US.UTF-8; **Язык** — en_US; «Английский язык (Британский)»: **Стандарт** — en_GB.UTF-8; **Язык** — en_GB;	Где: **LANG[$i]=ru_RU.UTF-8** — стандарт русского языка, возможность изменения данной настройки пользователем заблокирована; **LANGUAGE=ru** — русский язык.

Служба поиска файлов	Позволяет включить службу поиска файлов и задать параметры индексирования файлов.	Возможные значения:
		Включить службу поиска файлов — включить поиск файлов с помощью Baloo (**Indexing-Enabled=1**);
		Включить индексацию содержимого файлов — индексировать не только имена файлов, но и их содержимое (**only basic indexing=1**);
		Включить индексацию скрытых файлов и папок — индексировать также скрытые файлы и папки (**index hidden folders=1**).
		Файлы конфигурации:
		/etc/xdg/baloofilerc — машинная политика
		~/.config/baloofilerc — пользовательская политика
		Пример файла конфигурации:
		`[Basic Settings]`
		`Indexing-Enabled=1`
		`[General]`
		`index hidden folders=0`
		`only basic indexing=1`
		Примечание

Политика	Описание	Примечание
		Параметры **Включить индексацию содержимого файлов** и **Включить индексацию скрытых файлов и папок** имеют смысл только при включённом параметре **Включить службу поиска файлов**.

29.5.6.1. Внешний вид

Таблица 29.34. Внешний вид

Политика	Описание	Значение
Оформление рабочего стола	Позволяет выбрать оформление рабочего стола (определяет то, как отображаются различные компоненты Plasma), указав название темы (например, breeze-light). Используются темы оформления рабочего стола, доступные в **/usr/share/kf5/plasma/desktoptheme**. Для добавления новых тем необходимо установить пакеты, включающие в себя эти темы.	**default** — тема по умолчанию (Breeze) **breeze-dark** — Breeze, тёмный вариант **breeze-light** — Breeze, светлый вариант **oxygen** — Oxygen **air** — Air
Оформление рабочей среды	Позволяет установить тему оформления рабочей среды, указав название темы (например, org.kde.название.desktop или org.kde.название). Используются темы оформления рабочего стола, доступные в **/usr/share/kf5/plasma/look-and-feel/**. Для добавления новых тем необходимо установить пакеты, включающие в себя эти темы.	**org.kde.breeze.desktop** **org.kde.breezedark.desktop** **org.kde.oxygen** **org.kde.breezetwilight.desktop**

Политика	Описание	Значение
Тема заставки	Позволяет установить тему заставки, указав название темы (например, org.kde.название.desktop или org.kde.название). Используются темы заставки, доступные в **/usr/share/kf5/plasma/look-and-feel/**. Для добавления новых тем необходимо установить пакеты, включающие в себя эти темы.	**org.kde.breeze.desktop** **org.kde.oxygen**
Тема значков	Позволяет установить тему значков, указав название темы (например, gnome). Применение темы значков зависит от её наличия в системе. Используются темы значков, доступные в **/usr/share/icons/**. Для добавления новых тем необходимо установить пакеты, включающие в себя эти темы.	**Adwaita** **oxygen** **breeze** **breeze-dark** **gnome**
Тема курсора	Позволяет установить тему курсора мыши, указав название темы (например, Adwaita). Применение темы курсора зависит от её наличия в системе. Используются темы курсоров, доступные в **/usr/share/icons/**. Для добавления новых тем необходимо установить пакеты, включающие в себя эти темы.	**Adwaita** — Adwaita **Breeze_Snow** — Breeze, светлый вариант **KDE_Classic** — классический KDE **Oxygen_Black** — Oxygen, чёрный вариант **Oxygen_Blue** — Oxygen, синий вариант **Oxygen_White** — Oxygen, белый вариант **Oxygen_Yellow** — Oxygen, жёлтый вариант **Oxygen_Zion** — Oxygen Zion **jimmac** — jimmac **breeze_cursors** — Breeze

Политика	Описание	Значение
Цвета	Позволяет установить цветовую схему, указав название схемы (например, BreezeClassic). Применение цветовой схемы зависит от её наличия в системе. Используются цветовые схемы, доступные в **/usr/share/kf5/color-schemes**. Для добавления новых тем необходимо установить пакеты, включающие в себя эти темы.	Варианты цветовых схем: - **OxygenCold** — холодный Oxygen - **BreezeClassic** — Breeze, классический вариант - **BreezeLight** — Breeze, светлый вариант - **BreezeDark** — Breeze, тёмный вариант - **Oxygen** — Oxygen
Пользовательские политики		
Обои рабочего стола	Позволяет установить изображение в качестве фона рабочего стола, указав файл, содержащий изображение.	В качестве значения должна быть указана строка, содержащая путь (с точки зрения клиента) к файлу изображения. Например: - **/usr/share/wallpapers/table.png** — локальный путь к изображению; - **smb://dc1.test.alt/reGr/test.png** — путь в формате Linux к изображению в общем каталоге на сервере; - **\\computername\share\image.png** — путь в формате Windows к изображению в общем каталоге на сервере.
Включение панели фильтрации в файловом менеджере Dolphin	Позволяет включить или отключить панель фильтрации в файловом менеджере Dolphin.	-

29.5.6.2. Поведение рабочей среды

Таблица 29.35. Поведение рабочей среды

Политика	Описание	Примечание
Блокировка экрана	Позволяет регулировать параметры блокировки экрана.	Файлы конфигурации: - **/etc/xdg/kscreenlockerrc** — машинная политика - **~/.config/kscreenlockerrc** — пользовательская политика

Политика	Описание	Примечание

	Позволяет определить, сколько времени должно проходить перед включением блокировки экрана, настроить период отсрочки для разблокировки экрана без пароля.
	
	Настройка **Время до блокировки экрана при отсутствии активности** будет применена только в случае включения параметра **Автоматически блокировать экран**
		Пример файла конфигурации:
		
		`[Daemon]`
		`Autolock[$i]=1`
		`Timeout[$i]=12`
		`LockOnResume[$i]=1`
		`LockGrace[$i]=11`
		
		Где:
		
		▸ **Autolock=1** — автоматически блокировать экран;
		▸ **Autolock=0** — не блокировать экран автоматически;
		▸ **Autolock[$i]=1** — включить автоматическую блокировку экрана и заблокировать возможность изменения данной настройки пользователем;
		▸ **Timeout=12** — продолжительность периода отсутствия активности пользователя до запуска блокировщика экрана (в минутах);
		▸ **LockOnResume=1** — включить блокировку экрана рабочего стола после приостановки работы системы;
		▸ **LockOnResume=0** — отключить блокировку экрана рабочего стола после приостановки работы системы;
		▸ **LockOnResume[$i]=1** — включить блокировку экрана рабочего стола после приостановки работы системы и заблокировать возможность изменения данной настройки пользователем;
		▸ **LockGrace=11** — интервал времени после блокирования экрана, во время которого можно вернуться в систему без ввода пароля (в секундах).

Графические эффекты	Позволяет настроить включение или отключение графических эффектов при входе в систему	Файлы конфигурации:
		
		▸ **/etc/xdg/kwinrc** — машинная политика
		▸ **~/.config/kwinrc** — пользовательская политика
		
		Пример файла конфигурации:
		
		`[Compositing]`
		`Enabled=1`

Политика	Описание	Примечание
		Возможные значения: - **Enabled=1** — включить эффекты при входе в систему; - **Enabled=0** — не включать эффекты при входе в систему; - **Enabled[$i]=1** — включить эффекты при входе в систему и заблокировать возможность изменения данной настройки пользователем.

Задержка отрисовки	Позволяет установить уровень задержки и плавности анимации	Возможные значения:
		- **Принудительно низкая задержка (может привести к артефактам)** (**LatencyPolicy=ExtremelyLow**)
		- **Предпочитать низкую задержку** (**LatencyPolicy=Low**)
		- **Баланс скорости и плавности** (**LatencyPolicy=Medium**)
		- **Предпочитать более плавную анимацию** (**LatencyPolicy=High**)
		- **Принудительно наиболее плавная анимация» (по умолчанию)** (**LatencyPolicy=NONE**)
		
		Файлы конфигурации:
		- **/etc/xdg/kwinrc** — машинная политика
		- **~/.config/kwinrc** — пользовательская политика
		
		Пример файла конфигурации:
		`[Compositing]`
		`LatencyPolicy=Medium`

Открытие файла или каталога одним щелчком	Позволяет настроить открытие файла или каталога одним щелчком	Файлы конфигурации:
		- **/etc/xdg/kdeglobals** — машинная политика
		- **~/.config/kdeglobals** — пользовательская политика
		
		Пример файла конфигурации:
		`[KDE]`
		`SingleClick[$i]=1`

Политика	Описание	Примечание
		Возможные значения: - **SingleClick=1** — щелчок по файлу или каталогу открывает объект; - **SingleClick=0** — щелчок по файлу или каталогу выделяет объект; - **SingleClick[$i]=1** — щелчок по файлу или каталогу открывает объект, возможность изменения данной настройки пользователем заблокирована.
Режим активации окна	Позволяет определить как активируются окна при переключении фокуса.	Возможные значения: - **Фокус по щелчку** — при выборе этого значения (**FocusPolicy=FocusFollowMouse**), окно становится активным по щелчку по нему мышью; - **Фокус по щелчку** + **Приоритет мыши** (**FocusPolicy=FocusFollowMouse** + **NextFocusPrefersMouse=1**) — этот режим похож на **Фокус по щелчку**. Если система сама должна выбрать активное окно (например, при закрытии активного окна), предпочтение будет отдано окну, находящемуся под указателем мыши; - **Фокус следует за мышью** — при выборе этого значения (**FocusPolicy=FocusFollowsMouse**), окно активируется при перемещении в него указателя мыши. Окна, которые появляются под указателем мыши случайно, не будут получать фокус, так как предотвращение смены фокуса работает как обычно. Этот вариант похож на **Фокус по щелчку**, но щелчок не требуется; - **Фокус следует за мышью** + **Приоритет мыши** (**FocusPolicy=FocusFollowsMouse** + **NextFocusPrefersMouse=1**) — этот режим похож на **Фокус следует за мышью**. Если система сама должна выбрать активное окно (например, при закрытии активного окна), предпочтение будет отдано окну, находящемуся под указателем мыши. Данный режим следует выбрать для смены фокуса по наведению указателя мыши; - **Фокус под мышью** — при выборе этого значения (**FocusPolicy=FocusUnderMouse**), активным становится окно, находящееся под указателем мыши. Если последний указывает не на окно (а, например, на обои рабочего стола), фокус перемещается на окно, которое находилось под указателем

Политика	Описание	Примечание

		мыши последним. Примечание: предотвращение смены фокуса и переключение через Alt+Tab противоречат этому поведению и не будут работать;
		Фокус строго под мышью (**FocusPolicy=FocusStrictlyUnderMouse**) — этот режим схож с режимом **Фокус под мышью**, но имеет более узкое применение. Активным становится только то окно, которое находится под указателем мыши. При смещении указателя мыши с окна фокус теряется. Примечание: предотвращение смены фокуса и переключение через Alt+Tab противоречат этому поведению и не будут работать.
		
		Файлы конфигурации:
		/etc/xdg/kwinrc — машинная политика
		~/.config/kwinrc — пользовательская политика
		
		Пример файла конфигурации:
		`[Windows]`
		`FocusPolicy=FocusFollowMouse`
		`NextFocusPrefersMouse=0`

Пользовательские политики		
Обновление графического окружения Plasma	Если политика включена, при изменении пути до файла изображения рабочего стола сервис графического окружения Plasma-plasmashell будет автоматически обновляться	

29.5.6.3. Управление электропитанием

Данные политики позволяют настроить параметры энергосбережения в зависимости от режима электропитания: «Питание от сети», «Питание от батареи» и «Низкий уровень заряда».

Значения параметров прописываются в файл конфигурации:

- **/etc/xdg/powermanagementprofilesrc** — машинная политика;
- **~/.config/powermanagementprofilesrc** — пользовательская политика.

Таблица 29.36. Управление электропитанием

Политика	Описание	Файл конфигурации

Потухание экрана	Позволяет настроить время до угасания экрана (уменьшения яркости до нуля) в зависимости от режима электропитания.	Для указания значения используется точное время в минутах, заданное в миллисекундах. Если время в миллисекундах указано неверно и не соответствует целому значению в минутах, то время автоматически округляется к ближайшему целому значению в меньшую сторону, например:
		- 60000 — угасание монитора через 60000 миллисекунд, 1 минуту;
		- 80000 — угасание монитора через 80000 миллисекунд, 1 минуту;
		- 120000 — угасание монитора через 120000 миллисекунд, 2 минуты;
		- 600000 — угасание монитора через 600000 миллисекунд, 10 минут.
		
		Пример файла конфигурации:
		`[AC][DimDisplay]`
		`idleTime=800000`
		
		`[Battery][DimDisplay]`
		`idleTime=600000`
		
		`[LowBattery][DimDisplay]`
		`idleTime=600000`

Энергосбережение монитора	Позволяет настроить время до выключения монитора (при бездействии) в зависимости от режима электропитания.	Для указания значения используется точное время в минутах, заданное в секундах. Если время в секундах указано неверно и не соответствует целому значению в минутах, то время автоматически округляется к ближайшему целому значению в меньшую сторону, например: - 120 — выключение монитора через 120 секунд, 2 минуты; - 300 — выключение монитора через 300 секунд, 5 минут; - 600 — выключение монитора через 600 секунд, 10 минут; - 700 — выключение монитора через 600000 секунд, 11 минут. Пример файла конфигурации:

Политика	Описание	Файл конфигурации

		`[AC][DPMSControl]`
		`idleTime=800`
		
		`[Battery][DPMSControl]`
		`idleTime=600`
		
		`[LowBattery][DPMSControl]`
		`idleTime[$i]=60`

Яркость клавиатуры	Позволяет настроить яркость клавиатуры в зависимости от режима электропитания.	Для указания значения используется число от 0 до 100, например:
		- 0 — яркость клавиатуры 0 процентов;
		- 60 — яркость клавиатуры 60 процентов;
		- 100 — яркость клавиатуры 100 процентов.
		
		Пример файла конфигурации:
		
		`[AC]`
		`[KeyboardBrightnessControl]`
		`value=60`
		
		`[Battery]`
		`[KeyboardBrightnessControl]`
		`value=20`
		
		`[LowBattery]`
		`[KeyboardBrightnessControl]`
		`value[$i]=0`

Яркость экрана	Позволяет настроить яркость экрана в зависимости от режима электропитания.	Для указания значения используется число от 0 до 100, например:
		- 0 — яркость экрана 0 процентов;
		- 60 — яркость экрана 60 процентов;
		- 100 — яркость экрана 100 процентов.
		
		Пример файла конфигурации:
		
		`[AC][BrightnessControl]`
		`value=80`
		
		`[Battery][BrightnessControl]`

Политика	Описание	Файл конфигурации
		value=50 [LowBattery] [BrightnessControl] value=30

29.5.6.4. Настройки приложений

Таблица 29.37. Настройки приложений

Политика	Описание	Значение
Браузер по умолчанию	Позволяет выбрать браузер по умолчанию.	Возможные значения: **Yandex-Browser** **Firefox** **Chromium-gost** **Примечание** Применение настроек доступно только в случае, если в системе установлен выбранный браузер.

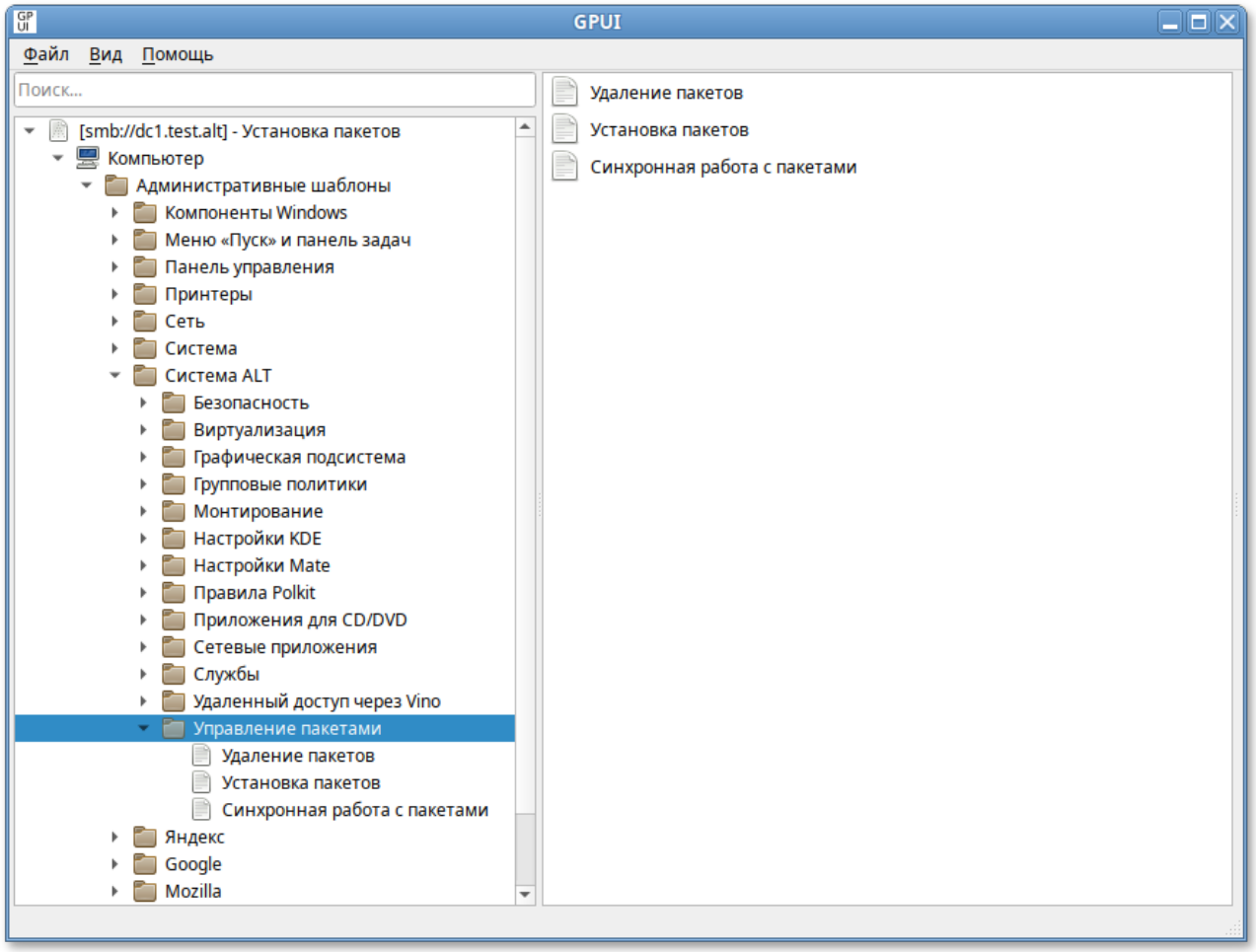
29.5.7. Управление пакетами

Эта групповая политика позволяет централизованно для компьютеров устанавливать и удалять пакеты.

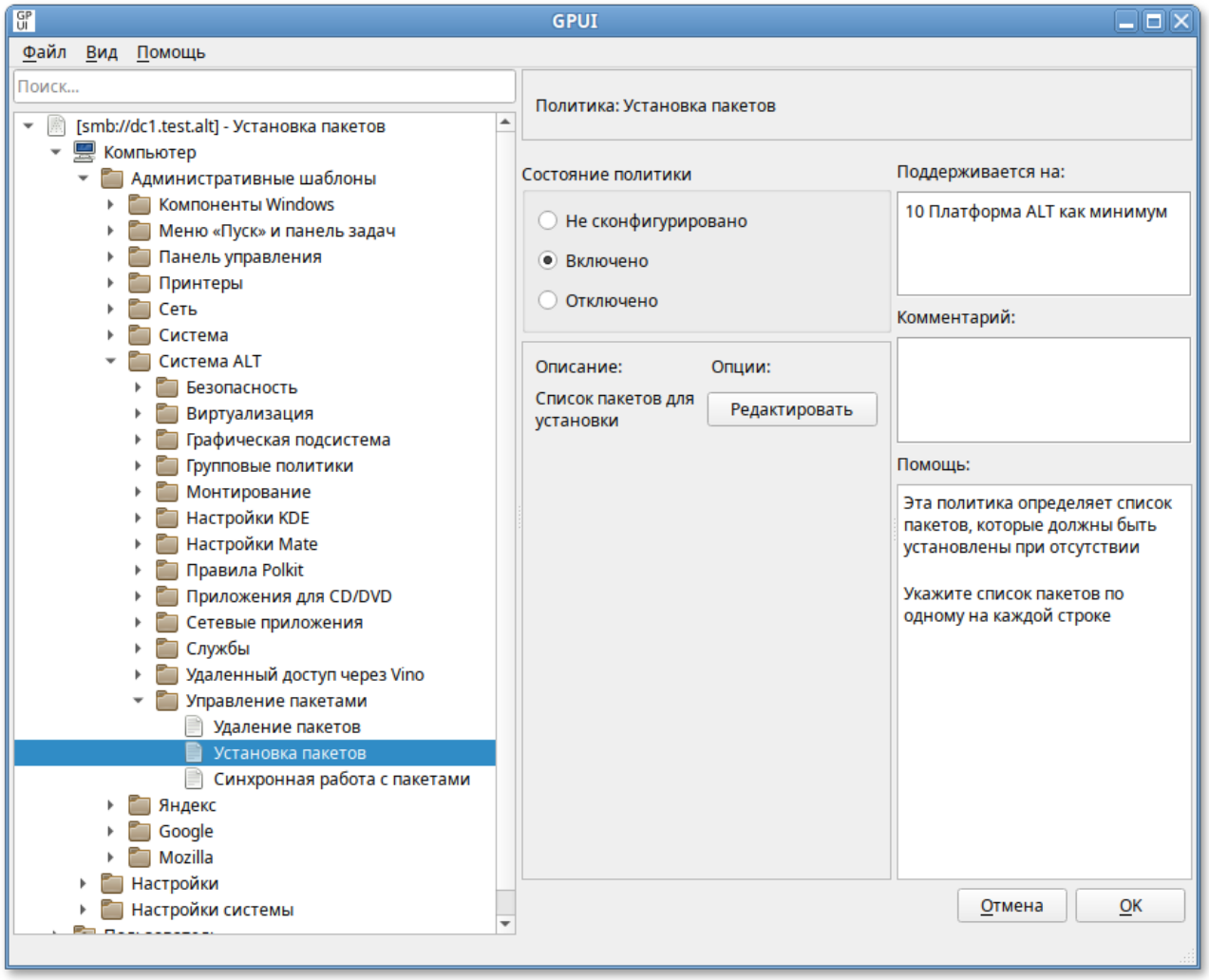
Примечание

Для возможности установки и удаления пакетов, на компьютерах, на которых будет применяться политика, должен быть установлен пакет *packagekit*.

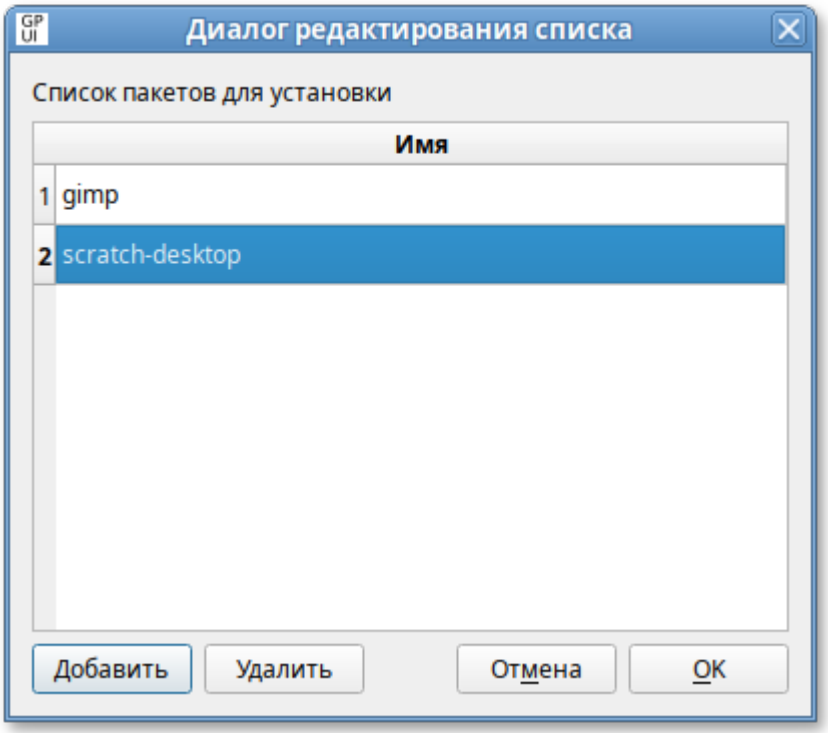
Для настройки политики следует перейти в **Компьютер/Пользователь → Административные шаблоны → Система ALT → Управление пакетами**. Выбрать раздел, в правом окне редактора отобразится список политик:



Для задания списка пакетов, которые необходимо установить, щелкнуть левой кнопкой мыши на политике **Установка пакетов**, откроется диалоговое окно настройки политики:



Для включения политики следует установить отметку в поле **Включено**. Для задания списка пакетов, которые должны быть установлены/удалены нажать кнопку **Редактировать** и в открывшемся окне ввести список пакетов, по одному на каждой строке:



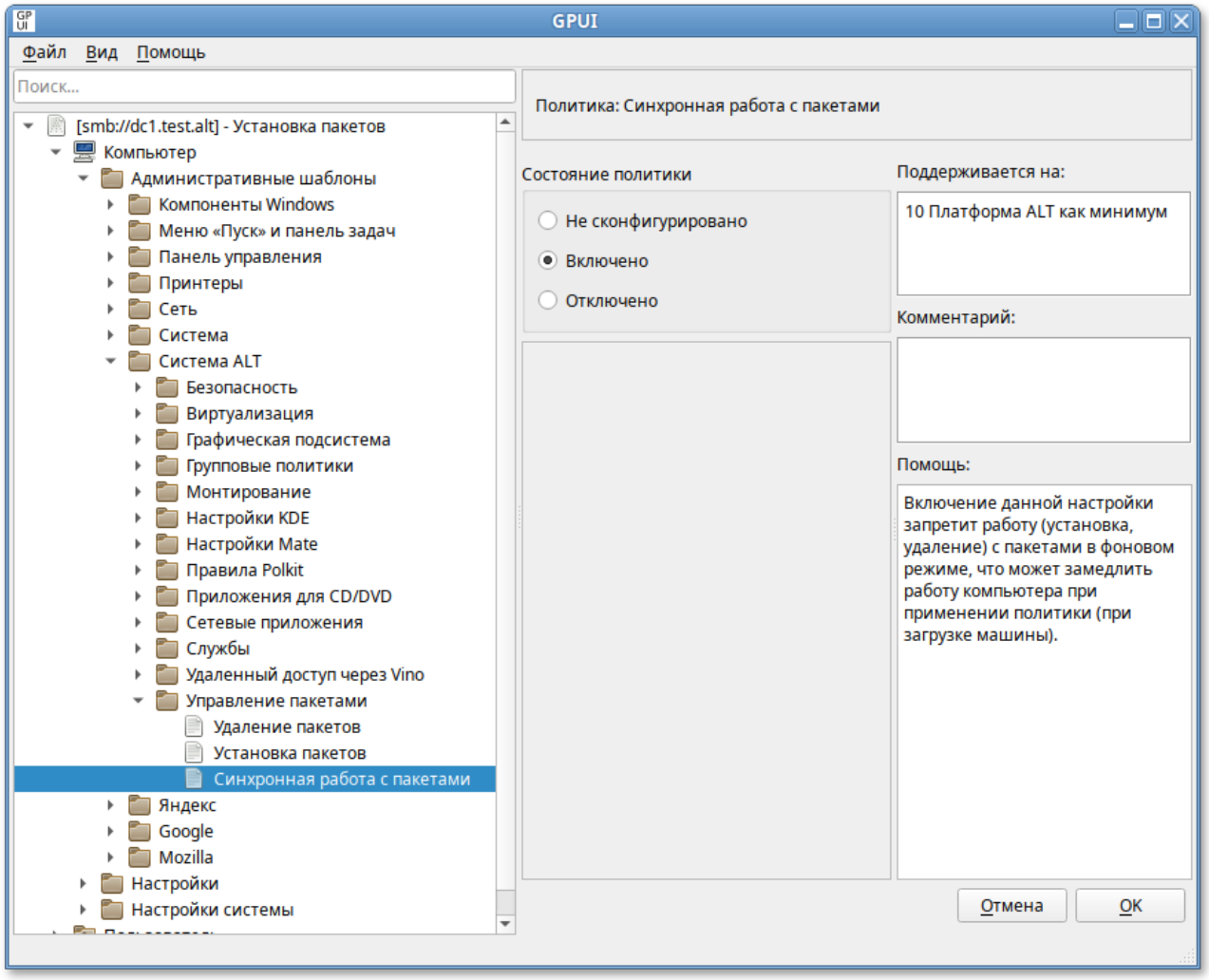
Для добавления/удаления строк можно воспользоваться соответствующими кнопками.

Примечание

Для задания списка пакетов, которые необходимо удалить, необходимо выбрать политику **Удаление пакетов**.

Можно также включить политику **Синхронная работа с пакетами**. Включение данной настройки запретит работу (установка, удаление) с пакетами в фоновом режиме, что может замедлить работу компьютера при применении политики (при загрузке машины, если политика машинная, или входе пользователя в систему, если политика пользовательская).

Для включения политики **Синхронная работа с пакетами** следует в разделе **Компьютер/ Пользователь → Административные шаблоны → Система ALT → Управление пакетами** выбрать пункт **Синхронная работа с пакетами**, в открывшемся окне установить отметку в поле **Включено** и нажать кнопку **OK**, для сохранения изменений:



Политики управления пакетами относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. раздел Экспериментальные групповые политики).

Все настройки политики управления пакетами хранятся в файлах **{GUID GPT}/Machine/Registry.pol** и **{GUID GPT}/User/Registry.pol**.

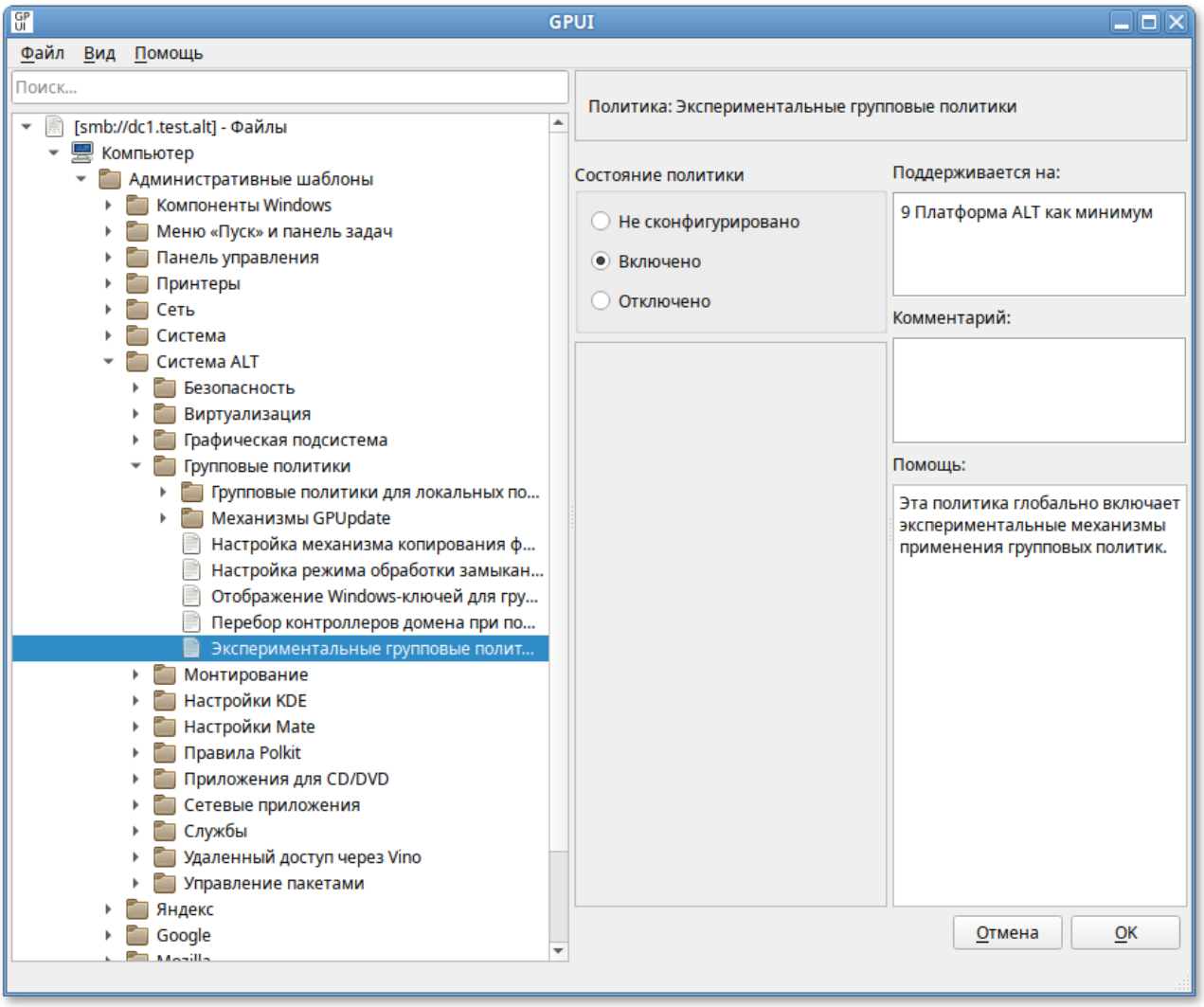
Пример файла **Registry.pol**:

```
PReg
[Software\BaseALT\Policies\GPUpdate;GlobalExperimental;;;]
[Software\BaseALT\Policies\Packages;Sync;;;]
[Software\BaseALT\Policies\Packages\Install;gimp;;;gimp]
[Software\BaseALT\Policies\Packages\Install;simple-scan;;;simple-scan]
[Software\BaseALT\Policies\Packages\Remove;python3-tools;;;python3-tools]
```

29.5.8. Экспериментальные групповые политики

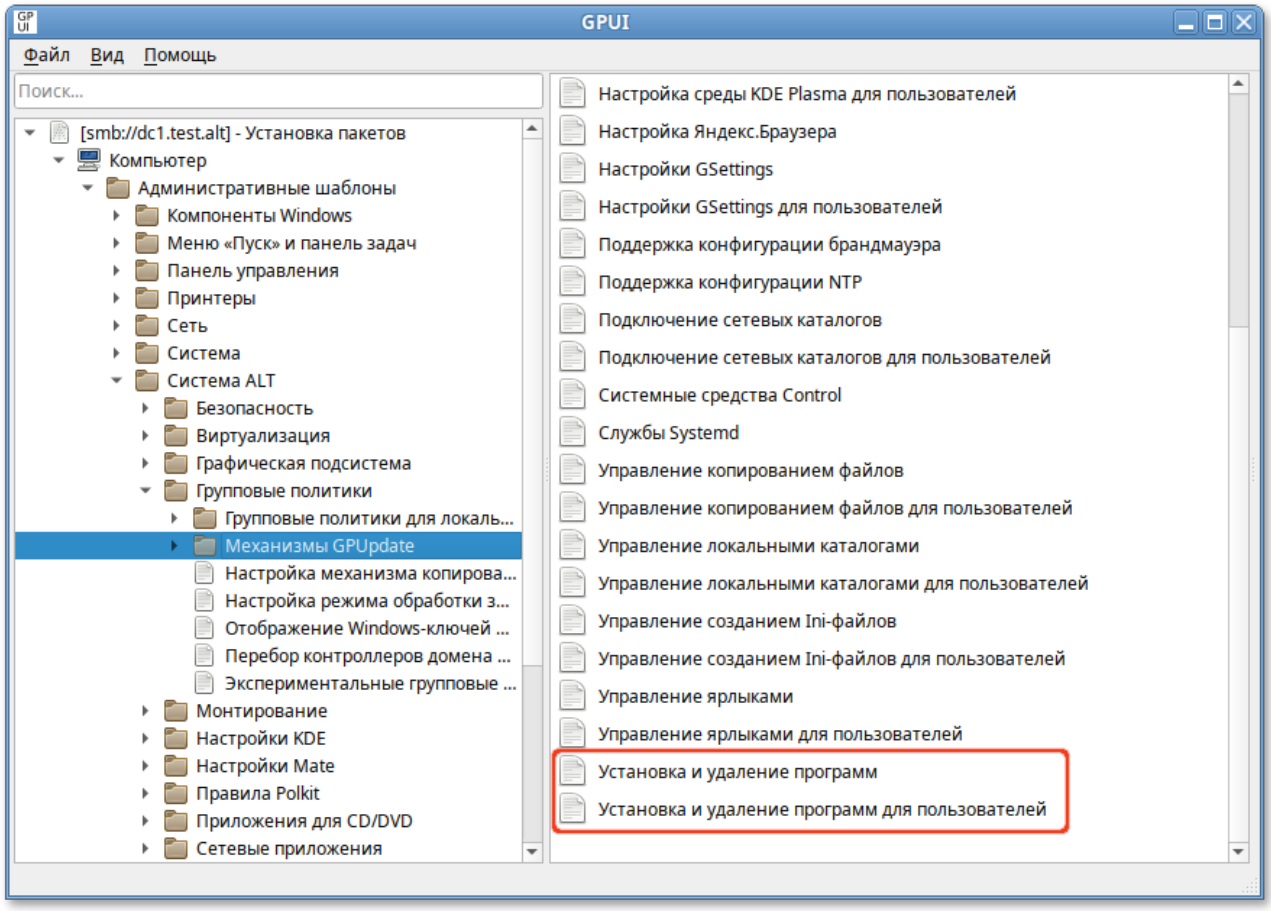
На тех машинах с ОС «Альт», где применяются экспериментальных политики, должны быть включены «Экспериментальные групповые политики».

Для включения экспериментальных групповых политик следует в разделе **Компьютер** → **Административные шаблоны** → **Система ALT** → **Групповые политики** выбрать пункт **Экспериментальные групповые политики** и установить в открывшемся окне отметку в поле **Включено**:



29.5.9. Механизмы GPUpdate

Каждый механизм применения групповых политик можно отдельно включить или отключить. Для этого следует включить/отключить соответствующую политику в разделе **Компьютер** → **Административные шаблоны** → **Система ALT** → **Групповые политики** → **Механизмы GPUpdate**. Например, включить/отключить механизм групповых политик управления пакетами (Packages) можно, включив/отключив политики **Установка и удаление программ** или **Установка и удаление программ для пользователей**:



29.5.10. Управление политиками браузера Chromium

Эти групповые политики позволяют централизованно управлять настройками интернет-браузера Google Chromium.

Механизм Chromium в составе пакета *gpupdate* формирует JSON-файл для браузера из шаблонов групповых политик. Во время запуска веб-браузер Google Chromium считывает файл **`/etc/chromium/policies/managed/policies.json`** и применяет параметры групповых политик. Групповые политики на основе **`policies.json`** предоставляют кроссплатформенную совместимость, что позволяет управлять браузерами в любом дистрибутиве Альт с установленным окружением рабочего стола.

Примечание

Для случаев, если требуется вести параллельно другой файл с конфигурациями, можно создать файл **`/etc/chromium/policies/managed/policies_local.json`** и вносить изменения в него. При коллизиях будет применена последняя прочитанная настройка.

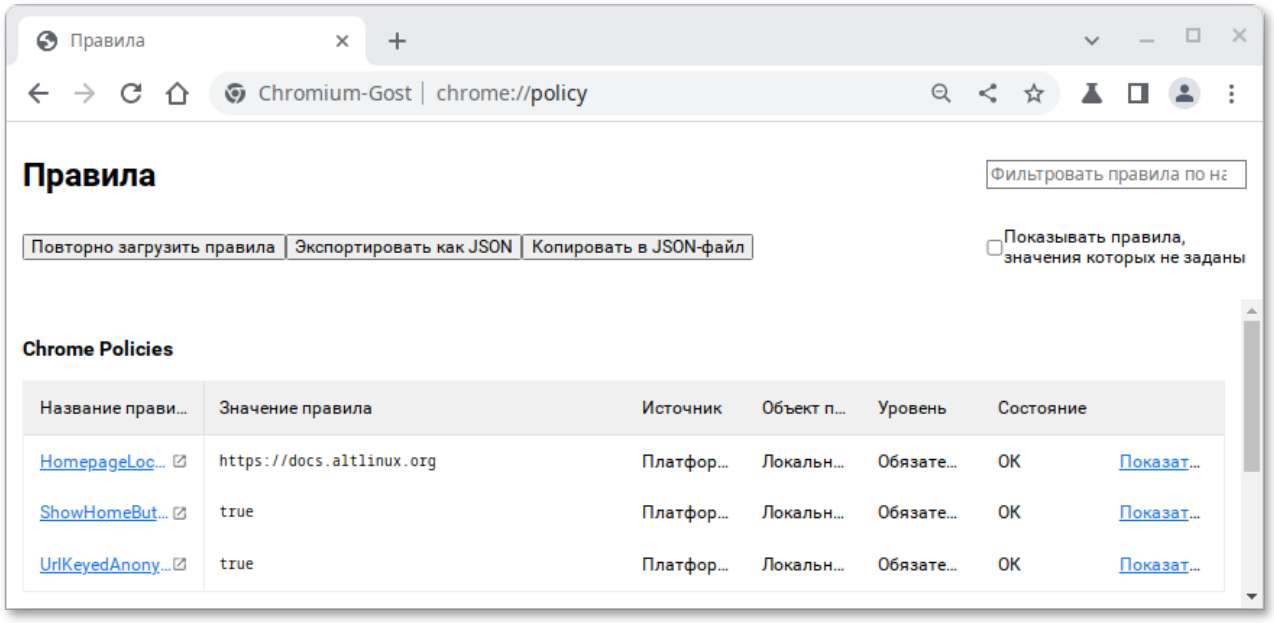
Примечание

Данный механизм реализован только для машинных политик.

Примечание

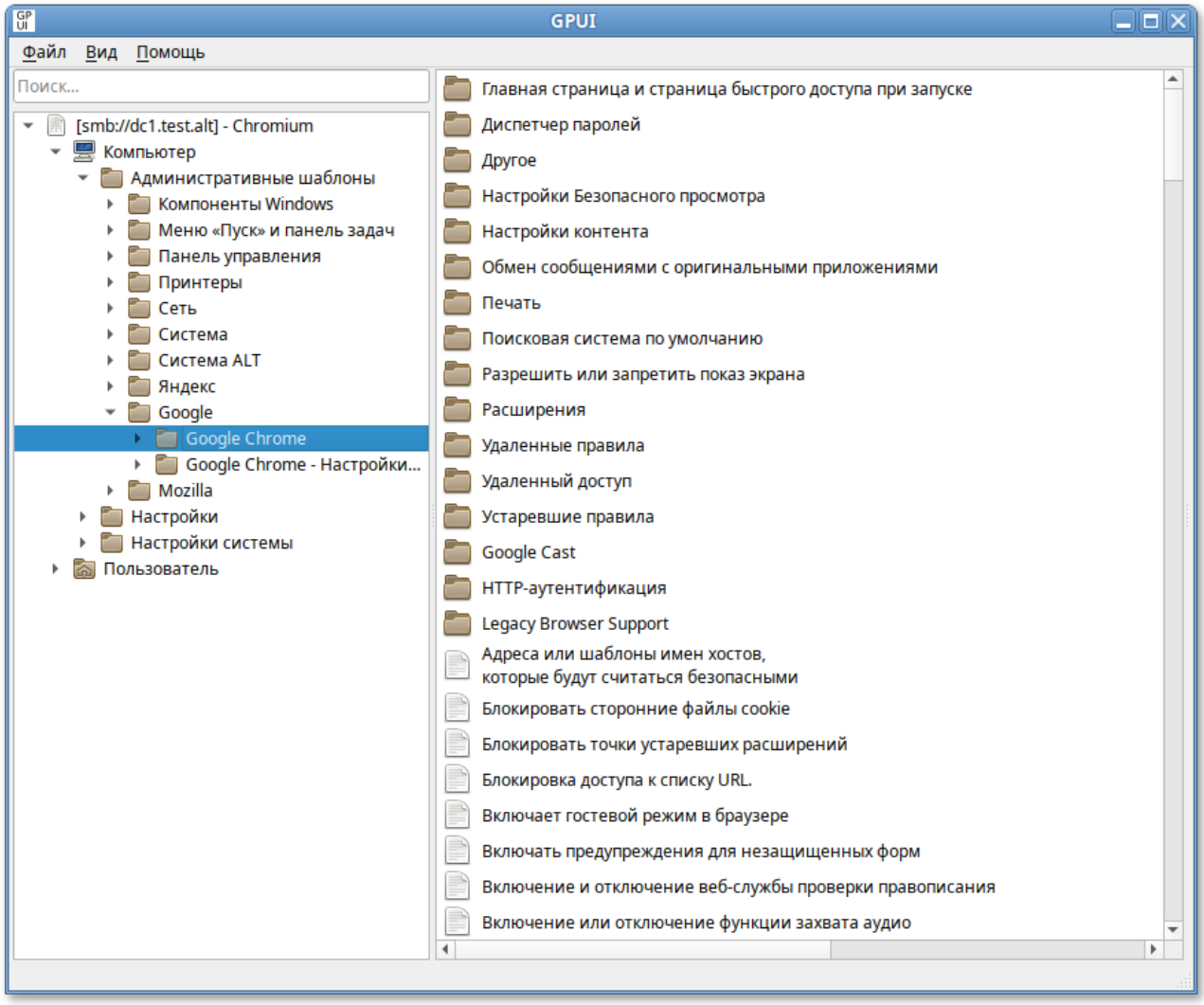
Настройка политик для браузера Chromium требует дополнительной установки ADMX-файлов Google Chrome (пакет *admx-chromium*).

Результат применения параметров групповой политики для Chromium можно проверить, указав в адресной строке URL: **`chrome://policy`**:

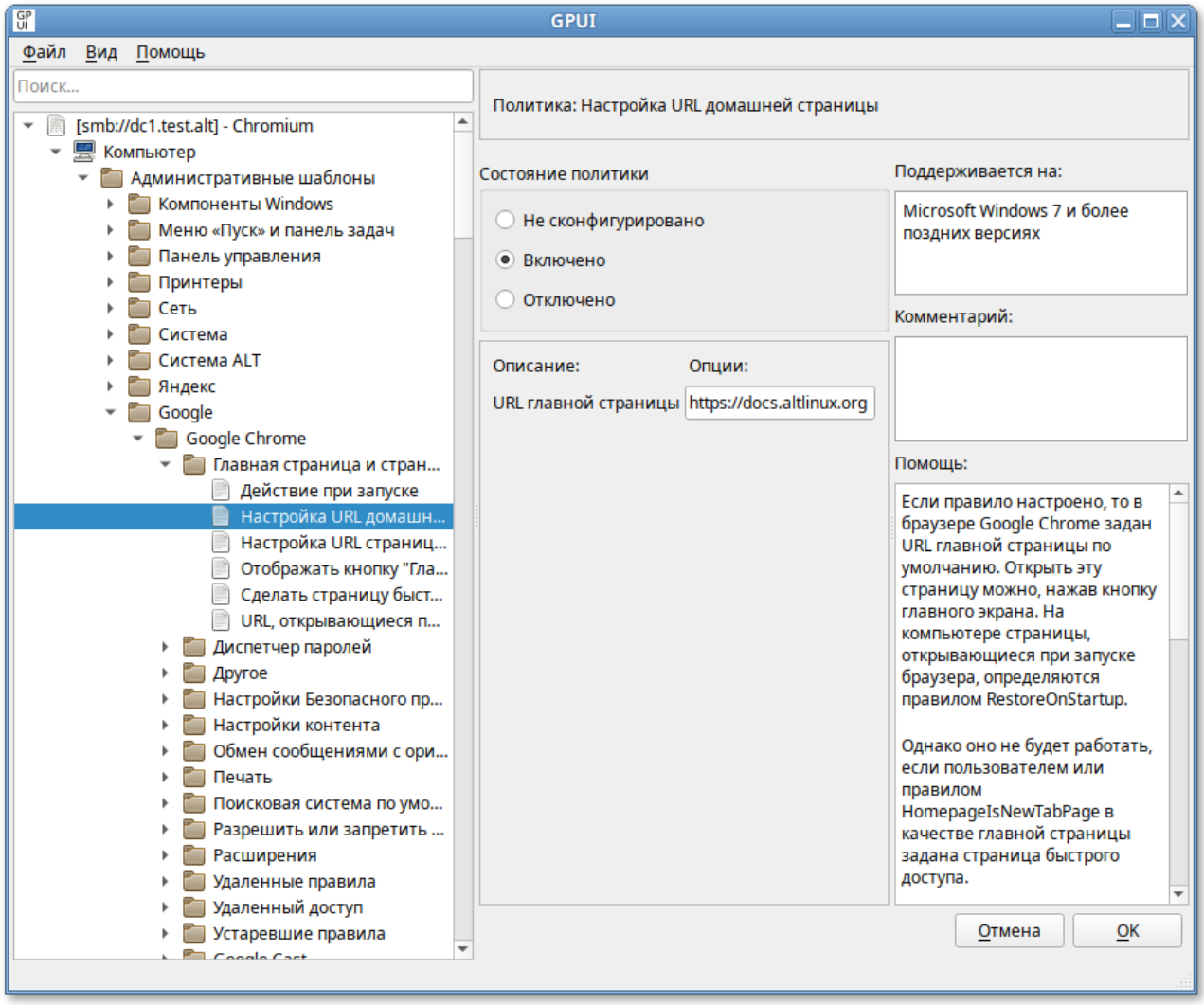


В качестве примера рассмотрим политику установки URL домашней страницы.

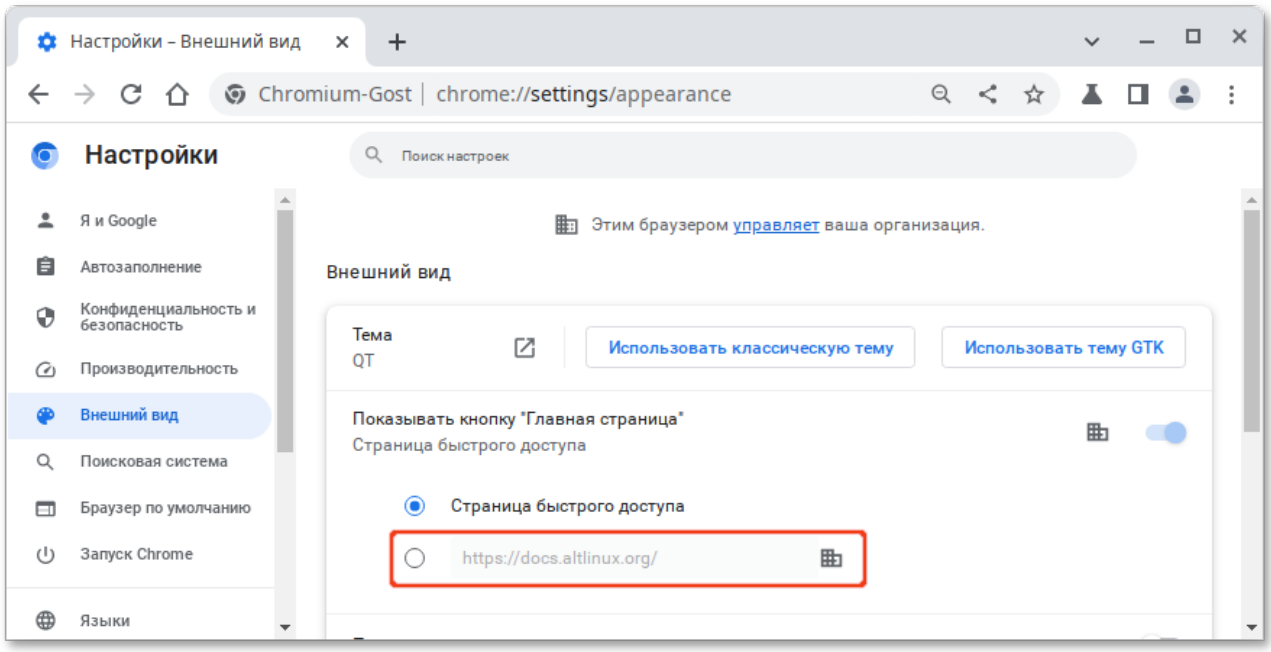
Для редактирования политик браузера Chromium следует перейти в **Компьютер** → **Административные шаблоны** → **Google** → **Google Chrome**. Отобразится список политик:



Для установки URL домашней страницы следует выбрать пункт **Главная страница и страница быстрого доступа при запуске**, щелкнуть левой кнопкой мыши на политике **Настройка URL домашней страницы**, откроется диалоговое окно настройки политики. Выбрать параметр **Включено**, в разделе **Параметры** ввести URL и нажать кнопку **ОК**:



Результат применения политики:



Все настройки политики браузера Chromium хранятся в файле **`{GUID GPT}/Machine/Registry.pol`**. Пример файла **`Registry.pol`**:

```
PReg[Software\Policies\Google\Chrome;HomepageLocation;;;https://
docs.altlinux.org]
```

В таблице Настройки веб-браузера Chromium описаны только некоторые политики. Полный список политик и их описание можно найти в браузере Chromium, указав в адресной строке URL: **chrome://policy** и установив отметку на пункте **Показывать правила, значения которых не заданы**.

Таблица 29.38. Настройки веб-браузера Chromium

Политика	Ключ	Описание
Действие при запуске	RestoreOnStartup	Настройка процесса запуска Chromium. При выборе значения **Восстановить последний сеанс** или «Открыть список URL и восстановить последний сеанс» будут отключены некоторые функции, такие как удаление данных о работе в браузере или сессионных файлов cookie при завершении работы. Если для политики указано значение **Открыть список URL и восстановить последний сеанс**, браузер будет восстанавливать предыдущий сеанс и открывать URL, заданные в политике **URL, открывающиеся при запуске**, в отдельном окне. Если пользователь не закроет страницы с этими URL, они также будут восстановлены в новом сеансе. Если политика находится в состоянии **Включено**, пользователи не смогут изменить эту настройку в Chromium.
Настройка URL домашней страницы	HomepageLocation	Позволяет установить URL домашней страницы и запрещает пользователям его изменять. Если политика находится в состоянии **Включено**, можно установить домашнюю страницу по умолчанию (открыть эту страницу в Chromium можно, нажав кнопку **Главная страница** на панели инструментов). Пользователи при этом не смогут изменить домашнюю страницу. Если политика находится в состоянии **Отключено**, пользователи не смогут установить домашнюю страницу. Если политика находится в состоянии **Не сконфигурировано**, пользователь может сам установить и изменить домашнюю страницу. Данная политика не будет работать, если пользователем или политикой «Сделать страницу быстрого доступа главной» в качестве главной страницы была задана страница быстрого доступа.
	NewTabPageLocation	Позволяет установить URL страницы быстрого доступа по умолчанию и запрещает пользователям его изменять.

Политика	Ключ	Описание
Настройка URL страницы быстрого доступа		Страница быстрого доступа появляется, когда пользователь открывает новую вкладку или окно. Политика не определяет, какие страницы открываются при запуске. Для этого применяется политика **Действие при запуске**. Но если страница быстрого доступа используется в качестве главной или стартовой страницы, эта политика также распространяется и на них. Если политика находится в состоянии **Не сконфигурировано** или URL не указан, используется страница быстрого доступа, установленная по умолчанию.
Отображать кнопку **Главная страница** на панели инструментов	ShowHomeButton	Позволяет управлять отображением кнопки **Главная страница** на панели инструментов. Если политика находится в состоянии **Включено**, кнопка **Главная страница** отображается на панели инструментов. Если политика находится в состоянии **Отключено**, кнопка **Главная страница** не будет отображаться. Если эта политика настроена, пользователи не смогут изменить эту настройку в Chromium. В противном случае пользователи смогут добавить или скрыть кнопку главного экрана.
Сделать страницу быстрого доступа главной	HomepageIsNewTabPage	Если политика находится в состоянии **Включено**, в качестве главной страницы используется страница быстрого доступа. Заданный URL главной страницы игнорируется. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, страница быстрого доступа открывается, только когда в качестве URL главной страницы указан путь **chrome://newtab**. Если эта политика настроена, пользователи не смогут изменить главную страницу в Chromium. Если политика не сконфигурирована, пользователи смогут выбрать, устанавливать ли страницу быстрого доступа в качестве главной.
URL, открывающиеся при запуске	RestoreOnStartupURLs	Если для политики **Действие при запуске** задано значение **Открыть одну или несколько страниц**, в данной политике можно настроить список URL-адресов. В противном случае при запуске будет открываться страница быстрого доступа.
	PasswordManagerEnabled	

Политика	Ключ	Описание
Включить сохранение паролей		Если политика находится в состоянии **Включено** или **Не сконфигурировано**, Chromium будет предлагать запоминать введенные пароли (а также предлагать их при следующем входе). Если политика находится в состоянии **Отключено**, пользователям будут доступны только ранее сохраненные пароли, а сохранить новые будет нельзя. Если политика настроена, пользователи не могут изменить её в Chromium. В противном случае пользователи при желании смогут отключить функцию сохранения паролей.
Включить поисковую систему по умолчанию	DefaultSearchProviderEnabled	Если политика находится в состоянии **Включено**, то при вводе в адресную строку текста (не URL) будет выполняться поиск в используемой по умолчанию поисковой системе. Задать поисковую систему по умолчанию можно с помощью других политик. Если значения для этих политик не установлены, пользователь может сам выбрать поисковую систему по умолчанию. Если политика находится в состоянии **Отключено**, то поиск текста, введенного в адресную строку, не выполняется.
Название поисковой системы по умолчанию	DefaultSearchProviderName	Если политика **Включить поисковую систему по умолчанию** включена, то данная политика задает название поисковой системы по умолчанию. Если параметр **Включить поисковую систему по умолчанию** не задан, то используется имя хоста, указанное в URL поискового запроса.
Показ URL страницы быстрого доступа в поисковой системе по умолчанию	DefaultSearchProviderNewTabURL	Если политика **Включить поисковую систему по умолчанию** включена, то данная политика указывает URL поисковой системы, используемой для страницы быстрого доступа. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, страница быстрого доступа не будет использоваться.
URL поиска для поисковой системы по умолчанию	DefaultSearchProviderSearchURL	Если политика **Включить поисковую систему по умолчанию** включена, то данная политика содержит URL поисковой системы, используемой по умолчанию. В URL должна быть строка '{searchTerms}', которая во время отправки запроса заменяется на текст пользователя.

Политика	Ключ	Описание
		URL поисковой системы Google можно указать так: '{google:baseURL}search?q={searchTerms}&{google:RLZ} {google:originalQueryForSuggestion} {google:assistedQueryStats} {google:searchFieldtrialParameter} {google:searchClient} {google:sourceId}ie={inputEncoding}'. URL поисковой системы Яндекс можно указать так: https://yandex.ru/search/?text={searchTerms}
Включить панель закладок	BookmarkBarEnabled	Если политика находится в состоянии **Включено**, в Chromium будет видна панель закладок. Если политика находится в состоянии **Отключено**, панель закладок будет всегда скрыта. Если эта политика настроена, пользователи не смогут её изменить. Если политика находится в состоянии **Не сконфигурировано**, пользователи смогут самостоятельно решать, использовать эту функцию или нет.
Разрешить пользователям менять фон на странице быстрого доступа	NTPCustomBackgroundEnabled	Если политика находится в состоянии **Отключено**, пользователи не смогут изменять фон страницы быстрого доступа. Уже используемые изображения удаляются без возможности восстановления. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, пользователи могут изменять фон страницы быстрого доступа.
Блокировать изображения на этих сайтах	ImagesBlockedForUrls	Позволяет задать список шаблонов URL для указания сайтов (значение * не поддерживается для этой политики), на которых запрещен показ изображений. Если политика находится в состоянии **Включено**, Chromium будет блокировать изображения на указанных сайтах. Если политика находится в состоянии **Не сконфигурировано**, то действует политика **Настройка изображений по умолчанию**) при условии, что оно задано. В противном случае применяются персональные настройки пользователя.
Блокировка доступа к списку URL	URLBlocklist	Если политика находится в состоянии **Включено**, страницы с запрещенными URL не загружаются (задаются шаблоны запрещенных URL). Если политика находится в состоянии **Не сконфигурировано**, браузер не блокирует URL.

Политика	Ключ	Описание
		Формат шаблона URL должен соответствовать требованиям, указанным на странице **https://www.chromium.org/administrators/url-blocklist-filter-format**. В политике URLAllowlist можно задавать не более 1000 исключений.
Всегда открывать PDF-файлы во внешнем приложении	AlwaysOpenPdfExternally	Если политика находится в состоянии **Включено**, встроенное средство просмотра PDF-файлов в Chromium отключается, они начинают обрабатываться как скачанный контент, а пользователю разрешается открывать их в приложении, установленном по умолчанию. Если политика находится в состоянии **Отключено**, для просмотра PDF-файлов будет использоваться плагин PDF (если он не отключен пользователем). Если политика находится в состоянии **Не сконфигурировано**, пользователи смогут настраивать этот параметр самостоятельно.
Всегда указывать место для скачивания	PromptForDownloadLocation	Если политика находится в состоянии **Включено**, то при скачивании каждого файла пользователь должен указать, в какой каталог его сохранить. Если политика находится в состоянии **Отключено**, скачивание выполняется без запроса каталога для сохранения. Если политика находится в состоянии **Не сконфигурировано**, пользователи могут выбрать каталог, в который всегда будут сохраняться файлы.
Выбор каталога для скачиваний	DownloadDirectory	В этой политике указывается каталог, в котором браузер Chromium сохраняет скачиваемые файлы. Данный каталог используется, даже если пользователь выбрал каталог для сохранения или установил флажок, позволяющий выбирать каталог при каждом скачивании файла. Эта политика отменяет действие политики DefaultDownloadDirectory. Если политика находится в состоянии **Не сконфигурировано**, браузер Chromium скачивает файлы в каталог по умолчанию, а пользователь может его изменить. Список переменных можно посмотреть на странице **https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables**.

Политика	Ключ	Описание
Доступ к поисковой системе по умолчанию в контекстном меню	DefaultSearchProviderContextMenuAccessAllowed	Позволяет использовать поисковую систему по умолчанию в контекстном меню. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, поиск в системе по умолчанию будет доступен в контекстном меню. Если политика находится в состоянии **Отключено**, поиск будет недоступен в контекстном меню. Значение этой политики применяется только в том случае, если включена политика **Включить поисковую систему по умолчанию**.
Доступность режима инкогнито	IncognitoModeAvailability	Определяет, может ли пользователь просматривать страницы в Chromium в режиме инкогнито. Если политика находится в состоянии **Включено** или значение не задано, страницы можно открывать в режиме инкогнито. Если политика находится в состоянии **Отключено**, пользователи не смогут открывать страницы в режиме инкогнито. Если для политики выбрано значение **Включить принудительно**, страницы можно просматривать ТОЛЬКО в режиме инкогнито.
Удаление истории просмотров и загрузок браузера	AllowDeletingBrowserHistory	Определяет, может ли пользователь удалять историю просмотров и скачиваний. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, то историю просмотров и скачиваний можно удалить. Если политика находится в состоянии **Отключено**, то историю просмотров и скачиваний удалить нельзя.
Разрешить вызов окна выбора файлов	AllowFileSelectionDialogs	Если политика находится в состоянии **Включено** или **Не сконфигурировано**, то пользователи смогут открывать в Chromium окна выбора файлов. Если политика находится в состоянии **Отключено**, и пользователь выполняет действия, для которых нужно открыть окно выбора файлов (например, импортирует закладки, загружает файлы, сохраняет ссылки и т.д.), вместо окна отображается сообщение и предполагается, что пользователь нажал кнопку **Отмена** в окне выбора файлов.
Включить поисковые подсказки	SearchSuggestEnabled	Если политика находится в состоянии **Включено**, в адресной строке Chromium при поиске будут появляться подсказки.

Политика	Ключ	Описание
		Если политика находится в состоянии **Отключено**, поисковые подсказки не отображаются. Эта политика не влияет на показ в строке поиска закладок и страниц из истории просмотров. Если политика настроена, пользователи не могут изменить её. Если политика не сконфигурирована, подсказки при поиске будут включены, но пользователи смогут отключить их в любое время.
Настройка изображений по умолчанию	DefaultImagesSetting	Если политика находится в состоянии **Включено** и выбрано значение 1 — **Разрешить показ изображений на всех сайтах**, на всех сайтах могут показываться изображения. При значении 2 — **Запретить показ изображений на всех сайтах**, показ изображений на сайтах запрещен. Если политика находится в состоянии **Не сконфигурировано**, показ изображений разрешен, но пользователи могут изменять этот параметр.
Разрешить полноэкранный режим	FullscreenAllowed	Если политика находится в состоянии **Включено** или **Не сконфигурировано**, то при наличии необходимых разрешений пользователи, приложения и расширения смогут включать полноэкранный режим, в котором виден только контент веб-страниц. Если политика находится в состоянии **Отключено**, то полноэкранный режим будет заблокирован для всех пользователей, приложений и расширений.
Управляемые закладки	ManagedBookmarks	Политика позволяет установить список закладок в Chromium. Если политика настроена, будет создан список закладок Каждая закладка представляет собой словарь, где ключам name и url соответствуют значения — название закладки и URL-адрес сайта ([{"name": "Документация","url": "docs.altlinux.org"},{"name": "Wiki","url": "altlinux.org"}]). По умолчанию папка называется «Управляемые закладки». Чтобы изменить это название, необходимо добавить в правило дополнительный словарь с единственным ключом **toplevel_name** и названием папки в качестве значения. Можно также задать подпапку для закладок. Для этого вместо ключа **url** следует использовать ключ **children**, а в качестве его значения указать список вложенных закладок или папок

Политика	Ключ	Описание
		([{"toplevel_name":"ALT"}, {"name":"BaseALT","url":"basealt.ru"}, {"name":"ALT docs","children":[{"name": "Документация","url": "docs.altlinux.org"}, {"name": "Wiki","url": "altlinux.org"}]}]). Chromium дополняет неполные URL так же, как при их вводе в адресной строке. Например, адрес altlinux.org будет преобразован в **`https://altlinux.org/`**. Пользователи не смогут изменять папки с закладками, а только скрывать их на панели. Управляемые закладки не синхронизируются с аккаунтом пользователя, а расширения не могут их изменять.
Включить анонимный сбор данных о URL	UrlKeyedAnonymizedDataCollectionEnabled	Если политика находится в состоянии **`Включено`**, то всегда выполняется анонимный сбор данных о URL (эти сведения отправляются в Google с целью улучшить поиск и просмотр веб-страниц). Если политика находится в состоянии **`Отключено`**, сбор данных о URL не выполняется. Если политика находится в состоянии **`Не сконфигурировано`**, пользователь может разрешить или запретить анонимный сбор данных о URL.
Удаление данных о работе в браузере при выходе	ClearBrowsingDataOnExitList	Политика позволяет настроить список данных о работе в браузере, которые должны удаляться, когда пользователь закрывает все окна браузера. Можно указать следующие типы данных: - browsing_history (история браузера) - download_history (история скачиваний) - cookies_and_other_site_data (файлы cookie и другие данные сайтов) - cached_images_and_files (изображения и другие файлы, сохраненные в кеше) - password_signin (пароли) - autofill (автозаполнение) - site_settings (настройки сайтов) - hosted_app_data (данные размещенных приложений) У этой политики нет приоритета над политикой **`Удаление истории просмотров и загрузок браузера`**. Эта политика работает, если политика **`Отключить синхронизацию данных с Google`** находится в состоянии **`Включено`**. В противном случае политика игнорируется. Если Chromium закрывается непредвиденно (например, из-за сбоя в работе браузера или ОС), данные о работе в браузере удаляются при следующей загрузке профиля.

Политика	Ключ	Описание
		Если политика находится в состоянии **Отключено**, то данные о работе, при закрытии браузера, не удаляются.
Отключить синхронизацию данных с Google	SyncDisabled	Если политика находится в состоянии **Включено**, синхронизация данных в Chromium с помощью сервисов, размещенных в Google, отключается. Полностью отключить сервис «Chrome Sync» можно через Google Admin console. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут самостоятельно решать, использовать ли им сервис «Chrome Sync».
Включает гостевой режим в браузере	BrowserGuestModeEnabled	Если политика находится в состоянии **Включено** или **Не сконфигурировано**, разрешается использовать гостевой доступ. При гостевом доступе все окна для профилей Chromium открываются в режиме инкогнито. При гостевом доступе все окна для профилей Chromium открываются в режиме инкогнито. Если политика находится в состоянии **Отключено**, в браузере не разрешается использовать гостевые профили.
Задать объем кеша в байтах	DiskCacheSize	Если для политики задано значение **None**, Chromium использует объем кеша по умолчанию для хранения кешированных файлов на диске. В этом случае пользователи не могут изменить правило. Если политика находится в состоянии **Включено** Chromium будет использовать указанный размер кеша независимо от того, указали ли пользователи значение экспериментального параметра **--disk-cache-size**. Объем кеша задается в байтах, например, чтобы задать размер кеша 300МБ, необходимо указать 314572800. Значения меньше нескольких мегабайтов округляются. Если политика находится в состоянии **Не сконфигурировано**, Chromium использует объем по умолчанию. В этом случае пользователи могут менять размер кеша с помощью экспериментального параметра **--disk-cache-size**. Указанное в правиле значение используется различными подсистемами в браузере как справочное. Поэтому фактический объем используемого дискового пространства может превышать указанное значение, но будет иметь такой же порядок.

Политика	Ключ	Описание
Список разрешенных серверов для аутентификации	AuthServerAllowlist	Это правило указывает, какие серверы можно использовать для встроенной проверки подлинности Windows (IWA). Встроенная проверка подлинности включается, только когда Chromium получает запрос на аутентификацию от прокси-сервера или от сервера из списка разрешенных. Если политика находится в состоянии **`Не сконфигурировано`**, Chromium отвечает на запросы IWA только после того, как определяет, находится ли сервер в интранете. Если сервер находится в Интернете, Chromium игнорирует поступающие от него IWA запросы (веб-сайту не разрешается использовать аутентификацию SPNEGO с помощью браузера). Названия серверов нужно разделять запятыми. Допустимы подстановочные знаки (*).

Управление расширениями (Позволяет управлять расширениями)	ExtensionSettings	Это правило контролирует настройки управления расширениями в Chromium, включая те, которые заданы другими правилами. Оно заменяет любые ранее действовавшие правила.
		
		Если политика находится в состоянии **`Отключено`** или **`Не сконфигурировано`**, пользователи могут самостоятельно настраивать расширения.
		
		Если политика находится в состоянии **`Включено`**, настройки расширений задает администратор с помощью кода, указанного в параметрах политики:
		
		▸идентификатор расширения или URL обновления привязывается только к одной конкретной настройке;
		▸идентификатор ***** действует на все расширения, для которых в политике не задана отдельная конфигурация;
		▸если указан URL обновления, заданная конфигурация применяется ко всем расширениям, в манифесте которых приведен этот URL.
		
		Пример значения:
		
		`{`
		`  "hdokiejnpimakedhajhdlcegeplioahd": {`
		`    "installation_mode": "force_installed",`
		`    "update_url": "https://clients2.google.com/service/update2/crx"`
		`  },`
		`  "pioclpoplcdbaefihamjohnefbikjilc": {`
		`    "installation_mode": "force_installed",`

Политика	Ключ	Описание

```
    "update_url": "https://clients2.google.com/
service/update2/crx"
  }
}
```

Параметры политики:

- **`allowed_types`** — типы приложений и расширений, которые пользователям разрешено устанавливать в браузере (допустимые строки: «extension», «hosted_app», «legacy_packaged_app», «tplatform_appeme», «theme», «user_script»). Используется только для настройки конфигурации по умолчанию со значением *****;
- **`blocked_install_message`** — уведомление (не более 1000 символов), которое будет появляться на устройствах пользователей при попытке установить запрещенные расширения;
- **`blocked_permissions`** — запрещает пользователям устанавливать и запускать расширения, требующие разрешений API (список доступных разрешений указан в манифесте расширения);
- **`installation_mode`** — указывает, разрешено ли добавлять заданные расширения. Допустимые режимы:
  - **`allowed`** — пользователи могут установить это расширение (поведение по умолчанию);
  - **`blocked`** — пользователи не могут установить это расширение;
  - **`removed`** — пользователи не могут установить это расширение. Если расширение было установлено, оно будет удалено;
  - **`force_installed`** — расширение устанавливается автоматически. Пользователи не могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр **`update_url`**);
  - **`normal_Installed`** — расширение устанавливается автоматически. Пользователи могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр **`update_url`**);

- **`install_sources`** — список URL страниц, с которых разрешено загружать и устанавливать расширения Необходимо разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода);

Политика	Ключ	Описание
		▪ **minimum_version_required** — отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; ▪ **update_url** — определяет, откуда загружается расширение. Можно указать URL интернет-магазина Chrome, Opera или использовать XML-файл: ▪ если расширение размещено в интернет-магазине Chrome, следует указать **https://clients2.google.com/service/update2/crx** ▪ если расширение размещено в интернет-магазине Opera, следует указать **https://extension-updates.opera.com/api/omaha/update/** ▪ **override_update_url** — указывает, что для всех последующих обновлений расширения будет использоваться URL из поля **update_url** или **update** в политике **ExtensionInstallForcelist**. Если эта политика не сконфигурирована или отключена, будет использоваться URL из манифеста расширения; ▪ **verified_contents_url** — указывает путь до файла **extension.verified_contents**. С его помощью расширение проверяется на доверие (используется, если нет доступа в интернет); ▪ **runtime_allowed_hosts** — разрешает взаимодействие расширений с указанными сайтами, даже если они указаны в поле **runtime_blocked_hosts**. Можно указать до 100 сайтов; ▪ **runtime_blocked_hosts** — запрещает расширениям взаимодействовать с указанными сайтами или изменять их, в том числе вставлять скрипты, получать доступ к файлам cookie и изменять веб-запросы. Можно указать до 100 сайтов; ▪ **toolbar_pin** — определяет, закреплен ли значок расширения на панели инструментов. Возможные значения: ▪ **force_pinned** — значок расширения закреплен на панели инструментов и постоянно виден Пользователь не может скрыть его в меню расширения; ▪ **default_unpinned** — расширение скрыто в меню расширений (по умолчанию), пользователь может закрепить его на панели инструментов.

29.5.11. Управление политиками браузера Firefox

Эти групповые политики позволяют централизованно управлять настройками интернет-браузера Mozilla Firefox.

Механизм Firefox в составе пакета *gpupdate* формирует JSON-файл для браузера из шаблонов групповых политик. Во время запуска веб-браузер Mozilla Firefox считывает собственный файл **policies.json** и применяет параметры групповых политик. Групповые политики на основе **policies.json** предоставляют кроссплатформенную совместимость, что позволяет управлять браузерами в любом дистрибутиве Альт с установленным окружением рабочего стола.

Путь к файлу **policies.json** в зависимости от версии веб-браузера Firefox:

- **/etc/firefox/policies** — новые версии;
- **/usr/lib64/firefox/distribution** — старые версии.

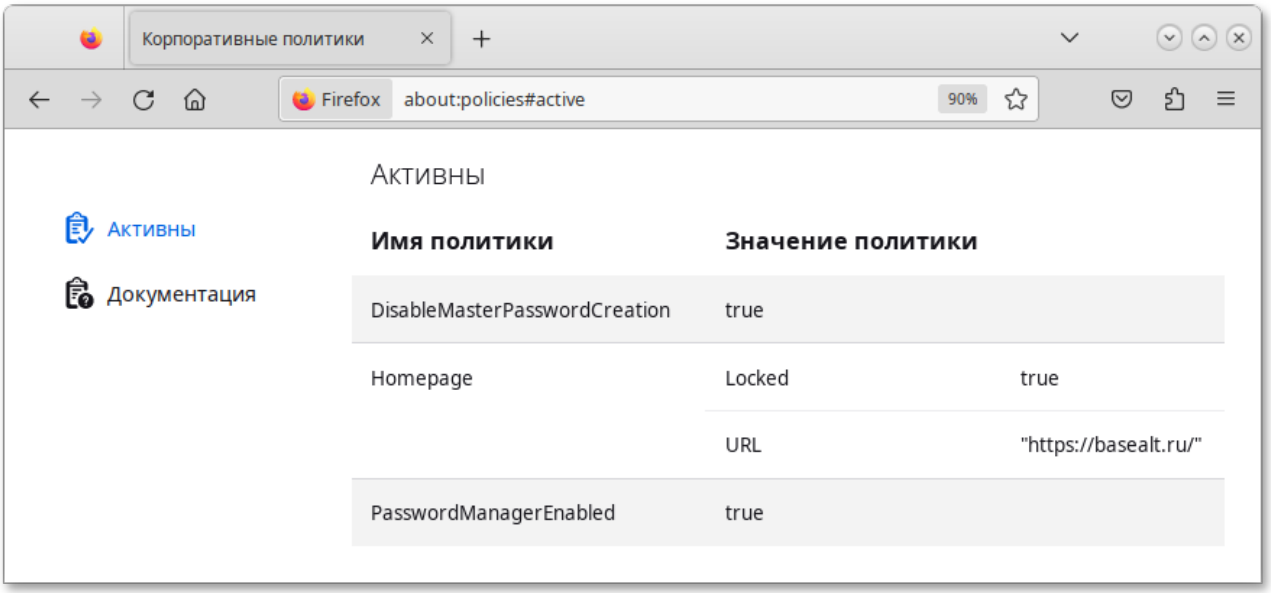
Примечание

Данный механизм реализован только для машинных политик.

Примечание

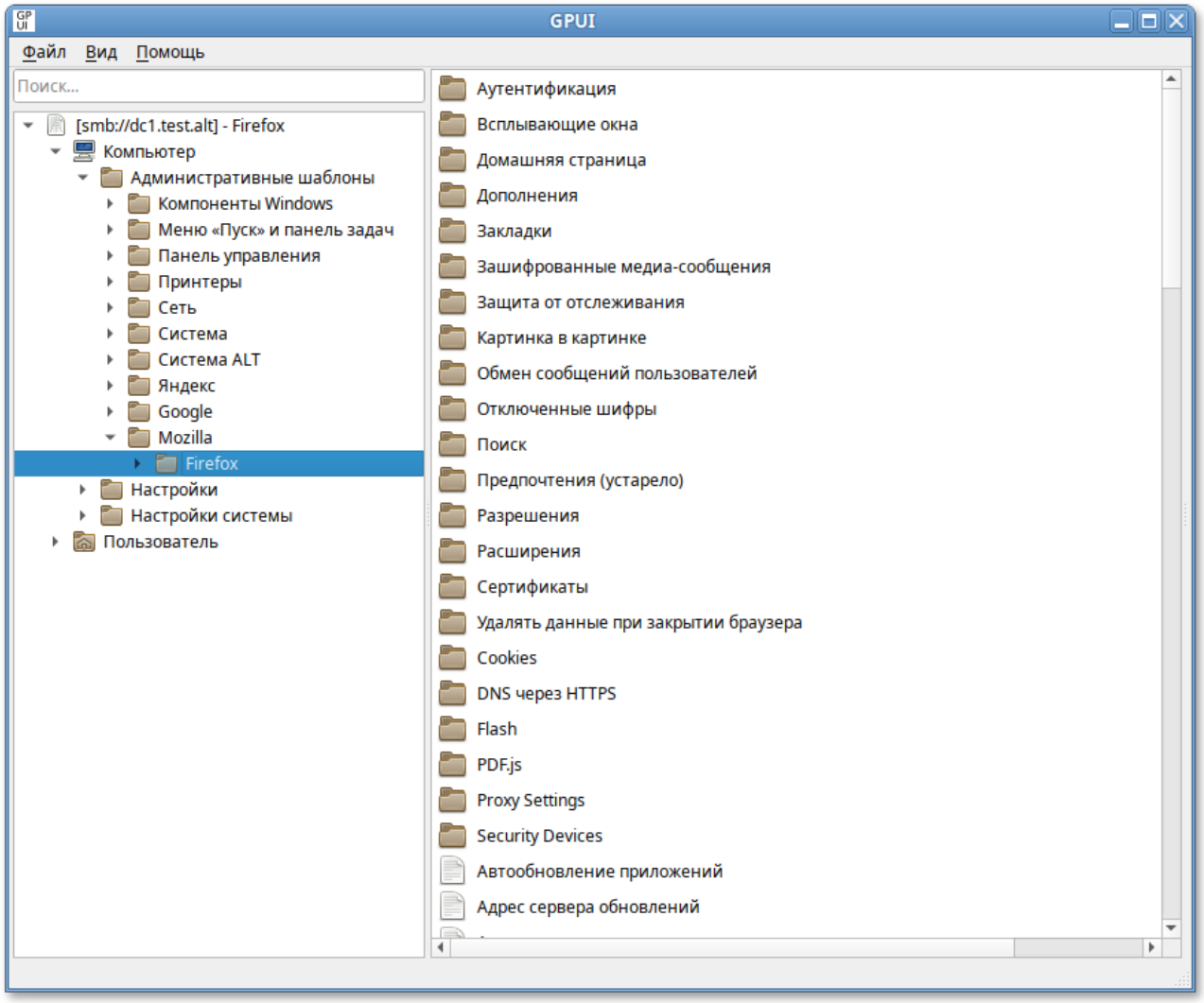
Настройка политик для браузера Mozilla Firefox требует дополнительной установки ADMX-файлов Firefox (пакет *admx-firefox*).

Результат применения параметров групповой политики для Mozilla Firefox можно проверить, указав в адресной строке URL: **about:policies#active**:

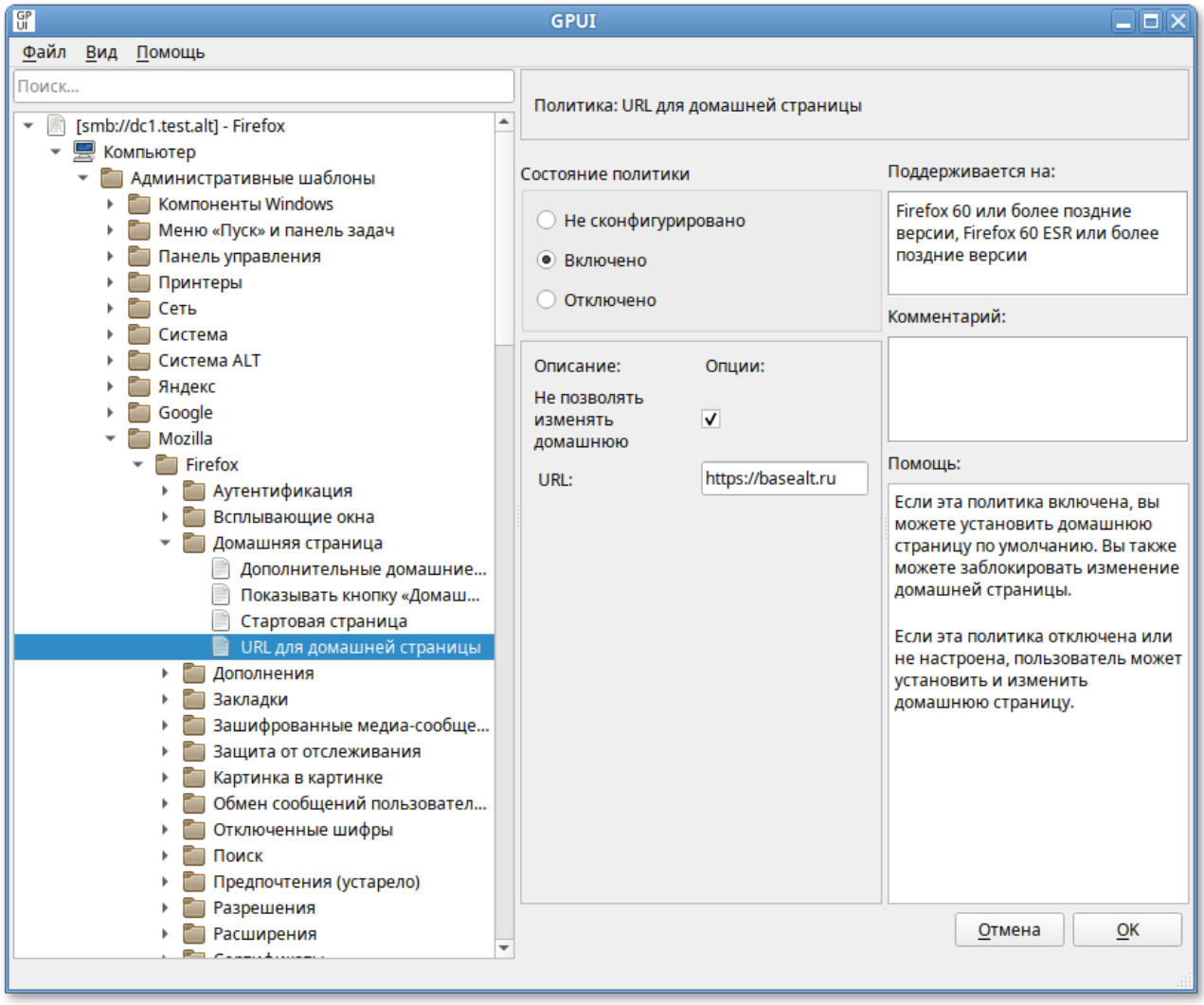


В качестве примера рассмотрим политику установки URL домашней страницы.

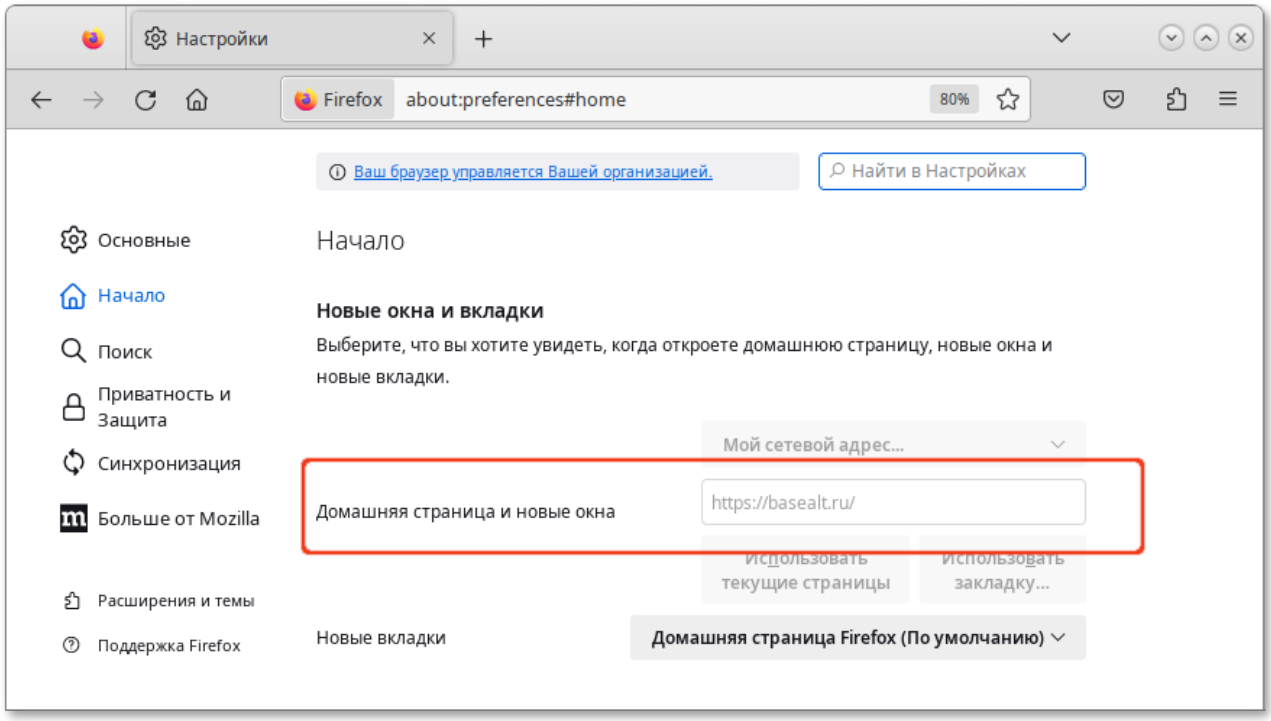
Для редактирования политик браузера Mozilla Firefox следует перейти в **Компьютер** → **Административные шаблоны** → **Mozilla** → **Firefox**:



Раскрыть группу **Домашняя страница**, щелкнуть левой кнопкой мыши на политике **URL для домашней страницы**, откроется диалоговое окно настройки политики. Выбрать параметр **Включено**, в разделе **Параметры** ввести URL и нажать кнопку **ОК**:



В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем:



Все настройки политики веб-браузера Firefox хранятся в файле **{GUID GPT}/Machine/Registry.pol**. Пример файла **Registry.pol**:

```
PReg[Software\Policies\Mozilla\Firefox\Homepage;URL;;;https://basealt.ru]
[Software\Policies\Mozilla\Firefox\Homepage;Locked;;;]
```

В таблице Настройки веб-браузера Mozilla Firefox описаны только некоторые политики. Полный список политик и их описание можно найти на странице описания шаблонов политик Mozilla Firefox или в браузере Mozilla Firefox, указав в адресной строке URL: **about:policies#documentation**.

Таблица 29.39. Настройки веб-браузера Mozilla Firefox

Политика	Ключ	Описание
Менеджер паролей	PasswordManagerEnabled	Позволяет запретить доступ к менеджеру паролей через настройки и блокирует about:logins. Если эта политика находится в состоянии **Включено** или **Не сконфигурировано**, менеджер паролей доступен в настройках и на странице about:logins. Если эта политика находится в состоянии **Отключено**, Firefox запрещает доступ к менеджеру паролей через настройки и блокирует about:logins.
Отключить создание мастер-пароля	DisableMasterPasswordCreation	Позволяет отключить возможность установить мастер-пароль (основной пароль). Если эта политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут создать мастер-пароль. Если эта политика находится в состоянии **Включено**, то она работает так же, как установка политики **Основной (главный) пароль** состояние **Отключено**, и пользователи не могут создать мастер-пароль. Если используются и политика «Отключить создание мастер-пароля», и «Основной (главный) пароль», то политика **Отключить создание мастер-пароля** имеет приоритет.
Предлагать сохранить логины	OfferToSaveLogins	Позволяет настроить будет ли Firefox предлагать запоминать сохранённые логины и пароли. Если политика находится в состоянии **Отключено**, Firefox не будет предлагать сохранять логины и пароли веб-сайтов. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, Firefox будет предлагать сохранять логины и пароли веб-сайтов.
	DisableDeveloperTools	Позволяет управлять доступом к инструментам разработчика.

Политика	Ключ	Описание
Отключить инструменты разработчика		Если политика находится в состоянии **Включено**, инструменты веб-разработчика недоступны в Firefox. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, инструменты веб-разработчика доступны в Firefox.
Отключить приватный просмотр	DisablePrivateBrowsing	Запрещает доступ к приватному просмотру. Если политика находится в состоянии **Включено**, приватный просмотр запрещен. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, приватный просмотр разрешен.
Нет закладок по умолчанию	NoDefaultBookmarks	Отключает создание закладок по умолчанию (идущих вместе с Firefox), и смарт-закладки (часто посещаемые, недавние). Если политика находится в состоянии **Включено**, закладки по умолчанию и смарт-закладки (наиболее посещаемые, недавние теги) не создаются. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, создаются закладки по умолчанию и смарт-закладки (наиболее посещаемые, последние теги). Примечание: эта политика эффективна только в том случае, если она используется до первого запуска профиля.
Запрос места загрузки	PromptForDownloadLocation	Позволяет указать должен ли пользователь выбирать каталог для загружаемых файлов Если политика находится в состоянии **Отключено**, файлы будут сохраняться в каталог, указанный в настройках (пользователю не предлагается указать место для загрузки файла). Если политика находится в состоянии **Включено**, пользователю будет всегда выдаваться запрос на сохранение файла. Если политика находится в состоянии **Не сконфигурировано**, пользователю будет выдаваться запрос на сохранение файла, но он может изменить значение по умолчанию.
Отключить историю форм	DisableFormHistory	Отключает запоминание истории поиска и данных форм. Если политика находится в состоянии **Включено**, Firefox не запоминает историю форм или поиска.

Политика	Ключ	Описание
		Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Firefox будет помнить историю форм и поиска.
Блокировка редактора настроек (about:config)	BlockAboutConfig	Блокирует доступ к странице about:config. Если эта политика находится в состоянии **Включено**, пользователь не может получить доступ к about:config. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может получить доступ к about:config.
Блокировка страницы управления профилями (about:profiles)	BlockAboutProfiles	Блокирует доступ к странице управления профилями (about:profiles). Если политика находится в состоянии **Включено**, пользователь не может получить доступ к профилям about:profiles. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может получить доступ к профилям about:profiles.
Блокировка информации об устранении неполадок	BlockAboutSupport	Блокирует доступ к странице about:support. Если политика находится в состоянии **Включено**, пользователь не может получить доступ к информации для устранения неполадок или about:support. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может получить доступ к информации для устранения неполадок или about:support.
Captive Portal (портал захвата)	CaptivePortal	Включает или отключает тест соединения (поддержку перехватывающего портала). Если политика находится в состоянии **Отключено**, то поддержка captive portal отключена. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, то поддержка captive portal включена. Примечание: Браузер Mozilla Firefox при запуске проверяет, требует ли используемое сетевое соединение вход в систему. Во время теста Firefox пытается подключиться к **http://detectportal.firefox.com/success.txt**, чтобы проверить возможность соединения с этим адресом. Этот адрес также используется для

Политика	Ключ	Описание
		проверки поддержки активного сетевого соединения IPv6. Отключение этой функциональности уменьшает количество автоматических подключений и может немного ускорить запуск браузера.
Отключить встроенную программу просмотра PDF (PDF.js)	DisableBuiltinPDFViewer	Отключает PDF.js, встроенный просмотрщик PDF в Firefox. Если политика находится в состоянии **Включено**, файлы PDF не просматриваются в Firefox. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, файлы PDF просматриваются в Firefox.
Отключить команды обратной связи	DisableFeedbackCommands	Отключает команды отправки отзывов в меню **Справка** (**Отправить отзыв…** и **Сообщить о поддельном сайте…**). Если политика находится в состоянии **Включено**, пункты меню **Отправить отзыв…** и **Сообщить о поддельном сайте…** недоступны из меню **Справка**. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пункты меню **Отправить отзыв…** и **Сообщить о поддельном сайте…** доступны из меню **Справка**.
Отключить снимки экрана Firefox	DisableFirefoxScreenshots	Отключает функцию Firefox Screenshots. Если политика находится в состоянии **Включено**, снимки экрана Firefox недоступны. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, доступны снимки экрана Firefox.
Отключить учетные записи Firefox	DisableFirefoxAccounts	Отключает службы, основанные на Аккаунте Firefox, включая синхронизацию. Если политика находится в состоянии **Включено**, учетные записи Firefox отключены, в том числе отключена синхронизация. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, доступны Аккаунты Firefox и синхронизация.
Отключить исследования Firefox	DisableFirefoxStudies	Запрещает Firefox выполнять исследования. Если политика находится в состоянии **Включено**, Firefox никогда не будет проводить исследования SHIELD или опросы Heartbeat. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может включить исследования SHIELD или опросы Heartbeat.

Политика	Ключ	Описание
		Для получения дополнительной информации см. **https://support.mozilla.org/en-US/kb/shield** и **https://wiki.mozilla.org/Firefox/Shield/Heartbeat**
Отключить кнопку «Забыть»	DisableForgetButton	Закрывает доступ к кнопке **Забыть**. Если политика находится в состоянии **Включено**, кнопка **Забыть о части истории веб-сёрфинга** недоступна. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, кнопка **Забыть о части истории веб-сёрфинга** доступна.
Запретить показывать пароли в сохраненных логинах	DisablePasswordReveal	Не позволяет просматривать пароли у сохранённых логинов. Если политика находится в состоянии **Включено**, пользователи не могут отображать пароли в сохраненных логинах. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут отображать пароли в сохраненных логинах.
Отключить Pocket	DisablePocket	Отключает сохранение страниц в Pocket. Если политика находится в состоянии **Включено**, Pocket недоступен. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Pocket доступен. Примечание: Pocket — это специальный сервис для хранения различной информации, найденной в ходе веб-сёрфинга.
Отключить импорт профиля	DisableProfileImport	Отключает команду меню для импорта данных из другого браузера. Если политика находится в состоянии **Включено**, опция **Импортировать данные из другого браузера…** в окне закладок недоступна. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, опция **Импортировать данные из другого браузера…** доступна.
Отключить обновление профиля	DisableProfileRefresh	Отключает кнопку **Обновить Firefox** на странице about:support.

Политика	Ключ	Описание
		Если политика находится в состоянии **Включено**, кнопка **Обновить Firefox** будет недоступна на странице about:support. Если эта политика отключена или не сконфигурирована, кнопка **Обновить Firefox** будет доступна.
Отключить безопасный режим	DisableSafeMode	Отключает функцию для перезапуска в безопасном режиме. Если политика находится в состоянии **Включено**, пользователь не может перезапустить браузер в безопасном режиме. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, безопасный режим разрешен.
Не проверять браузер по умолчанию	DontCheckDefaultBrowser	Отключает проверку браузера по умолчанию при запуске. Если политика находится в состоянии **Включено**, Firefox не проверяет, является ли он браузером по умолчанию при запуске. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Firefox при запуске проверяет, является ли он браузером по умолчанию.
Аппаратное ускорение	HardwareAcceleration	Отключает аппаратное ускорение. Если политика находится в состоянии **Отключено**, аппаратное ускорение не может быть включено. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, включено аппаратное ускорение.
Основной (главный) пароль	PrimaryPassword	Позволяет установить следует ли требовать или не давать использовать мастер-пароль. Если политика находится в состоянии **Отключено**, пользователи не могут создать основной пароль. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, пользователи могут создать основной пароль.
Прогнозирование сети	NetworkPrediction	Включает или отключает прогнозирование сети (предварительная выборка DNS). Предварительная выборка DNS — это технология, используемая Firefox для ускорения загрузки новых веб-сайтов.

Политика	Ключ	Описание
		Если политика находится в состоянии **Отключено**, прогнозирование сети (предварительная выборка DNS) будет отключено. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, будет включено прогнозирование сети (предварительная выборка DNS).
Новая вкладка	NewTabPage	Включает или отключает страницу новой вкладки. Если эта политика находится в состоянии **Отключено**, в новой вкладке будет загружена пустая страница. Если эта политика в состоянии **Включено** или **Не сконфигурировано**, в новой вкладке будет загружена страница по умолчанию.
Подсказки по поиску	SearchSuggestEnabled	Включает или отключает поисковые предложения. Если эта политика находится в состоянии **Отключено**, поисковые подсказки будут отключены. Если эта политика в состоянии **Включено**, поисковые подсказки будут включены. Если эта политика в состоянии **Не сконфигурировано**, поисковые подсказки будут включены, но пользователь может отключить их.
Показывать кнопку «Домашняя страница» на панели инструментов	ShowHomeButton	Включает кнопку **Домашняя страница** на панели инструментов. Если политика находится в состоянии **Отключено**, кнопка **Домашняя страница** не будет отображаться на панели инструментов. Если политика находится в состоянии **Включено**, кнопка **Домашняя страница** отображается на панели инструментов.
Блокировка менеджера дополнений (about:addons)	BlockAboutAddons	Блокирует доступ к менеджеру дополнений (about:addons). Если политика находится в состоянии **Отключено** или **Не сконфигурировано** пользователь может получить доступ к менеджеру дополнений (about:addons). Если политика находится в состоянии **Включено**, пользователь не может получить доступ к менеджеру дополнений (about:addons).
	Homepage	Устанавливает URL домашней страницы при старте браузера и, если необходимо, блокирует её смену.

Политика	Ключ	Описание
URL для домашней страницы		Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может установить и изменить домашнюю страницу. Если политика находится в состоянии **Включено**, можно установить домашнюю страницу по умолчанию, а также заблокировать возможность изменения домашней страницы.
SPNEGO	SPNEGO	Включает аутентификацию через SPNEGO/Kerberos. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, никаким веб-сайтам не разрешается использовать аутентификацию SPNEGO с помощью браузера. Если политика находится в состоянии **Включено**, указанным веб-сайтам разрешается использовать аутентификацию SPNEGO в браузере. Записи в списке имеют формат altlinux.org или https://altlinux.org
Не разрешать изменять настройки аутентификации	Authentication Locked	Блокирует настройки аутентификации от изменений пользователем. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, пользователь не может изменить параметры проверки подлинности. Если политика находится в состоянии **Отключено**, пользователь может изменить параметры проверки подлинности.
Разрешить неполное доменное имя (Non FQDN)	Authentication AllowNonFQDN	Разрешить SPNEGO или NTLM для неполных доменных имен (Non FQDN). Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, NTLM и SPNEGO не будут включены для неполных доменных имен. Если политика находится в состоянии **Включено** (и флажки отмечены), SPNEGO или NTLM будут включены для неполных доменных имен (Non FQDN).
Расширения для установки	Extensions\Install	Задаёт список URL-адресов или собственных путей для устанавливаемых расширений. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, расширения не устанавливаются.

Политика	Ключ	Описание
		Если политика находится в состоянии **Включено**, можно указать список URL-адресов или путей расширений, которые будут устанавливаться при запуске Firefox. При каждом изменении этого списка политики будут переустанавливаться. URL политики необходимо задавать в формате *.xpi (например, **https://addons.mozilla.org/firefox/downloads/file/3450175/adapter_rutoken_plugin-1.0.5.0.xpi**). Можно также указать путь на локальный каталог, в который политикой копирования файлов скопировать расширение в формате *.xpi.
Управление расширениями	ExtensionSettings	Это правило позволяет управлять всеми аспектами расширений. Политика сопоставляет идентификатор расширения с его конфигурацией. Если указан идентификатор расширения, конфигурация будет применяться только к указанному расширению. Конфигурация по умолчанию может быть установлена для специального идентификатора *****, который будет применяться ко всем расширениям, для которых не задана пользовательская конфигурация в этой политике. Чтобы получить идентификатор расширения, можно установите расширение и посмотреть идентификатор на странице about:support в разделе **Расширения**. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, расширения не будут управляться. Если политика находится в состоянии **Включено**, можно использовать JSON для описания политики управления расширениями. Пример JSON: `{ "*": { "blocked_install_message": "Custom error message" }, "adblockultimate@adblockultimate.net": { "installation_mode": "force_installed", "install_url": "file:///home/user/file.xpi" }, "rutokenplugin@rutoken.ru": { "installation_mode": "force_installed",`

Политика	Ключ	Описание

```
        "install_url": "https://
addons.mozilla.org/…/plugin.xpi"
    }
}
```

Конфигурация для каждого расширения — это еще один словарь, который может содержать следующие поля:

- **installation_mode** — режим установки расширения. Допустимые значения:
  - **allowed** — разрешает установку расширения пользователем (поведение по умолчанию). Поле **install_url** не используется и будет автоматически определено на основе идентификатора;
  - **blocked** — блокирует установку расширения и удаляет его, если оно уже установлено;
  - **force_installed** — расширение устанавливается автоматически и не может быть удалено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует **install_url**;
  - **normal_installed** — расширение устанавливается автоматически, но может быть отключено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует **install_url**;

- **install_url** — сопоставляется с URL-адресом, указывающим, откуда Firefox может загрузить расширение (при **force_installed** или **normal_installed**). При установке из локальной файловой системы следует использовать URL-адрес file:///. При установке с сайта addons.mozilla.org можно использовать URL-адрес в виде **https://addons.mozilla.org/firefox/downloads/file/3450175/adapter_rutoken_plugin-1.0.5.0.xpi**;
- **install_sources** — список источников, из которых разрешена установка расширений с использованием шаблонов соответствия URL. Этот параметр не нужен, если разрешена установка только определенных расширений по идентификатору. Данный параметр можно использовать только для конфигурации по умолчанию;
- **minimum_version_required** — отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения;

Политика	Ключ	Описание
		▸**allowed_types** — белый список разрешённых типов расширений/приложений, которые можно установить в Firefox. Значение представляет собой список строк (допустимые строки: «extension», «theme», «dictionary», «locale»). Этот параметр можно использовать только для конфигурации по умолчанию; ▸**override_update_url** — указывает, что для всех последующих обновлений расширения будет использоваться URL из поля **update_url** или **update** в политике **ExtensionInstallForcelist**. Если эта политика не сконфигурирована или отключена, будет использоваться URL из манифеста расширения; ▸**blocked_install_message** — сообщение об ошибке, которое будет отображаться для пользователей, если им заблокирована установка расширения. Этот параметр можно использовать только для конфигурации по умолчанию; ▸**restricted_domains** — массив доменов, на которых нельзя запускать сценарии контента. Этот параметр можно использовать только для конфигурации по умолчанию; ▸**updates_disabled** — логическое значение, указывающее, следует ли отключать автоматические обновления для отдельного расширения; ▸**default_area** — указывает, где должен быть размещен значок расширения. Возможные значения: **navbar** и **menupanel**.

29.5.12. Управление политиками «Яндекс.Браузера»

Эти групповые политики позволяют централизованно управлять настройками «Яндекс.Браузера».

Механизм Yandex в составе пакета *gpupdate* формирует JSON-файл для браузера из шаблонов групповых политик. Во время запуска «Яндекс.Браузер» считывает файл **/etc/opt/yandex/browser/policies/managed/policies.json** и применяет параметры групповых политик. Групповые политики на основе **policies.json** предоставляют кроссплатформенную совместимость, что позволяет управлять браузерами в любом дистрибутиве Альт с установленным окружением рабочего стола.

Примечание

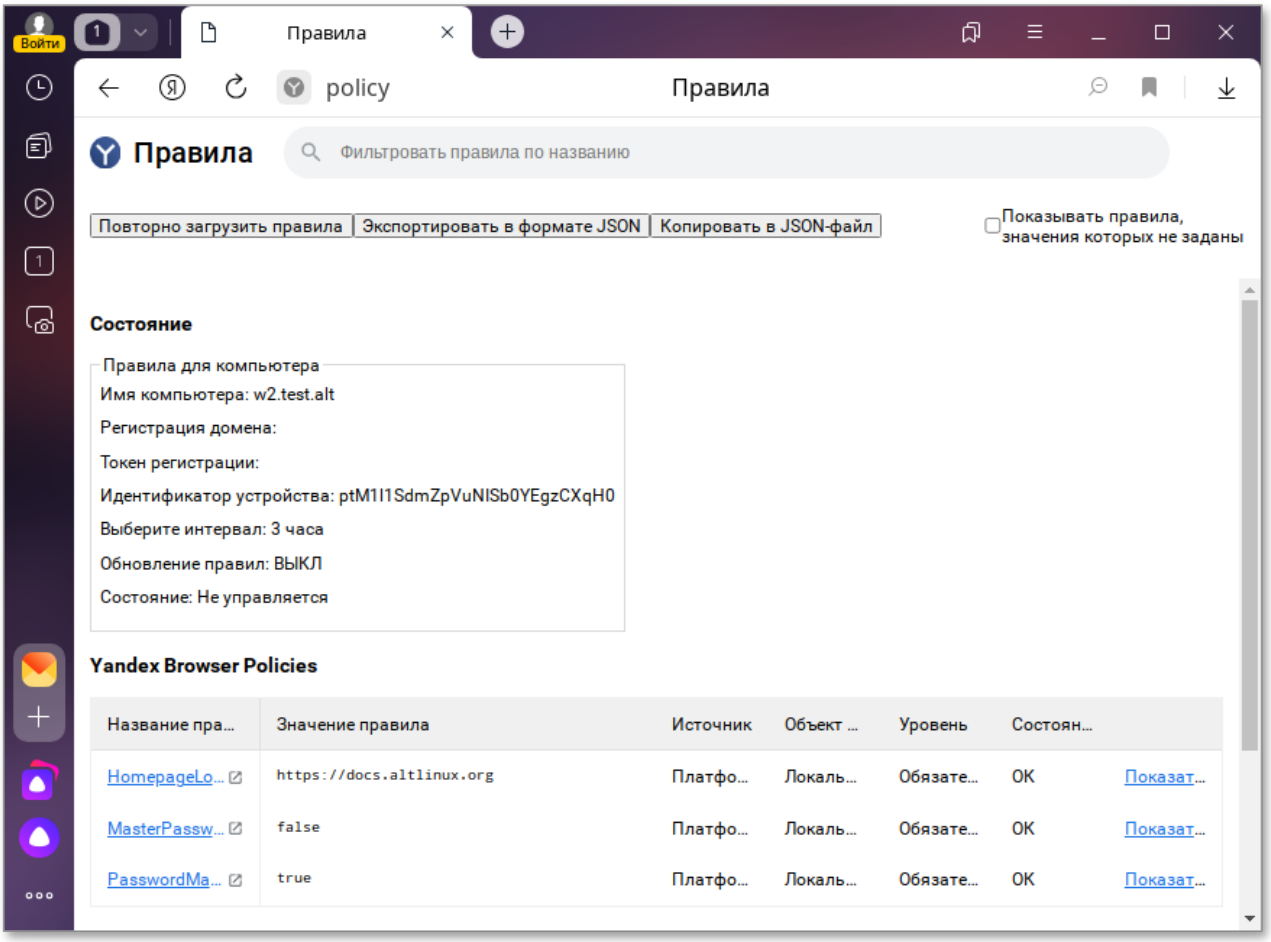
Для случаев, если требуется вести параллельно другой файл с конфигурациями, можно создать файл **/etc/opt/yandex/browser/policies/managed/policies_local.json** и вносить изменения в него. При коллизиях будет применена последняя прочитанная настройка.

Данный механизм реализован только для машинных политик.

Примечание

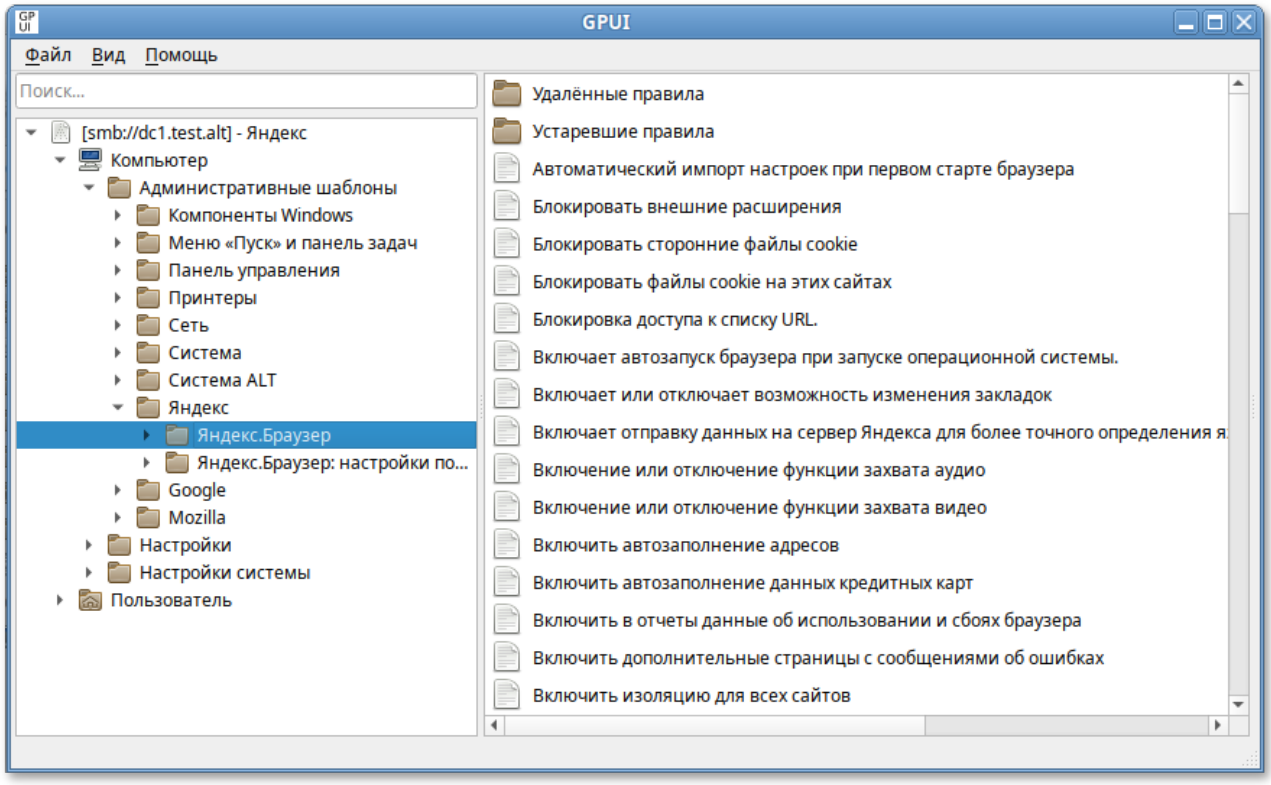
Настройка политик для «Яндекс.Браузера» требует дополнительной установки ADMX-файлов Yandex (пакет *admx-yandex-browser*).

Результат применения параметров групповой политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: **`browser://policy`**:

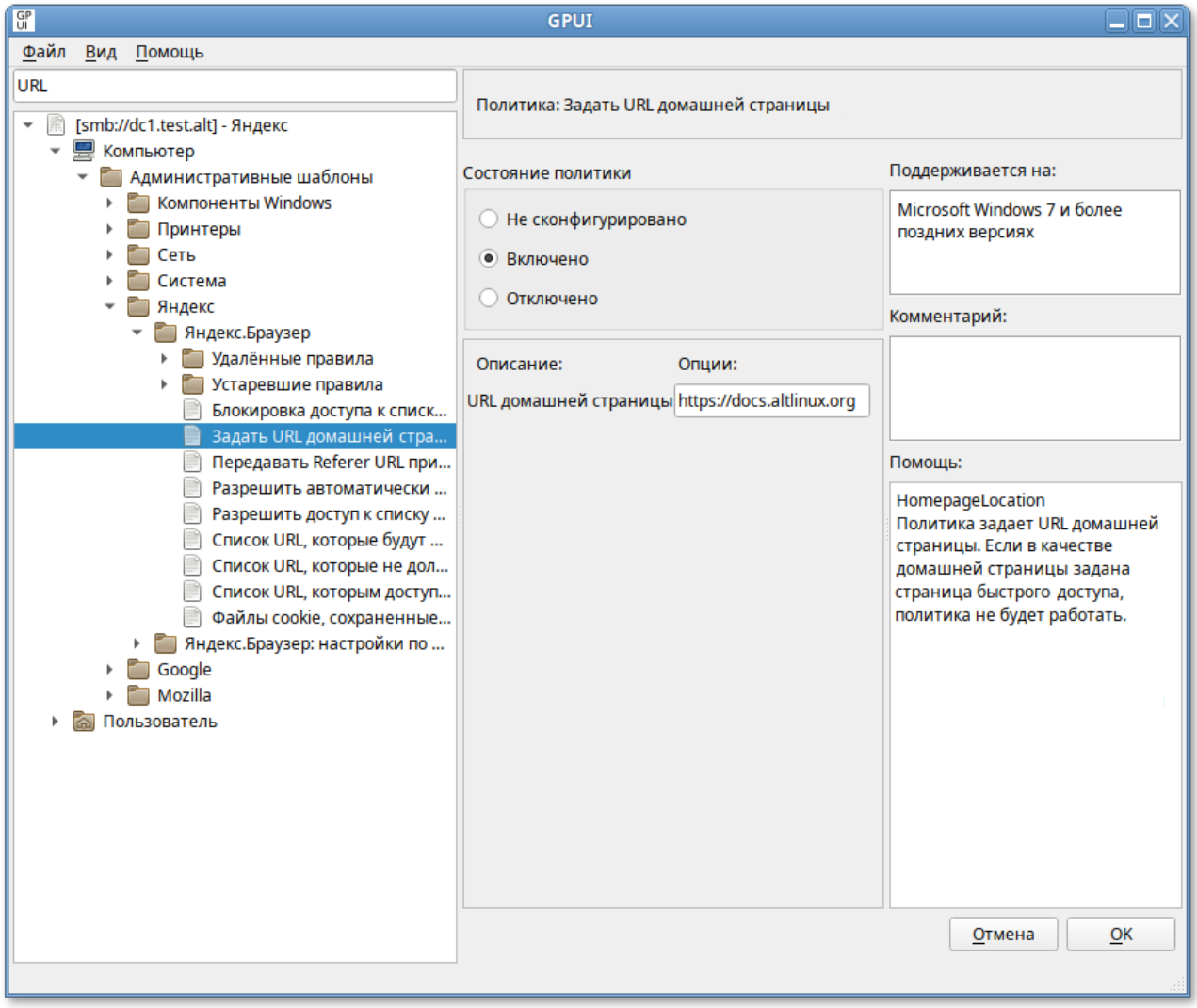


В качестве примера рассмотрим политику установки URL домашней страницы.

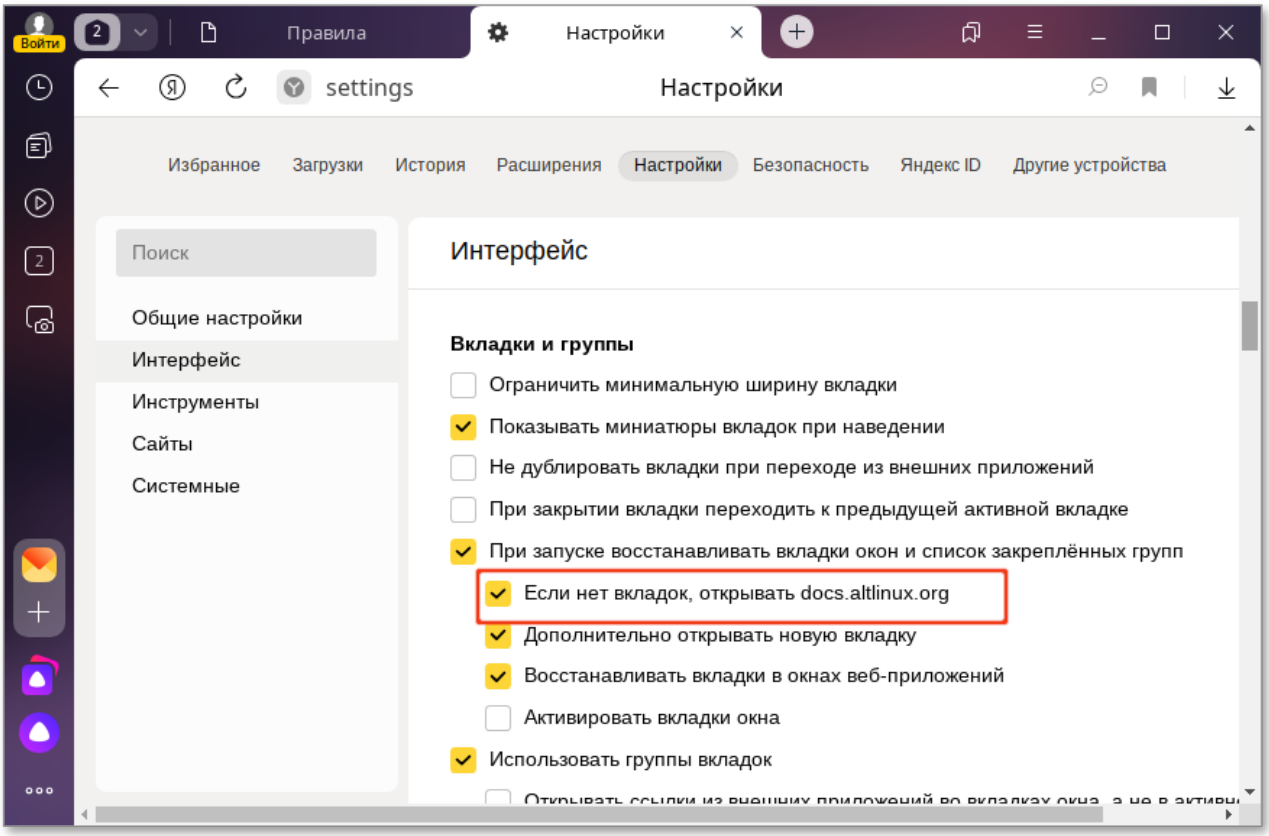
Для редактирования политик браузера «Яндекс.Браузера» следует перейти в **Компьютер** → **Административные шаблоны** → **Яндекс** → **Яндекс.Браузер**:



Для установки URL домашней страницы следует выбрать пункт **Главная страница и страница быстрого доступа при запуске**, щелкнуть левой кнопкой мыши на политике **Задать URL домашней страницы**, откроется диалоговое окно настройки политики. Выбрать параметр **Включено**, в разделе **Параметры** ввести URL и нажать кнопку **ОК**:



В результате применения данной политики будет установлена домашняя страница по умолчанию:



Домашняя страница откроется, если в последний раз браузер был закрыт без вкладок или сочетанием клавиш **Alt+Home**.

Все настройки политики «Яндекс.Браузера» хранятся в файле **{GUID GPT}/Machine/Registry.pol**. Пример файла **Registry.pol**:

```
Preg[Software\Policies\YandexBrowser;BlockExternalExtensions;;;]
[Software\Policies\YandexBrowser\URLBlocklist;https://mail.ru;; ;https://mail.ru]
[Software\Policies\YandexBrowser\AutoOpenFileTypes;pdf;;pdf]
[Software\Policies\YandexBrowser;HomepageLocation;;4;https://docs.altlinux.org]
```

В таблице Настройки «Яндекс.Браузера» описаны только некоторые политики. Полный список политик и их описание можно найти на странице описания политик «Яндекс.Браузера» или в «Яндекс.Браузере», указав в адресной строке URL: **browser://policy/** и установив отметку на пункте **Показывать правила, значения которых не заданы**.

Таблица 29.40. Настройки «Яндекс.Браузера»

Политика	Ключ	Описание
Включить или отключить панель закладок	BookmarkBarEnabled	Политика позволяет принудительно включить или принудительно отключить панель закладок в «Яндекс.Браузере». Если политика находится в состоянии **Включено**, панель закладок отображается. Если политика находится в состоянии **Отключено**, панель закладок не отображается.

Политика	Ключ	Описание
		Если политика находится в состоянии **Не сконфигурировано**, пользователь может самостоятельно решать, включить или отключить панель закладок.
Настроить закладки	EditBookmarksEnabled	Политика включает или отключает возможность изменения закладок. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, пользователи могут добавлять, изменять и удалять закладки. Если политика находится в состоянии **Отключено**, пользователи не могут добавлять, изменять и удалять закладки. Закладки, созданные до отключения политики, останутся доступными.
Задать форматы файлов, которые будут автоматически открываться после скачивания	AutoOpenFileTypes	Политика позволяет задать форматы файлов, которые будут автоматически открываться после скачивания. Если политика находится в состоянии **Включено**, в ней можно перечислить форматы файлов (без точки), которые будут автоматически открываться после скачивания (например, txt, jpg). Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, после скачивания будут автоматически открываться файлы только тех форматов, которые выбрал пользователь в контекстном меню загруженного файла (например, «Открывать JPG автоматически»).
Настроить показ всплывающих окон	DefaultPopupsSetting	Политика разрешает или запрещает всплывающие окна на всех сайтах. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, всплывающие окна блокируются на всех сайтах. Пользователи могут разрешать или блокировать всплывающие окна в настройках браузера. Если политика находится в состоянии **Включено**, администратор может определить режим применения политики: » **Блокировать на всех сайтах** » **Разрешить на всех сайтах** Пользователи не могут разрешать или блокировать всплывающие окна в настройках браузера.
Разрешить полноэкранный режим	FullscreenAllowed	

Политика	Ключ	Описание
		Политика разрешает или запрещает активацию полноэкранного режима. В этом режиме все элементы интерфейса «Яндекс.Браузера» скрыты, и на экране отображается только содержимое сайта. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, пользователи могут активировать полноэкранный режим, нажав **F11**. Полноэкранный режим может быть активирован приложениями и расширениями, если у них есть на это разрешения. Если политика находится в состоянии **Отключено**, полноэкранный режим отключен для всех пользователей, приложений и расширений.
Задать URL домашней страницы	HomepageLocation	Политика задает URL домашней страницы. Если в качестве домашней страницы задана страница быстрого доступа, политика не будет работать. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут сами установить URL домашней страницы в настройках браузера. Если политика находится в состоянии **Включено**, можно установить домашнюю страницу по умолчанию. URL должен иметь стандартный вид (например, **https://altlinux.org**). Домашняя страница откроется, если в последний раз браузер был закрыт без вкладок или сочетанием клавиш **Alt**+**Home**. Пользователи не могут менять домашнюю страницу в браузере.
Отключить контекстное меню для выделенного текста	InstaserpDisabled	Политика позволяет отключить контекстное меню, всплывающее при выделении текста на странице. Если политика находится в состоянии **Включено**, контекстное меню не показывается, пользователи не могут включить его в настройках (опция **При выделении текста показывать кнопки «Найти» и «Копировать»** неактивна). Если политика находится в состоянии **Отключено**, контекстное меню показывается, пользователи не могут отключить его в настройках. Если политика находится в состоянии **Не сконфигурировано**, контекстное меню показывается, пользователи могут отключить его в настройках.
Отображать боковую панель	SidePanelMode	Политика позволяет настроить режим отображения боковой панели и запретить пользователям его менять.

Политика	Ключ	Описание
		Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут самостоятельно настроить режим отображения боковой панели. Если политика находится в состоянии **Включено**, администратор может выбрать режим отображения боковой панели: ▸**Закрепить только на экране новой вкладки** ▸**Закрепить на сайтах** ▸**Скрыть**
Включить автозаполнение адресов	AutofillAddressEnabled	Политика разрешает пользователям автозаполнение адресов. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, автозаполнение адресов включено. Если политика находится в состоянии **Отключено**, автозаполнение адресов отключено, введенные адреса не сохраняются.
Настроить режим Инкогнито	IncognitoModeAvailability	Политика определяет, могут ли пользователи включать режим «Инкогнито». Если политика находится в состоянии **Не сконфигурировано**, пользователи могут открывать страницы в режиме Инкогнито. Если политика находится в состоянии **Включено**, администратор может определить режим применения политики: ▸**Принудительное использование режима Инкогнито** — режим «Инкогнито» всегда включен; ▸**Режим Инкогнито доступен** — пользователи могут просматривать страницы как в обычном режиме, так и в режиме «Инкогнито»; ▸**Режим Инкогнито отключён** — пользователи могут просматривать страницы только в обычном режиме. Если политика находится в состоянии **Отключено**, пользователи могут просматривать страницы только в обычном режиме.
Запретить использовать мастер-пароль	MasterPasswordDisabled	Политика запрещает пользователям использовать мастер-пароль. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может использовать мастер-пароль.

Политика	Ключ	Описание
		Если политика находится в состоянии **Включено**, мастер-пароль в браузере отключен.
Разрешить сохранять пароли	PasswordManagerEnabled	Политика разрешает сохранять пароли в браузере и автоматически подставлять их при авторизации на сайтах. Если политика находится в состоянии **Не сконфигурировано**, сохранение паролей в браузере включено. Пользователи могут включать и отключать сохранение паролей. Если политика находится в состоянии **Включено**, сохранение паролей включено. Пользователи не могут включать и отключать сохранение паролей. Если политика находится в состоянии **Отключено**, сохранение новых паролей отключено. Пользователи могут использовать уже сохраненные пароли. Пользователи не могут включать и отключать сохранение паролей.
Запретить сохранять историю просмотров	SavingBrowserHistoryDisabled	Политика запрещает сохранять историю просмотров и синхронизировать открытые вкладки. При синхронизации информация передается на сервер Яндекса по защищенному каналу. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, история посещенных страниц сохраняется в журнале браузера. Вкладки и Табло синхронизируются с сервером Яндекса. Пользователи могут импортировать историю из других браузеров. Если политика находится в состоянии **Включено**, история посещенных страниц не сохраняется в журнале браузера. Пользователи не могут включить сохранение истории посещенных страниц. Только Табло синхронизируются с сервером Яндекса. Возможность переноса истории вручную отключена.

Политика	Ключ	Описание
Выбрать папку кеша на диске	DiskCacheDir	Политика определяет место хранения данных кеша. Чтобы не потерять данные, не следует указывать в политике корневую папку или папку, которая используется в других целях. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, браузер использует папку по умолчанию, однако пользователи могут ее изменить с помощью параметра **disk-cache-dir**. Если политика находится в состоянии **Включено**, браузер хранит кеш на диске в заданной администратором папке. Пользователи не могут ее изменить с помощью параметра **disk-cache-dir**.
Задать объём кеша в байтах	DiskCacheSize	Политика позволяет задать объем кеша в байтах. Значение используется различными подсистемами в браузере как справочное. Поэтому фактический объем используемого дискового пространства может превышать указанное значение, но будет иметь такой же порядок. Если политика находится в состоянии **Не сконфигурировано**, браузер использует объем кеша по умолчанию. Если политика находится в состоянии **Включено**, браузер использует заданный размер кеша независимо от параметра **--disk-cache-size**. Указывается максимальный размер кеша в байтах. Например, 104857600 — это 100 МБ. Если политика находится в состоянии **Отключено**, браузер использует объем кеша по умолчанию, но пользователи могут менять размер кеша с помощью параметра **--disk-cache-size**.
Блокировать внешние расширения	BlockExternalExtensions	Политика позволяет запретить установку внешних расширений. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, установка внешних расширений разрешена. Если политика находится в состоянии **Включено**, установка внешних расширений запрещена.
Блокировать URL'ы из заданного списка	URLBlocklist	Политика блокирует доступ к URL и локальным файлам, которые внесены в черный список. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, браузер не блокирует URL.

Политика	Ключ	Описание
		Если политика находится в состоянии **Включено**, страницы запрещенных URL не загружаются. В политике можно перечислить шаблоны запрещенных URL. Политика не действует на URL со встроенным кодом JavaScript и динамически загружаемые данные. Общий формат шаблона URL: scheme://host:port/path, где: ▸scheme — схема обращения к ресурсу (например, http, https). Если префикс scheme:// не задан, блокируются все пути и все протоколы (http, https, ftp и т.д.). Блокировать внутренние URL с префиксом browser:// и chrome:// не рекомендуется; ▸host — полное доменное имя или IP-адрес хоста. Имя или IP-адрес хоста должны быть указаны обязательно. По умолчанию блокируются все субдомены хоста. Чтобы этого избежать, можно добавить точку (.) перед именем хоста. Звездочка (*) блокирует все домены; ▸port — номер порта. Можно указать номер от 1 до 65535. Если номер не указан, блокируются все порты; ▸path — URL-адрес. Общий формат шаблона локального файла file://path, где: ▸file — путь до конкретного файла .html; ▸path — абсолютный путь к каталогу с файлами (все пути, для которых path является префиксом, будут внесены в список).
Задать исключения для политики URLBlocklist (Разрешить доступ к списку URL)	URLAllowlist	Политика позволяет внести в белый список URL или локальный файл. Белый список разрешает доступ к явно перечисленным в нем URL и файлам, даже если они попадают под действие шаблонов из черного списка (см. описание политики **Блокировать URL'ы из заданного списка**). Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, исключений из правила URLBlocklist нет. Если политика находится в состоянии **Включено**, указанные URL становятся доступны пользователям и считаются исключениями из правила URLBlocklist. Политика позволяет настроить исключения для определенных протоколов, субдоменов, отдельных доменов, портов или путей. Политика URLAllowlist имеет приоритет над правилом URLBlocklist. В этом правиле можно указать не более 1000 URL. Форматы шаблонов см. в описании политики **Блокировать URL'ы из заданного списка**.

Политика	Ключ	Описание
Разрешить вызывать окно выбора файлов	AllowFileSelectionDialogs	Политика разрешает или запрещает отображать окно выбора файлов и управляет настройками загрузки. Если политика находится в состоянии **Включено** или **Не сконфигурировано**, пользователи могут открывать окна выбора файлов (импорт закладок или паролей, загрузка файлов, сохранение ссылок и т.д.). Пользователи также могут сохранить файл с помощью контекстного меню и изменять настройки в разделе **Загруженные файлы** (**Настройки** → **Инструменты** → **Загруженные файлы**). Если политика находится в состоянии **Отключено** и пользователь выполняет действия, для которых нужно открыть окно выбора файла (например, импорт закладок, загрузка файлов, сохранение ссылок и т.д.), вместо окна отображается сообщение и имитируется нажатие пользователем кнопки **Отмена** в окне выбора файлов. Пользователи также не смогут сохранить файл из контекстного меню и изменять настройки в разделе **Загруженные файлы**.
Ограничить инструменты разработчика	DeveloperToolsAvailability	Политика ограничивает использование инструментов разработчика. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, инструменты разработчика и консоль JavaScript запрещены только для расширений, ограниченных корпоративной политикой. Если политика находится в состоянии **Включено** можно установить ограничение на использование инструментов разработчика. Доступны следующие параметры: - **Запретить** - **Запретить для расширений, установленных в соответствии с корпоративной политикой, и разрешить во всех остальных случаях** - **Разрешить**
Управлять настройками расширений	ExtensionSettings	Политика управляет настройками расширений в «Яндекс.Браузере». Заменяет любые другие политики по настройке расширений. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут самостоятельно настраивать расширения.

Политика	Ключ	Описание

Если политика находится в состоянии **Включено**, настройки расширений задает администратор с помощью кода, указанного в параметрах политики:

- идентификатор расширения или URL обновления привязывается только к одной конкретной настройке;
- идентификатор ***** действует на все расширения, для которых в политике не задана отдельная конфигурация;
- если указан URL обновления, заданная конфигурация применяется ко всем расширениям, в манифесте которых приведен этот URL.

Пример значения:

```
{
  "hdokiejnpimakedhajhdlcegeplioahd": {
    "installation_mode": "force_installed",
    "update_url": "https://clients2.google.com/
service/update2/crx"
  },
  "pioclpoplcdbaefihamjohnefbikjilc": {
    "installation_mode": "force_installed",
    "update_url": "https://clients2.google.com/
service/update2/crx"
  }
}
```

Параметры политики:

- **allowed_types** — типы приложений и расширений, которые пользователям разрешено устанавливать в браузере (допустимые строки: «extension», «hosted_app», «legacy_packaged_app», «tplatform_appeme», «theme», «user_script»). Используется только для настройки конфигурации по умолчанию со значением *****;
- **blocked_install_message** — уведомление (не более 1000 символов), которое будет появляться на устройствах пользователей при попытке установить запрещенные расширения;
- **blocked_permissions** — запрещает пользователям устанавливать и запускать расширения, требующие разрешений API (список доступных разрешений указан в манифесте расширения);
- **installation_mode** — указывает, разрешено ли добавлять заданные расширения. Допустимые режимы:
  - **allowed** — пользователи могут установить это расширение (поведение по умолчанию);
  - **blocked** — пользователи не могут установить это расширение;

Политика	Ключ	Описание
		▫**removed** — пользователи не могут установить это расширение. Если расширение было установлено, оно будет удалено; ▫**force_installed** — расширение устанавливается автоматически. Пользователи не могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр **update_url**); ▫**normal_installed** — расширение устанавливается автоматически. Пользователи могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр **update_url**); ▫**install_sources** — список URL страниц, с которых разрешено загружать и устанавливать расширения Необходимо разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода); ▫**minimum_version_required** — отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; ▫**update_url** — определяет, откуда загружается расширение. Можно указать URL интернет-магазина Chrome, Opera или использовать XML-файл: ▫если расширение размещено в интернет-магазине Chrome, следует указать **https://clients2.google.com/service/update2/crx** ▫если расширение размещено в интернет-магазине Opera, следует указать **https://extension-updates.opera.com/api/omaha/update/** ▫**override_update_url** — указывает, что для всех последующих обновлений расширения будет использоваться URL из поля **update_url** или **update** в политике **ExtensionInstallForcelist**. Если эта политика не сконфигурирована или отключена, будет использоваться URL из манифеста расширения; ▫**verified_contents_url** — указывает путь до файла **extension.verified_contents**. С его помощью расширение проверяется на доверие (используется, если нет доступа в интернет); ▫**runtime_allowed_hosts** — разрешает взаимодействие расширений с указанными сайтами, даже если они указаны в поле **runtime_blocked_hosts**. Можно указать до 100 сайтов;

Политика	Ключ	Описание
		runtime_blocked_hosts — запрещает расширениям взаимодействовать с указанными сайтами или изменять их, в том числе вставлять скрипты, получать доступ к файлам cookie и изменять веб-запросы. Можно указать до 100 сайтов.

29.5.13. Управление политиками почтового клиента Thunderbird

Эти групповые политики позволяют централизованно управлять настройками почтового клиента Mozilla Thunderbird.

Примечание

Политики Thunderbird реализованы в механизме **gpupdate**, начиная с версии 0.12.0.

Механизм Thunderbird в составе пакета *gpupdate* формирует JSON-файл для почтового клиента из шаблонов групповых политик. Во время запуска Thunderbird считывает собственный файл **policies.json** и применяет параметры групповых политик. Для Thunderbird файл **policies.json** расположен по адресу **/etc/thunderbird/policies/**. Групповые политики на основе **policies.json** предоставляют кроссплатформенную совместимость, что позволяет управлять почтовым клиентом в любом дистрибутиве «Альт» с установленным окружением рабочего стола.

Примечание

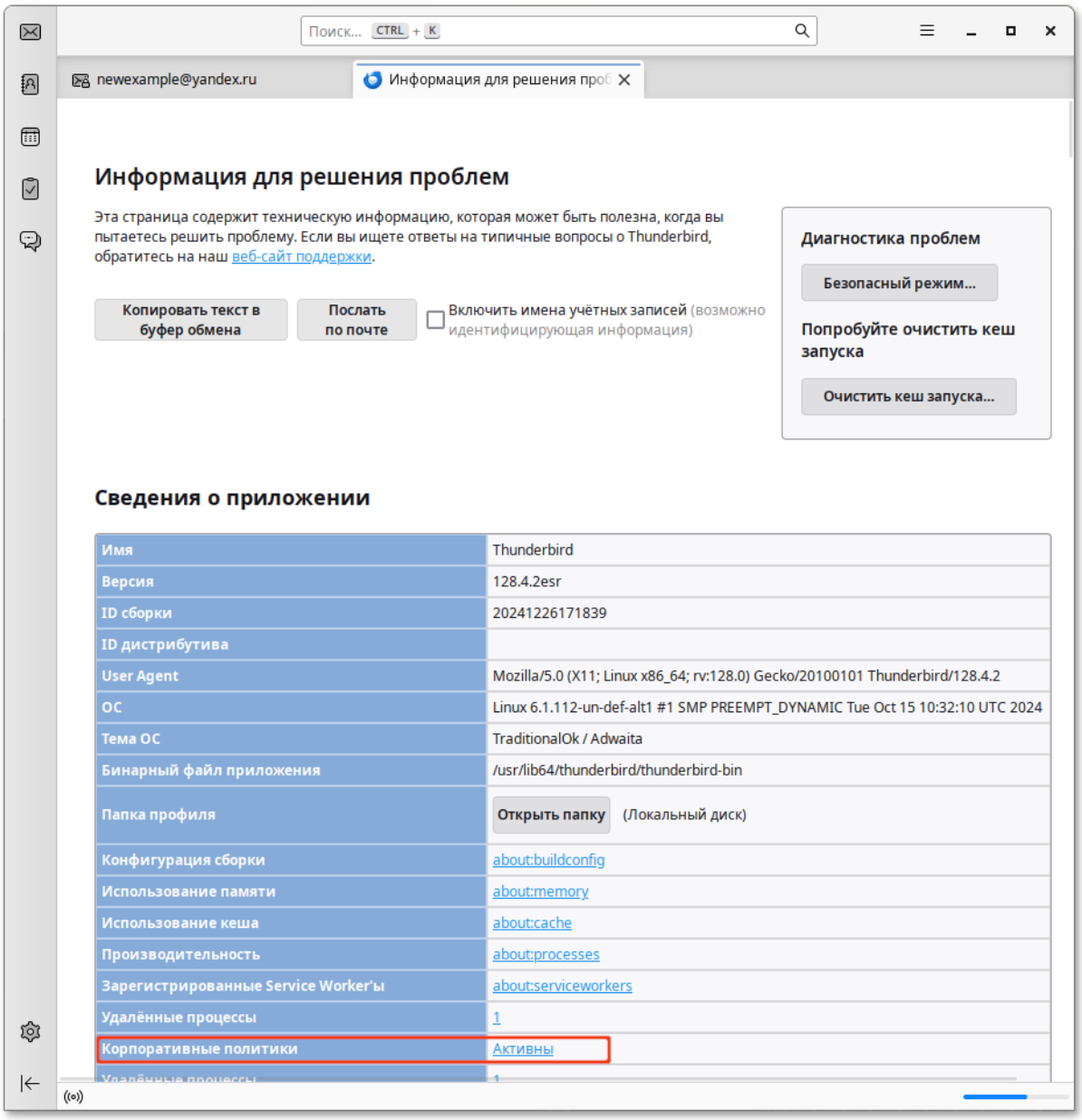
Данный механизм реализован только для машинных политик.

Примечание

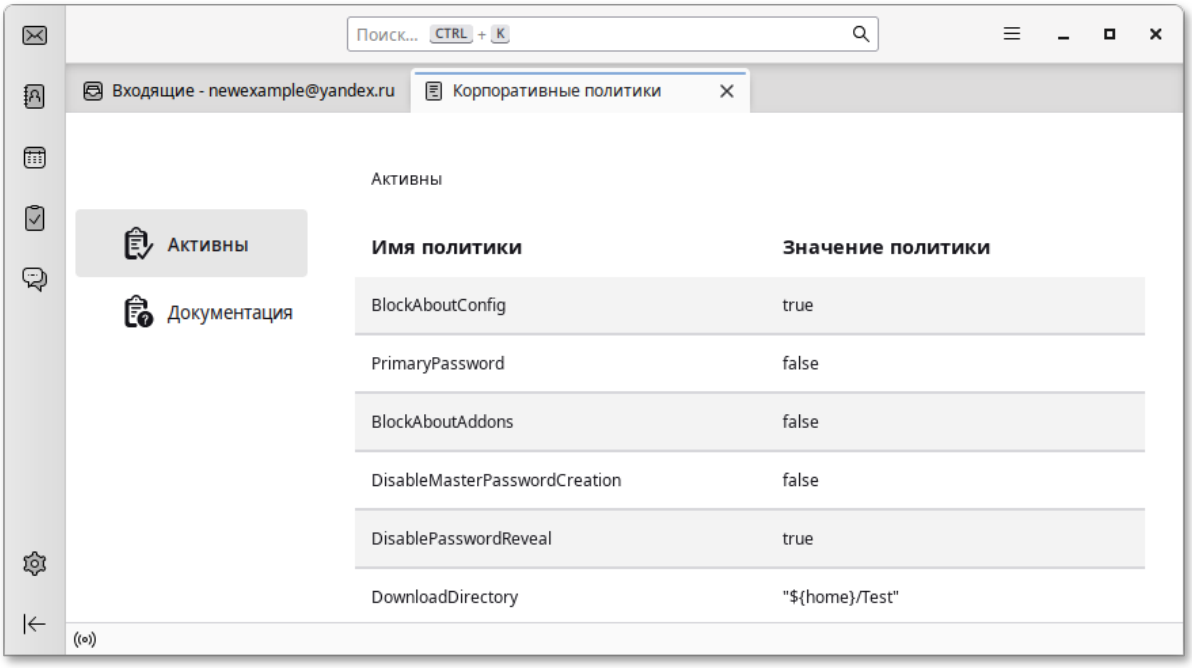
Настройка политик для почтового клиента Mozilla Thunderbird требует дополнительной установки ADMX-файлов Thunderbird (пакет *admx-thunderbird*).

Результат применения параметров групповой политики для Mozilla Thunderbird можно проверить, выполнив следующие действия:

1. В меню Thunderbird выбрать **Справка** → **Информация для решения проблем**.
2. На странице **Информация для решения проблем** в разделе **Сведения о приложении** найти строку **Корпоративные политики**. При наличии примененных настроек групповых политик, напротив строки **Корпоративные политики**, появится ссылка **Активны**:

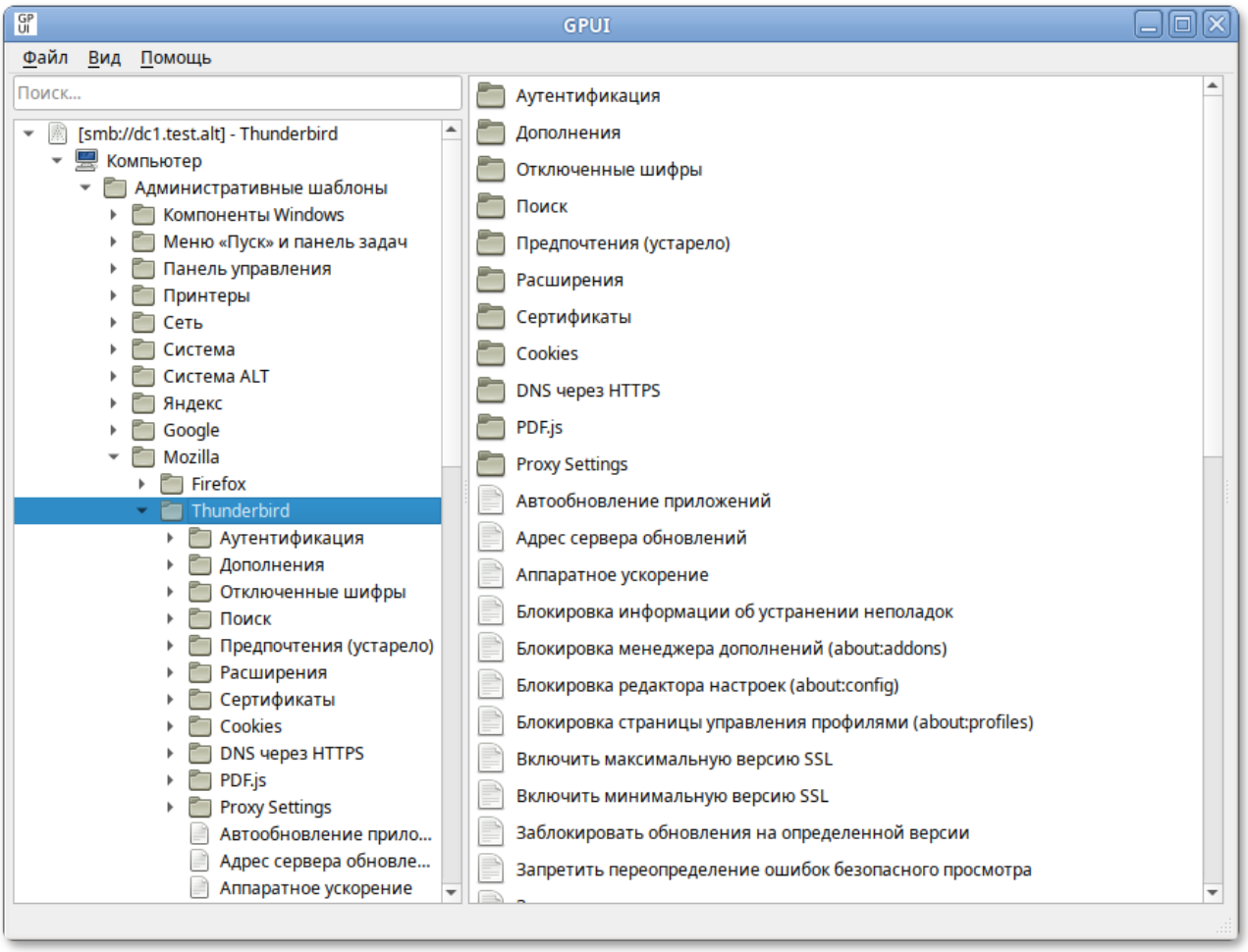


3. Перейти по ссылке **Активны**. Откроется страница со списком активных групповых политик Thunderbird:

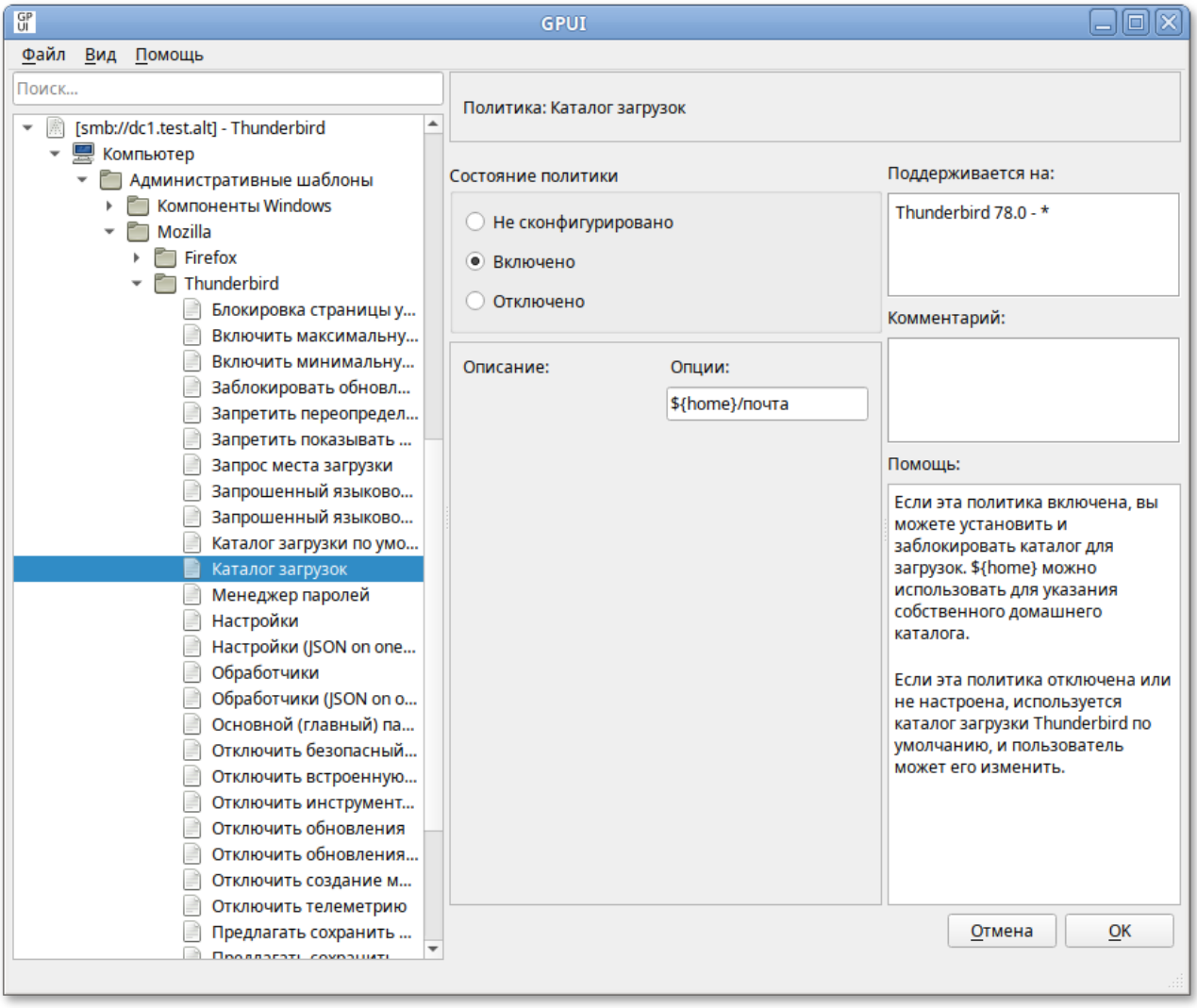


В качестве примера рассмотрим политику установки каталога для загрузок.

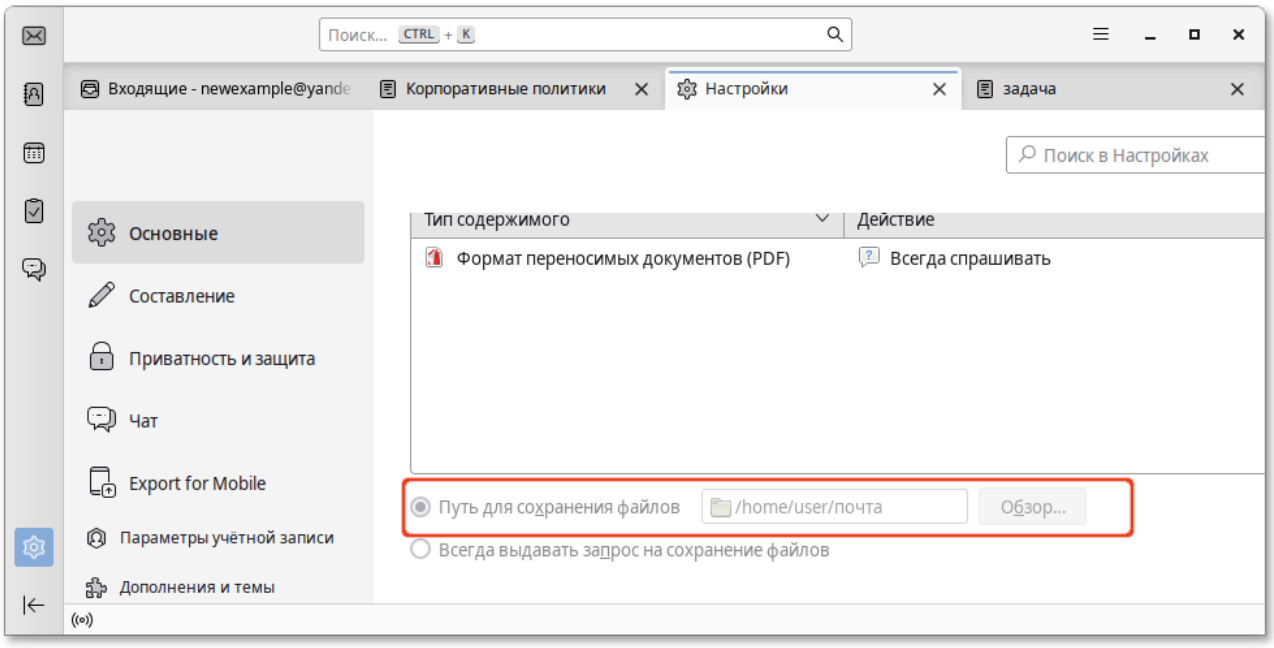
Для редактирования политик Mozilla Thunderbird следует перейти в **Компьютер** → **Административные шаблоны** → **Mozilla** → **Thunderbird**:



Выбрать политику **Каталог загрузок**, откроется диалоговое окно настройки политики. Выбрать параметр **Включено**, в разделе **Опция** указать путь к каталогу и нажать кнопку **OK**:



В результате применения данной политики будет установлен каталог для загрузок, а также будет заблокирована возможность изменения этого каталога пользователем:

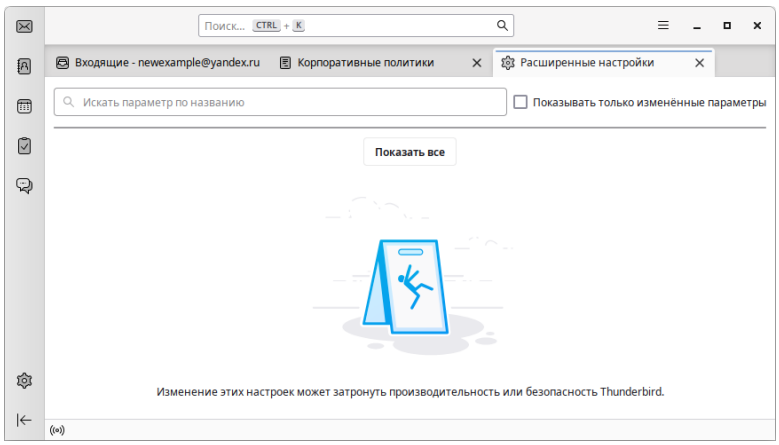


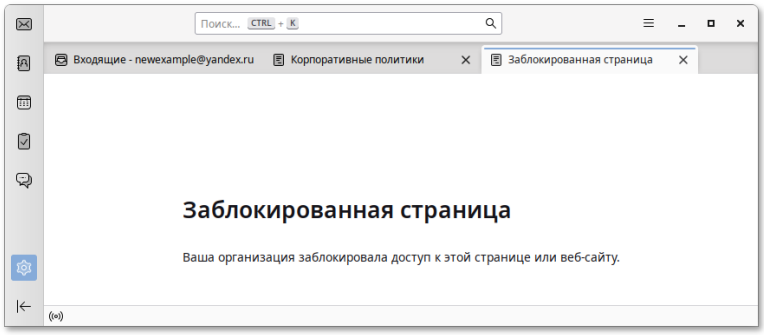
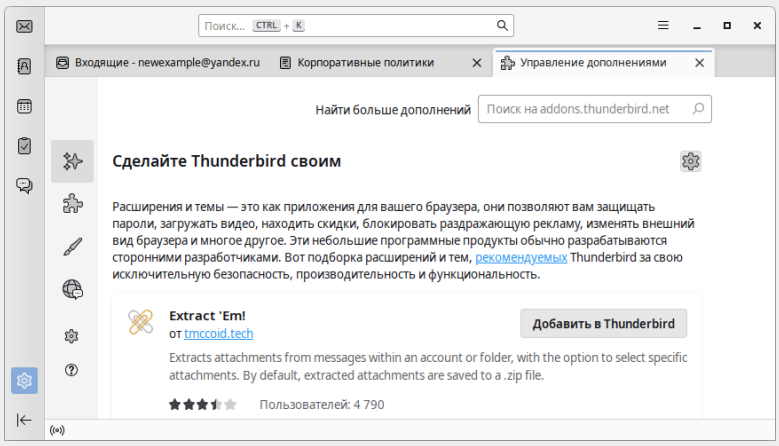
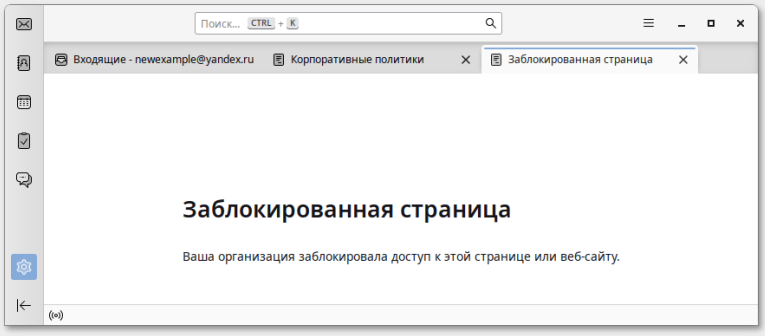
Все настройки политики хранятся в файле **`{GUID GPT}/Machine/Registry.pol`**. Пример файла **`Registry.pol`**:

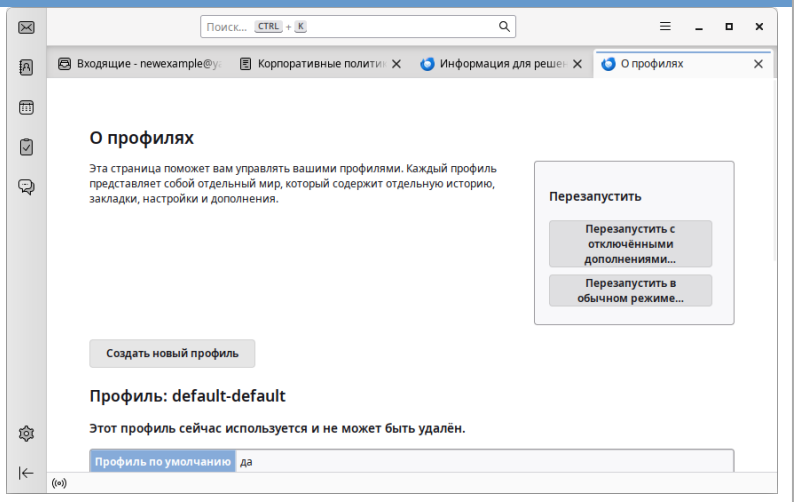
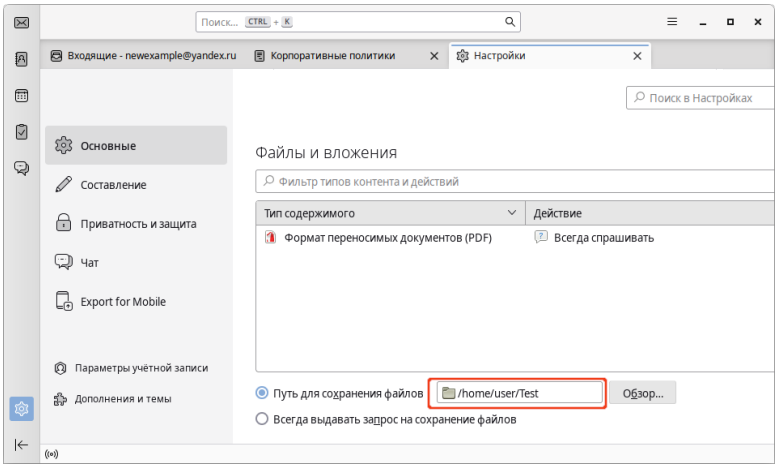
```
PReg
[Software\Policies\Mozilla\Thunderbird;PrimaryPassword;;;]
[Software\Policies\Mozilla\Thunderbird\Proxy;Mode;;;none]
[Software\Policies\Mozilla\Thunderbird\Authentication;Locked;;;]
[Software\Policies\Mozilla\Thunderbird;BlockAboutAddons;;;]
```

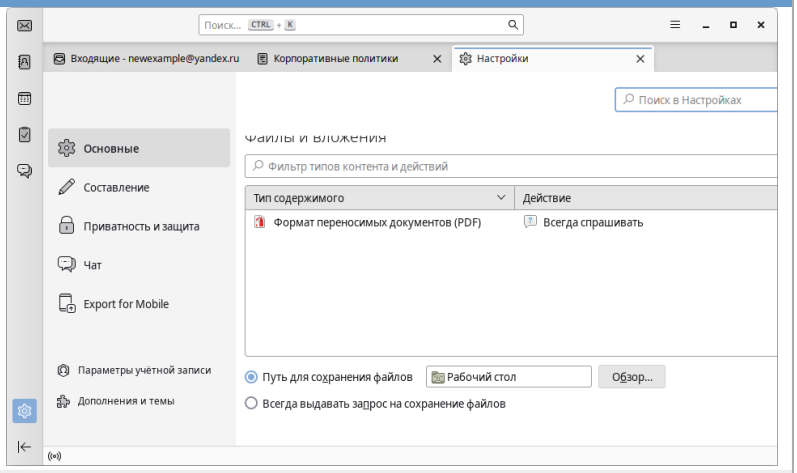
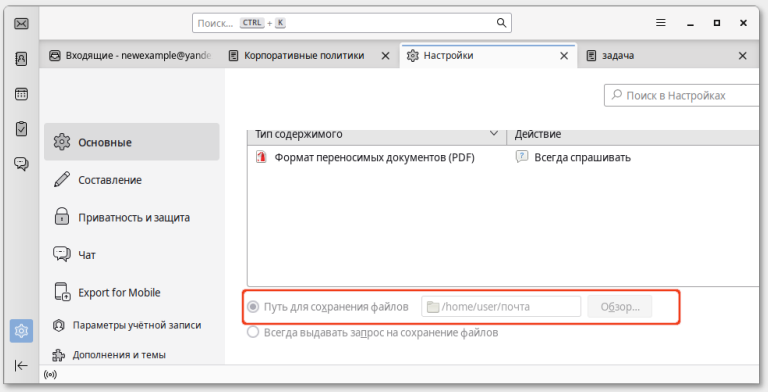
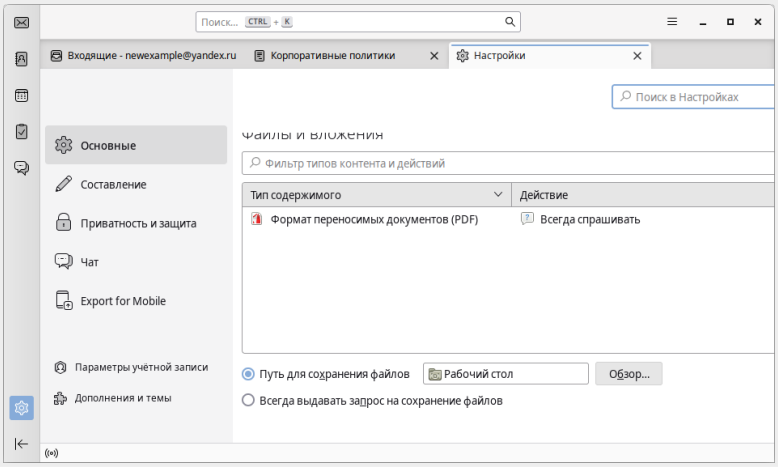
В таблице Настройки почтового клиента Thunderbird описаны только некоторые политики. Полный список политик и их описание можно найти на странице описания шаблонов политик Thunderbird или в почтовом клиенте Thunderbird в разделе **`Корпоративные политики`**.

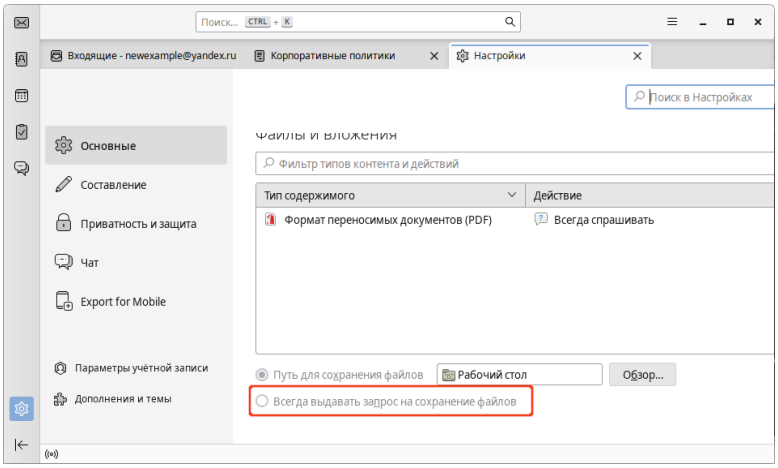
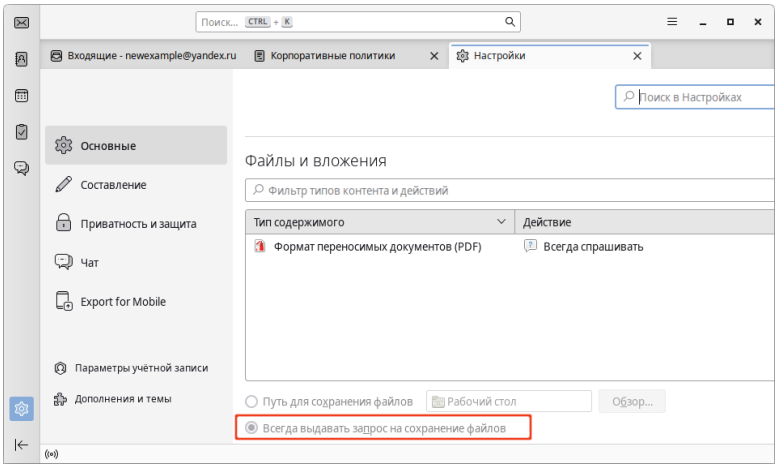
Таблица 29.41. Настройки почтового клиента Thunderbird

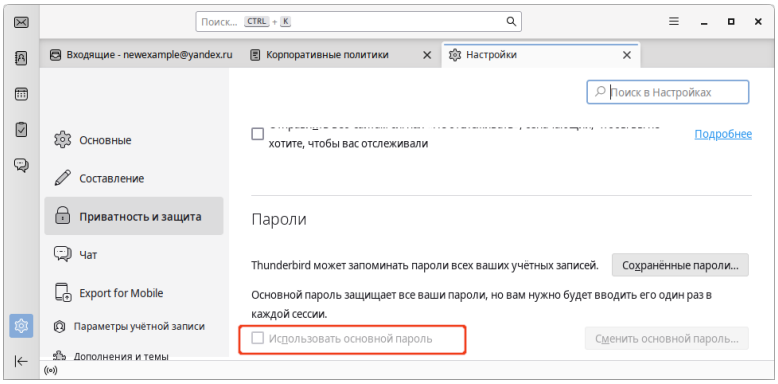
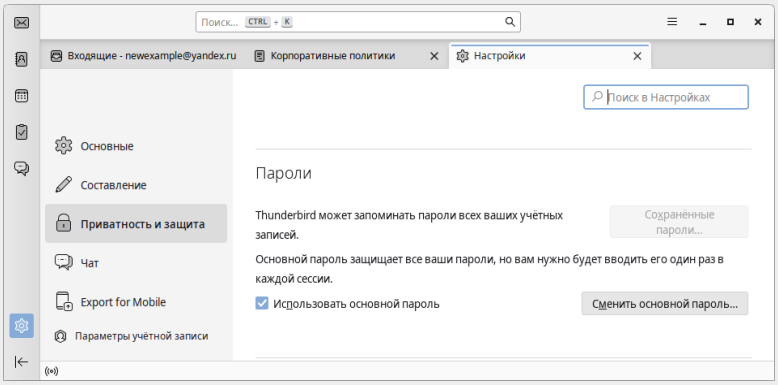
Политика	Ключ	Описание
Блокировка редактора настроек (about:config)	BlockAboutConfig	Блокирует доступ к странице about:config. Если эта политика находится в состоянии **`Отключено`** или **`Не сконфигурировано`**, пользователь может получить доступ к about:config: 

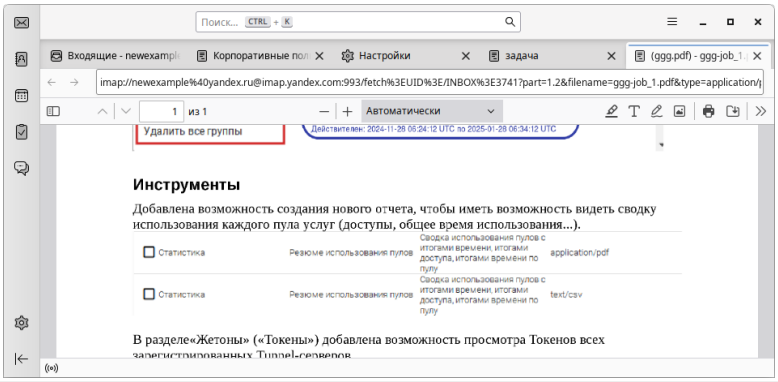
Политика	Ключ	Описание
		Если эта политика находится в состоянии **Включено**, пользователь не может получить доступ к редактору настроек about:config: 
Блокировка менеджера дополнений (about:addons)	BlockAboutAddons	Блокирует доступ к странице about:addons. Если эта политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может получить доступ к менеджеру дополнений и к about:addons:  Если эта политика находится в состоянии **Включено**, пользователь не может получить доступ к менеджеру дополнений или к about:addons: 
Блокировка страницы управления профилями (about:profiles)	BlockAboutProfiles	Блокирует доступ к странице about:profiles. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователь может получить доступ к about:profiles:

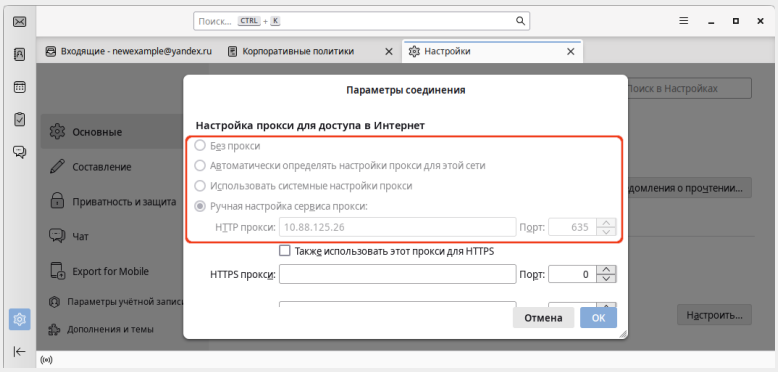
Политика	Ключ	Описание
		 Если политика находится в состоянии **Включено**, пользователь не может получить доступ к about:profiles.
Отключить инструменты разработчика	DisableDeveloperTools	Блокирует доступ к инструментам разработчика. Если политика находится в состоянии **Включено**, инструменты веб-разработчика недоступны в Thunderbird. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, инструменты веб-разработчика доступны в Thunderbird.
Каталог загрузки по умолчанию	DefaultDownloadDirectory	Устанавливает каталог для загрузок по умолчанию (переменную ${home} можно использовать для указания домашнего каталога пользователя). Если политика находится в состоянии **Включено**, можно установить каталог по умолчанию для загрузок:  Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, используется каталог загрузки Thunderbird по умолчанию:

Политика	Ключ	Описание
		
Каталог загрузки	DownloadDirectory	Устанавливает и фиксирует каталог для загрузок (переменную ${home} можно использовать для указания домашнего каталога пользователя). Если политика находится в состоянии **Включено**, можно установить и заблокировать каталог для загрузок:  Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, используется каталог загрузки Thunderbird по умолчанию, и пользователь может его изменить: 
Запрос места загрузки	PromptForDownloadLocation	Позволяет указать должен ли пользователь выбирать каталог для загружаемых файлов.

Политика	Ключ	Описание
		Если политика находится в состоянии **Отключено**, файлы будут сохраняться в каталог, указанный в настройках (пользователю не предлагается указать место для загрузки файла):  Если политика находится в состоянии **Включено**, пользователю будет всегда выдаваться запрос на сохранение файла:  Если политика находится в состоянии **Не сконфигурировано**, пользователю будет выдаваться запрос на сохранение файла, но он может изменить значение по умолчанию.
Основной (главный) пароль	PrimaryPassword	Позволяет установить следует ли требовать или не давать использовать мастер-пароль. Если политика находится в состоянии **Включено**, требуется основной пароль. Если политика находится в состоянии **Отключено** пользователи не могут создать основной пароль.

Политика	Ключ	Описание
		Если политика находится в состоянии **Не сконфигурировано**, пользователи могут создать основной пароль.
Отключить создание мастер-пароля	DisableMasterPasswordCreation	Позволяет отключить возможность установить мастер-пароль (основной пароль). Если эта политика находится в состоянии **Включено**, пользователи не могут создать мастер-пароль:  Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, пользователи могут создать мастер-пароль. Если используются и политика «Отключить создание мастер-пароля», и «Основной (главный) пароль», то политика **Отключить создание мастер-пароля** имеет приоритет.
Менеджер паролей	PasswordManagerEnabled	Позволяет запретить доступ к менеджеру паролей через настройки и блокировать about:logins. Если политика находится в состоянии **Отключено**, менеджер паролей недоступен в настройках:  Если политика находится в состоянии **Включено** или **Не сконфигурировано**, менеджер паролей доступен в настройках.

Политика	Ключ	Описание
Отключить встроенную программу просмотра PDF (PDF.js)	DisableBuiltinPDFViewer	Отключает PDF.js, встроенный просмотрщик PDF в Thunderbird. Если политика находится в состоянии **Включено**, файлы PDF не просматриваются в Thunderbird. Встроенный просмотрщик PDF отключается, PDF-файлы загружаются и отправляются во внешнюю среду. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, файлы PDF просматриваются в Thunderbird: 
Настройка параметров прокси-сервера		
Connection Type (Тип подключения)	Proxy/Mode	Позволяет указать тип подключения. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Thunderbird по умолчанию использует системный прокси-сервер. Если политика находится в состоянии **Включено**, можно задать тип подключения: - **Без прокси** (none) - **Использовать настройки системного прокси** (system) - **Настройка прокси вручную** (manual) - **Автоопределение настроек прокси** (autoDetect) - **Автоматическая конфигурация прокси** (autoConfig)
HTTP Proxy	Proxy/ HTTPProxy	Позволяет указать настройки HTTP Proxy. Если политика находится в состоянии **Включено**, можно задать HTTP-прокси, используемый при указании ручной конфигурации прокси. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Thunderbird не использует HTTP-прокси.
HTTPS Proxy	Proxy/ HTTPSProxy	Позволяет указать настройки HTTPS Proxy.

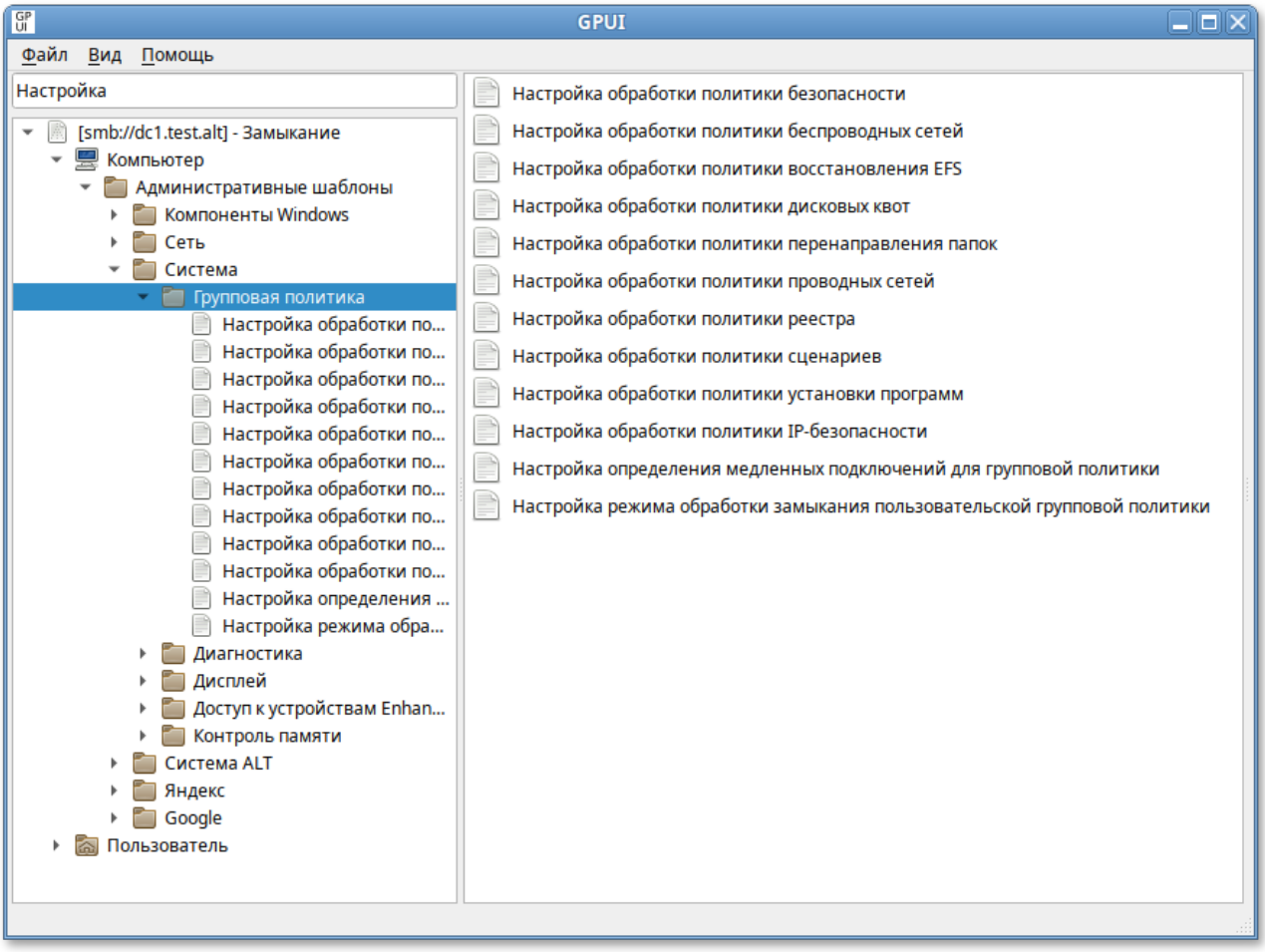
Политика	Ключ	Описание
		Если политика находится в состоянии **Включено**, можно задать HTTPS-прокси, используемый при указании ручной конфигурации прокси. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Thunderbird не использует HTTPS-прокси.
Do not allow proxy settings to be changed (Не разрешать изменять настройки прокси-сервера)	Proxy/Locked	Позволяет заблокировать настройки прокси-сервера. Если политика находится в состоянии **Включено**, настройки прокси-сервера не могут быть изменены пользователем:  Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, настройки прокси-сервера могут быть изменены пользователем.
Use HTTP proxy for HTTPS (Использовать HTTP-прокси для HTTPS)	Proxy/ UseHTTPProxyForAllProtocols	Позволяет указать, что для HTTPS следует использовать настройки HTTP-прокси. Если политика находится в состоянии **Включено**, HTTP-прокси используется для HTTPS, когда указана ручная настройка прокси. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Thunderbird не использует HTTPS-прокси, если не указано иное.
Do not prompt for authentication if password is saved (Не запрашивать аутентификацию, если пароль сохранен)	Proxy/AutoLogin	Позволяет указать не запрашивать аутентификацию, если пароль сохранен. Если политика находится в состоянии **Включено**, Thunderbird не будет запрашивать аутентификацию прокси при сохранении пароля. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, Thunderbird всегда будет запрашивать аутентификацию прокси.
Proxy Passthrough	Proxy/ Passthrough	Позволяет указать исключения (адреса, для которых не используется прокси).

Политика	Ключ	Описание
		Если политика находится в состоянии **Включено**, для указанных адресов настройки прокси-сервера не используются. Если политика находится в состоянии **Отключено** или **Не сконфигурировано**, исключения не используются.

29.5.14. Политика замыкания

Описание политики замыкания см. в разделе Замыкание групповой политики.

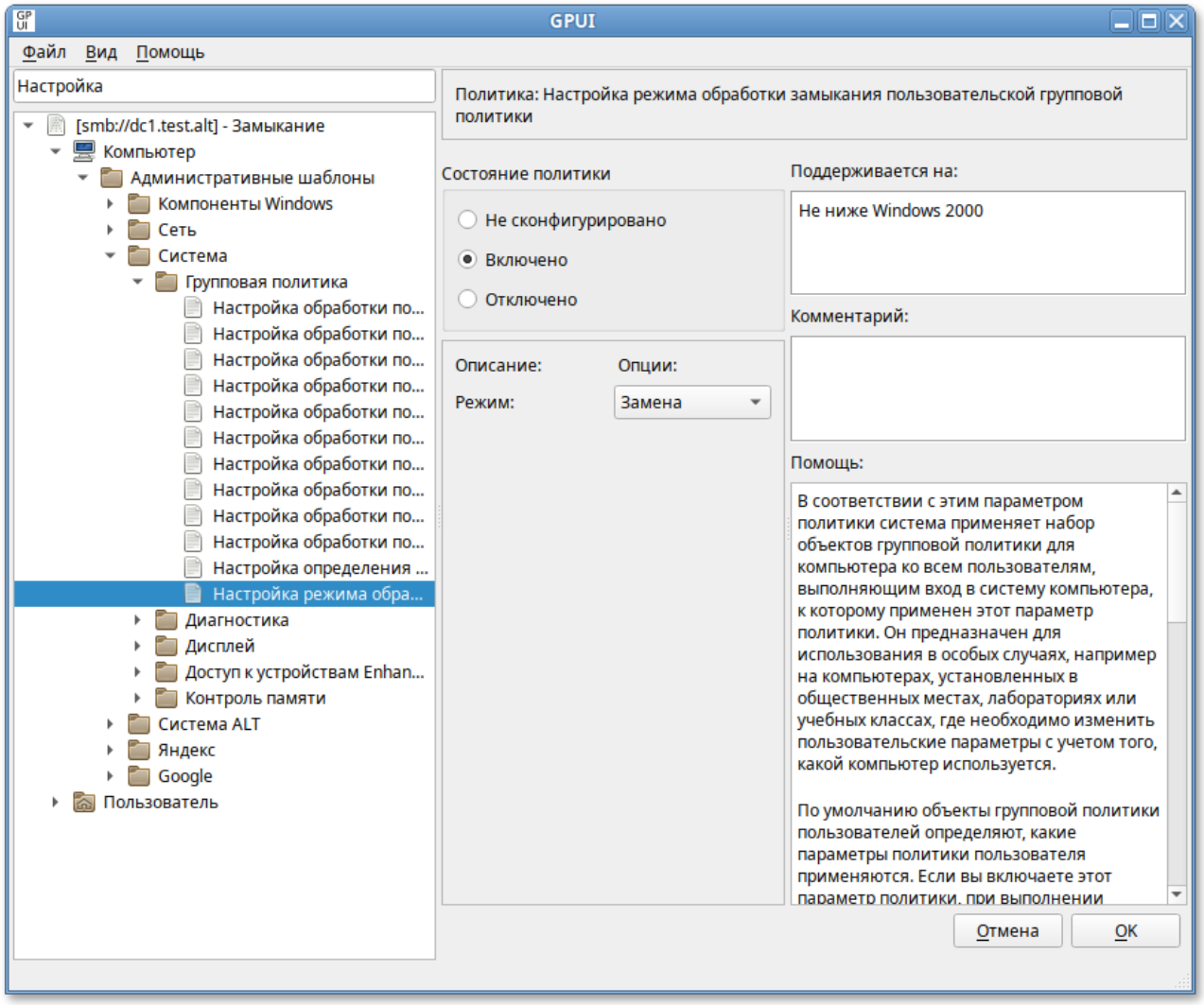
Для настройки этой политики следует перейти в **Компьютер → Административные шаблоны → Система → Групповая политика**:



Примечание

Для быстрого доступа к политике можно ввести в поле **Поиск…** ключевое слово.

Щелкнуть левой кнопкой мыши на политике **Настройка режима обработки замыкания пользовательской групповой политики**, откроется диалоговое окно настройки политики. Можно не задавать настройку политики, включить или отключить:



Если выбрать параметр **Включено**, в разделе **Опции** в выпадающем списке можно выбрать режим:

- **Слияние** — указывает, что параметры политики пользователя определенные в объектах групповой политики компьютера, и обычно применяемые параметры пользователя для этого пользователя должны быть объединены. Если возникает конфликт этих параметров политики, то параметры пользователя в объектах групповой политики компьютера имеют приоритет над обычными параметрами пользователя;

- **Замена** — указывает, что параметры политики пользователя, определенные в объектах групповой политики компьютера, заменяют параметры политики пользователя, обычно применяемые для этого пользователя.

Если выбрать параметр **Отключено** или не настраивать этот параметр политики, порядок применения параметров определяется объектами групповой политики для пользователей.

29.6. Редактирование предпочтений

Примечание

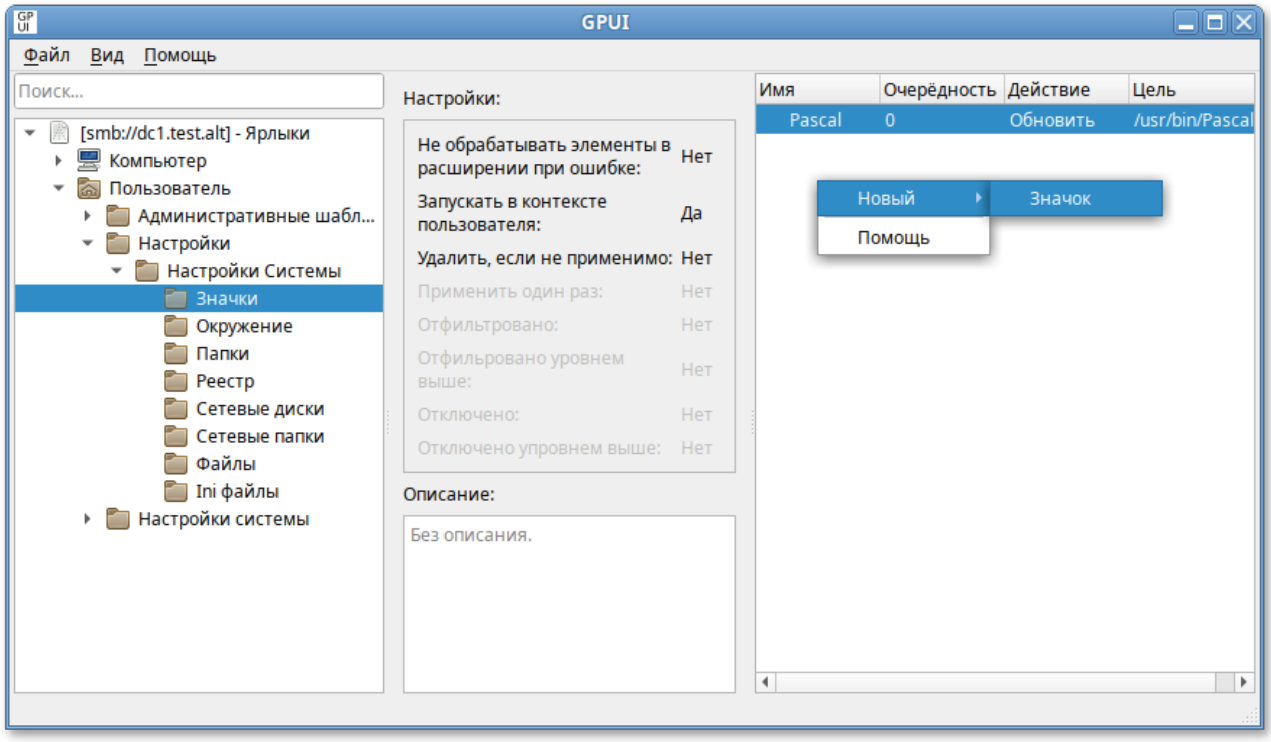
Если параметр предпочтения настраивается в секции **Компьютер**, групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном OU с компьютерами или пользователями.

29.6.1. Управление ярлыками

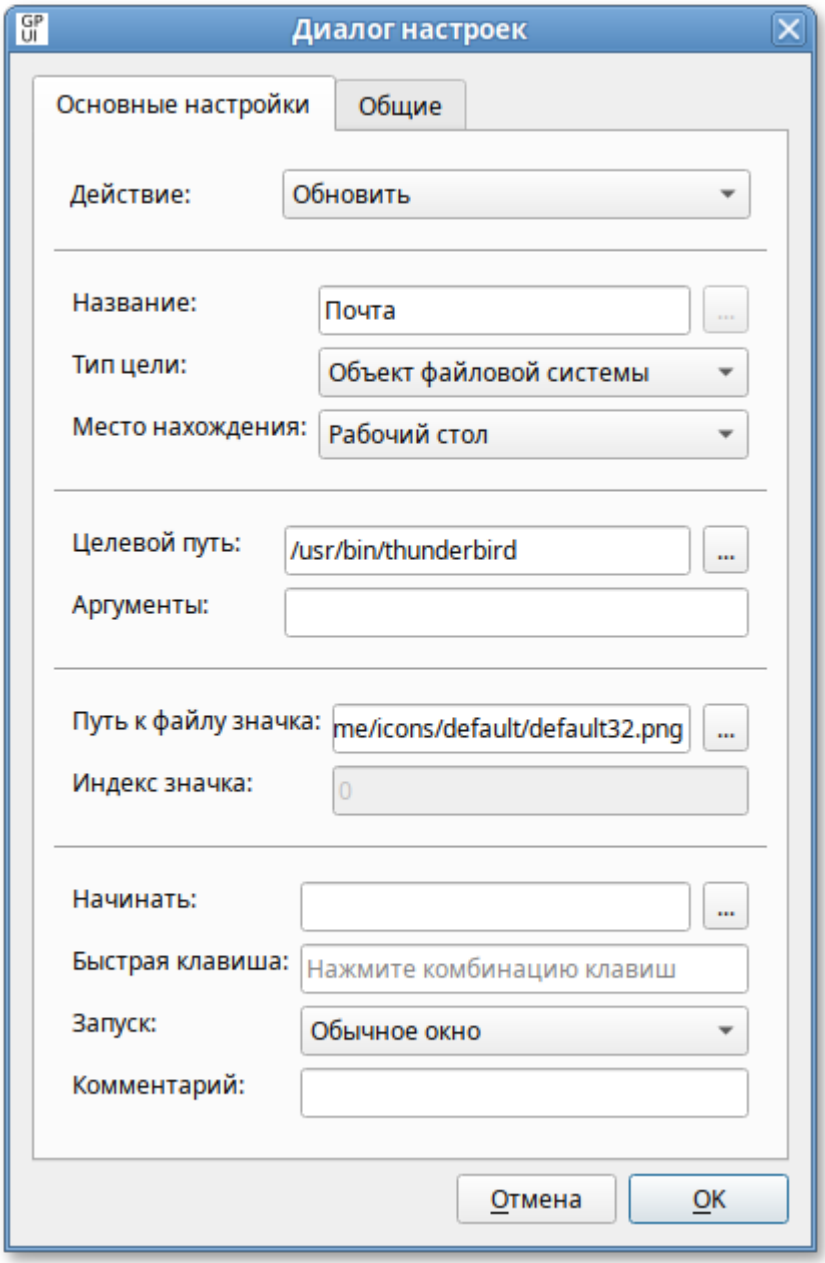
Групповая политика **Управление ярлыками** позволяет централизованно для компьютеров или пользователей:

- создавать ярлыки;
- удалять ярлыки;
- изменять свойства ярлыков.

Для настройки этой политики следует перейти в **Компьютер/Пользователь → Настройки → Настройки системы → Значки**. В контекстном меню свободной области выбрать пункт **Новый → Значок**



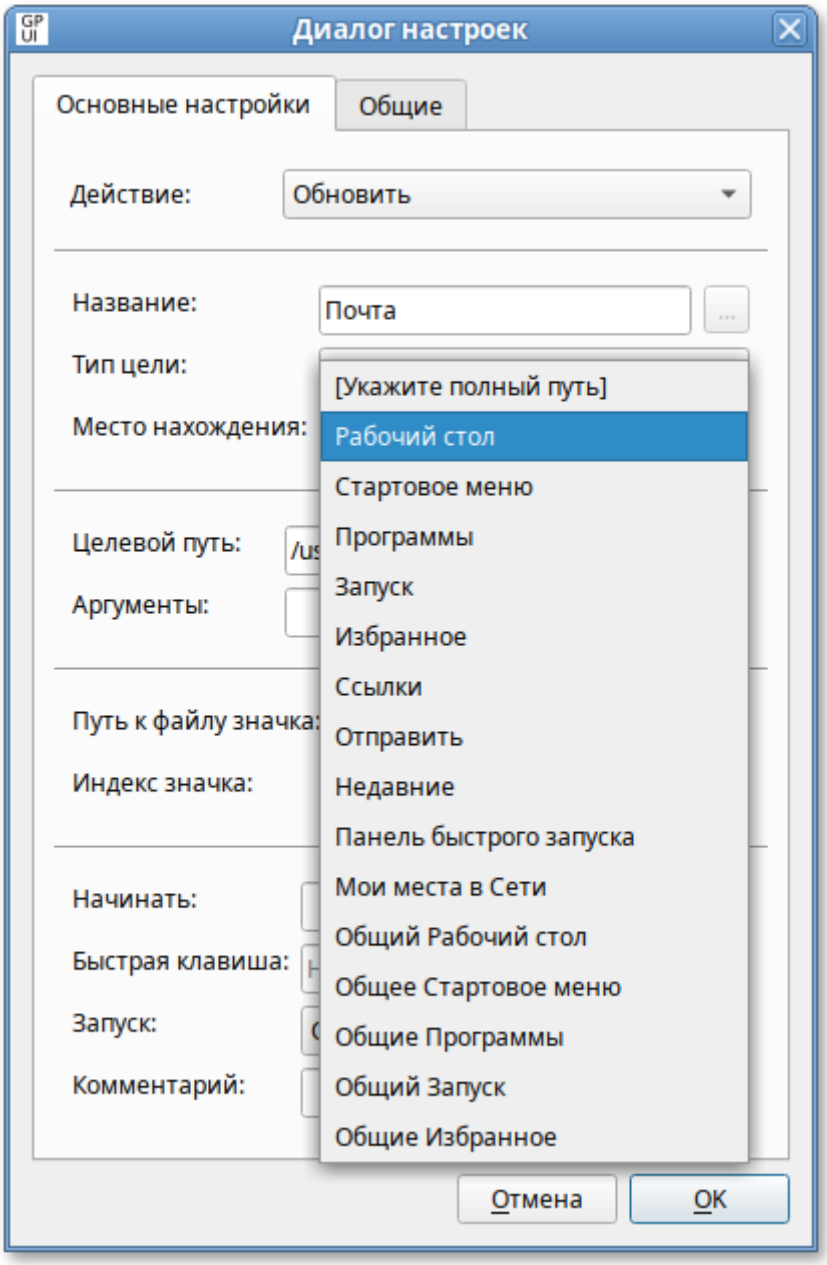
В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **Основные настройки**:

- **Действие** — действие, которое будет выполняться для ярлыка:
  - **Создать** — создание нового ярлыка;
  - **Удалить** — удаление ярлыка;
  - **Заменить** — удаление и повторное создание ярлыка. Если ярлык не существует, то это действие создает новый ярлык;
  - **Обновить** — изменение параметров существующего ярлыка. Если ярлык не существует, то это действие создает ярлык. Это действие отличается от **Заменить** тем, что не удаляет ярлык, а только обновляет параметры ярлыка, определенные в элементе настройки;
- **Название** — отображаемое имя для ярлыка. При изменении или удалении ярлыка имя должно совпадать с именем существующего ярлыка;

- **Тип цели** — тип конечного объекта, на который указывает ярлык (при изменении или удалении ярлыка выбранный тип объекта должен соответствовать существующему ярлыку):
  - **Объект файловой системы** — путь в ФС, например, файл, папка, диск, общий ресурс или компьютер;
  - **URL-адрес** — URL-адрес, например, веб-сайт;
  - **Объект оболочки** — объект, например, принтер, элемент рабочего стола или панели управления, файл, папка, общий ресурс, компьютер или сетевой ресурс;
- **Место нахождения** — место, где ярлык должен отображаться на компьютерах, для которых применяется политика. Размещения, отличные от **Общее…**, относятся к текущему пользователю. При изменении существующего ярлыка выбранное размещение должно совпадать с размещением существующего ярлыка. Если выбран пункт **Укажите полный путь**, то место задается полным путем в поле **Название** (при этом можно использовать переменные, например, чтобы разместить ярлык с именем **Почта** в подпапке **Ярлыки** в **Program Files**, необходимо ввести *%ProgramFilesDir%\Ярлыки\Почта*). Чтобы разместить ярлык в подпапке для выбранного размещения из списка, следует указать *<название подпапки>\<имя ярлыка>* в поле **Название**, например, чтобы разместить ярлык с именем **Почта** в подпапке **Ярлыки** в размещении **Рабочий стол**, необходимо ввести *Ярлыки/Почта* в поле **Название** и выбрать **Рабочий стол** в поле **Место нахождения**:



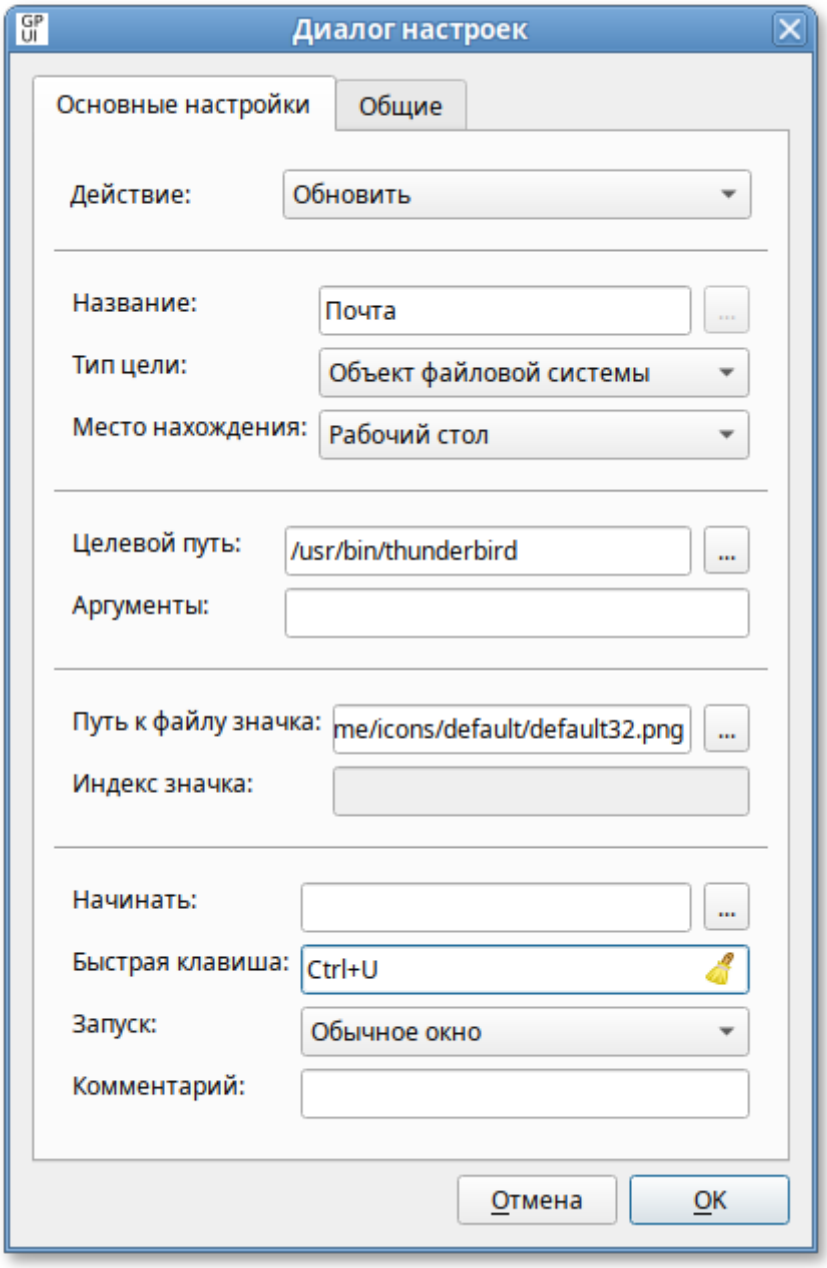
- **Целевой путь** — локальный путь (с точки зрения клиента) для типа **Объект файловой системы**, URL для типа **URL-адрес** или объект для типа **Объект оболочки**. Если выбран тип цели **Объект файловой системы** или **URL-адрес**, то это поле может принимать переменные. Это поле недоступно, если выбрано действие **Удалить**;

- **Аргументы** — аргументы, которые будут использоваться при открытии целевого файла или папки. Это поле доступно только в том случае, если выбран тип цели **Объект файловой системы**, и выбрано действие **Создать**, **Заменить** или **Обновить**;

- **Путь к файлу значка** и **Индекс значка** — значок для ярлыка. Для указания значка, отличного от значка по умолчанию необходимо выбрать значок или ввести полный путь к значку (с точки зрения клиента) и указать индекс значка. Поле **Путь к файлу значка** принимает переменные. Эти поля недоступны, если выбрано действие **Удалить**;

- **Начинать** — рабочий каталог, содержащий файлы, необходимые для конечного объекта. Это поле принимает переменные. Поле доступно в случае, если выбрано действие **Создать**, **Заменить** или **Обновить**;

- **Быстрая клавиша** — сочетание клавиш для запуска ярлыка. Чтобы назначить сочетание клавиш следует установить курсор в поле **Быстрая клавиша** и нажать комбинацию клавиш. Это поле недоступно, если выбрано действие **Удалить**. Чтобы удалить сочетание клавиш, можно нажать клавишу **CTRL** или **ALT**, или нажать на значок, расположенный справа от сочетания клавиш:



- **Запуск** — размер окна, в котором нужно открыть цель ярлыка. Поле доступно только в том случае, если выбран тип объекта **Объект файловой системы** или **Объект оболочки**, и выбрано действие **Создать**, **Заменить** или **Обновить**;

- **Комментарий** — всплывающая подсказка, когда указатель мыши приостановлен на ярлыке. Поле принимает переменные. Поле доступно только в том случае, если выбран тип объекта **Объект файловой системы** или **Объект оболочки**, и выбрано действие **Создать**, **Заменить** или **Обновить**.

Предупреждение

Чтобы ярлыку назначались корректные права (для пользовательской политики), необходимо установить отметку в пункте **Выполнять в контексте безопасности текущего пользователя** на вкладке **Общие**.

Все настройки политики управления ярлыками хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/Shortcuts/Shortcuts.xml**
- **{GUID GPT}/User/Preferences/Shortcuts/Shortcuts.xml**

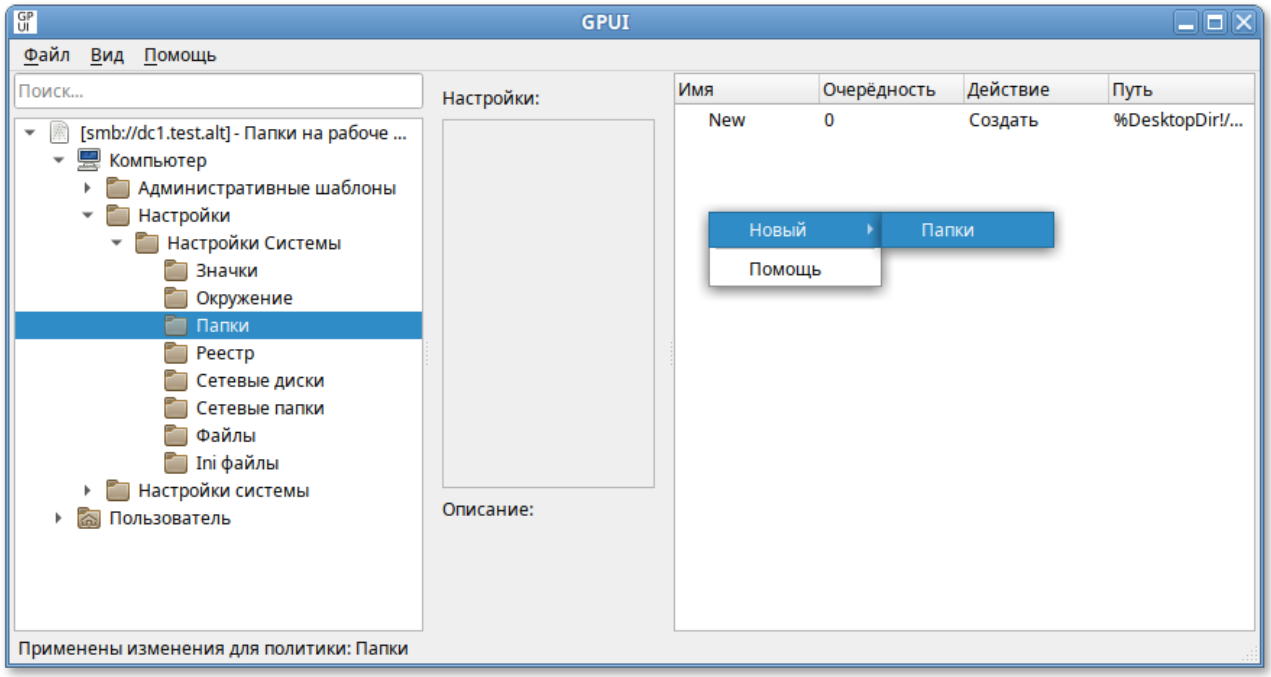
Пример файла **Shortcuts.xml**:

```
<?xml version="1.0" encoding="utf-8"?>
<Shortcuts clsid="{872ECB34-B2EC-401b-A585-D32574AA90EE}">
<Shortcut bypassErrors="0"
    changed="2022-11-17 11:07:40"
    clsid="{4F2F7C55-2790-433e-8127-0739D1CFA327}"
    desc=""
    image="0"
    name="Почта"
    removePolicy="0"
    status=""
    uid="{dfd45a36-4634-47d9-8a22-5f702fba21bc}"
    userContext="0">
<Properties
    action="U"
    arguments=""
    comment=""
    iconPath="/usr/lib64/thunderbird/chrome/icons/default/default32.png"
    pidl=""
    shortcutPath="%DesktopDir%\Почта"
    startIn=""
    targetPath="/usr/bin/thunderbird"
    targetType="FILESYSTEM"
    window=""/>
</Shortcut>
</Shortcuts>
```

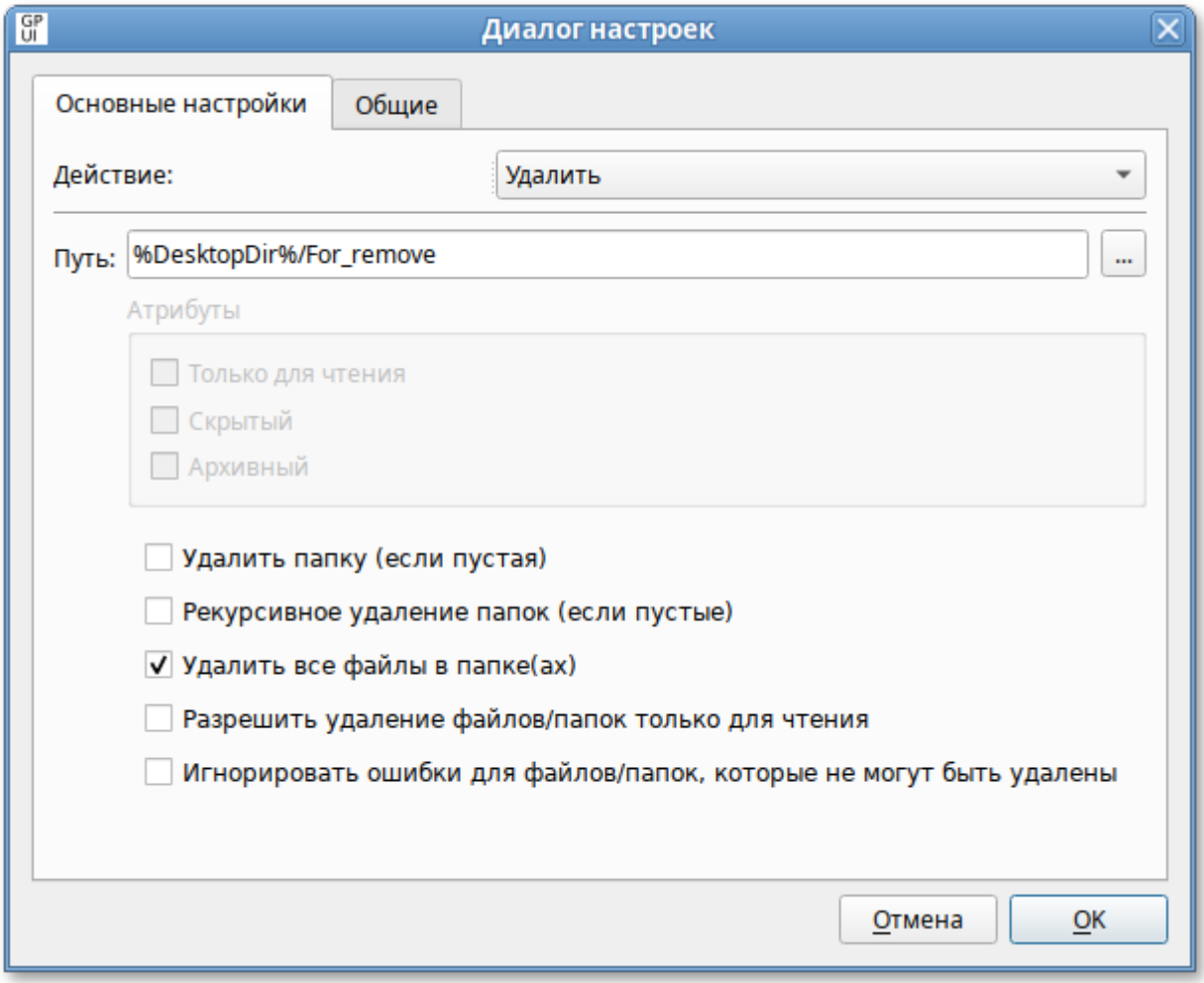
29.6.2. Управление каталогами

Групповая политика **Управление каталогами** позволяет для всех пользователей заданной группы создавать унифицированную структуру каталогов.

Для настройки этой политики следует перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы** → **Папки**. В контекстном меню свободной области выбрать пункт **Новый** → **Папки**



В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **Основные настройки**:

- **Действие** — действие, которое будет выполняться для папки:
  - **Создать** — создание новой папки;
  - **Удалить** — удаление папки;
  - **Заменить** — удаление и повторное создание папки. В результате выполнения действия **Заменить** содержимое существующей папки удаляется, и все существующие параметры папки перезаписываются. Если папка не существует, действие **Заменить** создает новую папку;
  - **Обновить** — изменение параметров существующей папки. Если папки не существует, то это действие создает новую папку. Это действие отличается от **Заменить** тем, что не удаляет папку, а только обновляет параметры;
- **Путь** — путь к папке (с точки зрения клиента). Это поле может содержать переменные (не следует вводить кавычки и завершающую косую черту);

Примечание

Список допустимых переменных (для систем «Альт»):
- машинные:
  - %HOME%, %HOMEPATH% — каталог **/etc/skel**;
  - %HOMEDRIVE%, %SystemRoot%, %SystemDrive% — корневой каталог (**/**);
  - %StartMenuDir% — каталог **/usr/share/applications**;
- пользовательские:
  - %LogonUser% — имя текущего пользователя (username);
  - %HOME%, %HOMEPATH% — домашний каталог текущего пользователя (**get_homedir(username)**);
  - %DesktopDir% — рабочий стол текущего пользователя (**get_desktop(username, variables['HOME'])**).

- **Атрибуты** — атрибуты файловой системы для папки (недоступны для действия **Удалить**):
  - **Только для чтения**;
  - **Скрытый**;
  - **Архивный**;

Следующие опции доступны только для действий **Заменить** и **Удалить**:

- **Удалить папку (если пустая)** — если включена эта опция, папка, указанная в поле **Путь**, удаляется, если она пуста. Пустая ли эта папка, оценивается после того, как были обработаны опции **Удалить все файлы в папке(ах)** и **Рекурсивное удаление папок (если пустые)**. При выборе действия **Удалить** эта опция включена по умолчанию и её невозможно отключить;
- **Рекурсивное удаление папок (если пустые)** — если включена эта опция, удаляется самый низкий уровень вложенных папок (если они пусты). Данное действие повторяется для каждой родительской папки до достижения папки, указанной в поле **Путь**. Пустые подпапки оцениваются после обработки опции **Удалить все файлы в папке(ах)**;

- **Удалить все файлы в папке(ах)** — если включена эта опция, удаляются все файлы в папке, которые разрешено удалять. Если также включена опция **Рекурсивное удаление папок (если пустые)**, то удаляются также все файлы, которые разрешено удалять во всех подпапках;

- **Разрешить удаление файлов/папок только для чтения** — если включена эта опция, атрибут **Только для чтения** игнорируются для удаляемых файлов и папок;

- **Игнорировать ошибки для файлов/папок, которые не могут быть удалены** — если включена эта опция, подавляются все сообщения об ошибках, возникающие из-за невозможности удаления файлов или папок. В противном случае, если совершается попытка удалить непустую папку, открытый файл, файл или папку, для которых пользователь не имеет разрешений или любой другой файл или папку, которые не могут быть удалены, возвращается ошибка.

Примечание

Атрибуты **Архивный**, **Скрытый** и **Только для чтения** применимы только для Windows систем.

Все настройки политики управления каталогами хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/Folders/Folders.xml**

- **{GUID GPT}/User/Preferences/Folders/Folders.xml**

Пример файла **Folders.xml**:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<Folders clsid="{77CC39E7-3D16-4f8f-AF86-EC0BBEE2C861}">
  <Folder clsid="{07DA02F5-F9CD-4397-A550-4AE21B6B4BD3}"
        name="MyDir"
        status="MyDir"
        image="2"
        bypassErrors="1"
        changed="2020-10-27 11:49:19"
        uid="{57F41C87-4A65-4561-BFFF-4219149DCBF7}">
    <Properties
        action="U"
        path="%DesktopDir%\MyDir"
        readOnly="0"
        archive="1"
        hidden="0"/>
  </Folder>
</Folders>
```

29.6.3. Управление INI-файлами

Групповая политика **Управление INI-файлами** позволяет:

- добавить свойство в файл параметров конфигурации (.ini);

- заменить свойство в INI-файле;

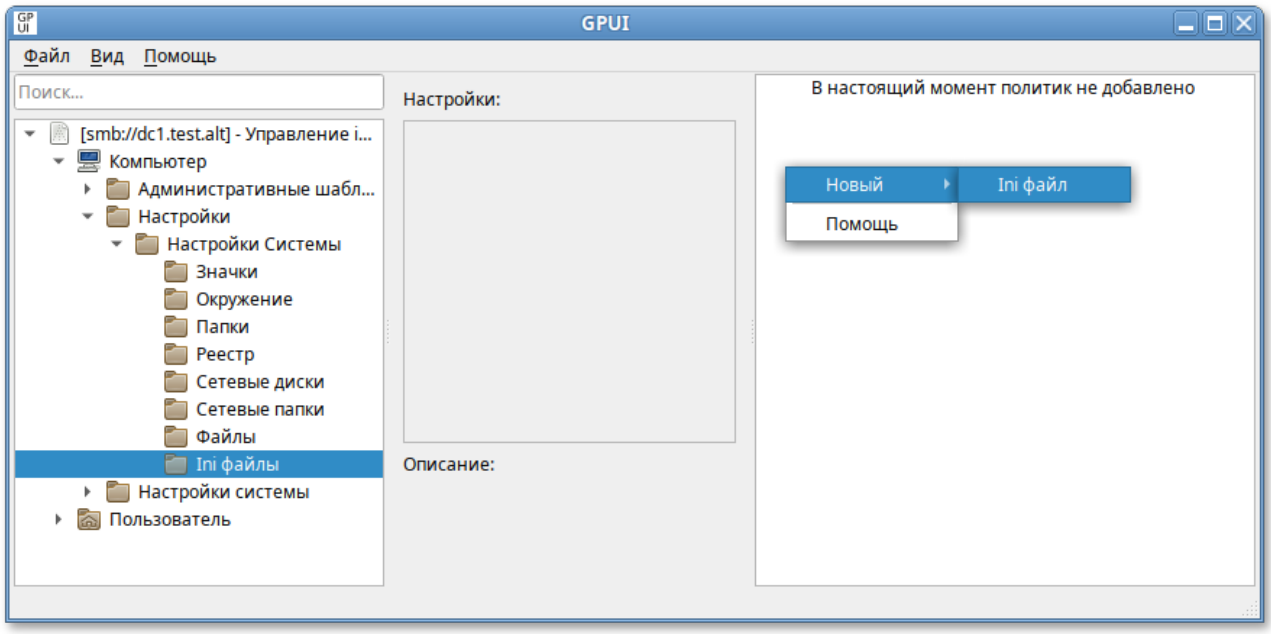
- удалить свойство из INI-файла;

- удалить раздел из INI-файла;
- удалить INI-файл.

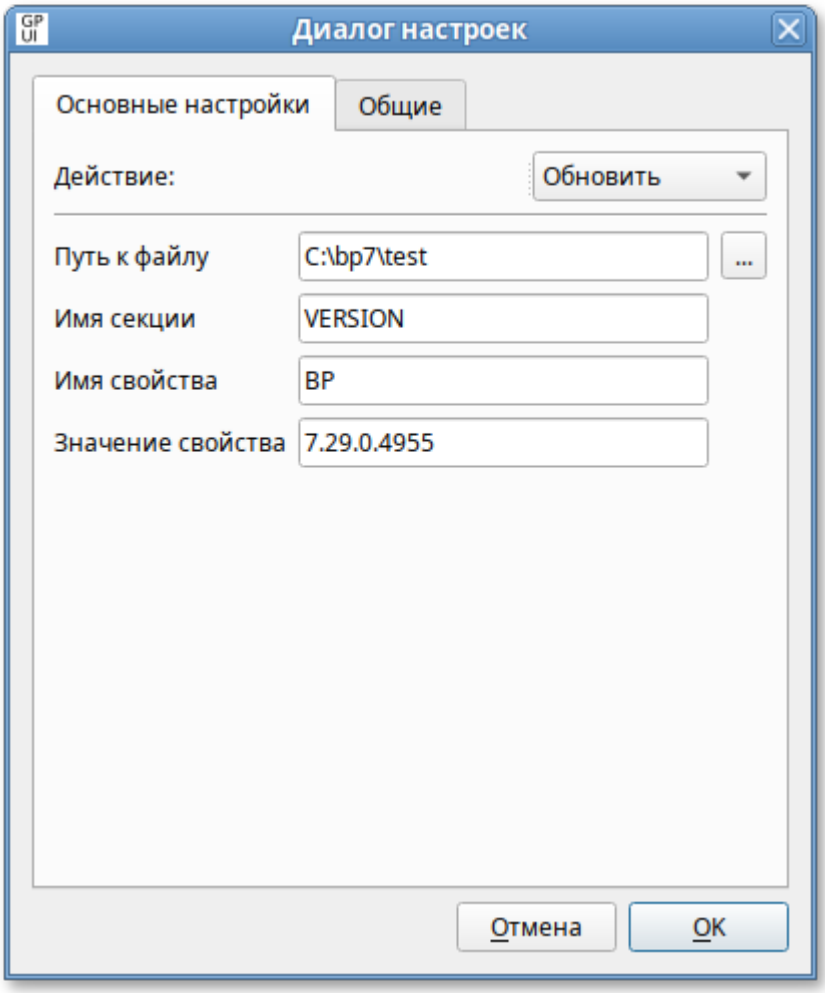
В разделах INI-файлов используется следующий формат:

```
[sectionA]
var01=value01

[sectionB]
var01=value01
var02=value02
```

Для настройки этой политики следует перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы** → **Ini файлы**. В контекстном меню свободной области выбрать пункт **Новый** → **Ini файл**



В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **Основные настройки**:

- **Действие** — действие, которое будет выполняться для INI-файла:
  - **Создать** — добавление свойства в INI-файл. Если файл не существует, он будет создан;
  - **Удалить** — удаление свойства или раздела из INI-файла (либо удаление INI-файла);
  - **Заменить** — удаление и повторное создание свойства в INI-файле. Суммарный итог действия **Заменить** — переопределение свойства. Если свойство не существует, действие **Заменить** создаст его;
  - **Обновить** — удаление и повторное создание свойства в INI-файле (аналогично действию **Заменить**);
- **Путь к файлу** — путь к INI-файлу с точки зрения клиента (путь не должен включать кавычки). Если файл и родительские папки не существуют, они будут созданы;
- **Имя секции** — имя раздела в файле, свойство которого нужно настроить или удалить. Чтобы удалить INI-файл целиком, следует оставить это поле пустым;
- **Имя свойства** — имя свойства, которое нужно настроить или удалить. Чтобы удалить целиком раздел файла или весь файл, следует оставить это поле пустым;

- **Значение свойства** — значение свойства. Значения могут содержать символы кавычек, которые, однако, при чтении значений приложением или операционной системой обычно удаляются. Все значения воспринимаются как текст. Если данное поле оставлено пустым, свойству присваивается пустое значение, что воспринимается как отсутствие свойства. Этот параметр доступен, если выбрано действие **Создать**, **Заменить** или **Обновить**.

Политики управления INI-файлами относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. раздел Экспериментальные групповые политики).

Все настройки политики управления INI-файлами хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/Inifiles/Inifiles.xml**
- **{GUID GPT}/User/Preferences/Inifiles/Inifiles.xml**

Пример файла **Inifiles.xml**:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<IniFiles clsid="{694C651A-08F2-47fa-A427-34C4F62BA207}">
  <Ini changed="2022-11-21 09:13:44"
       clsid="{EEFACE84-D3D8-4680-8D4B-BF103E759448}"
       image="3"
       name="version.ini"
       status="version.ini"
       uid="{ADAA9BCF-C2EA-4004-980F-CEDA823E3B91}"
       bypassErrors="1">
    <Properties
       path="C:\tmp\version.ini"
       section=""
       value=""
       property="BP"
       action="D"/>
  </Ini>
</IniFiles>
```

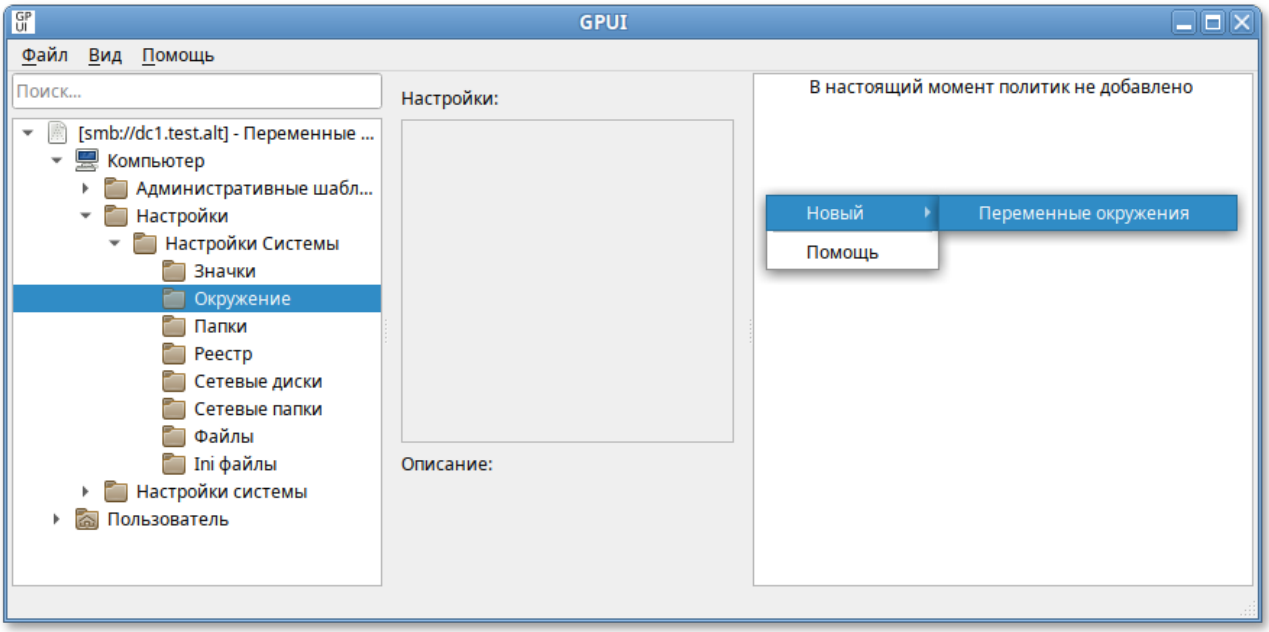
29.6.4. Управление переменными среды

Групповая политика **Управление переменными среды** позволяет централизованно для компьютеров или пользователей:

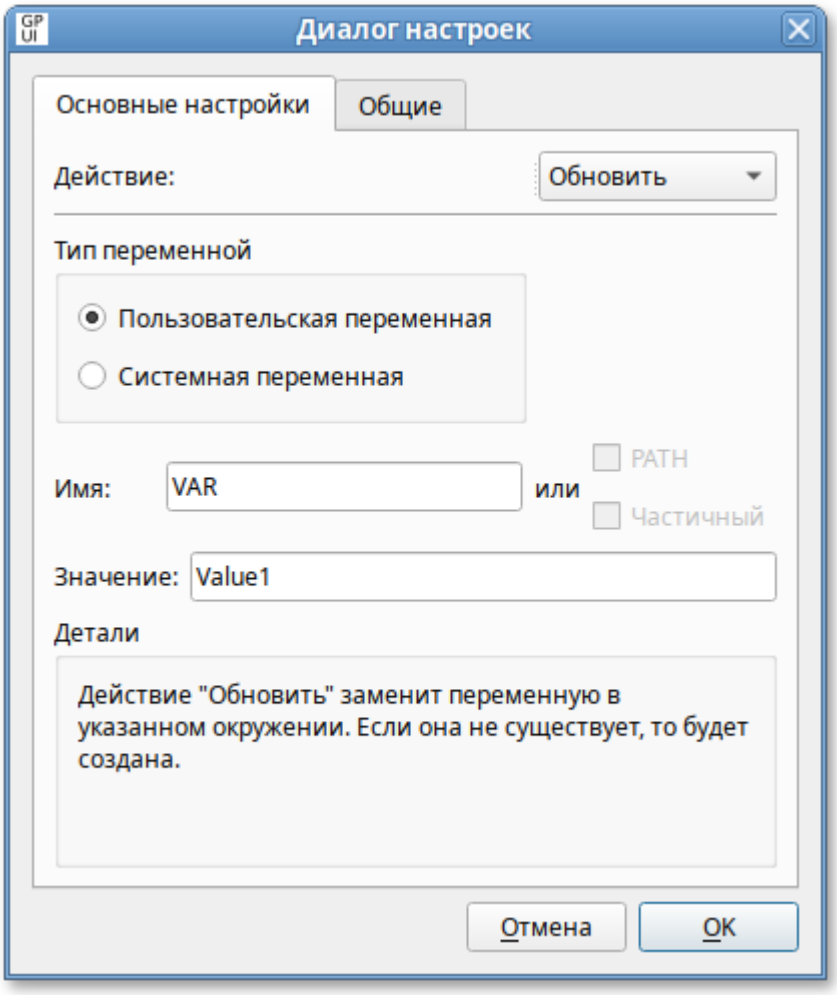
- создать постоянные пользовательские или системные переменные среды;
- удалить переменные среды;
- изменить переменные среды, например:
  - изменить приглашение командной строки (системная переменная PROMPT для Windows или PS1 для Linux (BASH));
  - изменить расположение папки временных файлов (системная переменная TEMP для Windows или TMPDIR для Linux);
  - заменить значение всей переменной PATH;
  - добавить сегменты в переменную PATH (разделенные точкой с запятой для Windows или двоеточием для Linux);

- удалить сегменты из переменной PATH.

Для настройки этой политики следует перейти в **Компьютер/Пользователь → Настройки → Настройки системы → Окружение**. В контекстном меню свободной области выбрать пункт **Новый → Переменные окружения**



В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **Основные настройки**:

- **Действие** — действие, которое будет выполняться для переменной среды:
  - **Создать** — создание новой переменной среды (если переменная среды с таким именем уже есть, например, создана локально, то её значение изменено не будет);
  - **Удалить** — удаление переменной среды;
  - **Заменить** — удаление и повторное создание переменной среды (если переменная среды с таким именем не существует, то это действие создаёт новую переменную среды);
  - **Обновить** — изменение параметров существующей переменной среды. Если переменная среды с таким именем не существует, то это действие создает новую переменную среды (фактически это действие полностью аналогично действию **Заменить**). Применение этого действия к сегменту переменной PATH не имеет практического эффекта; в этом сегменте возможно только изменение регистра текста;
- **Пользовательская переменная**:
  - параметр для переменной среды в разделе **Конфигурация пользователя** — влияние переменной среды будет для каждого пользователя независимым. Переменная среды хранится в разделе реестра HKEY_CURRENT_USER;
  - параметр для переменной среды в разделе **Конфигурация компьютера** — переменная среды будет влиять только на пользователя компьютера по умолчанию;

- **Системная переменная** — переменная среды будет влиять на всех пользователей компьютера. Переменная среды будет храниться в реестре в разделе HKEY_LOCAL_MACHINE;

- **Имя** — имя переменной среды, к которой применяется действие. Чтобы выбрать переменную PATH, следует оставить это поле пустым;

- **Значение** — значение переменной среды. В это поле можно вводить переменные;

- **PATH** — действие будет применяться к переменной PATH: можно создать/заменить значение переменной PATH или добавить/удалить сегмент значения переменной PATH. В поле **Имя** будет отмечено значение «PATH» и оно не будет доступно для редактирования. Эта опция доступна только в том случае, если выбран параметр **Системная переменная**;

- **Частичный** — добавить или удалить один сегмент переменной PATH. Эта опция доступна только в том случае, если выбраны **Системная переменная** и **PATH**.

Все настройки политики управления переменными среды хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/EnvironmentVariables/EnvironmentVariables.xml**

- **{GUID GPT}/User/Preferences/EnvironmentVariables/EnvironmentVariables.xml**

Пример файла **EnvironmentVariables.xml**:

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<EnvironmentVariables clsid="{BF141A63-327B-438a-B9BF-2C188F13B7AD}">
  <EnvironmentVariable clsid="{78570023-8373-4a19-BA80-2F150738EA19}"
        name="VAR"
        status="VAR = value_1"
        image="0"
        changed="2020-06-05 12:16:20"
        uid="{6738058D-5455-4D9A-9B84-78E87DDD18D7}"
        desc="environment variable example"
        bypassErrors="1">
    <Properties
        action="C"
        name="VAR"
        value="value_1"
        user="1"
        partial="0"/>
  </EnvironmentVariable>
  <EnvironmentVariable clsid="{78570023-8373-4a19-BA80-2F150738EA19}"
        name="PATH"
        status="PATH = value_2"
        image="2"
        changed="2020-06-05 12:16:48"
        uid="{15E854D6-C338-4AD2-BF8D-72292B364BA3}">
    <Properties
        action="U"
        name="PATH"
        value="value_2"
        user="0"
        partial="1"/>
  </EnvironmentVariable>
</EnvironmentVariables>
```

Примечание

Для того чтобы политики применились (под доменным пользователем), необходимо перелогиниться.

Проверить наличие переменных окружения можно, выполнив команду:

```
$ env |grep имя_переменной
```

Просмотреть все переменные, назначенные с помощью групповой политики, можно в файле **/etc/gpupdate/environment**:

```
TEMP DEFAULT="C:\tmp"
Var DEFAULT="Value1"
HTTPS_PROXY DEFAULT="https://10.0.66.52:3128"
```

29.6.5. Управление файлами

Групповая политика **Файлы** позволяет проводить операции с файлами: копировать файлы в нужное расположение, удалять, заменять, обновлять атрибуты файлов.

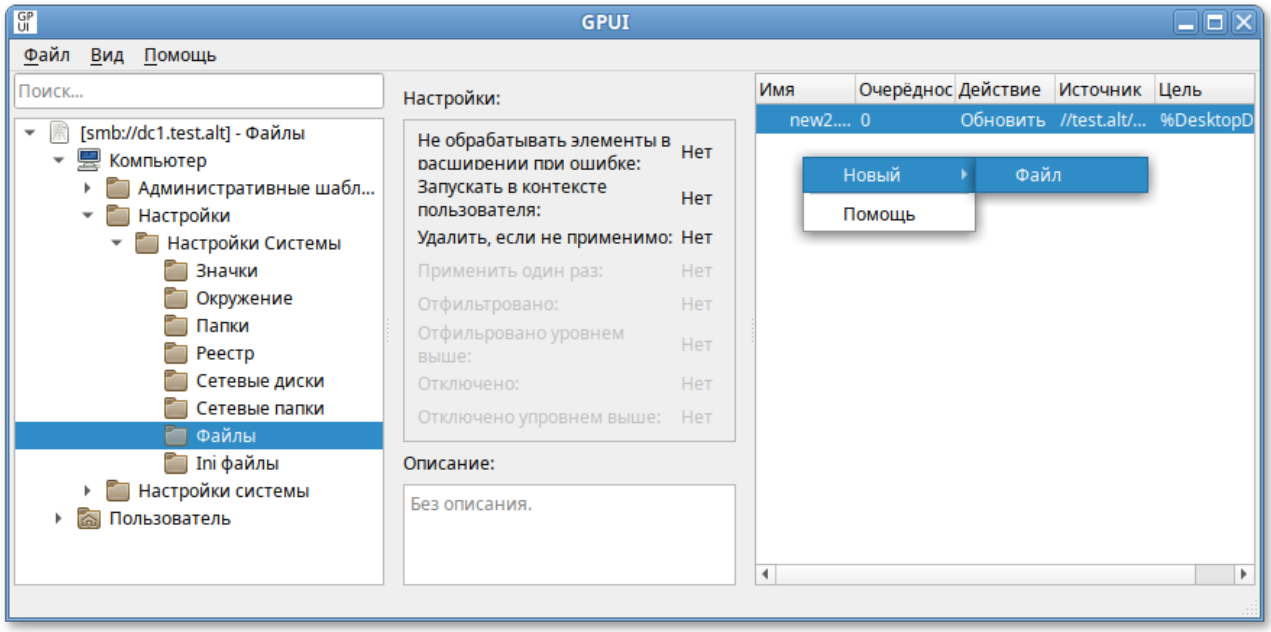
Для компьютеров или пользователей эта политика предоставляет возможность:

- копировать файл (или несколько файлов из одного каталога) в новое место, а затем настроить атрибуты этих файлов;
- удалить файл (или несколько файлов в одном каталоге;
- удалить файл (или несколько файлов в одном каталоге) и заменить его копией файла из исходного каталога;
- изменить атрибуты файла (или нескольких файлов в одном каталоге);
- изменить атрибуты, заменить или удалить все файлы с определённым расширением в одном каталоге;
- изменить атрибуты, заменить или удалить все файлы в определённом каталоге.

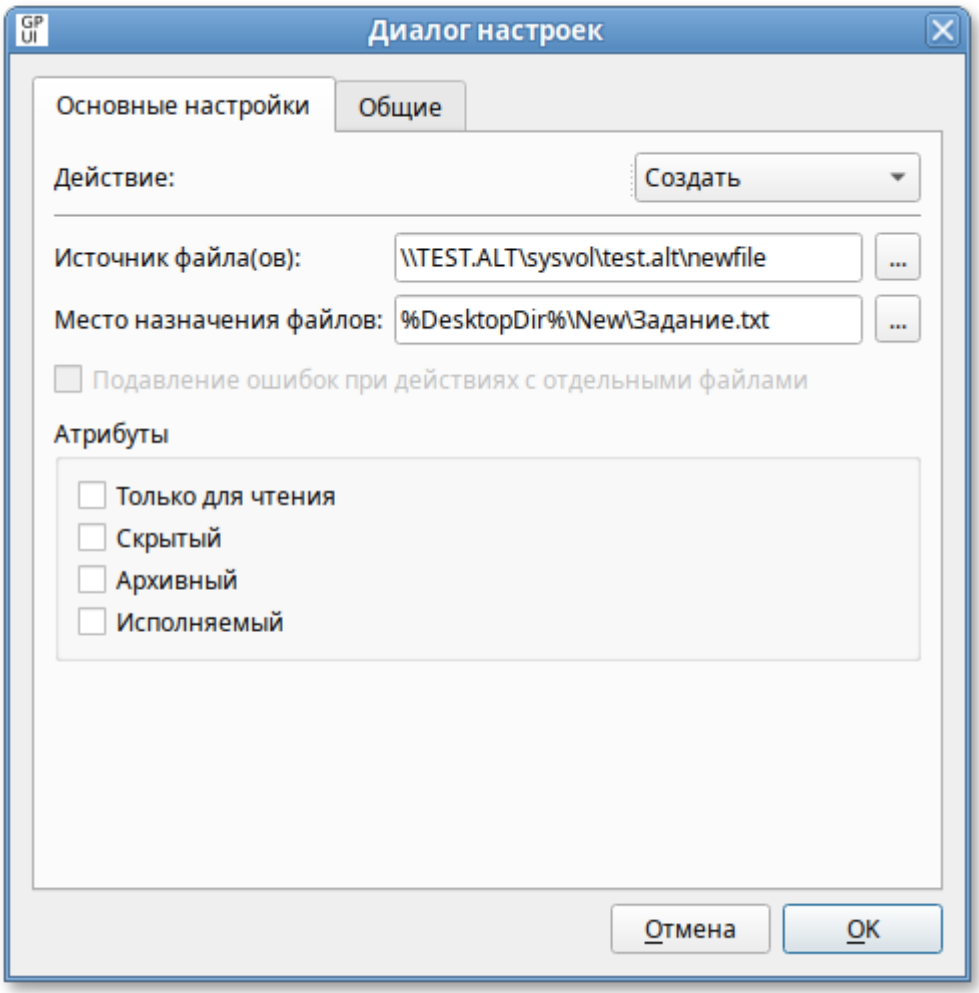
Примечание

В групповой политике **Файлы** нет встроенной возможности скопировать целиком каталог со всем содержимым. Вместо этого можно использовать политику **Папки**, которая позволяет создавать каталоги на компьютере, а для копирования файлов использовать групповую политику **Файлы**.

Для настройки этой политики следует перейти в **Компьютер/Пользователь → Настройки → Настройки системы → Файлы**. В контекстном меню свободной области выбрать пункт **Новый → Файл**



В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **Основные настройки**:

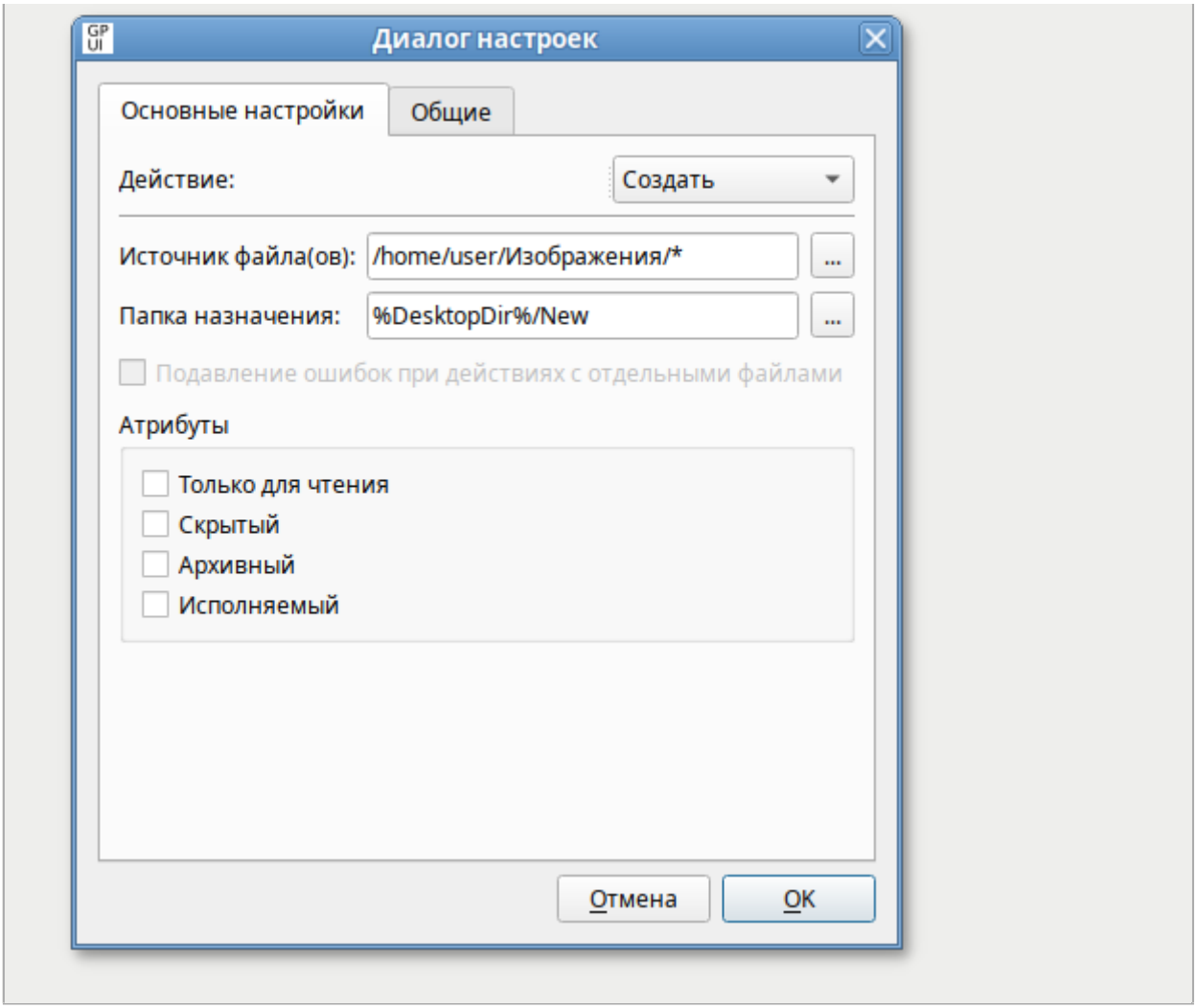
- **Действие** — действие, которое будет выполняться для файла(ов):
  - **Создать** — копирование файла (или нескольких файлов из одного каталога) из исходного местоположения в конечное, если файл еще не существует в местоположении назначения, и настройка атрибутов этих файлов;
  - **Удалить** — удаление файла (или нескольких файлов в одной папке);
  - **Заменить** — удаление файла (или нескольких файлов в одной папке), замена его другим файлом и настройка атрибутов этих файлов. Конечным результатом действия **Заменить** будет перезапись файлов в местоположении назначения. Если файл не существует в месте назначения, действие **Заменить** копирует его из исходного местоположения в место назначения;
  - **Обновить** — изменение параметров существующего файла (или нескольких файлов в одной папке). Это действие отличается от действия **Заменить** тем, что только обновляет атрибуты файла, определенные в элементе предпочтений. Все остальные атрибуты файла не изменяются. Если файл не существует, действие **Обновить** копирует его из исходного местоположения в место назначения;
- **Источник файла(ов)** — местоположение (с точки зрения клиента), из которого требуется скопировать исходные файлы. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Это поле может содержать переменные. Поле может содержать подстановочные знаки одного (?) или нескольких (*) символов, позволяя копировать или изменять несколько файлов (только для работы с файлами в ОС Windows). Поле недоступно для действия **Удалить**;

Примечание

Список допустимых переменных (для систем «Альт»):
- машинные:
  - %HOME%, %HOMEPATH% — каталог **/etc/skel**;
  - %HOMEDRIVE%, %SystemRoot%, %SystemDrive% — корневой каталог (**/**);
  - %StartMenuDir% — каталог **/usr/share/applications**;
- пользовательские:
  - %LogonUser% — имя текущего пользователя (username);
  - %HOME%, %HOMEPATH% — домашний каталог текущего пользователя (**get_homedir(username)**);
  - %DesktopDir% — рабочий стол текущего пользователя (**get_desktop(username, variables['HOME'])**).

Примечание

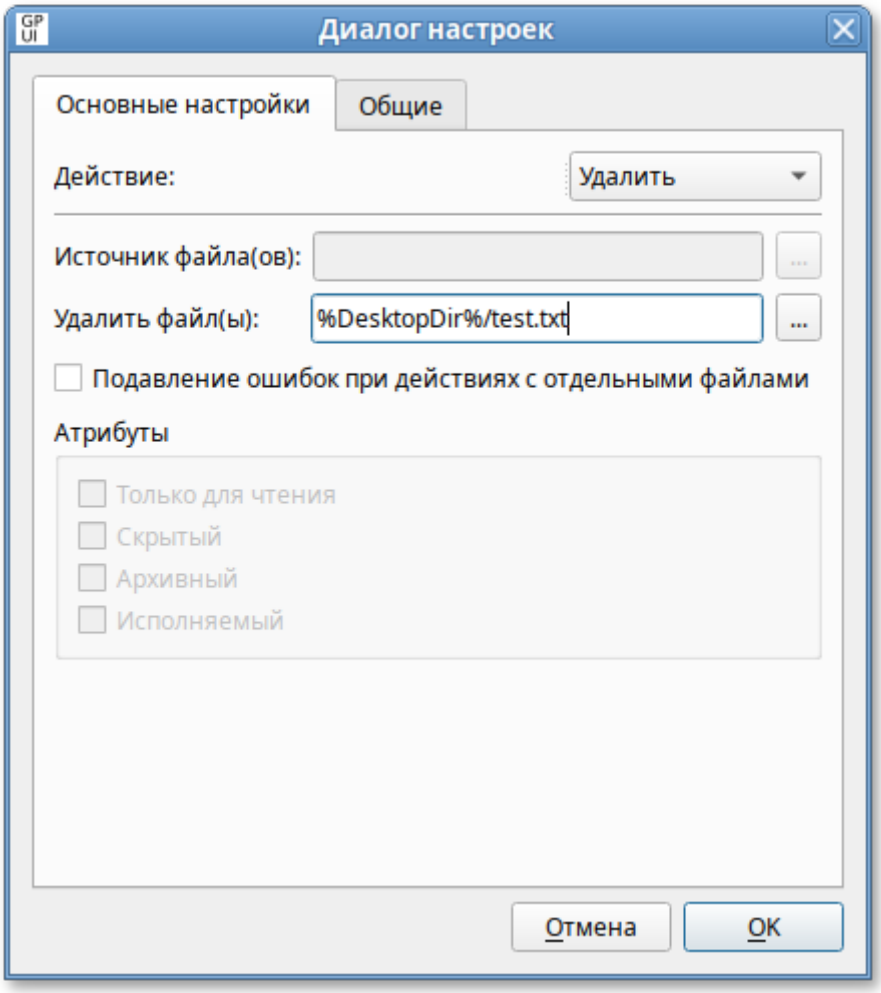
В настоящее время в ОС «Альт» можно использовать подстановочный знак (*) только для копирования всех файлов из папки:



- **Место назначения файлов** — местоположение папки (с точки зрения клиента), в которую требуется скопировать файлы, или местоположение файлов, которые требуется изменить. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Родительские папки создаются по мере необходимости. Необходимо включить имя файла, которое затем можно будет изменить, указав другое имя в поле Исходные файлы. Это поле может содержать переменные. Этот параметр доступен, если выбрано действие **Создать**, **Заменить** или **Обновить**, а поле **Источник файла(ов)** не содержит подстановочные знаки;

- **Папка назначения** — место назначения копирования файла или местоположение файла (с точки зрения клиента), который требуется изменить. Это местоположение может представлять полный путь UNC, или локальный путь, или сопоставленный диск со стороны клиента. Родительские папки создаются по мере необходимости. Это поле может содержать переменные. Этот параметр доступен, если выбрано действие **Создать**, **Заменить** или **Обновить**, а поле **Источник файла(ов)** включает подстановочные знаки;

- **Удалить файл(ы)** — путь к файлу (с точки зрения клиента), который требуется удалить. Чтобы удалить несколько файлов из одной папки необходимо включить в имя файла подстановочные знаки одного (?) или нескольких (*) символов (только для удаления файлов в ОС Windows). Этот параметр доступен, только если выбрано действие **Удалить**:



Примечание

В настоящее время в ОС «Альт» нельзя удалить несколько файлов из одной папки, включив в имя файла подстановочные знаки (? и *). Необходимо указывать файлы по одному.

- **Подавление ошибок при действиях с отдельными файлами** — разрешить передачу одного или нескольких файлов даже в случае сбоя передачи отдельных файлов. Не отображаются только ошибки, связанные с попыткой замены, удаления или настройки атрибутов файла. Такие ошибки могут быть вызваны тем, что файл используется, был отказ в доступе или исходный файл не найден. Если этот параметр включен, такие ошибки могут быть обнаружены только в файле трассировки. Этот параметр отличается от параметра пропуска ошибок предпочтений по умолчанию, который можно изменить на вкладке **Общее**;
- **Атрибуты** — атрибуты файловой системы для папки (недоступны для действия **Удалить**):
  - **Только для чтения**;
  - **Скрытый**;
  - **Архивный**;
  - **Исполняемый**.

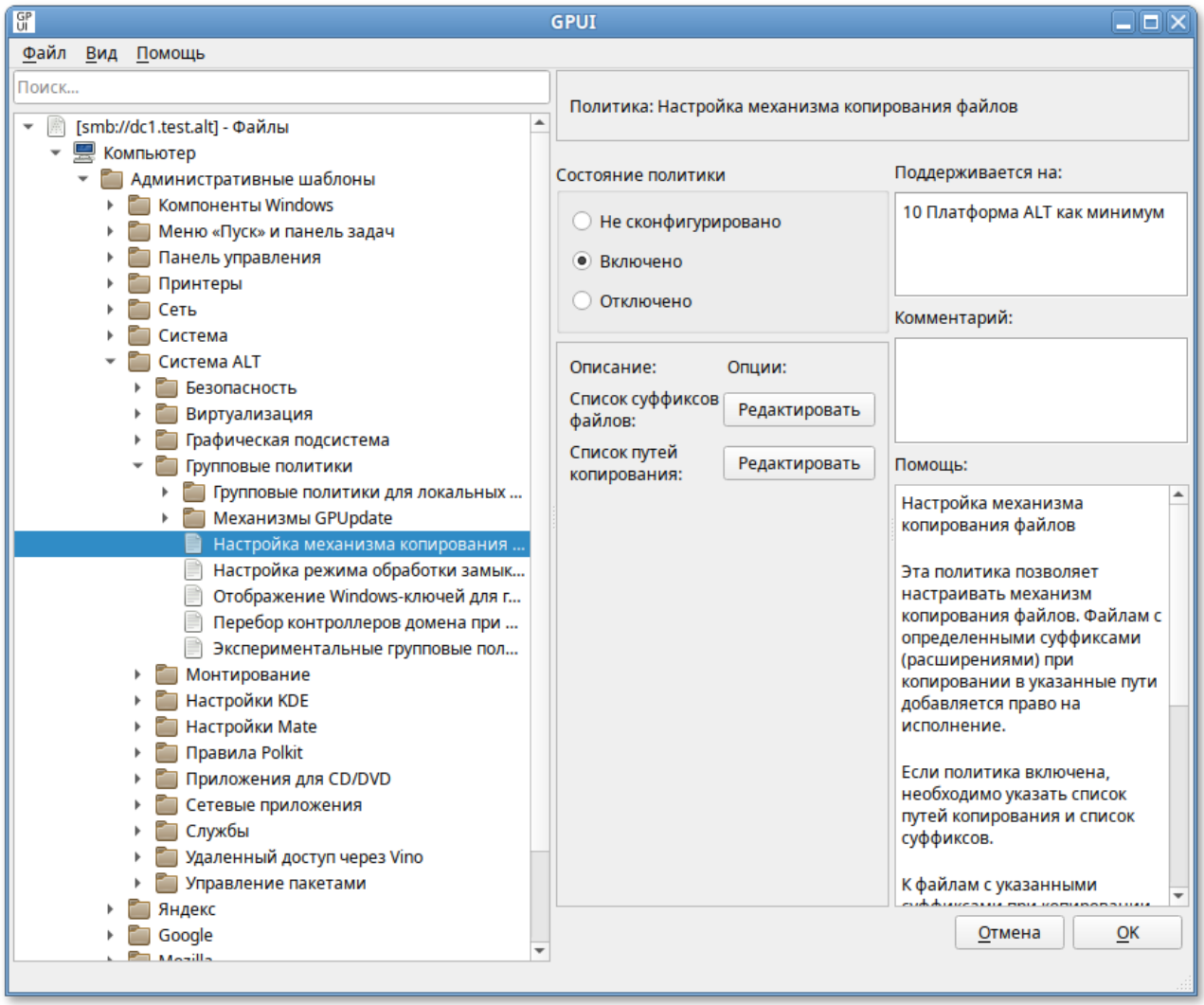
Примечание

Атрибуты **Архивный**, **Скрытый** и **Только для чтения** применимы только для Windows систем.

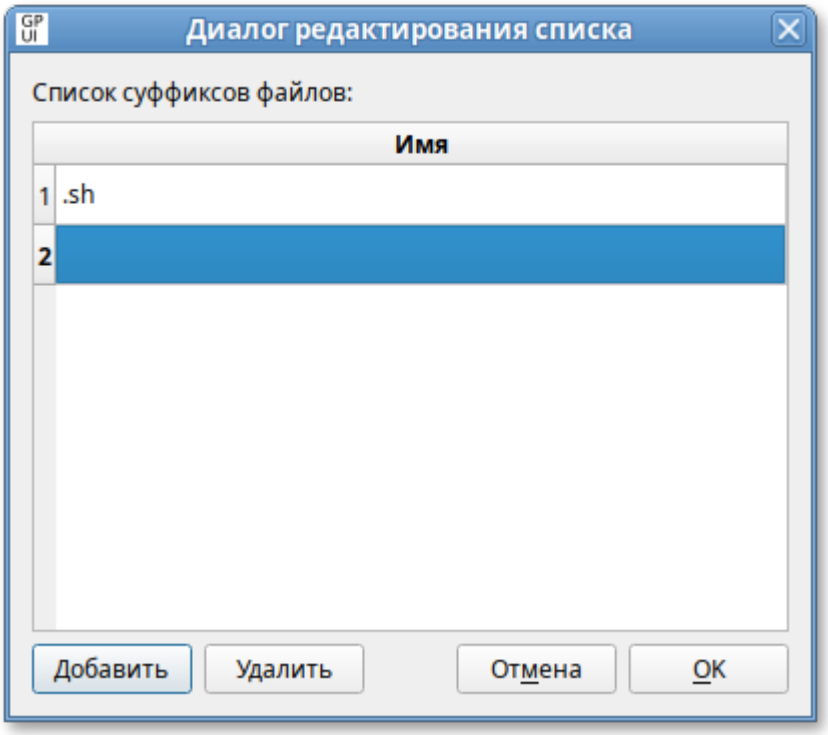
Политики управления файлами относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. раздел Экспериментальные групповые политики).

Опционально можно включить политику **Настройка механизма копирования файлов**. Данная политика конфигурирует механизм «копирования файлов», формируя список суффиксов (расширений), идентифицирующих файл как исполняемый (например, .sh), и список целевых путей копирования.

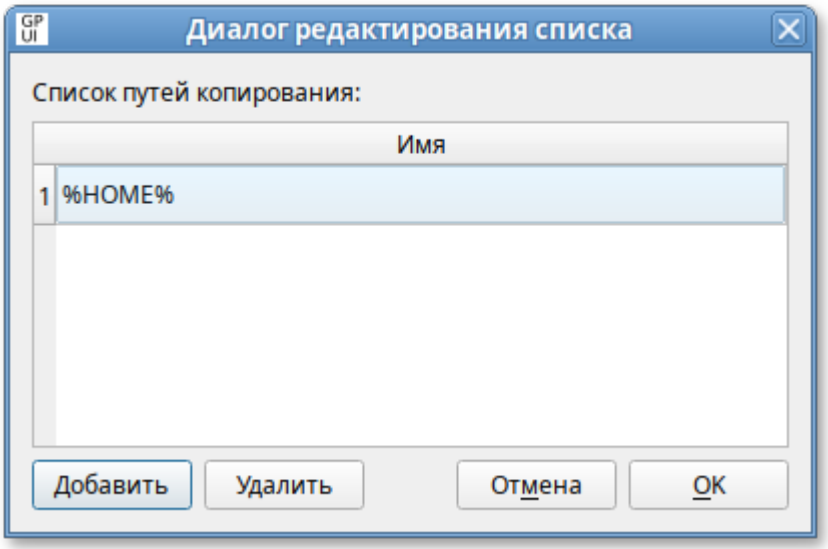
Для включения политики **Настройка механизма копирования файлов** следует в разделе **Компьютер → Административные шаблоны → Система ALT → Групповые политики** и выбрать пункт **Настройка механизма копирования файлов**. В открывшемся окне установить отметку в поле **Включено**:



Для задания списка суффиксов (расширений), идентифицирующих файл как исполняемый, в поле **Список суффиксов файлов** нажать кнопку **Редактировать** и в открывшемся окне ввести список суффиксов, по одному на каждой строке:



Для задания списка целевых путей копирования в поле **Список путей копирования** нажать кнопку **Редактировать** и в открывшемся окне ввести список путей, по одному на каждой строке:



В результате применения данной политики при копировании файлов с указанными суффиксами в назначенные пути, этим файлам будет задано право на выполнение (**chmod +x**).

Все настройки политики управления файлами хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/Files/Files.xml**
- **{GUID GPT}/User/Preferences/Files/Files.xml**

Пример файла **Files.xml**:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}">
  <File bypassErrors="0"
        changed="2023-08-20 13:18:25"
        clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}"
        desc="Файл с сервера"
        image="0"
        name="Задание.txt"
        removePolicy="0"
        status=""
        uid="{cd0d3cba-8698-4612-9c76-5e21da62cc48}"
        userContext="0">
    <Properties
        action="C"
        archive="0"
        executable="0"
        fromPath="\\TEST.ALT\sysvol\test.alt\newfile"
        hidden="0"
        readOnly="0"
        suppress="0"
        targetPath="%DesktopDir%\New\Задание.txt"/>
  </File>
</Files>
```

29.6.6. Управление общими каталогами

Групповая политика **Управление общими каталогами** позволяет:

- создать общие ресурсы и настроить их свойства;
- изменить путь к папке общего ресурса путём замены ресурса;
- удалить (вывести из общего доступа) или изменить лимит пользователей, функцию перечисления на основе доступа и комментарий для следующих объектов:
  - общий ресурс;
  - все общие ресурсы, кроме скрытых;
  - все скрытые ресурсы, кроме административных общих ресурсов с присвоением буквы диска;
  - все административные общие ресурсы с присвоением буквы диска;
  - все общие ресурсы.

Примечание

Для создания общего сетевого ресурса, папка, используемая при их создании, должна существовать на всех компьютерах, к которым применяется объект групповой политики. Вместе с удалением сетевого ресурса удаляется ссылка на папку, но не сама папка и её содержимое.

Примечание

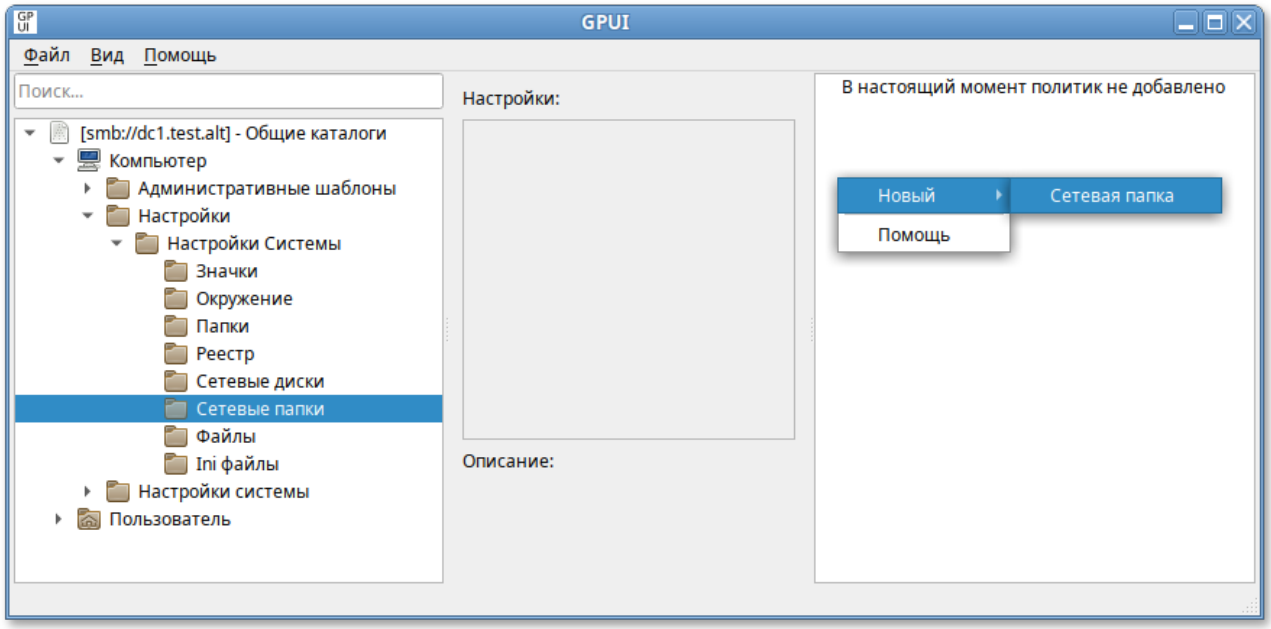
Для поддержки общих сетевых ресурсов с помощью политик на клиенте должны быть выполнены следующие условия:

- установлен пакет *samba-usershares*;
- **`control smb-conf-usershares`** установлен в enabled;
- в файле **`/etc/samba/smb.conf`** в секции [global] подключен файл **`/etc/samba/usershares.conf`** (include = /etc/samba/usershares.conf).

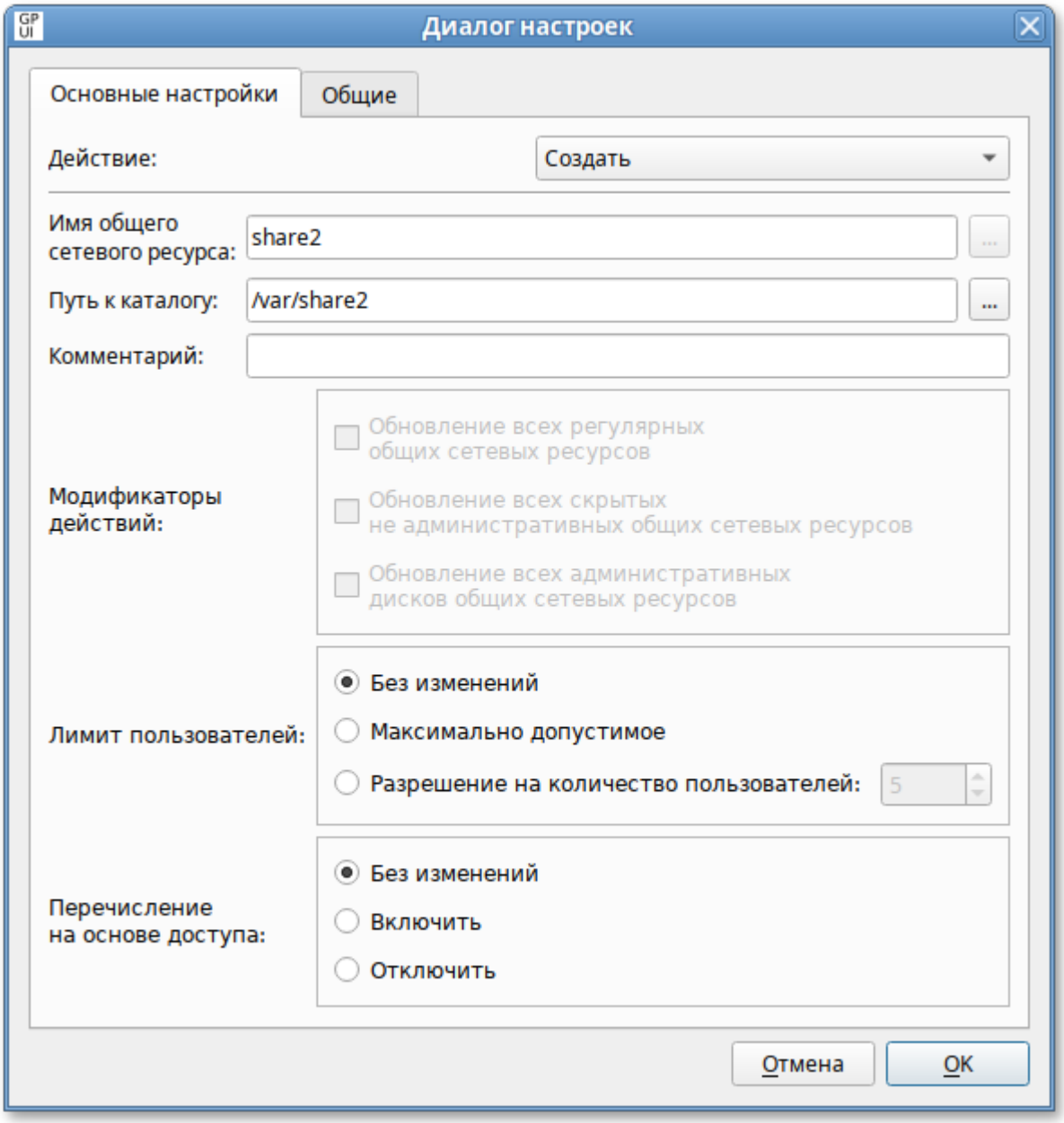
Примечание

Для создания или удаления папок с помощью групповой политики можно использовать предпочтение **Папки**.

Для настройки этой политики следует перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы** → **Сетевые папки**. В контекстном меню свободной области выбрать пункт **Новый** → **Сетевая папка**



В диалоговом окне **`Диалог настроек`** задать настройки политики:



Опции доступные на вкладке **`Основные настройки`**:

- **`Действие`** — действие, которое будет выполняться для общего сетевого ресурса:
  - **`Создать`** — создание нового сетевого ресурса;
  - **`Удалить`** — удаление общего ресурса;
  - **`Заменить`** — удаление и повторное создание сетевого ресурса. Суммарный итог действия **`Заменить`** — переопределение всех существующих параметров, связанных с общим ресурсом. Если сетевого ресурса не существует, то это действие создаёт новый сетевой ресурс;
  - **`Обновить`** — изменение параметров существующего сетевого ресурса. Если сетевого ресурса не существует, то это действие создаёт сетевой ресурс Это действие отличается от **`Заменить`** тем, что не удаляет сетевой ресурс, а только обновляет параметры сетевого ресурса, определённые в элементе настройки;

- **Имя общего сетевого ресурса** — имя общего ресурса. В этом поле можно указывать переменные;

- **Путь к каталогу** — путь к существующей папке, на которую будет указывать общий ресурс. В этом поле можно указывать переменные;

- **Комментарий** — текст для отображения в поле **Примечание** общего ресурса. Если выбрано действие **Обновить**, общий ресурс уже существует и данное поле оставлено пустым, существующий комментарий будет оставлен без изменений. В этом поле можно указывать переменные. Этот параметр доступен, если выбрано действие **Создать**, **Заменить** или **Обновить**;

- **Модификаторы действий** — изменять и удалять общие ресурсы конкретного типа можно не только индивидуально, но и все вместе. Эти параметры доступны, если выбранное действие — **Обновить** или **Удалить**:

  - **Обновление всех регулярных общих сетевых ресурсов** — изменение или удаление всех общих ресурсов, которые не являются скрытыми (с именами, оканчивающимися на $) или специальными (SYSVOL или NETLOGON);

  - **Обновление всех скрытых не административных общих сетевых ресурсов** — изменение или удаление всех скрытых общих ресурсов, за исключением административных общих ресурсов с буквенным обозначением дисков, ADMIN$, FAX$, IPC$ и PRINT$;

  - **Обновление всех административных дисков общих сетевых ресурсов** — изменение или удаление всех административных общих ресурсов с буквенным обозначением дисков (в их именах после буквы диска следует $);

- **Лимит пользователей** — настройка числа пользователей, которым можно одновременно подключаться к общему ресурсу:

  - **Без изменений** — не изменять допустимое число пользователей при обновлении общего ресурса (если этот параметр выбран при создании или замене общего ресурса, число пользователей будет настроено на максимально допустимое);

  - **Максимально допустимое** — неограниченное число пользователей;

  - **Разрешение на количество пользователей** — ограничить число пользователей (следует ввести допустимый максимум пользователей);

- **Перечисление на основе доступа** — настройка видимости папок общего ресурса:

  - **Без изменений** — не изменять видимость папок общего ресурса при обновлении общего ресурса;

  - **Включить** — сделать папки общего ресурса видимыми только при наличии доступа на чтение;

  - **Отключить** — сделать папки общего ресурса видимыми для всех пользователей.

Политики управления общими каталогами относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. раздел Экспериментальные групповые политики).

Все настройки политики управления общими каталогами хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/NetworkShares/NetworkShares.xml**
- **{GUID GPT}/User/Preferences/NetworkShares/NetworkShares.xml**

Пример файла **NetworkShares.xml**:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<NetworkShareSettings clsid="{520870D8-A6E7-47e8-A8D8-E6A4E76EAEC2}">
  <NetShare changed="2022-11-21 13:03:10"
        clsid="{2888C5E7-94FC-4739-90AA-2C1536D68BC0}"
        image="0"
        name="share2"
        status=""
        uid="{cd0d3cba-8698-4612-9c76-5e21da62cc48}"
        userContext="0"
        removePolicy="0">
    <Properties
        action="C"
        name="share2"
        path="/var/share2"
        comment=""
        limitUsers="NO_CHANGE"
        abe="NO_CHANGE"/>
  </NetShare>
</NetworkShareSettings>
```

29.6.7. Подключение сетевых дисков

Групповая политика **Подключение сетевых дисков** позволяет осуществлять доступ к сетевым общим каталогам как к каталогам в локальной файловой системе. Политика служит для создания, замены, обновления и удаления сопоставленных дисков и их свойств.

Точки монтирования для отображения общих ресурсов на машинах с ОС «Альт»:

- **/media/gpupdate/drives.system** — для системных ресурсов;
- **/media/gpupdate/.drives.system** — для скрытых системных ресурсов;
- **/run/media/USERNAME/drives** — для общих ресурсов пользователя;
- **/run/media/USERNAME/.drives** — для скрытых общих ресурсов пользователя.

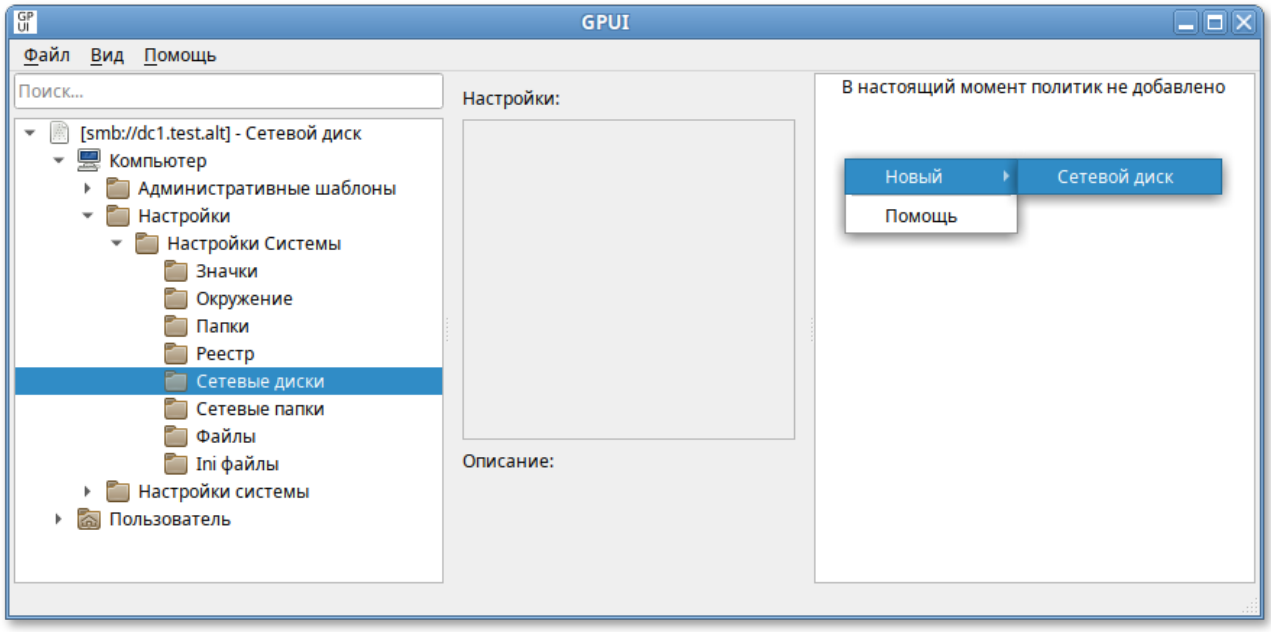
Примечание

Групповая политика **Подключение сетевых дисков** использует службу autofs, которая управляет автоматическим монтированием файловых систем.

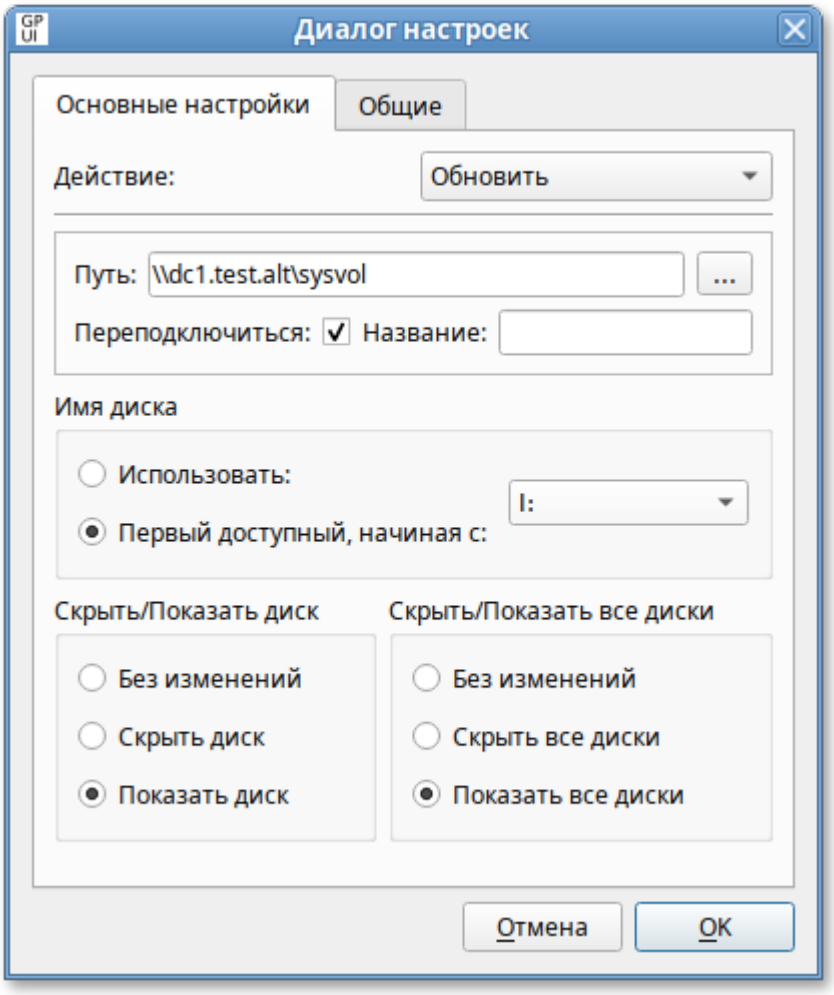
Значения параметров прописываются в файлы конфигурации:

- **/etc/auto.master.gpupdate.d/<имя>.autofs** и **/etc/auto.master.gpupdate.d/<имя>.conf** — для отображаемых ресурсов;
- **/etc/auto.master.gpupdate.d/<имя>_hide.autofs** и **/etc/auto.master.gpupdate.d/<имя>_hide.conf** — для скрытых ресурсов.

Для настройки этой политики следует перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы** → **Сетевые диски**. В контекстном меню свободной области выбрать пункт **Новый** → **Сетевой диск**



В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **`Основные настройки`**:

- **`Действие`** — поведение элемента настройки зависит от выбранного действия и от того, существует ли уже выбранная буква диска:
  - **`Создать`** — создание нового сетевого диска;
  - **`Удалить`** — удаление сетевого диска. Нельзя удалить локальный диск рабочей станции (жёсткий диск, CD-Drive);
  - **`Заменить`** — удаление и повторное создание сетевого диска. Если диск до этого не был до создан, то будет создан новый диск. Нельзя заменить локальный диск рабочей станции (жёсткий диск, CD-Drive);
  - **`Обновить`** — изменение параметров существующего сетевого диска или создание нового, если диска с заданной буквой не существует. Это действие отличается от **`Заменить`** тем, что оно не удаляет диск, а только обновляет настройки (кроме пути к общей папке и буквы);
- **`Путь`** — путь к общей папке или диску, который нужно отобразить (полный UNC-путь к сетевому общему ресурсу, например, **`\\server\sharename`**, **`\\server\hiddenshare$`** или **`\\server\sharename\foldername`**). Это поле может содержать переменные. Чтобы изменить существующий сетевой диск (определяемый по букве диска), следует оставить это поле пустым;

Примечание

Список допустимых переменных (для систем «Альт»):

- машинные:
  - %HOME%, %HOMEPATH% — каталог **/etc/skel**;
  - %HOMEDRIVE%, %SystemRoot%, %SystemDrive% — корневой каталог (**/**);
  - %StartMenuDir% — каталог **/usr/share/applications**;
- пользовательские:
  - %LogonUser% — имя текущего пользователя (username);
  - %HOME%, %HOMEPATH% — домашний каталог текущего пользователя (**get_homedir(username)**);
  - %DesktopDir% — рабочий стол текущего пользователя (**get_desktop(username, variables['HOME'])**).

Переподключиться — сохранять подключенный диск в настройках пользователя и повторно подключать его при каждом входе в систему;

Название — пользовательское имя для диска (можно оставить это поле пустым);

Примечание

Если в названии есть кириллица или пробелы, то название необходимо заключить в двойные кавычки.

Имя диска — буква, на которую будет назначен диск:

- чтобы назначить сетевому диску первую доступную букву диска, следует выбрать **Первый доступный, начиная с**, а затем выбрать букву диска, с которой начинать проверку доступности букв;
- чтобы назначить сетевому диску определённую букву, следует выбрать **Использовать**, а затем выбрать букву диска (если рабочая станция уже использует выбранную здесь букву, сопоставление дисков групповой политики завершится неудачно);
- чтобы изменить существующее сопоставление диска (определяемое буквой диска), следует выбрать **Использовать**, а затем выбрать букву диска;
- чтобы удалить все сопоставления дисков начиная с определённой буквы, следует выбрать **Удалить, начиная с**, а затем выбрать букву диска, с которой следует начать удаление сопоставлений дисков. Физические диски пропускаются без ошибок. Данный параметр доступен только при выбранном действии **Удалить**;
- чтобы удалить определенный сопоставленный диск, следует выбрать **Удалить**, а затем выбрать букву диска. Данный параметр доступен только при выбранном действии **Удалить**;

Примечание

Пункт **Имя диска** совместно с **Первый доступный, начиная с** рекомендуется использовать для дисков, которые должны подключаться в ОС Windows. Так как если будет создано несколько дисков с данными параметрами, то в ОС «Альт» будет отображаться только один диск (последний).

- Параметры **Скрыть/Показать** — настройка отображения сопоставленного диска (параметры **Скрыть/Показать диск** имеют приоритет над параметрами **Скрыть/Показать все диски**):
  - **Без изменений** — оставить отображение сопоставленного диска неизменным;
  - **Скрыть диск** — скрыть диск в окне файлового менеджера;
  - **Показать диск** — отобразить диск в окне файлового менеджера.

Примечание

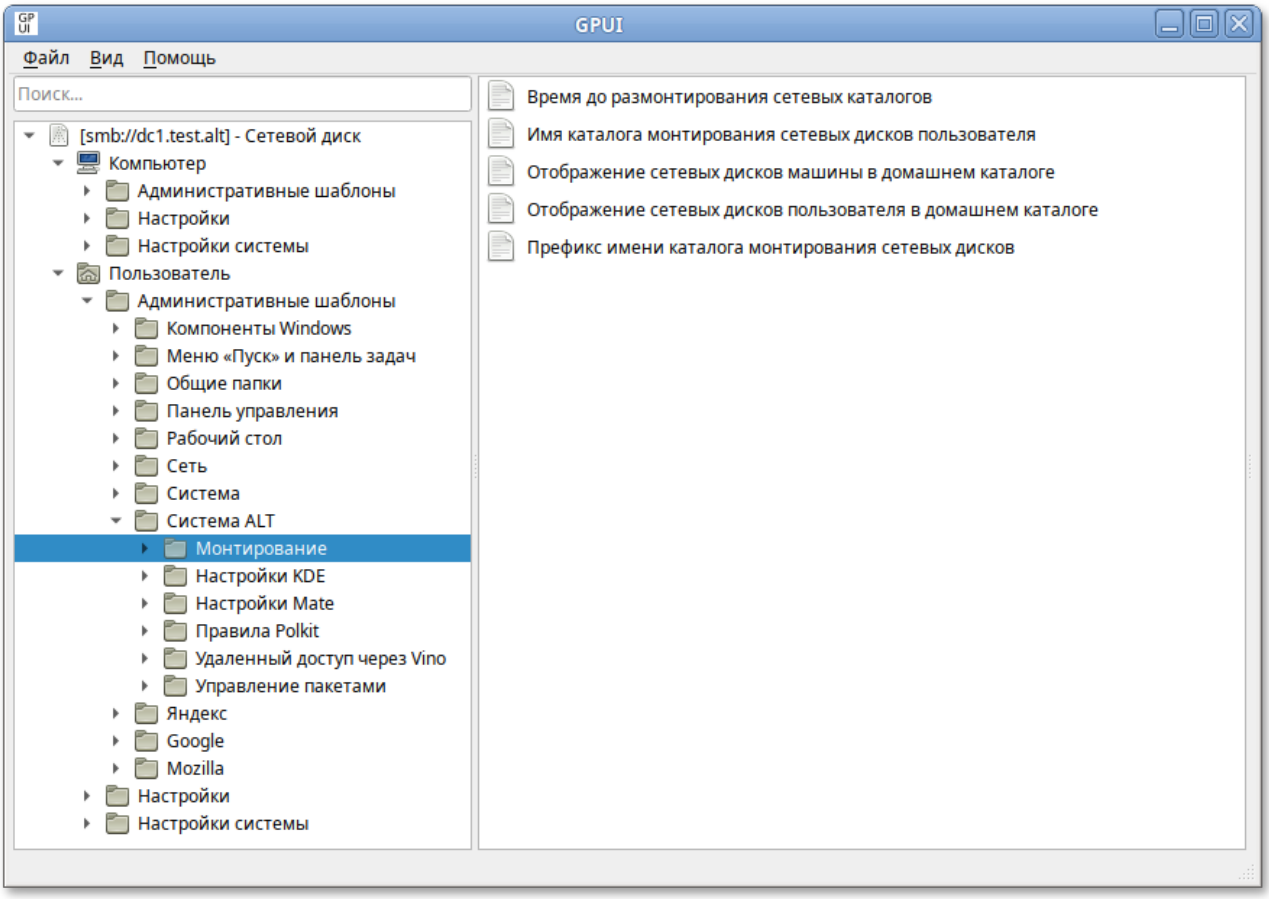
При выборе параметра **Показать диск** к точке монтирования (файл **/etc/auto.master.gpupdate.d/<имя>.autofs**) добавляется опция **--browse**. В этом случае для данной точки монтирования будет создан пустой каталог, независимо от того, смонтирована ли какая-либо файловая система в него или нет.

Это удобно так как доступные автоматически монтируемые файловые системы будут показаны как существующие каталоги, даже если их файловые системы в данный момент не смонтированы.

При выборе параметра **Скрыть диск** необходимо запомнить название каталога, так как доступ к этому каталогу можно получить только при непосредственном обращении к нему. Каталог будет создан и файловая система будет смонтирована только при попытке доступа к нему. Незадействованный ресурс по истечении таймаута (по умолчанию 120 секунд) будет отмонтирован, а каталог удалён.

29.6.7.1. Дополнительные настройки

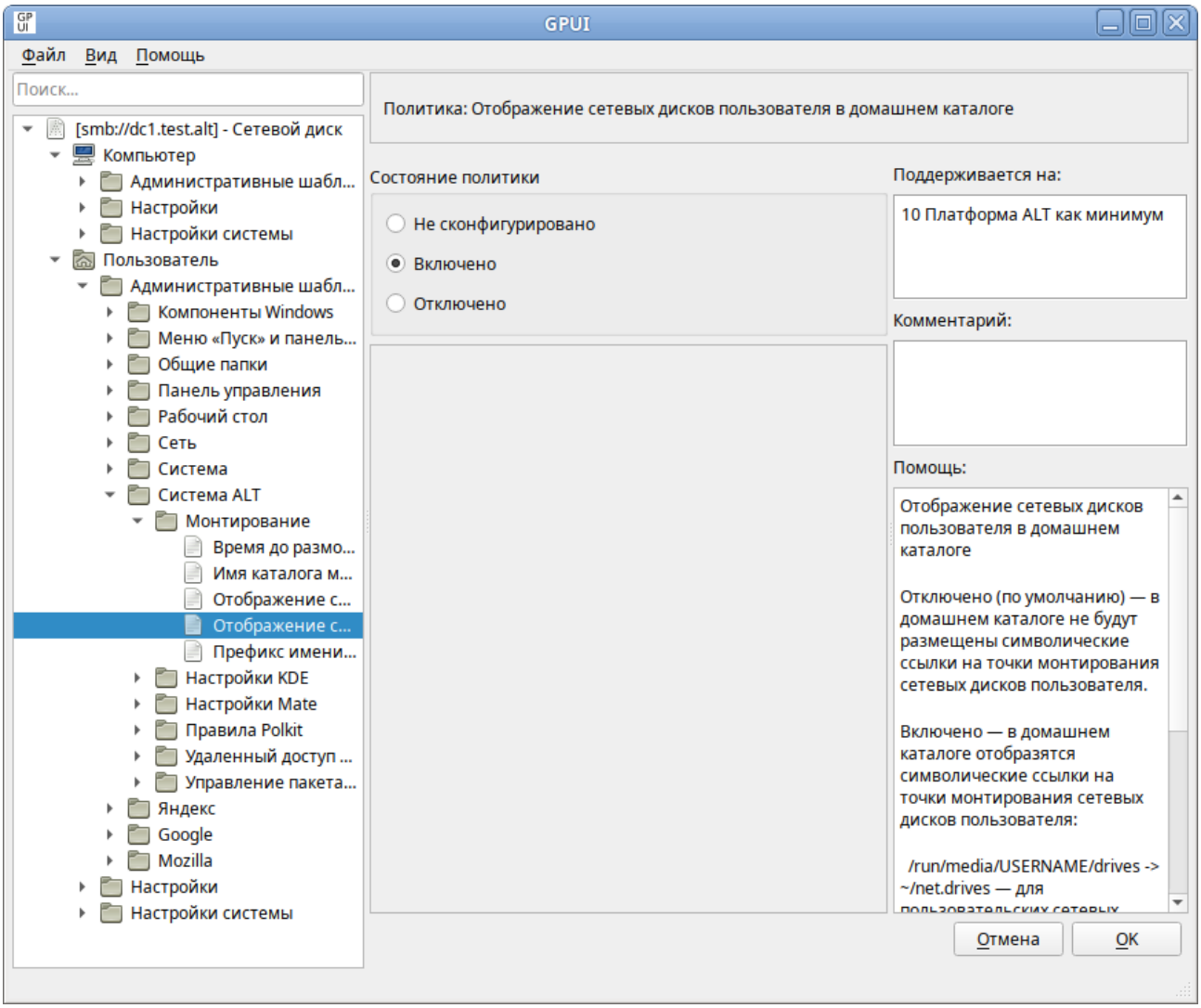
Политики монтирования находятся в разделе **Компьютер/Пользователь** → **Административные шаблоны** → **Система ALT** → **Монтирование**:



29.6.7.1.1. Отображение сетевых дисков в домашнем каталоге

Если необходимо, можно включить отображение ссылок (symlink) на соответствующий сетевой ресурс в домашнем каталоге пользователя (чтобы можно было очевидно наблюдать смонтированные ресурсы). Для этого следует включить политики монтирования **Отображение сетевых дисков пользователя в домашнем каталоге** и/или **Отображение сетевых дисков машины в домашнем каталоге**.

Для включения политики монтирования необходимо щёлкнуть на нужной политике, в открывшемся окне установить отметку в поле **Включено** и нажать кнопку **OK**:

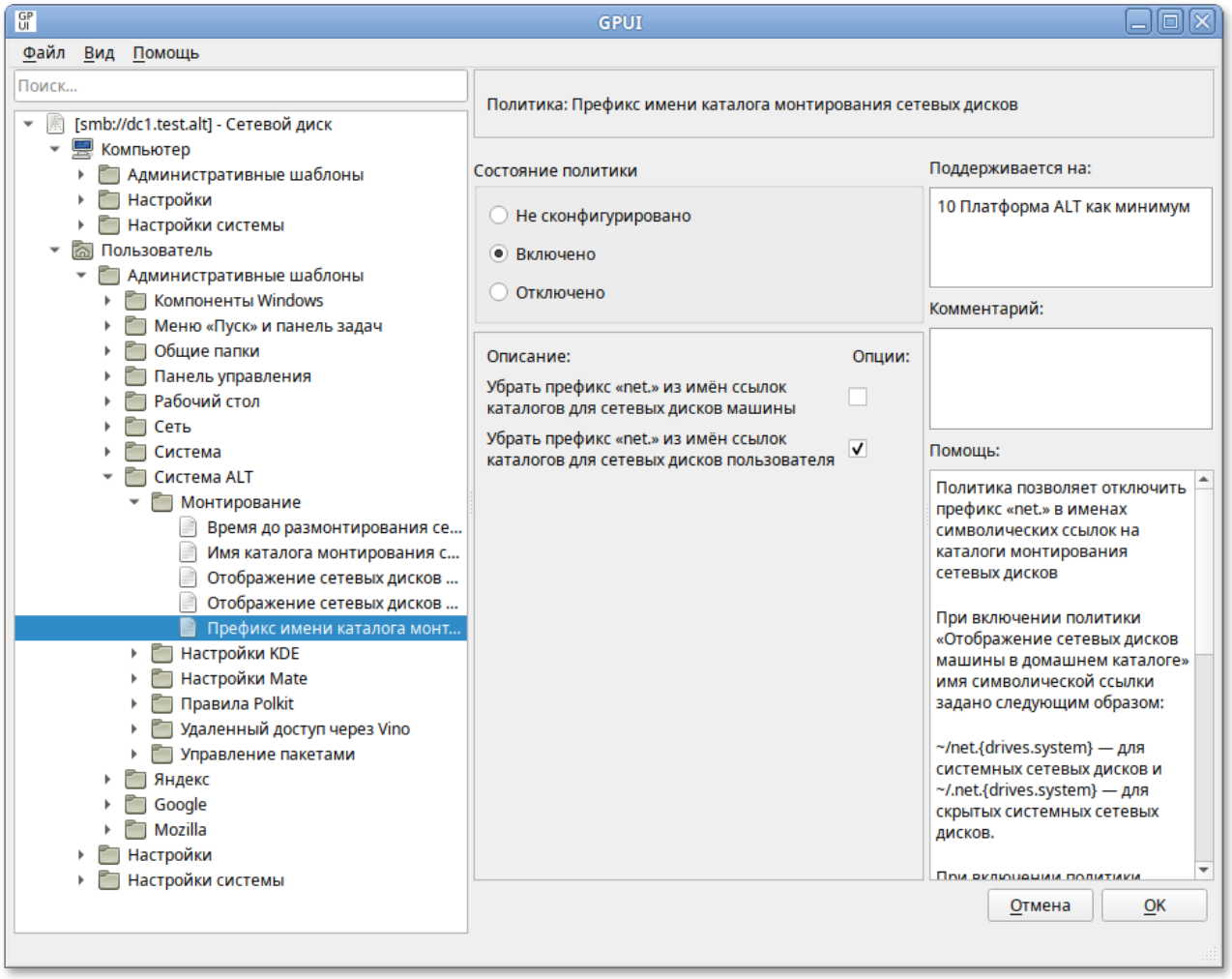


Если включены политики отображения сетевых дисков в домашнем каталоге, в домашнем каталоге пользователя появятся ссылки:

- **`~/net.drives.system`** — ссылка на **`/media/gpupdate/drives.system`**;
- **`~/.net.drives.system`** — ссылка на **`/media/gpupdate/.drives.system`**;
- **`~/net.drives`** — ссылка на **`/run/media/USERNAME/drives`**;
- **`~/.net.drives`** — ссылка на **`/run/media/USERNAME/.drives`**;

29.6.7.1.2. Префикс имени каталога монтирования сетевых дисков

Политика **Префикс имени каталога монтирования сетевых дисков** (**Пользователь → Административные шаблоны → Система ALT → Монтирование**) позволяет отключить префикс «net.» в именах символических ссылок на каталоги монтирования сетевых дисков:



Если политика отключена или не сконфигурирована, имена символических ссылок на каталоги монтирования начинаются с префикса «net.»:

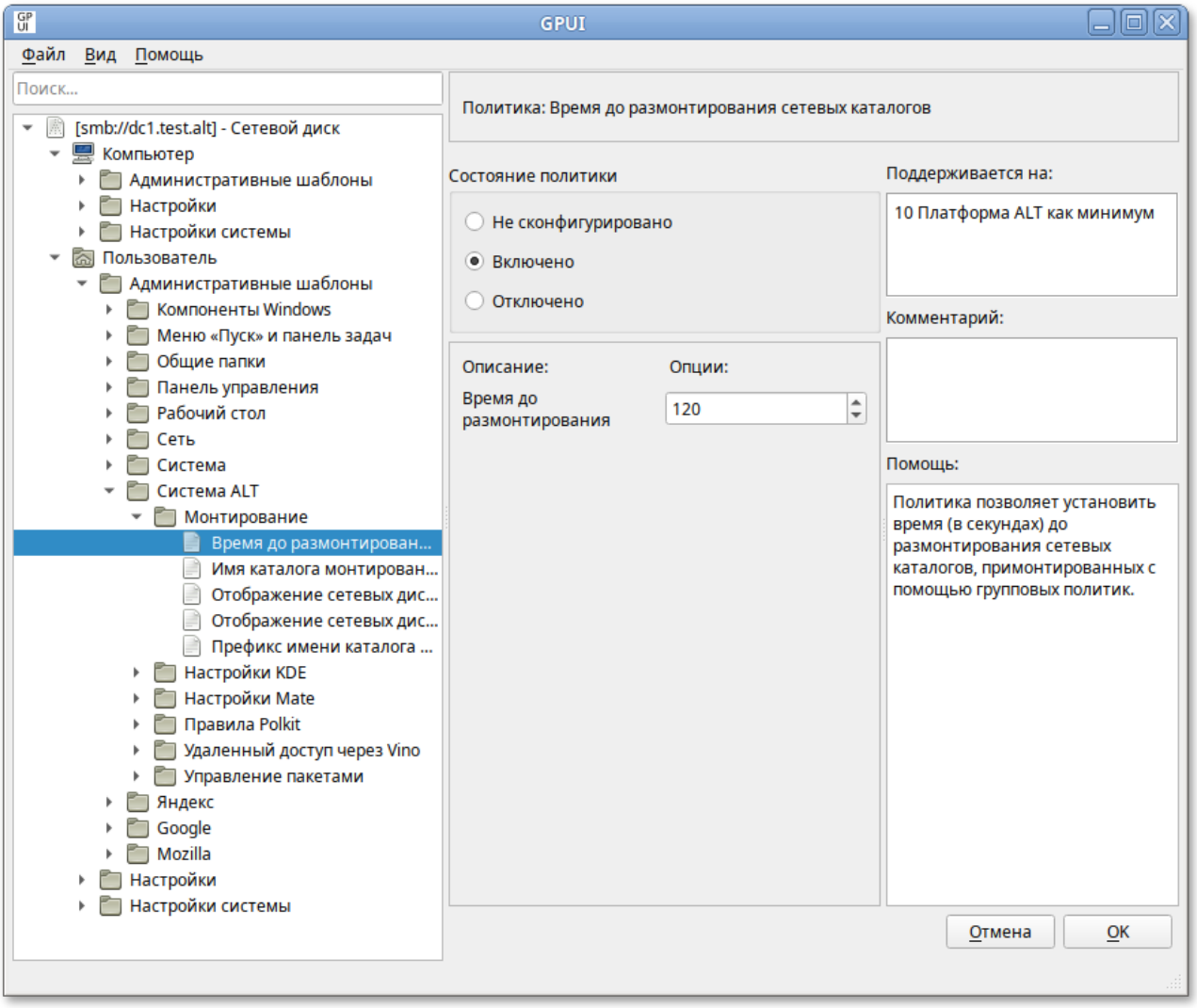
- **`~/net.drives`** — ссылка на **`/run/media/USERNAME/drives`** для общих ресурсов пользователя;
- **`~/.net.drives`** — ссылка на **`/run/media/USERNAME/.drives`** для скрытых общих ресурсов пользователя.

Если политика включена, префикса «net.», в именах символических ссылок на каталоги монтирования, не будет:

- **`~/drives`** — ссылка на **`/run/media/USERNAME/drives`** для общих ресурсов пользователя;
- **`~/.drives`** — ссылка на **`/run/media/USERNAME/.drives`** для скрытых общих ресурсов пользователя.

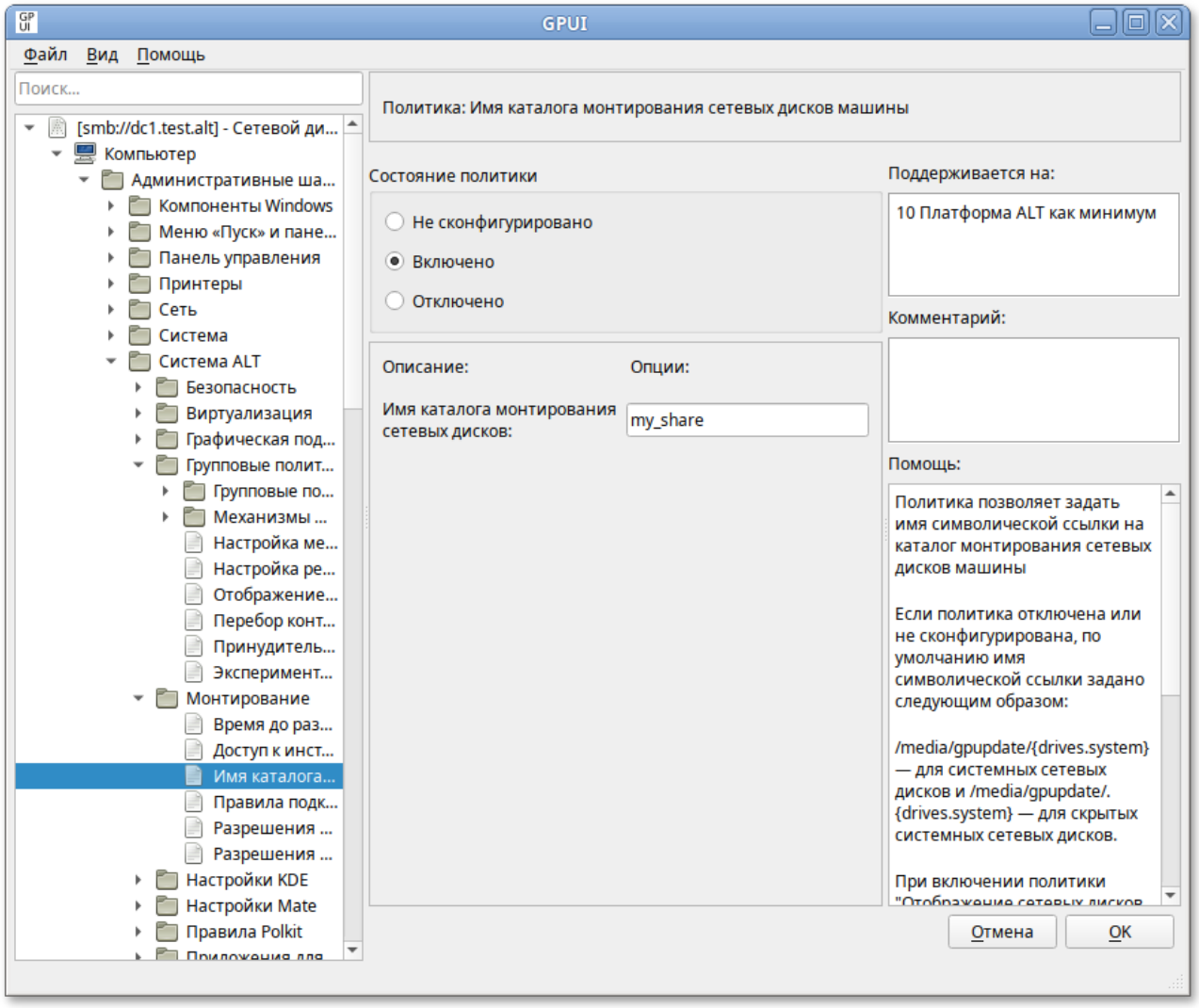
29.6.7.1.3. Время до размонтирования сетевых каталогов

Политика **Время до размонтирования сетевых каталогов** (**Компьютер/Пользователь → Административные шаблоны → Система ALT → Монтирование**) позволяет установить время (в секундах) до размонтирования сетевых каталогов, примонтированных с помощью групповых политик.



29.6.7.1.4. Имя каталога монтирования сетевых дисков машины

Политика **Имя каталога монтирования сетевых дисков машины** (**Компьютер → Административные шаблоны → Система ALT → Монтирование**) позволяет задать имя символической ссылки на каталог монтирования сетевых дисков машины:



Если политика отключена или не сконфигурирована, по умолчанию имя символической ссылки задано следующим образом:

- **/media/gpupdate/drives.system** — для системных сетевых дисков;
- **/media/gpupdate/.drives.system** — для скрытых системных сетевых дисков;
- **~/net.drives.system** — для системных сетевых дисков (при включенной политике **Отображение сетевых дисков машины в домашнем каталоге**);
- **~/.net.drives.system** — для скрытых системных сетевых дисков (при включенной политике **Отображение сетевых дисков машины в домашнем каталоге**).

Если политика включена, имя символической ссылки будет задано следующим образом:

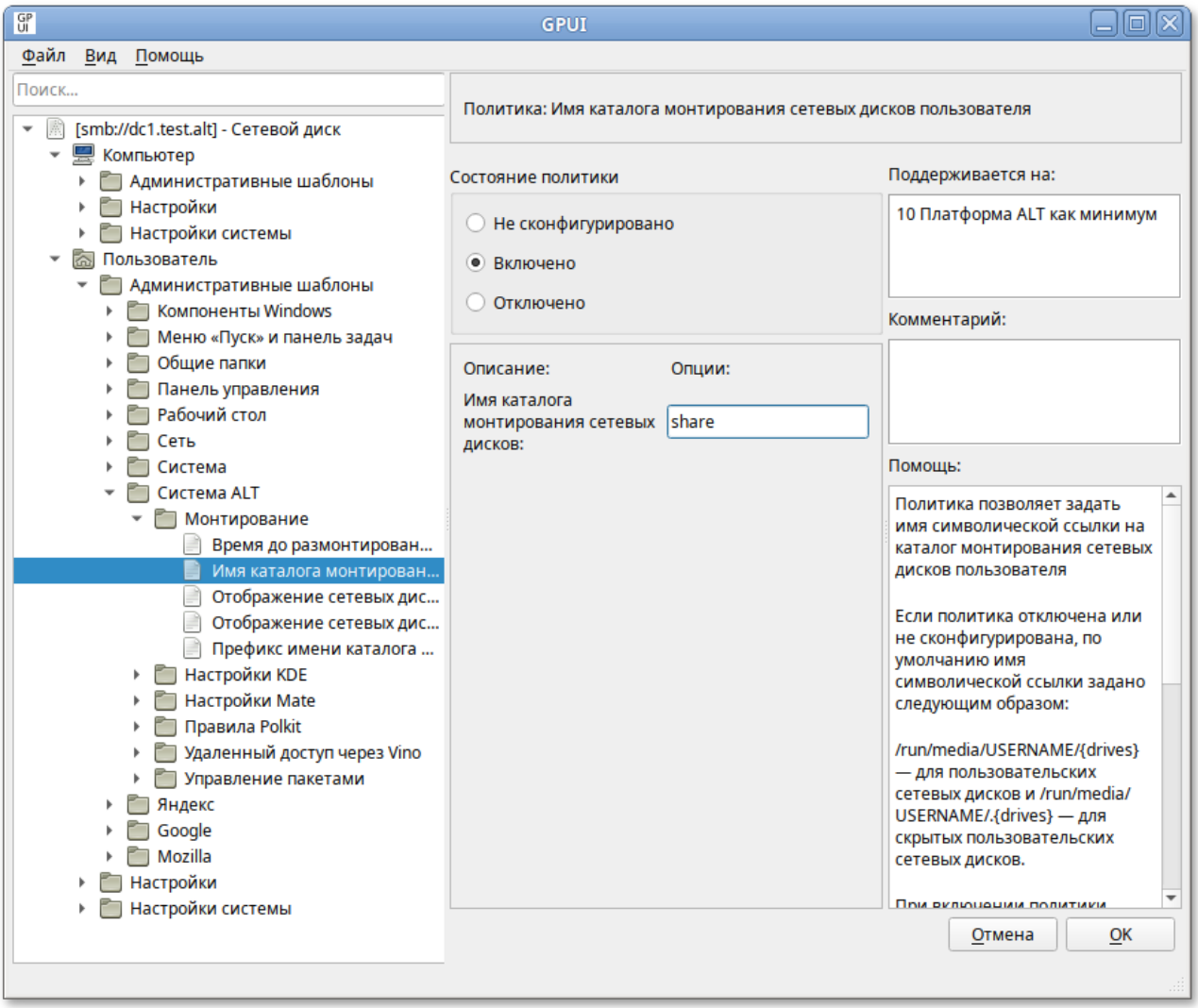
- **/media/gpupdate/<имя>.system** — для системных сетевых дисков;
- **/media/gpupdate/.<имя>.system** — для скрытых системных сетевых дисков;
- **~/net.<имя>.system** — для системных сетевых дисков (при включенной политике **Отображение сетевых дисков машины в домашнем каталоге**);
- **~/.net.<имя>.system** — для скрытых системных сетевых дисков (при включенной политике **Отображение сетевых дисков машины в домашнем каталоге**);

- **~/<имя>.system** — для системных сетевых дисков (при включенных политиках **Отображение сетевых дисков машины в домашнем каталоге** и **Префикс имени каталога монтирования сетевых дисков**);

- **~/.<имя>.system** — для скрытых системных сетевых дисков (при включенных политиках **Отображение сетевых дисков машины в домашнем каталоге** и **Префикс имени каталога монтирования сетевых дисков**).

29.6.7.1.5. Имя каталога монтирования сетевых дисков пользователя

Политика **Имя каталога монтирования сетевых дисков пользователя** (**Пользователь** → **Административные шаблоны** → **Система ALT** → **Монтирование**) позволяет задать имя символической ссылки на каталог монтирования сетевых дисков пользователя:



Если политика отключена или не сконфигурирована, по умолчанию имя символической ссылки задано следующим образом:

- **/run/media/USERNAME/drives** — для общих ресурсов пользователя;

- **/run/media/USERNAME/.drives** — для скрытых общих ресурсов пользователя;

- **~/net.drives** — для общих ресурсов пользователя (при включенной политике **Отображение сетевых дисков машины в домашнем каталоге**);

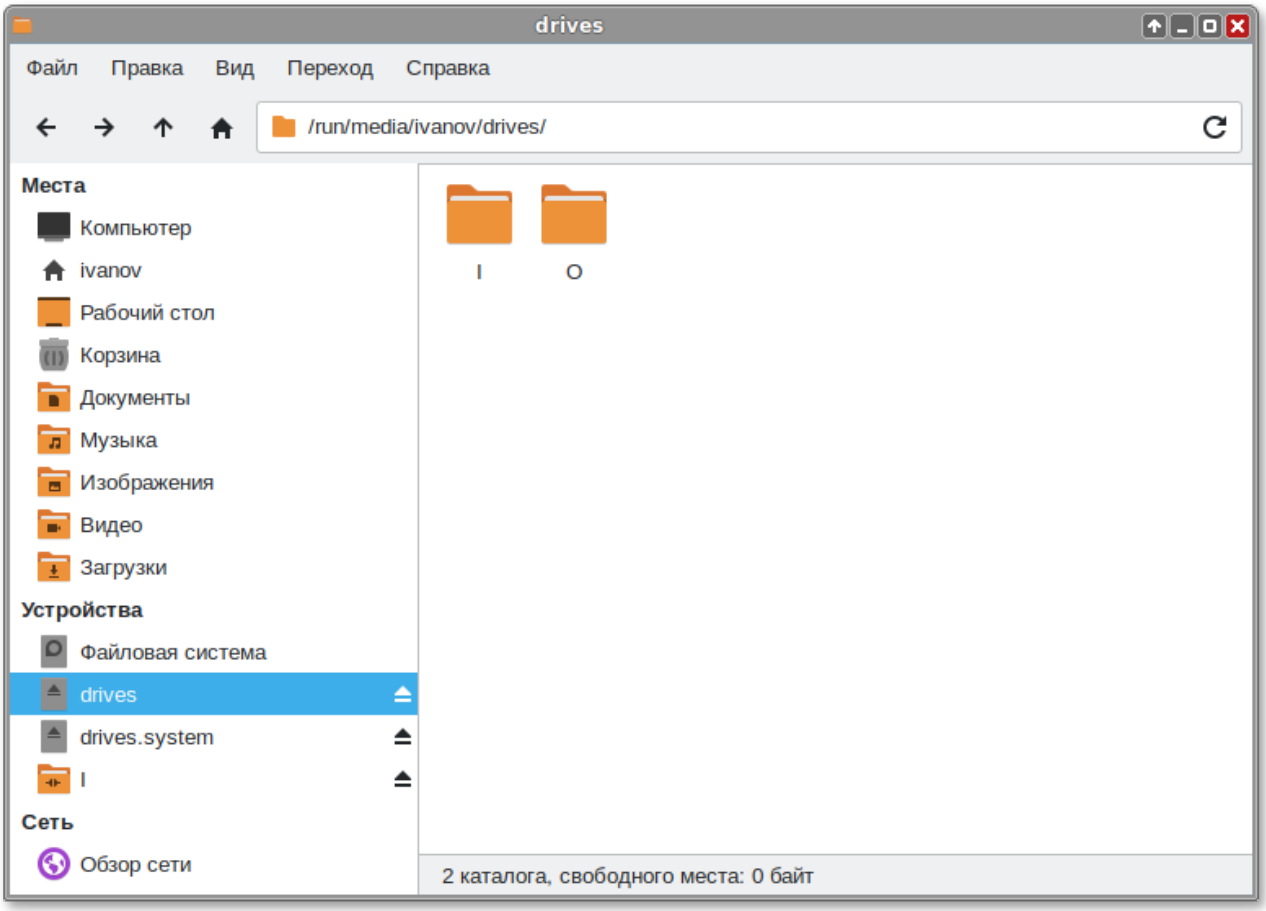
- **~/.net.drives** — для скрытых общих ресурсов пользователя (при включенной политике **Отображение сетевых дисков машины в домашнем каталоге**).

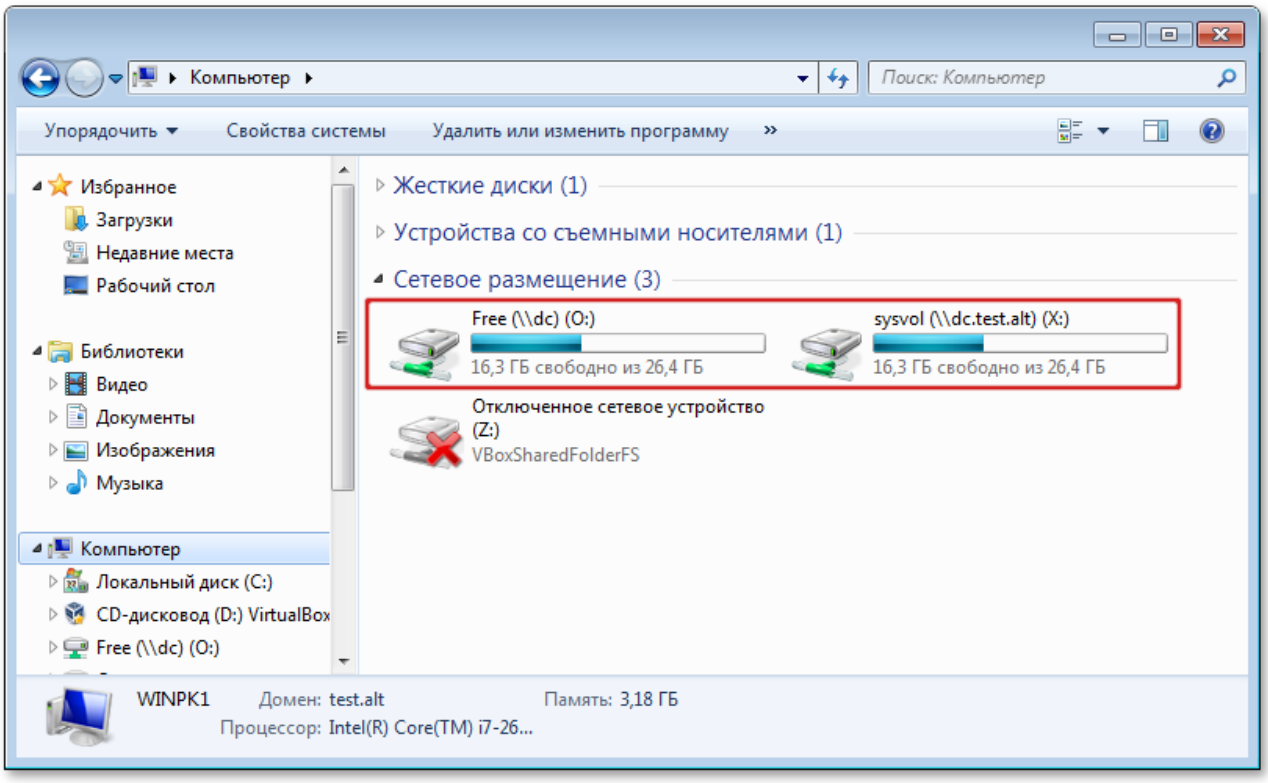
Если политика включена, имя символической ссылки будет задано следующим образом:

- **/run/media/USERNAME/<имя>** — для общих ресурсов пользователя;
- **/run/media/USERNAME/.<имя>** — для скрытых общих ресурсов пользователя;
- **~/net.<имя>** — для общих ресурсов пользователя (при включенной политике **Отображение сетевых дисков пользователя в домашнем каталоге**);
- **~/.net.<имя>** — для скрытых общих ресурсов пользователя (при включенной политике **Отображение сетевых дисков пользователя в домашнем каталоге**);
- **~/<имя>** — для общих ресурсов пользователя (при включенных политиках **Отображение сетевых дисков пользователя в домашнем каталоге** и **Префикс имени каталога монтирования сетевых дисков**);
- **~/.<имя>** — для скрытых общих ресурсов пользователя (при включенных политиках **Отображение сетевых дисков пользователя в домашнем каталоге** и **Префикс имени каталога монтирования сетевых дисков**).

29.6.7.2. Результат применения политики

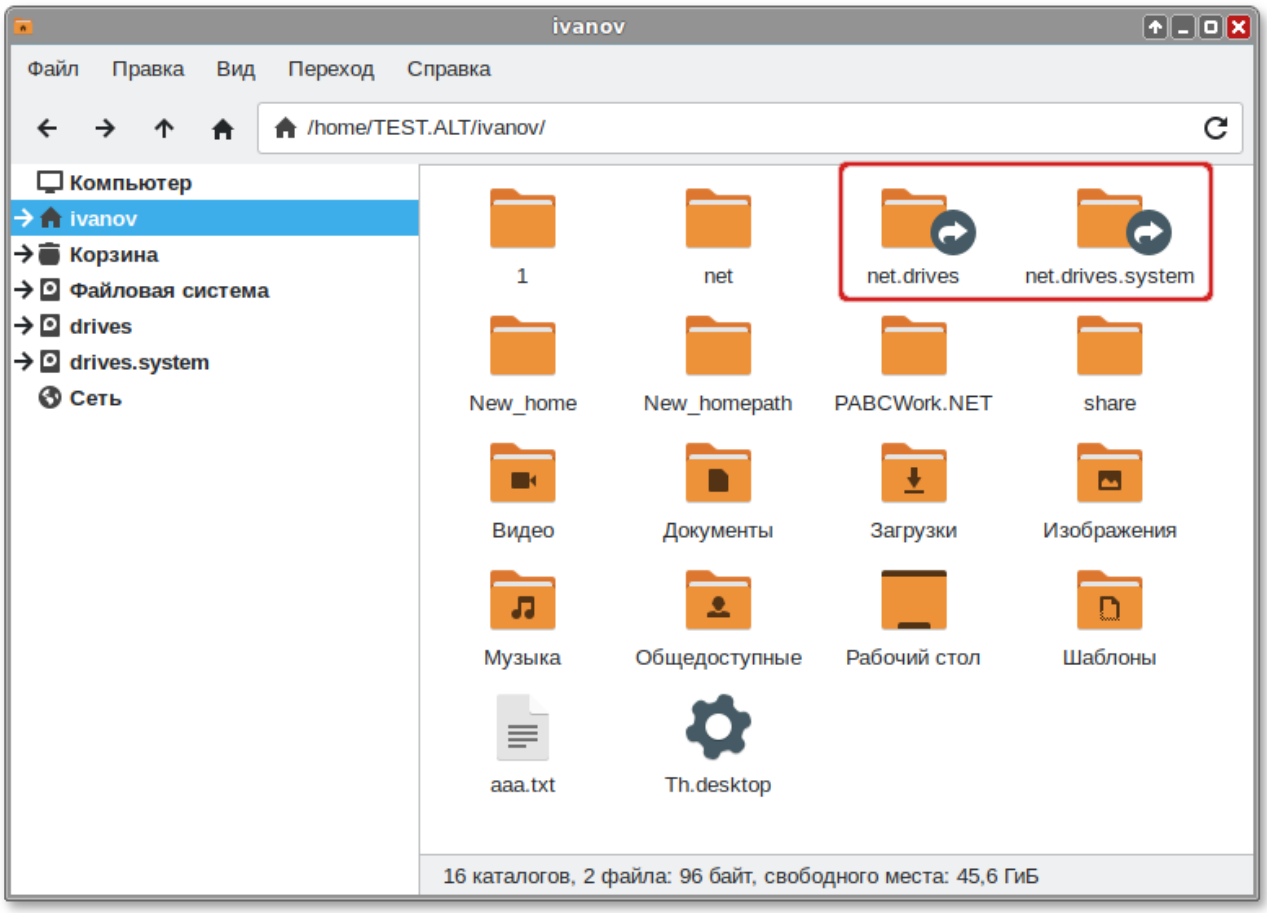
После обновления политик в сессии пользователя будет подключен сетевой диск, доступный из файлового менеджера и других программ:



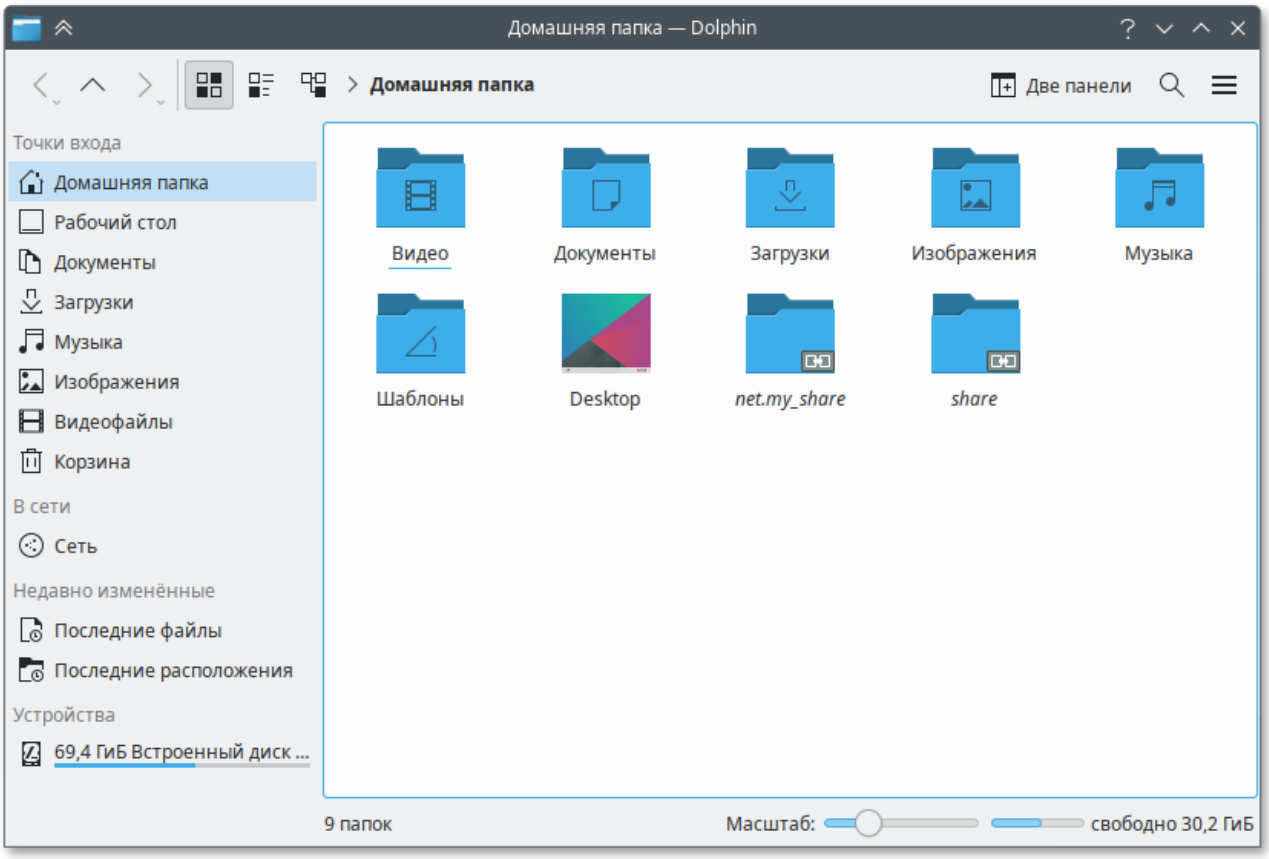


Если включена политика **`Отображение сетевых дисков в домашнем каталоге`**, в домашнем каталоге пользователя появятся ссылки:

- **`~/net.drives.system`** — ссылка на **`/media/gpupdate/drives.system`**;
- **`~/.net.drives.system`** — ссылка на **`/media/gpupdate/.drives.system`**;
- **`~/net.drives`** — ссылка на **`/run/media/USERNAME/drives`**;
- **`~/.net.drives`** — ссылка на **`/run/media/USERNAME/.drives`**;



Сетевые диски в файловом менеджере Dolphin (включена политика **`Отображение сетевых дисков в домашнем каталоге`**, задано **`Имя каталога монтирования сетевых дисков машины`** — my_share, задано **`Имя каталога монтирования сетевых дисков пользователя`** — share, для сетевых дисков пользователя отключен префикс .net):



Примечание

В приведенном выше примере:

```
net.my_share -> /media/gpupdate/my_share
share -> /run/media/<пользователь>/share
```

Все настройки политики подключения сетевого диска хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/Drives/Drives.xml**
- **{GUID GPT}/User/Preferences/Drives/Drives.xml**

В одном GPO возможно задать подключение более одного сетевого диска. Пример файла **Drives.xml** с двумя сетевыми дисками:

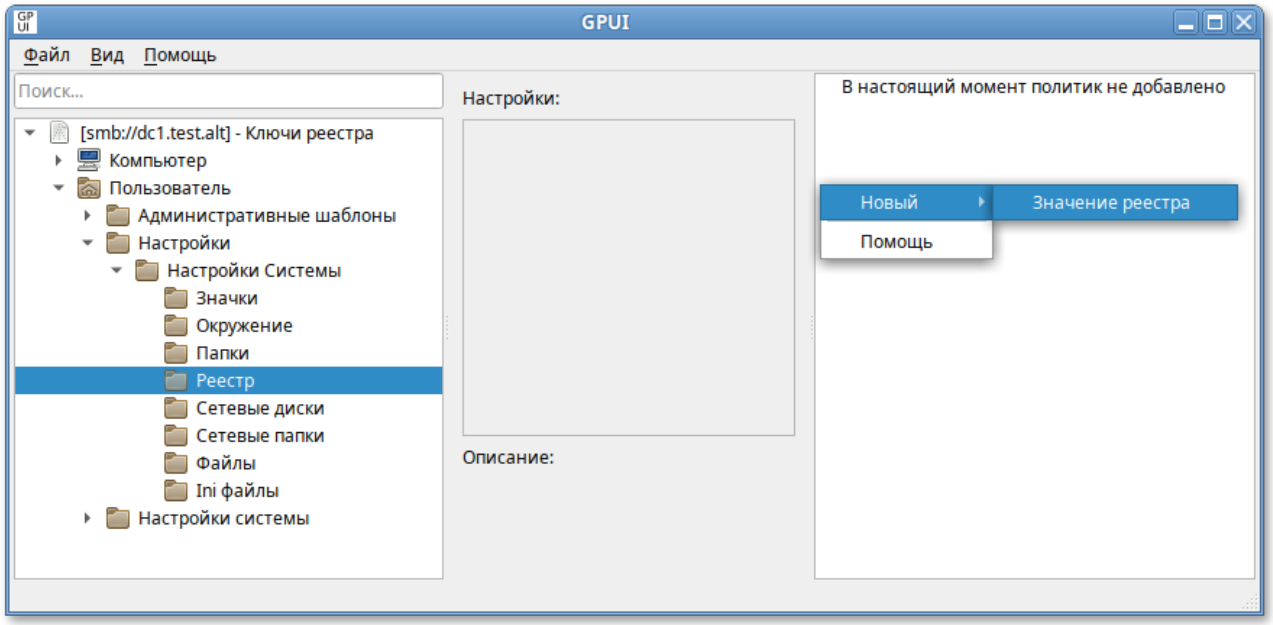
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<Drives clsid="{8FDDCC1A-0C3C-43cd-A6B4-71A6DF20DA8C}">
<Drive bypassErrors="0"
        changed="2022-11-29 16:28:32"
        clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}"
        desc=""
        image="2"
        name="\\dc\Free"
        removePolicy="0"
        status="O:"
        uid="{D070D4D6-DEB5-4DDE-9A53-6AB33C90352A}"
        userContext="0">
```

```
        <Properties
            action="U"
            allDrives="SHOW"
            cpassword=""
            label=""
            letter="O"
            path="\\dc\Free"
            persistent="1"
            thisDrive="SHOW"
            useLetter="1"
            userName=""/>
    </Drive>
    <Drive bypassErrors="0"
            changed="2022-11-29 14:34:53"
            clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}"
            desc=""
            image="2"
            name="I:"
            status="I:"
            uid="{4BDA1724-4BBF-4B4D-B299-E81080D9A4B5}"
            userContext="0">
        <Properties
            action="U"
            allDrives="SHOW"
            cpassword=""
            label=""
            letter="I"
            path="\\dc1.test.alt\sysvol"
            persistent="1"
            thisDrive="SHOW"
            useLetter="0"
            userName=""/>
    </Drive>
    </Drives>
```

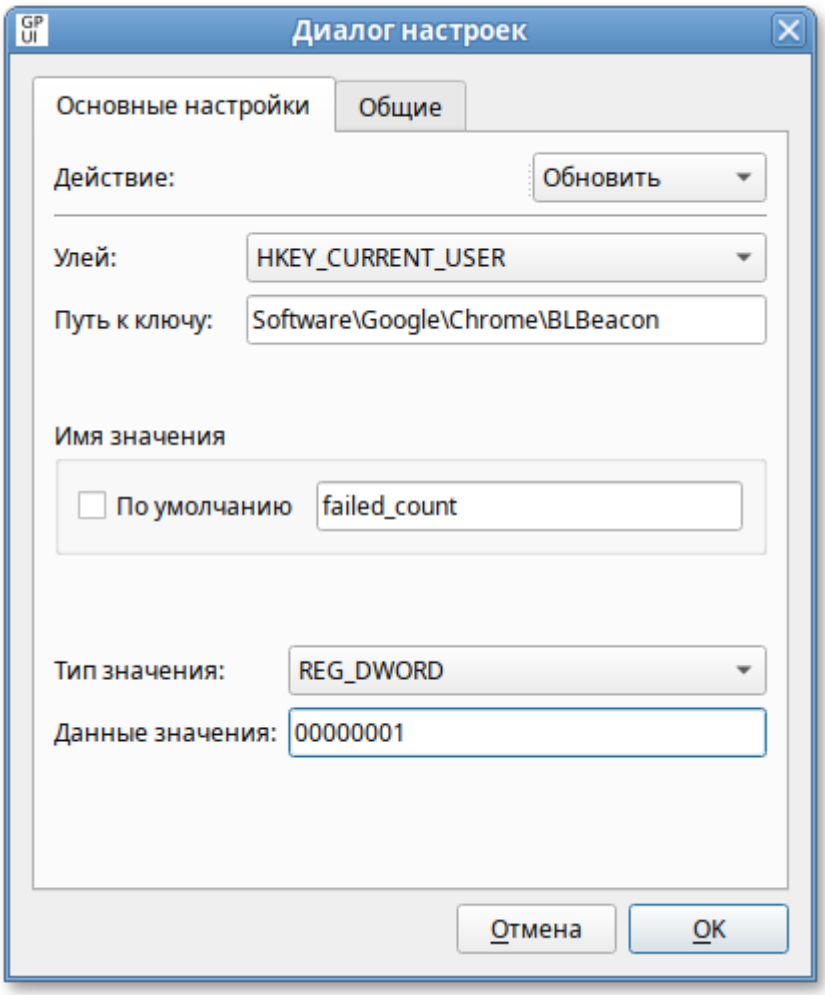
29.6.8. Настройка реестра

Групповая политика **`Настройка реестра`** позволяет управлять настройками реестра Windows.

Для настройки этой политики следует перейти в **Компьютер/Пользователь** → **Настройки** → **Настройки системы** → **Реестр**. В контекстном меню свободной области выбрать пункт **Новый** → **Значение реестра**



В диалоговом окне **Диалог настроек** задать настройки политики:



Опции доступные на вкладке **Основные настройки**:

- **Действие** — действие, которое будет выполняться для элемента реестра:
  - **Создать** — создание нового значения или раздела реестра;

- **Удалить** — удаление значения или раздела реестра и всех его значений и подразделов;
- **Заменить** — удаление и повторное создание значения или раздела реестра. Если целевым объектом является значение реестра, то конечным результатом действия будет перезапись всех существующих параметров, сопоставленных данному значению реестра. Если целевым объектом является раздел реестра, то конечным результатом будет удаление всех значений и подразделов реестра, и останется только имя значения по умолчанию без данных. Если значение или раздел реестра не существует, то действие **Заменить** приведет к созданию нового значения или раздела;
- **Обновить** — изменение параметров существующего значения или раздела реестра. Это действие отличается от **Заменить** тем, что оно обновляет только параметры, определенные в элементе настройки. Все остальные параметры значения или раздела реестра остаются прежними. Если значение или раздел реестра не существует, то действие **Обновить** приведет к созданию нового значения или раздела;

Улей — улей (куст) для раздела реестра:

- **HKEY_CLASSES_ROOT** — информация о зарегистрированных в Windows типах файлов (это псевдоним для HKEY_LOCAL_MACHINE\Software\Classes);
- **HKEY_CURRENT_USER** — настройки пользователя, вошедшего в Windows (это псевдоним для HKEY_USERS\куст текущего пользователя). HKEY_USERS\.Default используется в том случае, когда HKEY_CURRENT_USER настроен в разделе конфигурации компьютера;
- **HKEY_LOCAL_MACHINE** — настройки, относящиеся к компьютеру (параметр по умолчанию для политики компьютера). Эти параметры применяются ко всем пользователям компьютера;
- **HKEY_USERS** — настройки для всех пользователей (параметр по умолчанию для политики пользователя). Эти параметры применяются к отдельным пользователям;
- **HKEY_CURRENT_CONFIG** — сведения о настройках оборудования (это псевдоним для HKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current);

Путь к ключу — путь к ключу. Не нужно указывать улей и вводить косую черту до или после пути. Это поле воспринимает переменные процесса настройки;

Имя значения — для настройки значения следует установить, либо отметку в пункте **По умолчанию**, чтобы принять значение раздела по умолчанию, либо ввести имя настраиваемого значения. Чтобы настроить только раздел, следует оставить это поле пустым. В этом поле можно указать переменные;

Тип значения — тип значения. Данный параметр доступен только при выбранном действии **Создать**, **Заменить** или **Обновить** и введённом значении **Имя значения**;

Данные значения — значения реестра. Чтобы настроить только раздел, следует оставить это поле пустым. В этом поле можно указать переменные. Данный параметр доступен только при выбранном действии **Создать**, **Заменить** или **Обновить** и введенном значении **Имя значения**.

Все настройки политики управления настройками реестра Windows хранятся в файлах:

- **{GUID GPT}/Machine/Preferences/Registry/Registry.xml**
- **{GUID GPT}/User/Preferences/Registry/Registry.xml**

Пример файла **Registry.xml**:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<RegistrySettings clsid="{A3CCFC41-DFDB-43a5-8D26-0FE8B954DA51}">
  <Registry changed="2022-11-21 18:36:20"
        clsid="{9CD4B2F4-923D-47f5-A062-E897DD1DAD50}"
        image="12"
        name="failed_count"
        status="failed_count"
        uid="{D5855321-D2BA-4595-BD28-4DF452BFF65F}"
        bypassErrors="1">
    <Properties
        action="U"
        displayDecimal="0"
        hive="HKEY_CURRENT_USER"
        key="Software\Google\Chrome\BLBeacon"
        name="failed_count"
        type="REG_DWORD"
        value="00000001">
        <SubProp id="" mask="0" value="0"/">
    </Properties>
  </Registry>
</RegistrySettings>
```

29.6.9. Указание прокси-сервера

С помощью групповых политик можно указать прокси-сервер.

Примечание

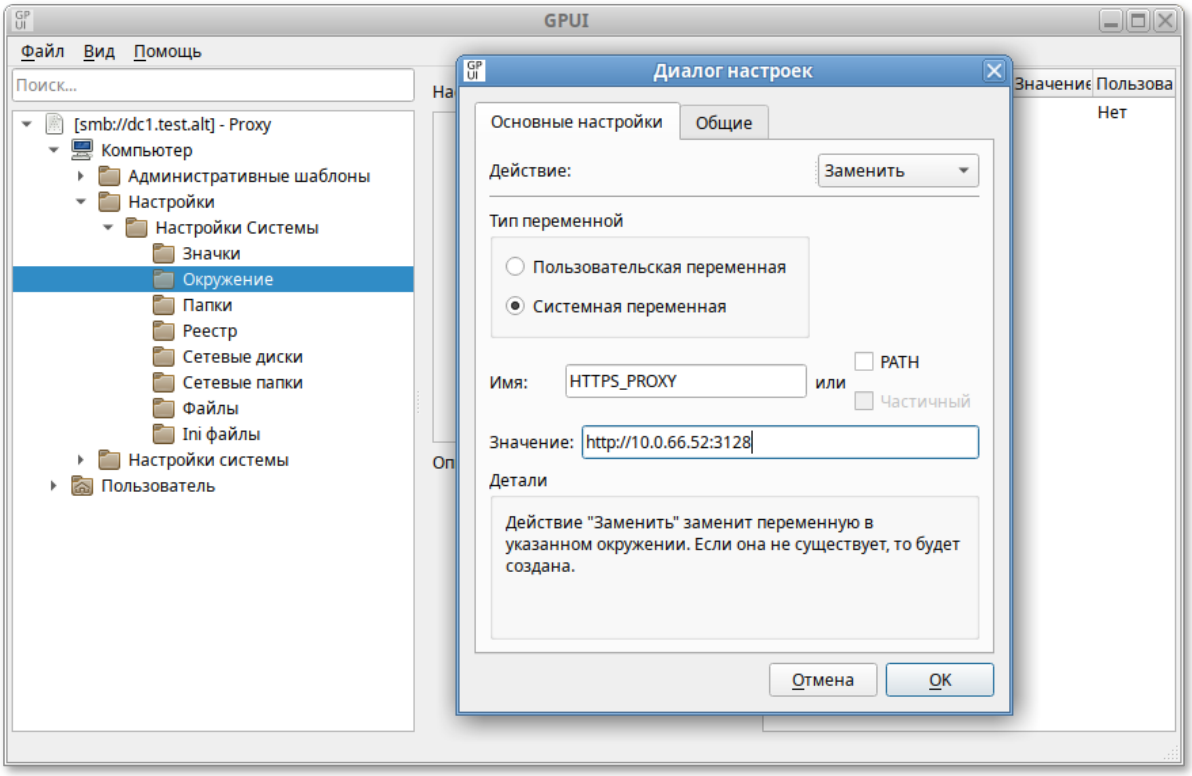
Если прокси-сервер был настроен в модуле **Прокси-сервер** ЦУС, предварительно необходимо удалить эти настройки и в файле **/etc/sysconfig/network** удалить строки:

```
HTTP_PROXY=
HTTPS_PROXY=
FTP_PROXY=
NO_PROXY=
```

Для настройки этой политики используется политика управления переменными среды (см. раздел Управление переменными среды).

Настройка политики для указания прокси-сервера:

1. Настроить групповую политику управления переменными окружения:



- в поле **Действие** выбрать пункт **Заменить**;
- в поле **Имя** указать имя переменной: **HTTPS_PROXY**;
- в поле **Значение** указать адрес и порт прокси-сервера, и, при необходимости, аутентификационные данные в формате **http://username:password@address:port**

2. Аналогичным способом создать настройки окружения для переменных **HTTP_PROXY** и **FTP_PROXY** (в поле **Имя** указывать соответственно **HTTP_PROXY**, **FTP_PROXY**).

Проверка применения политики:

1. Применить групповые политики на целевом компьютере, выполнив команду:

```
$ gpupdate
```

2. Повторно авторизоваться на целевом компьютере.

3. Проверить наличие переменных окружения, выполнив команду:

```
$ env |grep PROXY
HTTP_PROXY=http://10.0.66.52:3128
HTTPS_PROXY=http://10.0.66.52:3128
FTP_PROXY=http://10.0.66.52:3128
```

4. Запустить веб-браузер, убедиться, что сайты открываются через прокси-сервер.

29.6.10. Настройка периодичности запроса конфигураций

Для изменения периодичности запроса конфигураций можно создать файлы:

- **/etc/systemd/user/gpupdate-user.timer.d/override.conf** — изменение пользовательского таймера;
- **/etc/systemd/system/gpupdate.timer.d/override.conf** — изменение системного таймера.

С указанием периодичности запроса конфигураций, например:

```
[Timer]
OnUnitActiveSec = 10min
```

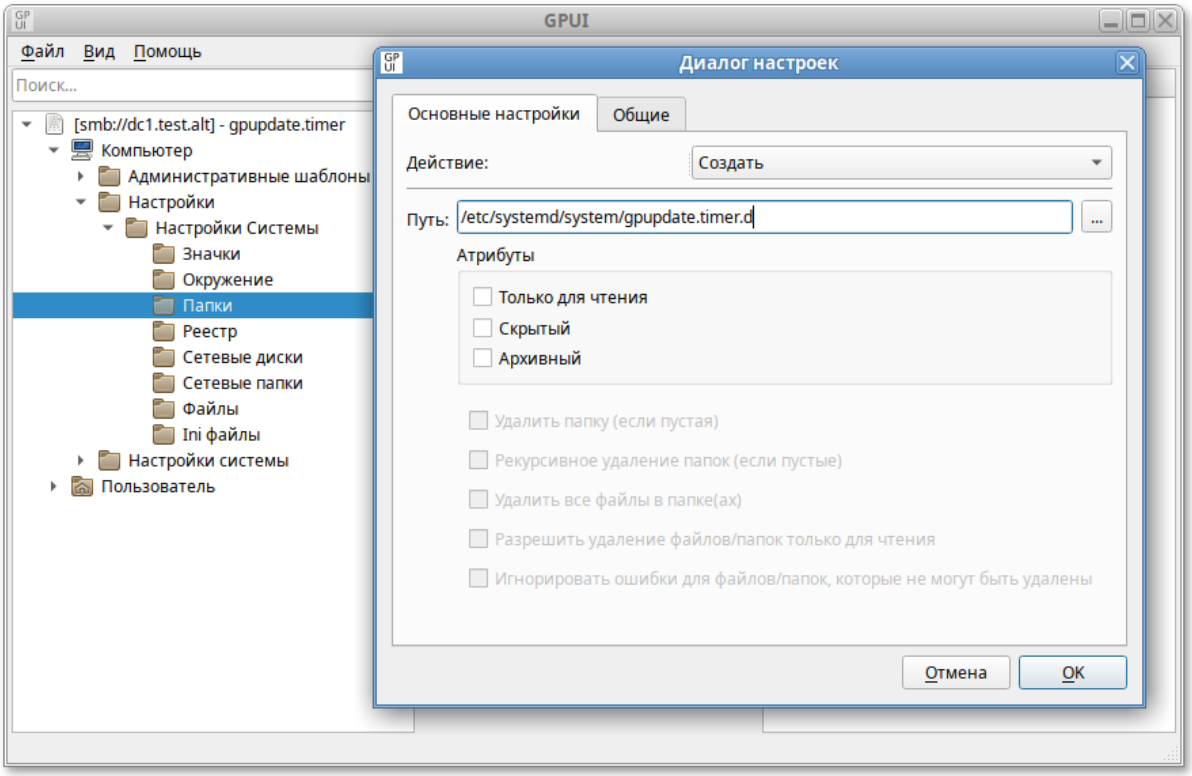
где 10min — периодичность запроса конфигураций.

Периодичность запроса конфигураций (запроса gpupdate) можно установить с помощью групповых политик.

Для настройки этой политики используются политика управления каталогами (см. раздел Управление каталогами) и политика управления INI-файлами (см. раздел Управление INI-файлами).

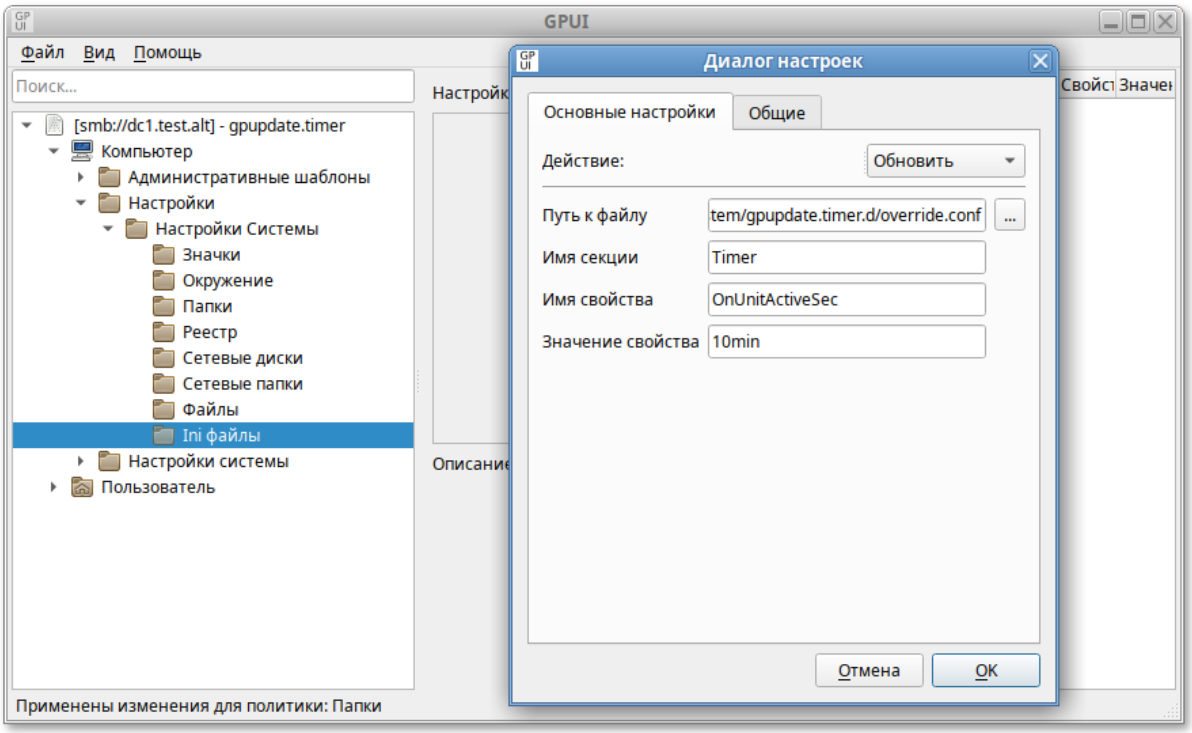
Пример настройки политики задания периодичности запроса конфигураций:

1. Настроить групповую политику создания каталога:



- в поле **Действие** выбрать пункт **Создать**;
- в поле **Путь** указать **/etc/systemd/system/gpupdate.timer.d** (или **/etc/systemd/system/gpupdate-user.timer.d** для пользовательского таймера).

2. Настроить групповую политику создания INI-файла:



- в поле **Действие** выбрать пункт **Обновить**;
- в поле **Путь к файлу** указать **/etc/systemd/system/gpupdate.timer.d/override.conf** (или **/etc/systemd/system/gpupdate-user.timer.d/override.conf** для пользовательского таймера);
- в поле **Имя секции** указать **Timer**;
- в поле **Имя свойства** указать **OnUnitActiveSec**;
- в поле **Значение свойства** указать периодичность запроса, в данном примере 10 минут: **10min**.

Проверка применения политики:

1. Применить групповые политики на целевом компьютере, выполнив команду:

```
$ gpupdate
```

2. Выполнить команду (или перезагрузить компьютер):

```
# systemctl daemon-reload
```

3. Убедиться, что политика применилась, выполнив команды

```
$ cat /etc/systemd/system/gpupdate.timer.d/override.conf
[Timer]
OnUnitActiveSec = 10min
```

```
$ systemctl status gpupdate.timer
…
 Active: active (waiting) since Mon 2024-06-10 16:29:23 EET; 44s ago
Trigger: Mon 2024-06-10 16:39:25 EET; 9min left
```

Примечание

Применить пользовательские настройки можно, выполнив команду:

```
$ systemctl --user daemon-reload
```

Примечание

Файл **override.conf** подменяет настройки системной библиотеки в файле **/lib/systemd/system/gpupdate.timer** только если значение секции **Timer** в файле **override.conf** меньше, чем значение аналогичной секции в **gpupdate.timer**.

29.7. Управление logon-скриптами

Групповые политики позволяют запускать сценарии запуска и завершения работы компьютера, входа и выхода из системы пользователя. Возможно связать один или несколько файлов сценариев (scripts) с четырьмя инициируемыми событиями:

- Для машины:
  - Запуск компьютера (Startup)
  - Выключение компьютера/Завершение работы (Shutdown)
- Для пользователя:
  - Вход пользователя (Logon)
  - Выход пользователя (Logoff)

Система выполняет сценарии на языках, которые поддерживает клиентский компьютер. В среде Windows эту задачу выполняет Windows Script Host (WSH), который поддерживает языки сценариев, включая bat, cmd, VBScript и Jscript. В случае, если указано более одного сценария, они будут выполняться согласно перечню в списке.

Примечание

В сценариях, запускаемых на машинах на базе ОС «Альт», необходимо в первой строке указывать шебанг, например, *#!/usr/bin/env bash*

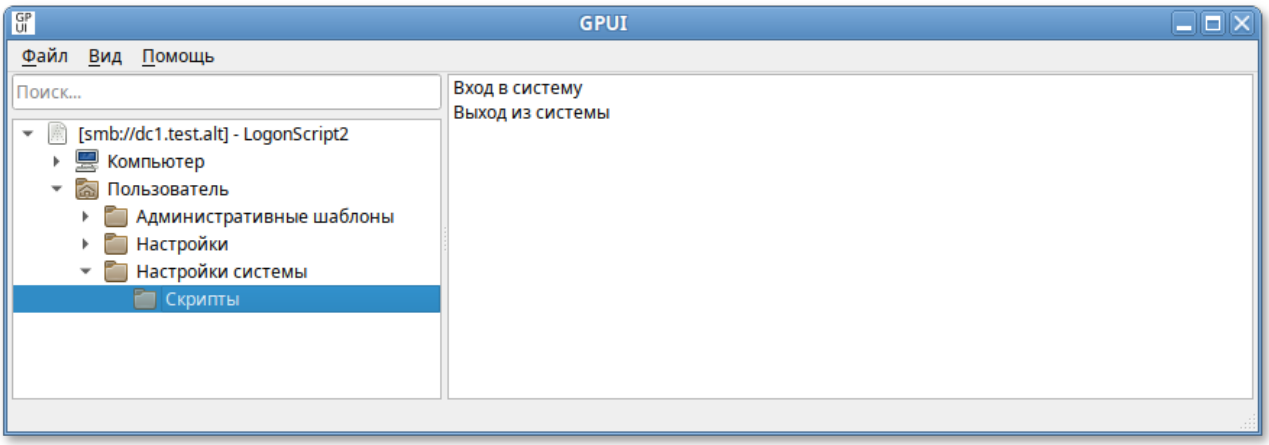
Примечание

Если сценарии (scripts) хранятся в SYSVOL, они реплицируются между контроллерами домена. SYSVOL доступен всем членам домена, что гарантирует запуск сценария.

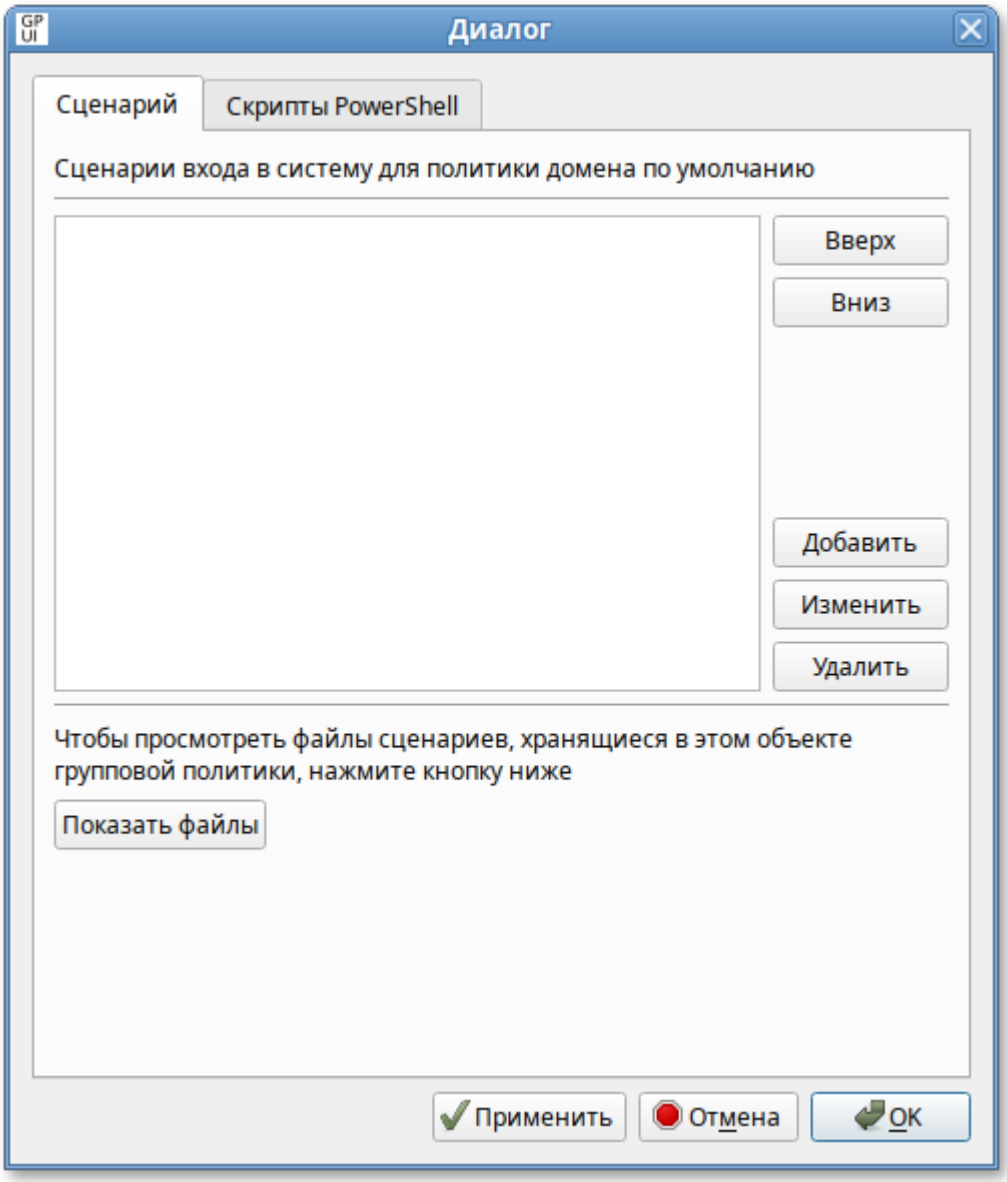
29.7.1. Сценарии для входа/выхода пользователя

Для удобства можно скопировать нужные сценарии в каталог **User\Scripts\Logon** (например, **\\test.alt\sysvol\test.alt\Policies\{20DDB816-421B-4861-8AC5-007E56CB67D0}\User\Scripts\Logon**) или **User\Scripts\Logoff** соответствующей политики.

Для настройки политики следует перейти в **Пользователь** → **Настройки системы** → **Скрипты**. Щёлкнуть левой кнопкой мыши на политике **Вход в систему** или **Выход из системы**:

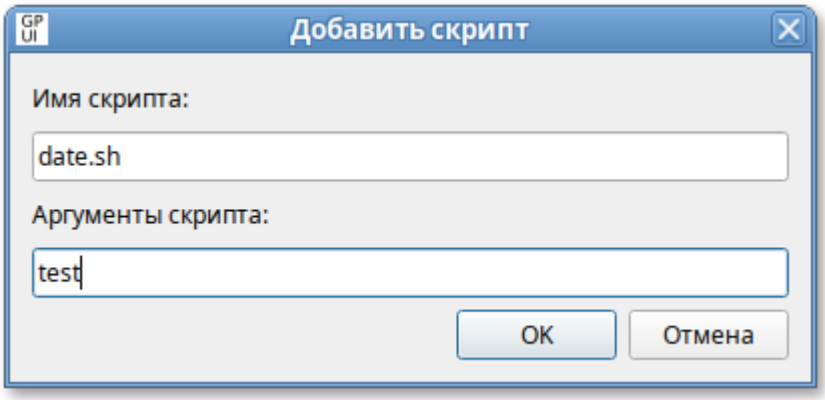


В диалоговом окне свойств политики нажать кнопку **Добавить**:



В диалоговом окне **Добавить скрипт** в поле **Имя скрипта** ввести путь к сценарию, в поле **Аргументы скрипта** ввести необходимые параметры аналогично вводу этих параметров в командной строке. Нажать кнопку **OK**.

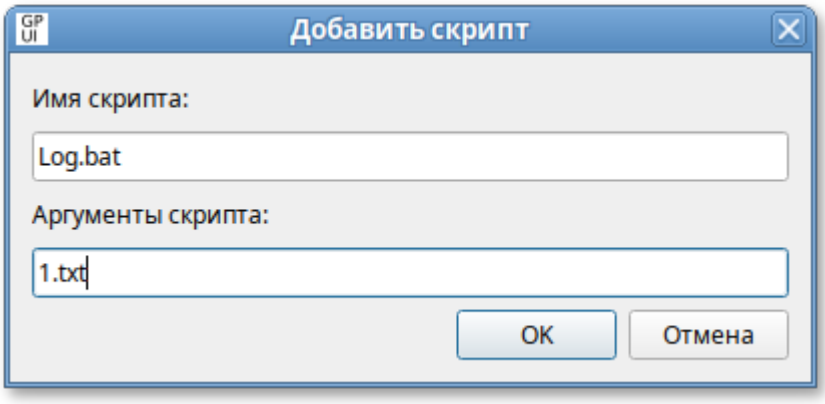
Пример добавления сценария для ОС «Альт»:



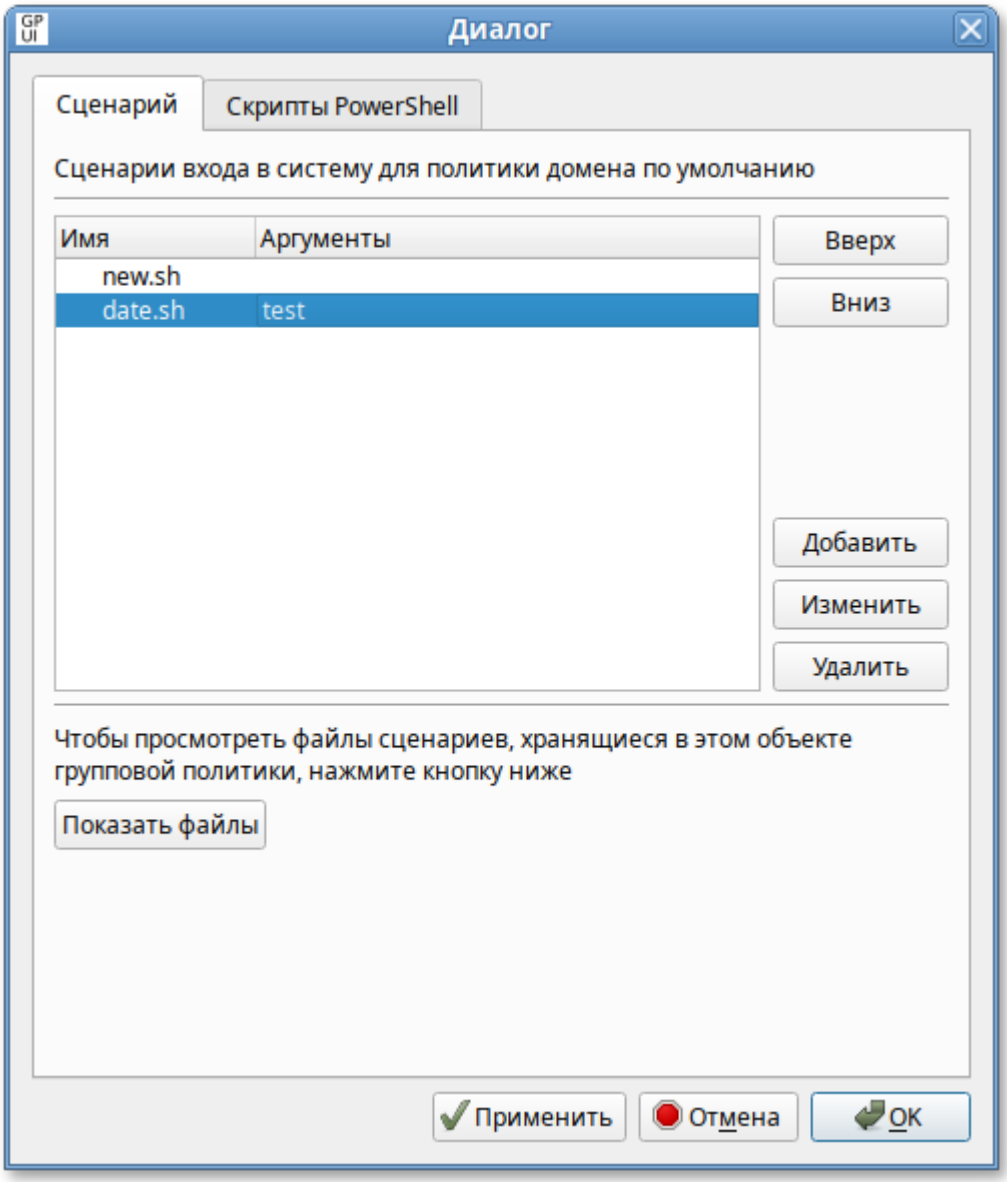
Примечание

Применение локальных скриптов реализовано в механизме **gpupdate** версии 0.9.11. В версиях ниже скрипты для ОС «Альт» должны находиться в GPT настраиваемого объекта групповой политики.

Пример добавления сценария для ОС Windows (можно указать локальный скрипт на компьютере клиента):



При назначении нескольких сценариев они будут применяться в заданном порядке. Чтобы переместить сценарий в списке вверх/вниз, следует выбрать его в списке и нажать кнопку **Вверх**/**Вниз**. Для того чтобы изменить параметры сценария, необходимо выбрать его в списке и нажать кнопку **Изменить**. Кнопка **Удалить** предназначена для удаления сценария из списка:

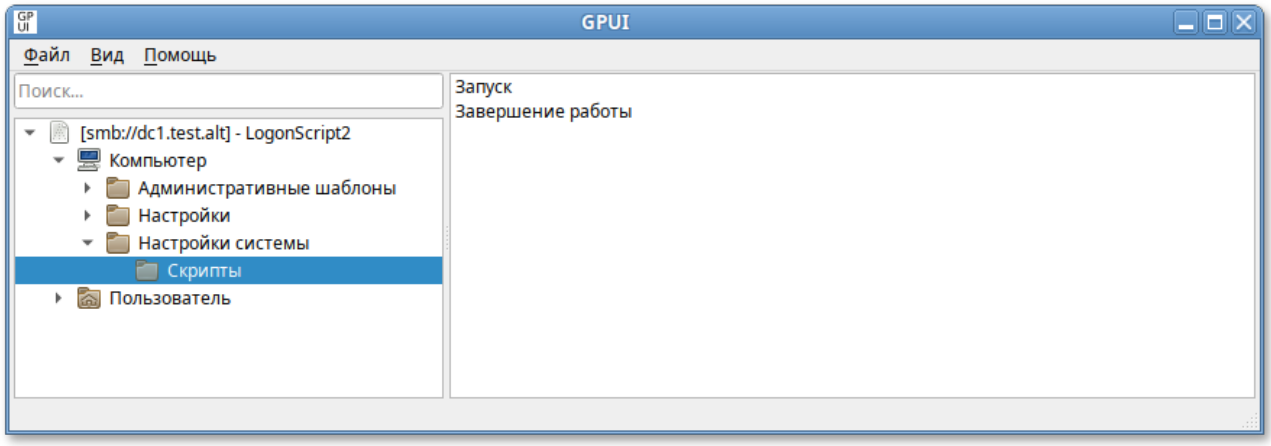


На вкладке **Скрипты PowerShell** можно добавить сценарии с расширением ***.ps1**.

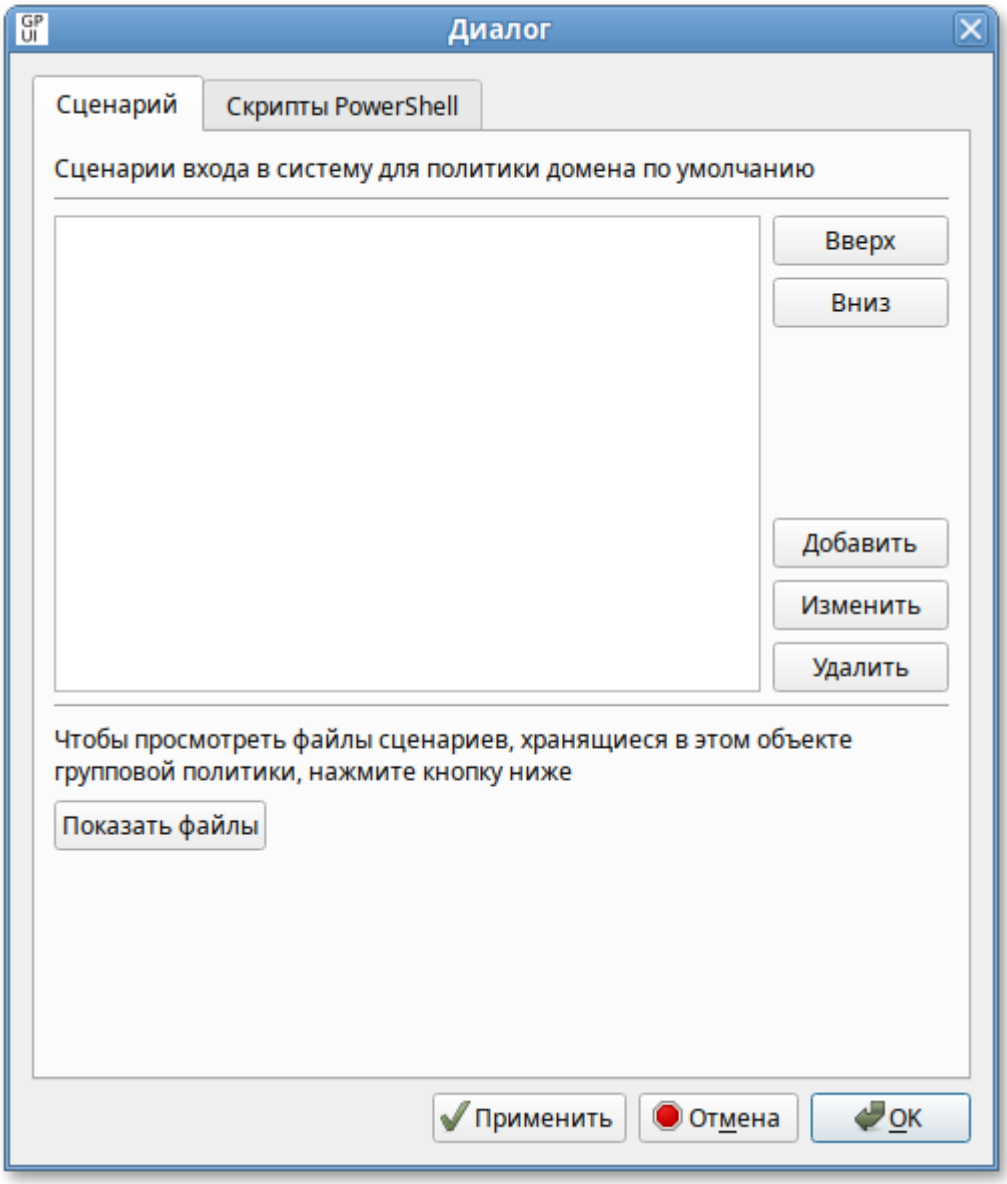
29.7.2. Сценарии для автозагрузки или завершения работы компьютера

Для удобства можно скопировать нужные сценарии в каталог **Machine\Scripts\Startup** (например, **\\test.alt\sysvol\test.alt\Policies\{20DDB816-421B-4861-8AC5-007E56CB67D0}\Machine\Scripts\Startup**) или **Machine\Scripts\Shutdown** соответствующей политики.

Для настройки политики следует перейти в **Компьютер** → **Настройки системы** → **Скрипты**. Щёлкнуть левой кнопкой мыши на политике **Запуск** или **Завершение работы**:

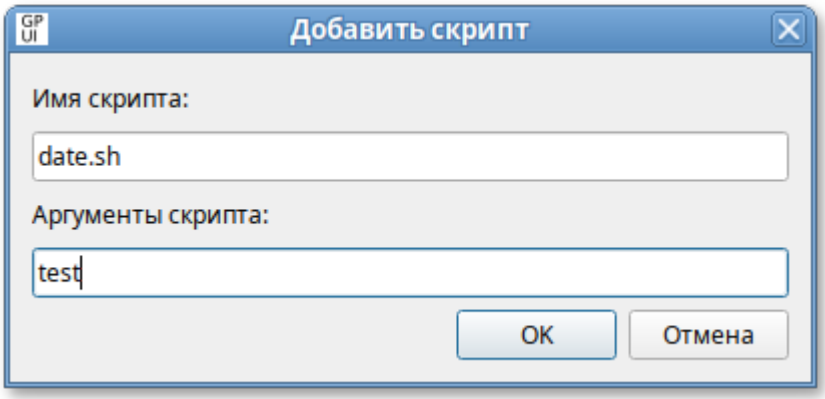


В диалоговом окне свойств политики нажать кнопку **Добавить**:



В диалоговом окне **Добавить скрипт** в поле **Имя скрипта** ввести путь к сценарию, в поле **Аргументы скрипта** ввести необходимые параметры аналогично вводу этих параметров в командной строке. Нажать кнопку **OK**.

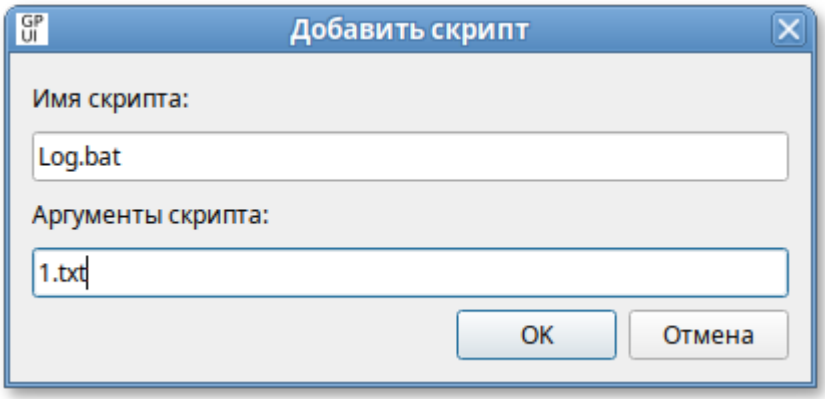
Пример добавления сценария для ОС «Альт»:



Примечание

Применение локальных скриптов реализовано в механизме *gpupdate* версии 0.9.11. В версиях ниже скрипты для ОС «Альт» должны находиться в GPT настраиваемого объекта групповой политики.

Пример добавления сценария для ОС Windows (можно указать локальный скрипт на компьютере клиента):



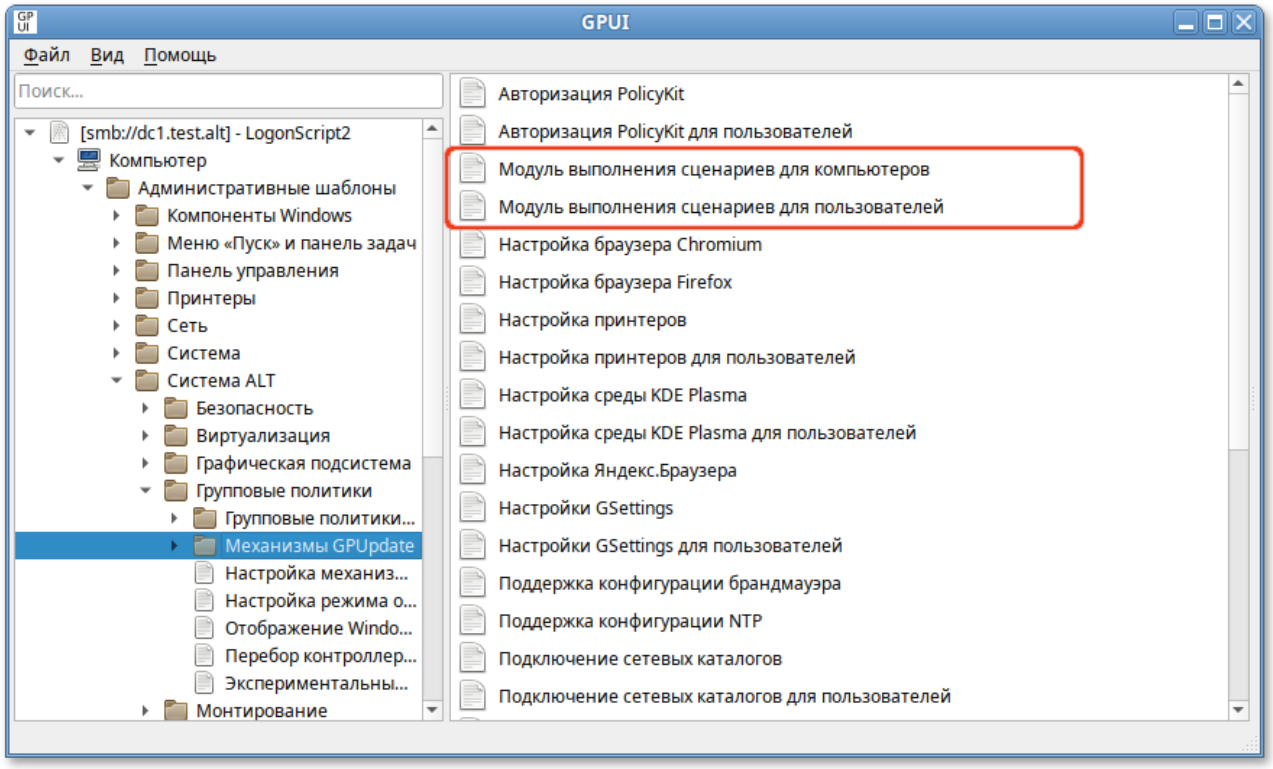
При назначении нескольких сценариев они будут применяться в заданном порядке. Чтобы переместить сценарий в списке вверх/вниз, следует выбрать его в списке и нажать кнопку **Вверх**/**Вниз**. Для того чтобы изменить параметры сценария, необходимо выбрать его в списке и нажать кнопку **Изменить**. Кнопка **Удалить** предназначена для удаления сценария из списка.

На вкладке **Скрипты PowerShell** можно добавить сценарии с расширением ***.ps1**.

29.7.3. Включение экспериментальных групповых политик

Политики управления logon-скриптами относятся к экспериментальным, поэтому на машинах с ОС «Альт» где они применяются должны быть включены экспериментальные групповые политики (подробнее см. раздел Экспериментальные групповые политики).

Включить/отключить механизм групповых политик управления logon-скриптами также можно, включив/отключив политики **Модуль выполнения сценариев для компьютеров** или **Модуль выполнения сценариев для пользователей** (**Компьютер** → **Административные шаблоны** → **Система ALT** → **Групповые политики** → **Механизмы GPUpdate**):



29.7.4. Файлы настроек политики

Файлы сценариев входа и выхода пользователя (за исключением локальных) хранятся в каталогах: **{GUID GPT}/User/Scripts/Logon** и **{GUID GPT}/User/Scripts/Logoff**. Настройки политики для сценариев входа и выхода пользователя хранятся в файле **{GUID GPT}/User/Scripts/scripts.ini**. В файле **scripts.ini** перечисляются все скрипты, выполняемые в сценариях входа и выхода пользователя из системы. Сценарии входа начинаются с преамбулы **[Logon]**, сценарии выхода начинаются с преамбулы **[Logoff]**.

Пример файла **scripts.ini**:

```
[Logon]
0CmdLine=date.sh
0Parameters=test
1CmdLine=test.sh
1Parameters=new
[Logoff]
0CmdLine=touch.sh
0Parameters=
1CmdLine=Logoff.bat
1Parameters=1.txt
2CmdLine=C:\share\Logon.bat
2Parameters=
```

Файлы сценариев запуска и завершения работы компьютера (за исключением локальных) хранятся в каталогах: **{GUID GPT}/Machine/Scripts/Shutdown** и **{GUID GPT}/Machine/Scripts/Startup**. Настройки политики для сценариев запуска и завершения работы компьютера хранятся в файле **{GUID GPT}/Machine/Scripts/scripts.ini**. В файле **scripts.ini** перечисляются все скрипты, выполняемые в сценариях запуска и завершения работы компьютера. Сценарии запуска компьютера начинаются с преамбулы **[Startup]**, сценарии завершения работы начинаются с преамбулы **[Shutdown]**.

Пример файла **scripts.ini**:

```
[Startup]
0CmdLine=hello.bat
0Parameters=
1CmdLine=notescript.vbs
1Parameters=
2CmdLine=notescript2.vbs
2Parameters=
3CmdLine=touch.bat
3Parameters=
[Shutdown]
0CmdLine=touch.bat
0Parameters=
```

Файл **scripts.ini** закодирован в формате UTF-16LE (little-endian).

Примечание

Настройки политики для скриптов PowerShell хранятся в файлах **{GUID GPT}/User/Scripts/pgscripts.ini** (для сценариев входа и выхода пользователя) и **{GUID GPT}/Machine/Scripts/pgscripts.ini** (для запуска и завершения работы компьютера).

29.7.5. Диагностика проблем

См. раздел Диагностика проблем при работе с политикой скриптов.

Глава 30. Расширение возможностей ГП

30.1. Схема административных шаблонов (ADMX)

30.2. Разработка новой политики

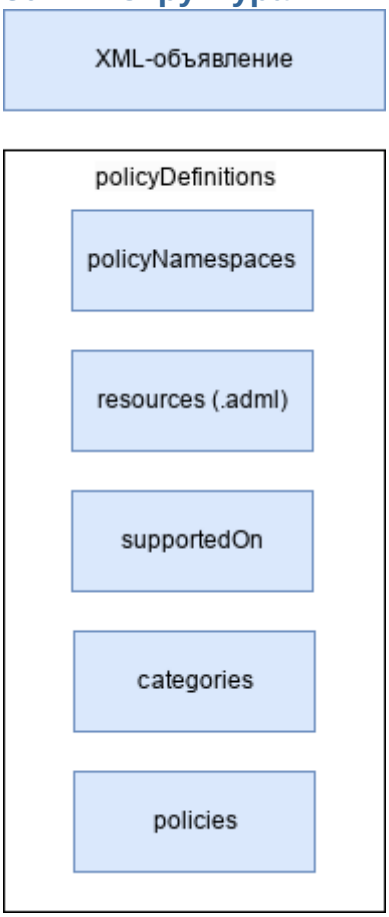
30.1. Схема административных шаблонов (ADMX)

Административные шаблоны представляют собой два типа XML-файлов:

- независимый от языка файл (ADMX), описывающий структуру категорий и параметры политики административных шаблонов, отображаемых в редакторе управления групповыми политиками;
- набор зависящих от языка файлов (ADML), которые предоставляют локализованные части, отображаемые в редакторе управления групповыми политиками. Каждый ADML-файл представляет один язык, для которого требуется поддержка.

Каждому ADMX-файлу должен соответствовать свой ADML-файл с таким же именем.

30.1.1. Структура ADMX-файла



ADMX-файл состоит из семи разделов:

- XML-объявление. XML-объявлением является заголовок файла, который не рассматривается в качестве фрагмента ADMX-документа, но является его необходимой частью и помещается в начале файла для того, чтобы указать на то, что это XML-документ;
- policyDefinitions. Элемент, который содержит все остальные элементы ADMX-файла;
- policyNamespaces. Этот элемент определяет уникальное пространство имён для данного ADMX-файла. Данный элемент также обеспечивает сопоставление с пространствами имен во внешних файлах, если ADMX-файл ссылается на элементы category, определенные в другом ADMX-файле;
- resources. Определяет требования к ресурсам определенного языка и минимальную необходимую версию связанного ADML-файла;
- supportedOn. Определяет ссылки на локализованные текстовые строки, определяющие ОС или приложения, на которые влияет определенный параметр политики;
- categories. Содержит список категорий, в которых параметр политики текущего ADMX-файла будет отображаться в редакторе объектов групповой политики;
- policies. Содержит определения отдельных параметров политики.

XML-объявление не считается частью документа ADMX. Однако рекомендуется начинать файл ADMX с объявления XML, чтобы указать, что это документ XML.

Синтаксис XML-объявления:

```
<?xml version="<версия>" encoding="<кодировка"?>
```

где:

- *version* — версия XML, используемая в документе (обязательный атрибут). В настоящее время поддерживается только версия 1.0;
- *encoding* — информация о кодировке символов, используемая анализаторами XML-документов. ADMX-файлы всегда имеют кодировку UTF-8.

Примечание

XML-объявление не должно предваряться комментариями, пробелами или другими инструкциями по обработке XML.

Элемент policyDefinitions — это элемент документа для ADMX-файла, который определяет набор параметров политики реестра. Элемент policyDefinitions также объявляет пространство имен по умолчанию для всех элементов в ADMX-файле.

Синтаксис элемента *policyDefinitions*:

```
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVerison.MinorVersion>"
schemaVersion="<MajorVerison.MinorVersion>"
xmlns=" http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions" >
  <policyNamespaces> … </policyNamespaces>
  <supersededAdm> … </supersededAdm>
  <resources> … </resources>
  <supportedOn> … </supportedOn>
  <categories> … </categories>
  <policies> … </policies>
</policyDefinitions>
```

Атрибуты элемента *policyDefinitions* описаны в таблице Атрибуты элемента policyDefinitions.

Таблица 30.1. Атрибуты элемента policyDefinitions

Атрибут	Обязательный	Описание
xmlns:xsd	Нет	Обозначение элементов и типов данных, используемых в схеме пространства имен
xmlns:xsi	Нет	Обозначение пространства имён экземпляра XML-схемы, предоставленной в самом пространстве

Атрибут	Обязательный	Описание
revision	Да	Версия ADMX-файла, которая в большинстве случаев предназначена для отслеживания внесенных изменений. Синтаксис: `revision="<MajorVerison.MinorVersion>"` где MajorVersion и MinorVersion являются номерами версии, например, revision="1.0"
schemaVersion	Да	Указывает версию схемы, используемую средствами работы с ГП для определения того, поддерживается ли ими формат конкретных ADMX-файлов. Синтаксис этой команды идентичен синтаксису revision
xmlns	Нет	Пространство имен схемы ГП

Примечание

Инструменты ГП успешно используют файлы ADMX-файлы, которые не содержат атрибутов xmlns. Но эти атрибуты должны входить в состав ADMX-файла, так как, в противном случае, он может не пройти проверку на правильность формата XML-файла.

Дочерние элементы *policyDefinitions* описаны в таблице Дочерние элементы policyDefinitions.

Таблица 30.2. Дочерние элементы policyDefinitions

Элемент	Обязательный	Описание

policyNamespaces	Да	Определяет уникальное имя пространства имен политики в файле ADMX, а также любых пространств имен, на которые оно ссылается в других файлах ADMX.
		
		Синтаксис:
		
		`<policyNamespaces>`
		`  <target> … </target>`
		`  <using> … </using>`
		`</policyNamespaces>`
		
		где:
		
		▸target — определяет уникальное имя пространства имен политики в ADMX-файле (обязательный элемент);
		▸using — ссылается на существующую категорию или имя supportOn из другого пространства имен политики.

supersededAdm	Нет	Данный элемент ссылается на имя ADM-файла, заменяемого ADMX-файлом
resources	Да	

Элемент	Обязательный	Описание
		Определяет требования для ресурсов определенного языка и минимальную необходимую версию связанного ADML-файла. Синтаксис: `<resources minRequiredRevision="<MajorVerison.MinorVersion>" fallbackCulture="<language name>"/>` где: ▸minRequiredRevision — минимальный уровень версии соответствующего ADML-файла; ▸fallbackCulture — язык, который будет использоваться, если ни в одном расположении не будет найден соответствующий ADML-файл. Если этот атрибут не указан будет использоваться английский язык.
supportedOn	Нет	Определяет сопоставление ссылки на локализированные строки текста с ОС или приложениями, на которые влияют конкретные параметры политики. Синтаксис: `<supportedOn> <definitions> … </definitions> </supportedOn>` Элементы definitions содержат информацию о поддерживаемой версии.
categories	Нет	Содержит список категорий, в которых параметр политики текущего ADMX-файла будет отображаться в редакторе управления групповыми политиками. Синтаксис: `<categories> <category> … </category> </categories>` Элемент category указывает имя уникальной категории, которая будет отображаться в редакторе объектов групповой политики.
policies	Нет	Содержит список определений параметров политики. Синтаксис:

Элемент	Обязательный	Описание
		<policies> <policy> … </policy> </policies> Дочерний элемент policy соответствует одному параметру ГП, отображаемому в редакторе объектов групповой политики. Элемент *policy* описывает всю информацию о параметре политики, но включает ссылку на определение параметра.

Синтаксис элемента *category*:

```
<category name="<logical or friendly name>"
displayName="$(string.<category text>)"
explainText="$(string.<help text>)">
  <parentCategory> … </parentCategory>
  <seeAlso> … </seeAlso>
  <keywords> … </keywords>
</category>
```

Атрибуты элемента *category* описаны в таблице Атрибуты элемента category.

Таблица 30.3. Атрибуты элемента category

Атрибут	Обязательный	Описание
name	Да	Имя, которое будет использоваться для конкретного поддерживаемого приложения и версии
displayName	Да	Ссылка на текстовую строку категории, расположенную в таблице строк ADML-файла
explainText	Нет	Текст объяснения или справки, связанный с конкретной категорией

Дочерние элементы *category* описаны в таблице Дочерние элементы category.

Таблица 30.4. Дочерние элементы category

Элемент	Обязательный	Описание
parentCategory	Да	Ссылка на родительскую категорию
seeAlso	Нет	Ссылка на другой элемент, который может быть связан с этим. Этот элемент не поддерживается и будет игнорироваться текущей ГП
keywords	Нет	Содержит индексные слова, которые можно использовать для поиска элементов. Этот элемент не поддерживается и будет игнорироваться текущей ГП

Синтаксис элемента *policy*:

```
<policy name="<logical or friendly name>"
class="Machine|User|Both"
displayName="$(string.<category text>)"
explainText="$(string.<help text>)"
presentation="$(presentation.<parameter>)"
key="<registry key>"
valueName="<registry valuename>">
  <parentCategory> … </parentCategory>
  <supportedOn> … </supportedOn>
  <enabledValue> … </enabledValue>
  <disabledValue> … </disabledValue>
  <enabledList> … </enabledList>
  <disabledList> … </disabledList>
  <elements> … </elements>
</policy>
```

Атрибуты элемента *policy* описаны в таблице Атрибуты элемента policy.

Таблица 30.5. Атрибуты элемента policy

Атрибут	Обязательный	Описание
name	Да	Уникальное имя элемента политики (строка, желательно без пробелов и специальных символов)
class	Да	Определяет, где в каком разделе редактора ГП будет размещён элемент политики: компьютере, пользователе или в обоих узлах. Может принимать значения: «User», «Machine» или «Both»
displayName	Да	Имя, отображаемое в GPUI или оснастке консоли управления ГП. Ссылка на строку, расположенную в ADML-файле
explainText	Нет	Текст объяснения или справки, связанный с элементом политики. Ссылка на строку, расположенную в ADML-файле
presentation	Нет	Подписи параметров политики. Ссылка на строки, расположенные в ADML-файле
key	Да	Местоположение ключа реестра, в котором будет создан параметр реестра
valueName	Нет	Значение реестра, которое будет настроено для этого конкретного элемента политики

Дочерние элементы *policy* описаны в таблице Дочерние элементы policy.

Таблица 30.6. Дочерние элементы policy

Элемент	Обязательный	Описание
parentCategory	Да	Ссылка на родительскую категорию (раздел, в котором будет отображаться политика)
supportedOn	Нет	Логическое имя supportOn, определенное в элементе supportOn для этого файла (ссылка на поддерживаемые продукты)
enabledValue	Нет	Значение, которое раздел реестра примет, если политика включена. Синтаксис:

Элемент	Обязательный	Описание

		<pre><enabledValue>
		  <delete /> | <decimal> … </decimal> | <string> … </string>
		</enabledValue></pre>
		где:
		- *delete* — удалить значение или ключ реестра;
		- *decimal* — десятичное беззнаковое число;
		- *string* — строка, ограниченая 255 символами.

disabledValue	Нет	Значение, которое раздел реестра примет, если политика отключена. См. описание enabledValue.

enabledList	Нет	Набор значений и ключей реестра, представляющих включенное состояние элемента политики
		
		Синтаксис:
		<pre><enabledList defaultKey="<registry subkey>">
		  <item> … </item>
		</enabledList></pre>
		где:
		- атрибут *defaultKey* — подраздел реестра по умолчанию для всех элементов;
		- *item* — подраздел реестра со связанным значением.

disabledList	Нет	Набор значений и ключей реестра, представляющих отключенное состояние элемента политики. См. описание enabledList
elements	Нет	Один из пяти типов параметров (см.ниже), которые можно задать в настройке политики

Синтаксис элемента *elements*:

```
<elements>
  <boolean> … </boolean>
  <decimal> … </decimal>
  <text> … </text>
  <enum> … </enum>
  <list> … </list>
</elements>
```

Дочерние элементы *elements* описаны в таблице Дочерние элементы elements.

Таблица 30.7. Дочерние элементы elements

Элемент	Обязательный	Описание

boolean	Нет	Представляет логический элемент в политике.
		
		Синтаксис:
		
		`<boolean id="<ID>"`
		`  clientExtension="<GUID>"`
		`  key="<RegKey>"`
		`  valueName="<Name>">`
		`  <trueValue> … </trueValue>`
		`  <falseValue> … </falseValue>`
		`  <trueList> … </trueList>`
		`  <falseList> … </falseList>`
		`</boolean>`
		
		где:
		
		▪ атрибут *id* — сопоставление с элементом (обязательный);
		▪ атрибут *clientExtension* — клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом;
		▪ атрибут *key* — местоположение ключа реестра, под которым будет создан параметр реестра;
		▪ атрибут *valueName* — значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный);
		▪ *trueValue* — устанавливает значение на основе истинного условия;
		▪ *falseValue* — устанавливает значение на основе ложного условия;
		▪ *trueList* — устанавливает значения на основе истинного состояния;
		▪ *falseList* — устанавливает значения на основе ложного состояния.
		
		Пример:
		
		`<boolean id="OrgXfceThunar_blocker"`
		`key="Software\BaseALT\Policies\PolkitLocks"`
		`valueName="org.xfce.thunar">`
		`  <trueValue>`
		`  <decimal value="1" />`
		`  </trueValue>`
		`  <falseValue>`
		`  <decimal value="0" />`
		`  </falseValue>`
		`</boolean>`
		
		Для элемента *boolean* в ADMX-файле требуется элемент checkBox с соответствующим идентификатором в ADML-файле.

decimal	Нет	

Элемент	Обязательный	Описание

		Представляет числовой/десятичный элемент в политике. Число может быть определено для хранения в виде числового или строкового репрезентативного значения
		
		Синтаксис:
		
		`<decimal id="<ID>"`
		`clientExtension="<GUID>"`
		`key="<RegKey>"`
		`valueName="<Name>"`
		`required="true|false"`
		`minValue="<MinValue>"`
		`maxValue="<MaxValue>"`
		`storeAsText="true|false"`
		`soft="true|false" />`
		
		где:
		
		▸атрибут *id* — сопоставление с элементом (обязательный);
		▸атрибут *clientExtension* — клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом;
		▸атрибут *key* — местоположение ключа реестра, под которым будет создан параметр реестра;
		▸атрибут *valueName* — значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный);
		▸атрибут *required* — требует ввести значение в поле параметра;
		▸атрибут *minValue* — минимально допустимое значение;
		▸атрибут *maxValue* — максисмально допустимое значение;
		▸атрибут *soft* — следует ли перезаписывать существующий подраздел;
		▸атрибут *storeAsText* — если true, сохранить десятичное значение как значение реестра REG_SZ.
		
		Пример:
		
		`<decimal id="OrgMateSessionIdleDelay_setter"`
		`valueName="org.mate.session.idle-delay"`
		`minValue="1"`
		`maxValue="2147483647" />`
		
		Для элемента *decimal* требуется элемент decimalTextBox с соответствующим идентификатором в ADML-файле.

text	Нет	Представляет текстовый элемент в политике. Синтаксис:

Элемент	Обязательный	Описание

		<pre><text id="<ID>"
		  clientExtension="<GUID>"
		  key="<RegKey>"
		  valueName="<Name>"
		  required="true|false"
		  maxLength="<maxLength>"
		  expandable="true|false"
		  soft="true|false" /></pre>
		где:
		▸атрибут *id* — сопоставление с элементом (обязательный);
		▸атрибут *clientExtension* — клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом;
		▸атрибут *key* — местоположение ключа реестра, под которым будет создан параметр реестра;
		▸атрибут *valueName* — значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный);
		▸атрибут *required* — требует ввести значение в поле параметра;
		▸атрибут *maxLength* — максисмально допустимое количество символов;
		▸атрибут *expandable* — если true, значение подраздела реестра будет создано как расширяемый строковый тип (REG_EXPAND_SZ) вместо строкового типа (REG_SZ);
		▸атрибут *soft* — следует ли перезаписывать существующий подраздел.
		
		Пример:
		<pre><text id="OrgMateBackgroundSecondaryColor_setter"
		  valueName="org.mate.background.secondary-color" /></pre>
		Элемент *text* допускает строковые значения длиной до 1023 символов.
		
		Для элемента text требуется соответствующий элемент textBox или comboBox с соответствующим идентификатором в ADML-файле.

enum	Нет	Представляет элемент перечисления.
		
		Синтаксис:
		<pre><enum id="<ID>"
		  clientExtension="<GUID>"
		  key="<RegKey>"</pre>

Элемент	Обязательный	Описание

```
  valueName="<Name>"
  required="true|false">
  <item> … </item>
</enum>
```

где:

- атрибут *id* — сопоставление с элементом (обязательный);
- атрибут *clientExtension* — клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом;
- атрибут *key* — местоположение ключа реестра, под которым будет создан параметр реестра;
- атрибут *valueName* — значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный);
- атрибут *required* — требует ввести значение в поле параметра;
- *item* — представляет набор отображаемых имен с одним значением или набор значений подразделов реестра.
  Синтаксис:

```
<item displayName="$(string.<placeholder for text>)">
  <item> … </item>
</item>
```

  где *displayName* — ссылка на отображаемую строку, расположенную в таблице строк ADML-файла.

Пример:

```
<enum id="OrgMateColorShadingType_setter"
required="true" valueName="org.mate.background.color-
shading-type">
  <item displayName="$(string.org-mate-background-
color-shading-type-horizontal-gradient)">
    <value>
      <string>horizontal-gradient</string>
    </value>
  </item>
  <item displayName="$(string.org-mate-background-
color-shading-type-vertical-gradient)">
    <value>
      <string>vertical-gradient</string>
    </value>
  </item>
  <item displayName="$(string.org-mate-background-
color-shading-type-solid)">
    <value>
      <string>solid</string>
    </value>
  </item>
</enum>
```

Элемент	Обязательный	Описание
		Элемент *enum* обычно связан с элементом раскрывающегося списка в редакторе объектов групповой политики. Для элемента *enum* требуется элемент dropdownList с соответствующим идентификатором в ADML-файле.

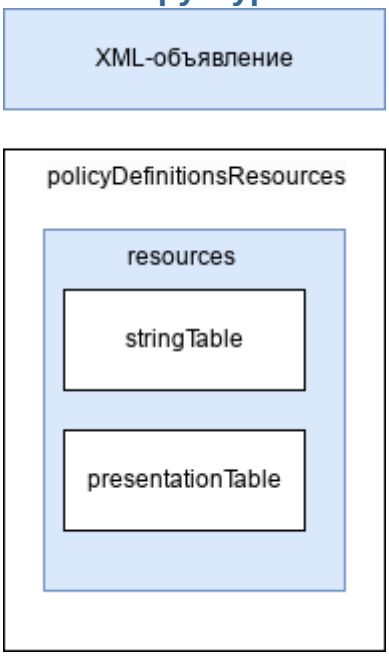
list	Нет	Представляет элемент списка в политике.
		
		Синтаксис:
		
		`<list id="<ID>"`
		`clientExtension="<GUID>"`
		`key="<RegKey>"`
		`valuePrefix="<Name>">`
		`additive="true|false"`
		`expandable="true|false"`
		`explicitValue="true|false" >`
		`</ list>`
		
		где:
		
		▸атрибут *id* — сопоставление с элементом (обязательный);
		▸атрибут *clientExtension* — клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом;
		▸атрибут *key* — местоположение ключа реестра, под которым будет создан параметр реестра;
		▸атрибут *valuePrefix* — префикс, добавляемый к увеличенному целому числу, создает подраздел реестра, используемый при настройке значений политики (обязательный);
		▸атрибут *additive* — если для этого параметра указано значение true, существующие подразделы не удаляются, а значения, установленные в списке, добавляются к существующим подразделам;
		▸атрибут *explicitValue* — если для этого параметра указано значение true, пользователь должен указать значение подраздела реестра и имя подраздела реестра. В списке отображаются два столбца: один для имени и один для данных;
		▸атрибут *expandable* — если true, значение подраздела реестра будет создано как расширяемый строковый тип (REG_EXPAND_SZ) вместо строкового типа (REG_SZ).
		
		Пример:
		
		`<list id="InstallPackagesList"`
		`key="Software\BaseALT\Policies\Packages\Install"`
		`additive="true"/>`

Элемент	Обязательный	Описание
		Для элемента *list* требуется элемент listBox с соответствующим идентификатором в ADML-файле.

Примечание

Если элемент *elements* определен, он должен содержать хотя бы один дочерний элемент. Количество и тип элементов, определенных в ADMX-файле, должны соответствовать элементам presentation, определенным в соответствующем ADML-файле.

30.1.2. Структура ADML-файла



ADML-файл состоит из пяти разделов:

- XML-объявление. XML-объявлением является заголовок файла, который не рассматривается в качестве фрагмента ADML-документа, но является его необходимой частью и помещается в начале файла для того, чтобы указать на то, что это XML-документ;
- policyDefinitionResources. Содержит объявление пространства имен по умолчанию для всех элементов ADML-файла. Данный элемент содержит все остальные элементы ADML-файла;
- resources. Содержит элементы stringTable и presentationTable для указанного языка. Эти два элемента должны быть определены в ADML-файле в определенном порядке: элемент stringTable, за которым следует элемент presentationTable, как того требует схема ADMX;
- stringTable. Используя этот элемент ADML-файла, можно указать заголовок параметра ГП, текст с описанием, текст со ссылкой на поддержку, названия категорий, а также подписи для параметров. Элемент stringTable нельзя объявлять более одного раза. Данный элемент включает в себя вложенные элементы string, позволяющие определить все указанные выше данные;

- presentationTable. Представляет собой структуру дочерних элементов управления параметрами отдельных параметров ГП, включая всевозможные флажки, переключатели, подписи, подсказки и прочее. Дочерними элементами являются элементы presentation, которые представляют собой отображаемые сведения параметров для параметров политики.

Элемент *policyDefinitionResources* — это элемент документа для ADMX-файла, который определяет набор параметров политики реестра. Элемент policyDefinitions также объявляет пространство имен по умолчанию для всех элементов в ADMX-файле.

Синтаксис элемента *policyDefinitionResources*:

```
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVerison.MinorVersion>"
schemaVersion="<MajorVerison.MinorVersion>"
xmlns=" http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions" >
  <displayName> … </displayName>
  <description> … </description>
  <annotation> … </annotation>
  <resources> … </resources>
</policyDefinitionResources>
```

Атрибуты элемента *policyDefinitionResources* описаны в таблице Атрибуты элемента policyDefinitionResources.

Таблица 30.8. Атрибуты элемента policyDefinitionResources

Атрибут	Обязательный	Описание
xmlns:xsd	Нет	Обозначение элементов и типов данных, используемых в схеме пространства имен
xmlns:xsi	Нет	Обозначение пространства имён экземпляра XML-схемы, предоставленной в самом пространстве
revision	Да	Версия ADMX-файла. Синтаксис: `revision="<MajorVerison.MinorVersion>"` где MajorVersion и MinorVersion являются номерами версии, например, revision="1.0"
schemaVersion	Да	Указывает версию схемы, используемую средствами работы с ГП. Синтаксис этой команды идентичен синтаксису revision
xmlns	Нет	Пространство имен схемы ГП

Дочерние элементы *policyDefinitionResources* описаны в таблице Дочерние элементы policyDefinitionResources.

Таблица 30.9. Дочерние элементы policyDefinitionResources

Элемент	Обязательный	Описание
	Да	Локализованное название политики, содержащееся в ADML-файле

Элемент	Обязательный	Описание
displayName		
description	Нет	Описание параметров политики, содержащееся в ADML-файле
annotation	Да	Локализованный комментарий

resources	Нет	Содержит элементы *stringTable* и *presentationTable* для указанного языка.
		
		Синтаксис:
		
		`<resources>`
		`  <stringTable> … </stringTable>`
		`  <presentationTable> … </presentationTable>`
		`</resources>`

Дочерние элементы *resources* описаны в таблице Дочерние элементы resources.

Таблица 30.10. Дочерние элементы resources

Элемент	Обязательный	Описание

stringTable	Нет	Содержит отображаемые строки для следующих видов информации:
		
		- заголовок параметра групповой политики;
		- описание групповой политики;
		- определения поддерживаемых продуктов (SupportedOn);
		- названия категорий и описание категории;
		- подписи для параметров.
		
		Синтаксис:
		
		`<stringTable>`
		`  <string> … </string>`
		`</stringTable>`
		
		Элемент stringTable нельзя объявлять более одного раза.

presentationTable	Нет	Таблица элементов представления, представляющая структуру элементов управления параметрами для отдельных параметров групповой политики. Расположение элементов управления параметрами включает в себя: тип элемента ввода параметров (поле редактирования, ползунок, выпадающий список, флажки, переключатели); подписи и текст подсказки для ввода параметров; а также значения по умолчанию и диапазон возможных значений для каждого параметра. Синтаксис:

Элемент	Обязательный	Описание
		<presentationTable> <presentation> … </presentation> </presentationTable> Если в ADML-файле нет элементов представления, элемент PresentationTable можно опустить. Если элемент PresentationTable включен в ADML-файл, необходимо определить хотя бы один элемент представления. Элемент PresentationTable определяется в ADML-файле не более одного раза.

Синтаксис элемента *presentation*:

```
<presentation id="<logical or friendly name>">
  <text> … </text>
  <decimalTextBox> … </decimalTextBox>
  <textBox> … </textBox>
  <checkBox> … </checkBox>
  <comboBox> … </comboBox>
  <dropdownList> … </dropdownList>
  <listBox> … </listBox>
</presentation>
```

Атрибуты элемента *presentation* описаны в таблице Атрибуты элемента presentation.

Таблица 30.11. Атрибуты элемента presentation

Атрибут	Обязательный	Описание
id	Да	Указывает логическое имя при ссылке на информацию о представлении для определенного параметра политики

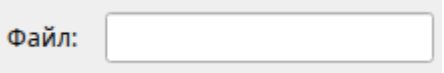
Дочерние элементы presentation описаны в таблице Дочерние элементы presentation.

Таблица 30.12. Дочерние элементы presentation

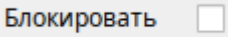
Элемент	Обязательный	Описание
text	Да	Локализованная строка. Используется для определения текста, расположенного выше и ниже поля ввода параметра. Синтаксис: <text>Локализованная строка</text>
decimalTextBox	Нет	Текстовое поле с элементом управления прокруткой или без него для ввода десятичных чисел в качестве параметра настройки политики. Должен быть связан с элементом decimal, определенным в элементе elements.

Элемент	Обязательный	Описание

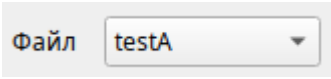
		Синтаксис:
		
		`<decimalTextBox refId="Sample_NumericTextLabel">Метка:</decimalTextBox>`
		
		где:
		
		атрибут *refId* — сопоставление с элементом.
		
		Пример:
		
		`<decimalTextBox refId="OrgMateScreensaverLockDelay_setter" defaultValue="3"> Скорость повтора </decimalTextBox>`

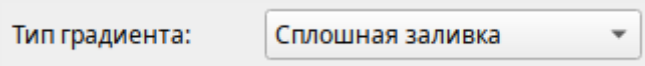
textBox	Нет	Текстовое поле. Этот элемент должен быть связан с элементом text, определенным в elements.
		
		Синтаксис:
		
		`<textBox refId="<ID>"> <label> … </label> <defaultValue> … </defaultValue> </textBox>`
		
		где:
		
		атрибут *refId* — сопоставление с элементом;
		label — подпись для параметра текстового поля (обязательный);
		defaultValue — строка, по умолчанию отображаемая в текстовом поле.
		
		Пример:
		
		`<textBox refId="OrgMateFilename_setter"> <label>Файл:</label> </textBox>`
		
		 

checkBox	Нет	Элемент флажка. Должен быть связан с элементом boolean, определенным в элементе elements. Синтаксис:

Элемент	Обязательный	Описание
		<checkBox refId="<ID> defaultChecked="true|false"> Placeholder label: </checkBox> где: атрибут *refId* — сопоставление с элементом (обязательный); атрибут *defaultChecked* — значение по умолчанию. Если не указано, атрибуту defaultChecked будет присвоено значение false. Пример: <checkBox refId="OrgXfceThunar_blocker"> Блокировать </checkBox> 
comboBox	Нет	Поле со списком со значениями по умолчанию или предлагаемыми записями. Должно быть связано с элементом text, определенным в элементе elements. Синтаксис: <comboBox refId="<ID> noSort="true|false"> <label> … </label> <default> … </default> <suggestion> … </suggestion> </comboBox> где: атрибут *refId* — сопоставление с элементом (обязательный); атрибут *noSort* — если true, отображать предлагаемые значения в определенном порядке элементов предложения; в противном случае отсортировать предлагаемые значения в алфавитном порядке. Если не указано, атрибуту noSort будет присвоено значение false; *label* — подпись для параметра (обязательный); *defaul* — строка, по умолчанию отображаемая в параметре; *suggestion* — строка раскрывающегося списка. Пример:

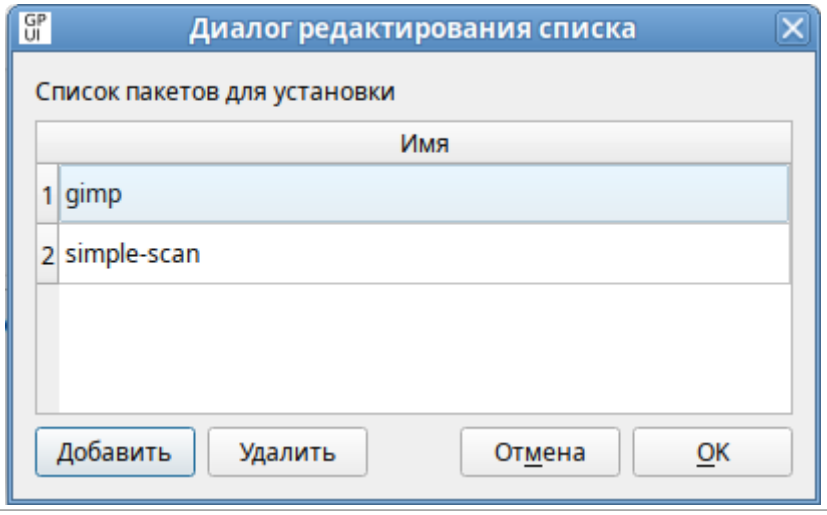
Элемент	Обязательный	Описание

		<pre><comboBox refId="OrgMateFilename_setter">
		  <label>Файл</label>
		  <default>None</default>
		  <suggestion>testA</suggestion>
		  <suggestion>testB</suggestion>
		  <suggestion>testC</suggestion>
		</comboBox></pre>
		 

dropdownList	Нет	Раскрывающийся список, с помощью которого пользователь может выбрать одну из отображаемых записей. Должен быть связан с элементом enum, определенным в элементе elements.
		
		Синтаксис:
		
		<pre><dropdownList refId="<ID>"
		  noSort="true|false">
		  defaultItem="<NumericValue>">
		  Placeholder label:
		</dropdownList></pre>
		где:
		
		▸атрибут *refId* — сопоставление с элементом (обязательный);
		▸атрибут *noSort* — если true, создать элемент spin; в противном случае создать текстовое поле для ввода чисел. Если не указано, атрибуту noSort будет присвоено значение true;
		▸атрибут *defaultItem* — числовое значение, определяющее выбор из списка элементов по умолчанию. Список элементов нумеруется, начиная с 0.
		
		Пример:
		
		<pre><dropdownList noSort="true" defaultItem="0"
		refId="OrgMateColorShadingType_setter">
		  Тип градиента:
		</dropdownList></pre>
		 

listBox	Нет	Представляет параметр списка с кнопками «Добавить» и «Удалить». Это единственный параметр, который можно использовать для управления несколькими значениями под одним ключом. Должен быть связан с элементом list, определенным в элементе elements. Синтаксис:

Элемент	Обязательный	Описание

		`<listBox refId="ID">Описание:</listBox>`
		где:
		атрибут *refId* — сопоставление с элементом.
		Пример:
		`<listBox refId="InstallPackagesList">`
		`  Список пакетов для установки`
		`</listBox>`
		 

Примечание

Дочерние элементы, указанные в элементе *presentation*, должны соответствовать элементам, определенным в элементе elements ADMX-файла.

30.1.3. Связывание информации из ADMX и ADML-файлов

В синтаксисе ADMX, элементы, управляющие представлением или локализованным отображением параметра, определяются в ADML-файле. Информация же, определяющая тип данных и значение параметра, задается в ADMX-файле. Различные элементы из этих двух файлов используются для создания определений параметров для настроек политики.

Ниже рассмотрен пример использования двух параметров checkbox для настройки одной политики.

Фрагмент XML из файла **`example.admx`** с элементом policy, который содержит два элемента флажка (checkbox):

```
<policy name="Sample_Checkbox" class="User"
displayName="$(string.Sample_Checkbox)"
explainText="$(string.Sample_Checkbox_Help)"
presentation="$(presentation.Sample_Checkbox)"
key="Software\BaseALT\Policies\gsettings">
  <parentCategory ref="system:ALT_Background_Mate" />
  <supportedOn ref="system:SUPPORTED_AltP9" />
  <elements>
    <boolean id="Checkbox_1" valueName="ExampleCheckbox1">
      <trueValue>
        <decimal value="1" />
      </trueValue>
      <falseValue>
        <decimal value="0" />
      </falseValue>
    </boolean>

    <boolean id="Checkbox_2" valueName="ExampleCheckbox2">
      <trueValue>
        <decimal value="0" />
      </trueValue>
      <falseValue>
        <decimal value="1" />
      </falseValue>
    </boolean>
  </elements>
</policy>
```

Фрагмент XML из файла **`example.admx`** с элементом policy, который содержит два элемента флажка (checkbox):

```
<presentation id="Sample_Checkbox">
  <checkBox refId="Checkbox_1">Первый параметр</checkBox>
  <checkBox refId="Checkbox_2" defaultChecked="true">Второй параметр — отмечен по
умолчанию</checkBox>
</presentation>
```

Примечание

Каждому ADMX-файлу должен соответсвовать ADML-файл с тем же именем. Редактор объектов групповой политики отобразит сообщение об ошибке, если не сможет найти соответствующий ADML-файл для каждого прочитанного ADMX-файла.

Есть две области координации между файлами ADMX и ADML:

1. Ссылка верхнего уровня между установкой политики и отображением её параметров. Политика, определяемая с помощью элемента *policy* в ADMX-файле, ссылается на определенный элемент *presentation* в ADML-файле через атрибут *presentation* элемента *policy*. В данном примере атрибут *presentation* определен как *presentation="$(presentation.Sample_Checkbox)"*. Текст *presentation.Sample_Checkbox* сообщает редактору объектов групповой политики ссылаться на элемент *presentationTable* ADML-файла, используя атрибут *id*, для которого установлено значение Sample_Checkbox.

Количество типов данных, а также тип данных (boolean, decimal, text, enum, item и list), определенные в элементе *elements* в ADMX-файле, должны соответствовать количеству и типу параметров, определенных в ADML-файле в элементе *presentation* (checkBox , textBox, decimalTextBox, ComboBox, dropdownList и listBox).

2. Ссылка между представлением типа данных в элементе *elements* и определением параметра в элементе *presentation*.

   В примере элемент *elements* содержит два элемента *boolean*:

```
<elements>
  <boolean id="Checkbox_1" valueName="ExampleCheckbox1">
    …
  </boolean>

  <boolean id="Checkbox_2" valueName="ExampleCheckbox2">
    …
  </boolean>
</elements>
```

   Элемент *presentation* содержит два элемента *checkBox*:

```
<presentation id="Sample_Checkbox">
  <checkBox refId="Checkbox_1">…</checkBox>
  <checkBox refId="Checkbox_2" defaultChecked="true">…</checkBox>
</presentation>
```

   Атрибут *id* элемента *boolean* используется для соответствия связанному элементу *checkBox*, на который ссылается атрибут *refId*.

В следующей таблице показано, как сопоставляется тип данных в ADMX-файле, с определением параметра в ADML-файле.

Таблица 30.13. Сопоставление

Тип данных в ADMX-файле	Определение параметра в ADML-файле
boolean	checkBox
text	textBox
decimal	decimalTextBox
text	comboBox
enum или item	dropdownList
list	listBox

30.1.4. Рекомендации для создания ADMX-файлов

При создании ADMX-файлов следует придерживаться следующих рекомендаций:

1. Чтобы избежать отображения повторяющихся узлов в редакторе объектов групповой политики, не следует использовать название категории, которое было ранее определено в родительской категории. Например, создание двух ADMX-файлов с одинаковой категорией приведет к тому, что редактор объектов групповой политики создаст два узла с одинаковым именем. Вместо этого следует создать собственный базовый файл (см.ниже), на который будут ссылаться все разрабатываемые ADMX-файлы.

2. Чтобы избежать циклических ссылок, один ADMX-файл не должен ссылаться на элементы категории другого ADMX-файла. Вместо этого базовую категорию компонента следует поместить в отдельный базовый файл.

3. Каждое пространство имен политики для ADMX-файла должно быть уникальным. Пространство имен политики определяется в целевом элементе ADMX-файла.

Создание пользовательского базового файла:

1. Создать ADMX-файл **`MyCompany.admx`** с определением категории MyCompany:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <policyNamespaces>
    <target prefix="mycompany" namespace="MyCompany.Policies.MyCompany" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <categories>
    <category name="MyCompany"
      displayName="$(string.MyCompany)"
      explainText="$(string.MyCompany_Help)" />
  </categories>
</policyDefinitions>
```

2. Создать ADML-файл **`ru-RU/MyCompany.adml`**, который будет содержать локализованное название категории:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="1.0" schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <displayName>Определение базовой категории</displayName>
  <description>Этот файл содержит определение базовой категории организации.
  </description>
  <resources>
    <stringTable>
      <string id="MyCompany">Моя организация</string>
      <string id="MyCompany_Help">Содержит параметры конфигурации,
      специфичные для организации.</string>
    </stringTable>
  </resources>
</policyDefinitionResources>
```

Чтобы обратиться к базовому файлу MyCompany, следует включить атрибут ***`using`*** в элемент ***`policyNamespaces`***. Атрибут пространства имен должен соответствовать пространству имен, определенному в пользовательском базовом файле (в примере ***`MyCompany.Policies.MyCompany`***). Атрибутом префикса может быть любое имя, уникальное для ADMX-файла. Рекомендуется по возможности использовать строку атрибута префикса из пользовательского базового файла, чтобы избежать путаницы. Например, следующий фрагмент файла **`example.admx`** определяет пространство имен и ссылается на базовый файл MyCompany в элементе ***`policyNamespaces`***:

```
<policyNamespaces>
  <target prefix="example" namespace="MyCompany.Policies.Example" />
  <using prefix="mycompany" namespace="MyCompany.Policies.MyCompany" />
</policyNamespaces>
```

30.2. Разработка новой политики

Программа gpupdate состоит из ряда механизмов, позволяющих обращаться к настройкам ОС «Альт». Механизмы обращаются к интерфейсам системы или отдельных приложений через API. Через систему механизмов gpupdate пользователю доступно создание собственных ГП так, чтобы не менять содержимое пакетов admx и gpupdate. В этом случае при очередном обновлении пакетов в системе не нарушится работа ГП — базовых и собственных. Появляется возможность создать свой набор политик, необходимый для внутреннего использования.

Механизмы применения параметров, которые позволяют создавать собственные политики:

- Systemd. Управление запуском служб Systemd;
- Polkit. Механизм Polkit отвечает за безопасность и управляет разрешениями при обращении к системным процессам;
- Gsettings. Управление настройками системной базы реестра dconf;
- Control. Механизм Control управляет состоянием конфигурационных файлов;
- Скрипты загрузки системы и авторизации пользователя (logon/logoff/startup/shutdown).

Примечание

Скрипты загрузки системы и авторизации пользователя (Logon/logoff/startup/shutdown) не связаны с подготовкой ADMX-файлов и формируются через раздел настроек системы (работа со скриптами подробно описана на странице: Управление logon-скриптами).

Шаги создания новой политики:

1. Подобрать механизм реализации политики — systemd, control, gsettings, polkit;
2. Загрузить шаблоны ADMX-файлов для выбранного механизма;
3. Описать в ADMX-файлах (admx + adml) структуру новой политики и её описание на русском или английском языке;
4. Проверить корректность кода в ADMX-файлах, открыв редактор групповых политик — GPUI в «Альт» или RSAT в Windows;
5. Загрузить собственный набор административных шаблонов групповых политик (admx) на контроллер домена в каталог Sysvol.

30.2.1. Пример для механизма Systemd

Подсистема инициализации и управления службами Systemd в ГП «Альт» может запускать или останавливать службы. Systemd позволяет задавать расписание запуска служб, выполнять монтирование и многое другое. Через ГП «Альт» возможно управление самостоятельно созданной пользовательской службой.

Примечание

Просмотреть список загруженных служб можно, выполнив команду:

```
$ systemctl list-units --type service --all
```

Получить список всех установленных файлов модулей можно, выполнив команду:

```
$ systemctl list-unit-files
```

Пример создания новой политики для веб-сервера Apache (служба httpd2):

1. Создать файл **MySystemd.admx**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0" xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/
PolicyDefinitions">
  <policyNamespaces>
    <target prefix="systemdunits"
namespace="BaseALT.Policies.MySystemdUnits" />
    <using prefix="system" namespace="BaseALT.Policies.System" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <policies>
<policy class="Machine" displayName="$(string.httpd2_service)"
explainText="$(string.httpd2_service_help)"
key="Software\BaseALT\Policies\SystemdUnits"
valueName="httpd2.service" name="httpd2.service">
      <parentCategory ref="system:ALT_Systemd"/>
      <supportedOn ref="system:SUPPORTED_AltP9"/>
      <enabledValue>
        <decimal value="1"/>
      </enabledValue>
      <disabledValue>
        <decimal value="0"/>
      </disabledValue>
    </policy>
  </policies>
</policyDefinitions>
```

2. Создать файл **ru-RU/MySystemd.adml**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>Определения служб</displayName>
  <description>Этот файл содержит дополнительные определения systemd-служб</
description>
  <resources>
    <stringTable>
      <string id="httpd2_service">Веб-сервер Apache</string>
      <string id="httpd2_service_help">Эта политика определяет,
включен ли systemd юнит веб-сервера Apache.
      </string>
    </stringTable>
  </resources>
</policyDefinitionResources>
```

3. Создать файл **en-US/MySystemd.adml**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>Services definitions</displayName>
  <description>This file contains the systemd services definitions</
description>
  <resources>
    <stringTable>
      <string id="httpd2_service">Apache Web Server</string>
      <string id="httpd2_service_help">This policy determines whether the
systemd unit of Apache Web Server is enabled.
      </string>
    </stringTable>
  </resources>
</policyDefinitionResources>
```

4. Скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPUI.

   В Windows RSAT:

   - файл **MySystemd.admx** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions**
   - файл **ru-RU/MySystemd.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\ru-RU**
   - файл **en-US/MySystemd.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\en-US**

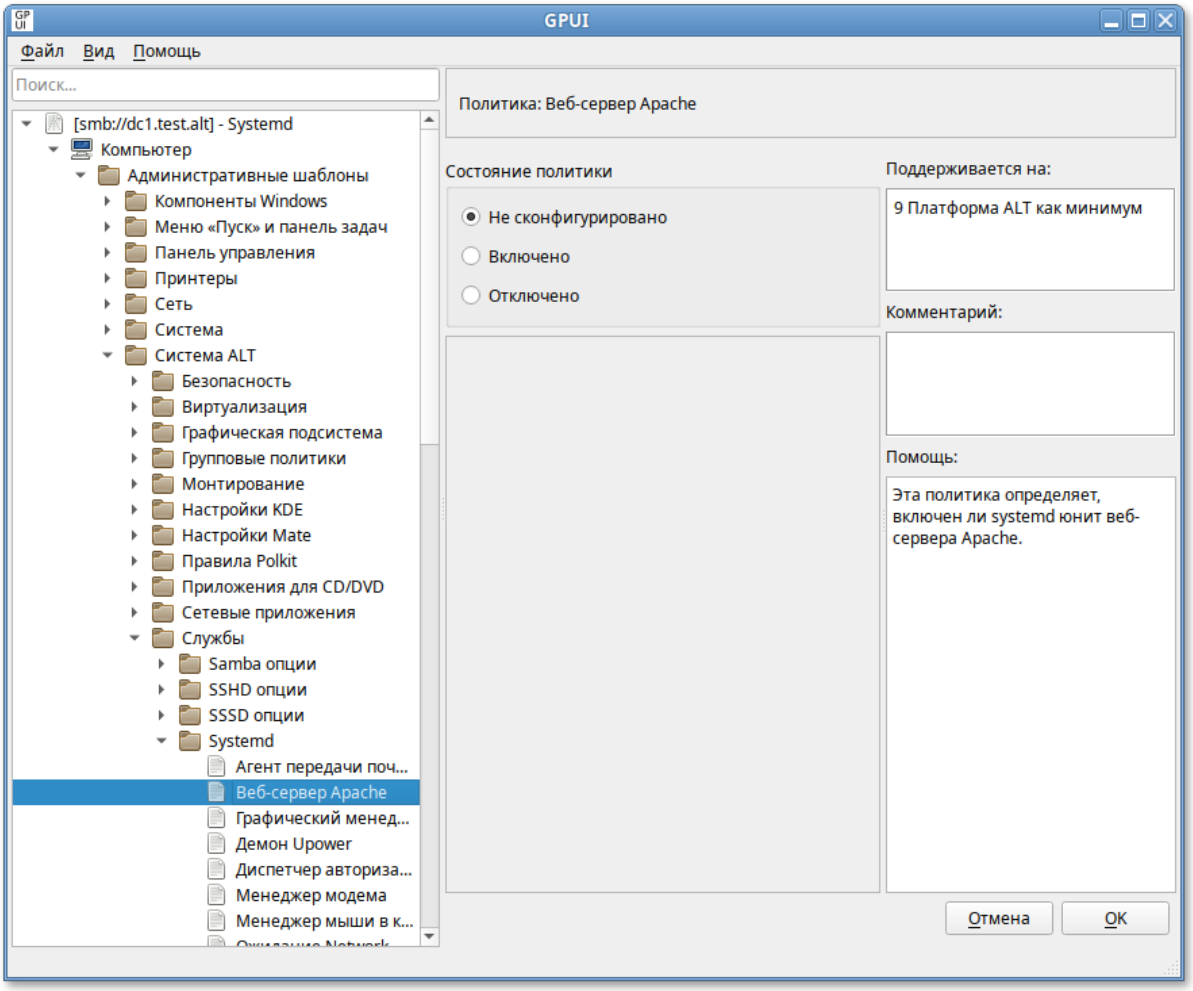
   Windows RSAT автоматически проверит корректность этих файлов.

   В GPUI:

   - файл **MySystemd.admx** в каталог **/usr/share/PolicyDefinitions**
   - файл **ru-RU/MySystemd.adml** в каталог **/usr/share/PolicyDefinitions/ru-RU**

- файл **en-US/MySystemd.adml** в каталог **/usr/share/PolicyDefinitions/en-US**

5. Проверить корректность кода, открыв редактор групповых политик — GPUI в «Альт» или RSAT в Windows.



6. Если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (**/var/lib/samba/sysvol/<DOMAIN>/Policies/**).

30.2.2. Пример для механизма Control

Подсистема Control в Linux-дистрибутивах является интерфейсом управления конфигурацией системы. Возможно написание собственных Control-интерфейсов для изменения системных или прикладных настроек, управляемых в дальнейшем через групповые политики.

Примечание

Просмотреть список опций Control можно, выполнив команду:

```
# control
```

Примечание

Ниже рассмотрен пример создания admx для Control osec-send:

```
# control osec-send help
mail: Mail root
journal: Write to systemd journal
```

Пример создания новой политики для Control osec-send:

1. Создать файл **MyControl.admx**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <policyNamespaces>
    <target prefix="control" namespace="BaseALT.Policies.MyControl" />
    <using prefix="system" namespace="BaseALT.Policies.System" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <policies>
    <policy class="Machine" displayName="$(string.osec-send)"
    explainText="$(string.osec-send_help)"
key="Software\BaseALT\Policies\Control"
    name="osec-send" presentation="$(presentation.osec-send)">
      <parentCategory ref="system:ALT_Services"/>
      <supportedOn ref="system:SUPPORTED_AltP9"/>
      <elements>
        <enum id="osec-send_setter" required="true" valueName="osec-send">
          <item displayName="$(string.osec-send_mail)">
            <value>
              <string>mail</string>
            </value>
          </item>
          <item displayName="$(string.osec-send_journal)">
            <value>
              <string>journal</string>
            </value>
          </item>
        </enum>
      </elements>
    </policy>
  </policies>
</policyDefinitions>
```

2. Создать файл **ru-RU/MyControl.adml**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>Определения политик управления системными компонентами</
displayName>
```

```
<description>Этот файл содержит определения политик управления системными ко
мпонентами.</description>
  <resources>
    <stringTable>
      <string id="osec-send">Отчет подсистемы osec</string>
      <string id="osec-send_help">Политика позволяет определить куда
отправлять ежедневный отчёт:

Почта — отправлять отчёт на почтовый ящик пользователя root

Журнал — записывать отчёт в системный журнал
      </string>
      <string id="osec-send_mail">Почта</string>
      <string id="osec-send_journal">Журнал</string>
    </stringTable>
    <presentationTable>
      <presentation id="osec-send">
        <dropdownList noSort="true" defaultItem="0" refId="osec-
send_setter">Куда отправлять отчёт:
        </dropdownList>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

3. Создать файл **`en-US/MyControl.adml`**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>Control installed facilities definitions</displayName>
  <description>This file contains the control installed facilities
definitions.</description>
  <resources>
    <stringTable>
      <string id="osec-send">Osec Subsystem Report</string>
      <string id="osec-send_help">The policy allows you to determine where
to send the daily report:

Mail — Mail root

Journal — Write to systemd journal
      </string>
      <string id="osec-send_mail">Mail</string>
      <string id="osec-send_journal">Journal</string>
    </stringTable>
    <presentationTable>
      <presentation id="osec-send">
        <dropdownList noSort="true" defaultItem="0" refId="osec-
send_setter">Where to send the report:
        </dropdownList>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

4. Скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPUI.

   В Windows RSAT:

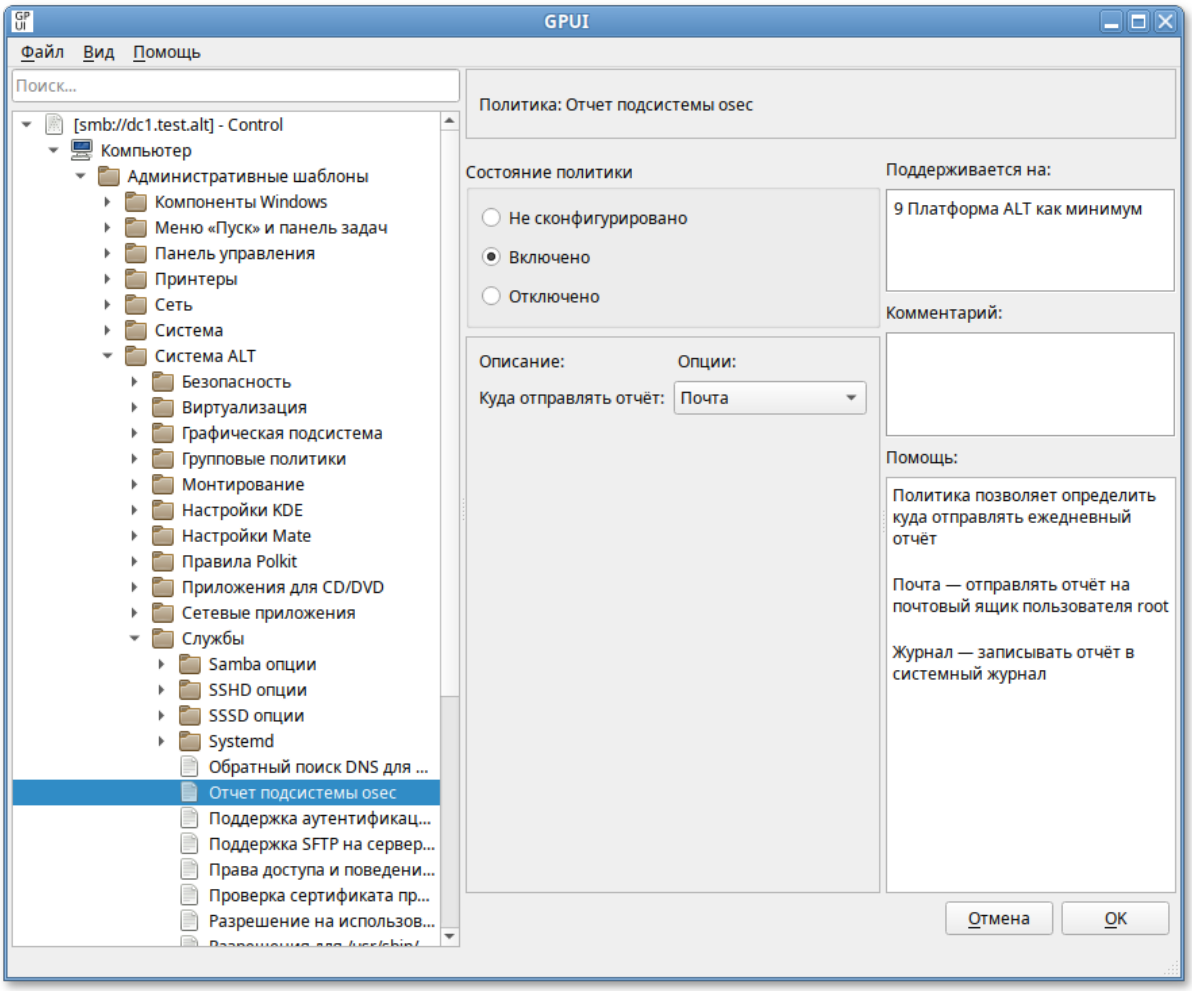
   - файл **MyControl.admx** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions**
   - файл **ru-RU/MyControl.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\ru-RU**
   - файл **en-US/MyControl.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\en-US**

   Windows RSAT автоматически проверит корректность этих файлов.

   В GPUI:

   - файл **MyControl.admx** в каталог **/usr/share/PolicyDefinitions**
   - файл **ru-RU/MyControl.adml** в каталог **/usr/share/PolicyDefinitions/ru-RU**
   - файл **en-US/MyControl.adml** в каталог **/usr/share/PolicyDefinitions/en-US**

5. Проверить корректность кода, открыв редактор групповых политик — GPUI в «Альт» или RSAT в Windows.



6. Если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (**/var/lib/samba/sysvol/<DOMAIN>/Policies/**).

30.2.3. Пример для механизма Gsetting

Конфигурация DE Mate хранится в базе dconf, ключами которой управляет консольное приложение GSettings. Механизм gpupdate управляет ключами Gsettings и через них редактирует ключи dconf. На текущий день через ГП можно настраивать целый ряд параметров графической среды Mate — от фона рабочего стола до хранителя экрана. Можно также добавить новые политики для незадействованных ключей Gsettings.

Примечание

Посмотреть все доступные схемы Gsettings можно, выполнив команду:

```
$ gsettings list-schemas
```

Посмотреть все ключи Gsettings можно, выполнив команду:

```
$ gsettings list-recursively
```

Примечание

Ниже рассмотрен пример создания admx для ключа idle-delay схемы org.mate.session:

```
$ gsettings list-keys org.mate.session
gnome-compat-startup
show-hidden-apps
idle-delay
required-components-list
default-session
auto-save-session
logout-prompt
logout-timeout
session-start
$ gsettings get org.mate.session idle-delay
5
```

Ключ idle-delay позволяет управлять настройкой «Считать компьютер простаивающим через».

Пример создания новой политики для ключа idle-delay схемы org.mate.session:

1. Создать файл **MyGsettings.admx**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <policyNamespaces>
```

```
    <target prefix="gsettings" namespace="BaseALT.Policies.MyGsettings" />
    <using prefix="system" namespace="BaseALT.Policies.System" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <policies>
    <policy name="OrgMateSessionIdleDelayUser" class="User"
     displayName="$(string.org-mate-session-idle-delay)"
     explainText="$(string.org-mate-session-idle-delay_help)"
     key="Software\BaseALT\Policies\gsettings"
     presentation="$(presentation.OrgMateSessionIdleDelayUser-pr)">
     <parentCategory ref="system:ALT_Screensaver_Mate" />
       <supportedOn ref="system:SUPPORTED_AltP9" />
         <elements>
           <decimal id="OrgMateSessionIdleDelay_setter"
valueName="org.mate.session.idle-delay"
           minValue="1" maxValue="2147483647" />
         </elements>
    </policy>
    <policy name="OrgMateSessionIdleDelayMachine" class="Machine"
     displayName="$(string.org-mate-session-idle-delay)"
     explainText="$(string.org-mate-session-idle-delay_help)"
     key="Software\BaseALT\Policies\gsettings"
     presentation="$(presentation.OrgMateSessionIdleDelayMachine-pr)">
     <parentCategory ref="system:ALT_Screensaver_Mate" />
     <supportedOn ref="system:SUPPORTED_AltP9" />
       <elements>
         <decimal id="OrgMateSessionIdleDelay_setter"
valueName="org.mate.session.idle-delay"
         minValue="1" maxValue="2147483647" />
         <boolean id="OrgMateSessionIdleDelay_setter_blocker"
key="Software\BaseALT\Policies\GSettingsLocks"
         valueName="org.mate.session.idle-delay">
           <trueValue>
             <decimal value="1" />
           </trueValue>
           <falseValue>
             <decimal value="0" />
           </falseValue>
         </boolean>
       </elements>
     </policy>
  </policies>
</policyDefinitions>
```

2. Создать файл **`ru-RU/MyGsettings.adml`**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>Определения списка настроек рабочего окружения MATE</
displayName>
    <description>Этот файл содержит определения настроек рабочего окружения
MATE.</description>
    <resources>
      <stringTable>
        <string id="org-mate-session-idle-delay">Считать компьютер
простаивающим через</string>
```

```
        <string id="org-mate-session-idle-delay_help">Устанавливает
количество минут,
        по истечении которых компьютер будет считаться простаивающим.

Опция «Блокировать» — (доступна только для машинной политики) запрещает
изменение
данной настройки пользователем. Блокировка политики делает её приоритетнее
аналогичной политики для пользователя.
        </string>
    </stringTable>
    <presentationTable>
      <presentation id="OrgMateSessionIdleDelayUser-pr">
        <text>Количество минут, по истечении которого компьютер будет
считаться простаивающим</text>
        <decimalTextBox refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Время в минутах</decimalTextBox>
      </presentation>
      <presentation id="OrgMateSessionIdleDelayMachine-pr">
        <text>Количество минут, по истечении которого компьютер будет
считаться простаивающим</text>
        <decimalTextBox refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Время в минутах:</decimalTextBox>
        <checkBox
refId="OrgMateSessionIdleDelay_setter_blocker">Блокировать</checkBox>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

3. Создать файл **`en-US/MyGsettings.adml`**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>MATE desktop configurations definitions</displayName>
    <description>This file contains the desktop MATE configurations
definitions.</description>
    <resources>
      <stringTable>
        <string id="org-mate-session-idle-delay">Consider the computer idle
after</string>
        <string id="org-mate-session-idle-delay_help">Sets the number of
minutes after which the computer will be considered idle.

The "Block" option — (available only for machine policy) prevents the user
from changing this setting. Blocking a policy makes it a priority over a
similar policy for the user.
        </string>
    </stringTable>
    <presentationTable>
      <presentation id="OrgMateSessionIdleDelayUser-pr">
        <text>Number of minutes after which the computer will be considered
idle</text>
        <decimalTextBox refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Time in minutes</decimalTextBox>
      </presentation>
      <presentation id="OrgMateSessionIdleDelayMachine-pr">
```

```
        <text>Number of minutes after which the computer will be considered
idle</text>
        <decimalTextBox refId="OrgMateSessionIdleDelay_setter"
defaultValue="1">Time in minutes:</decimalTextBox>
        <checkBox
refId="OrgMateSessionIdleDelay_setter_blocker">Блокировать</checkBox>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

4. Скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPUI.

   В Windows RSAT:

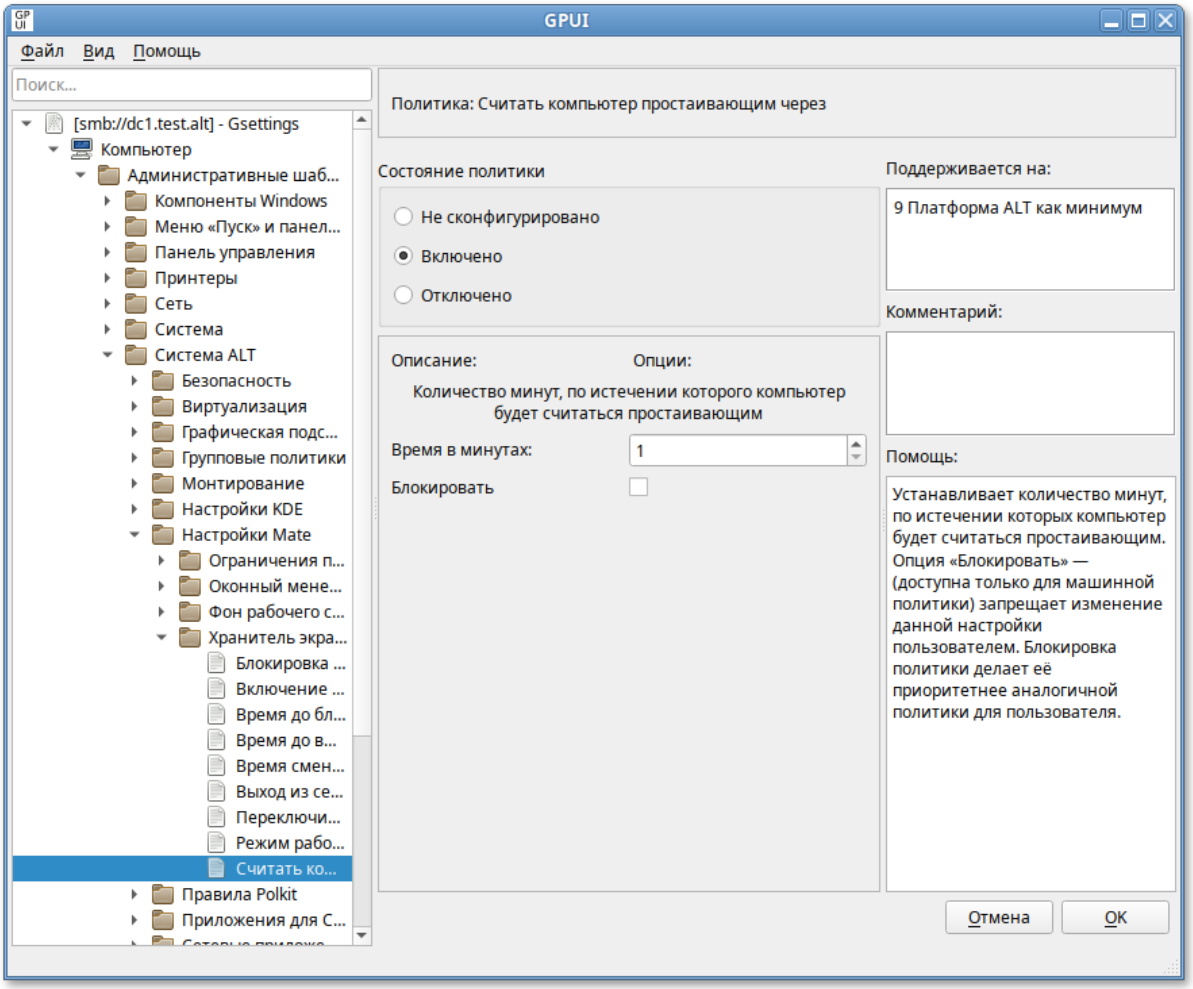
   - файл **MyGsettings.admx** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions**
   - файл **ru-RU/MyGsettings.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\ru-RU**
   - файл **en-US/MyGsettings.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\en-US**

   Windows RSAT автоматически проверит корректность этих файлов.

   В GPUI:

   - файл **MyGsettings.admx** в каталог **/usr/share/PolicyDefinitions**
   - файл **ru-RU/MyGsettings.adml** в каталог **/usr/share/PolicyDefinitions/ru-RU**
   - файл **en-US/MyGsettings.adml** в каталог **/usr/share/PolicyDefinitions/en-US**

5. Проверить корректность кода, открыв редактор групповых политик — GPUI в «Альт» или RSAT в Windows.



6. Если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (**`/var/lib/samba/sysvol/<DOMAIN>/Policies/`**).

30.2.4. Пример для механизма Polkit

Библиотека Polkit выполняет в ОС роль ограничителя действий приложений, преимущественно работающих на шине D-Bus. Polkit позволяет установить степень ограничений для непривилегированного процесса при обращении к привилегированному. Например, ограничить доступ пользователя к настройкам сети или монтированию блочного устройства (USB-накопителя) только для тех пользователей, которые знают пароль суперпользователя. Действия приложений, для которых заложены Polkit-ограничения, называются «actions». На основе указанных действий «actions» возможно формирование правил «polkit-rules», согласно которым в ОС и определится степень ограничений для программ и пользователей. Механизм gpupdate умеет автоматически формировать polkit-правила. Благодаря этому возможно добавление новых групповых политик для polkit-правил.

Примечание

Все политики находятся в каталоге **`/usr/share/polkit-1/actions/`** в формате *.policy Каждая политика представляет собой xml-файл, в котором описываются запросы к polkit.

Вывести список всех действий, определённых в **`/usr/share/polkit-1/actions/`** можно, выполнив команду

```
$ pkaction
```

Пример создания admx для действия org.xfce.thunar (запуск thunar от суперпользователя):

1. Создать файл **`MyPolkit.admx`**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <policyNamespaces>
    <target prefix="xfce" namespace="BaseALT.Policies.MyPolkit" />
    <using prefix="system" namespace="BaseALT.Policies.System" />
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <policies>
    <policy class="Machine" displayName="$(string.org-xfce-thunar)"
        explainText="$(string.org-xfce-thunar_help)"
        key="Software\BaseALT\Policies\Polkit"
        name="org.xfce.thunar"
        valuename="org.xfce.thunar"
        presentation="$(presentation.OrgXfceThunar-pr)">
      <parentCategory ref="system:ALT_Polkit" />
      <supportedOn ref="system:SUPPORTED_AltP10" />
      <elements>
        <enum id="OrgXfceThunar_setter" valueName="org.xfce.thunar"
required="true">
          <item displayName="$(string.org-xfce-thunar-No)">
            <value>
              <string>No</string>
            </value>
          </item>
          <item displayName="$(string.org-xfce-thunar-Yes)">
            <value>
              <string>Yes</string>
            </value>
          </item>
          <item displayName="$(string.org-xfce-thunar-Auth-self)">
            <value>
              <string>Auth_self</string>
            </value>
          </item>
          <item displayName="$(string.org-xfce-thunar-Auth-admin)">
            <value>
              <string>Auth_admin</string>
            </value>
          </item>
          <item displayName="$(string.org-xfce-thunar-Auth-self-keep)">
            <value>
              <string>Auth_self_keep</string>
            </value>
          </item>
          <item displayName="$(string.org-xfce-thunar-Auth-admin-keep)">
            <value>
              <string>Auth_admin_keep</string>
            </value>
```

```
          </item>
        </enum>
        <boolean id="OrgXfceThunar_blocker"
key="Software\BaseALT\Policies\PolkitLocks" valueName="org.xfce.thunar">
          <trueValue>
            <decimal value="1" />
          </trueValue>
          <falseValue>
            <decimal value="0" />
          </falseValue>
        </boolean>
      </elements>
    </policy>
  </policies>
</policyDefinitions>
```

2. Создать файл **ru-RU/MyPolkit.adml**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>Определения политик Xfce</displayName>
  <description>Этот файл содержит определения политик для управления Xfce.</
description>
  <resources>
    <stringTable>
      <string id="org-xfce-thunar">Ограничение возможности запуска Thunar от
суперпользователя</string>
      <string id="org-xfce-thunar_help">Политика управляет ограничением
возможности запуска Thunar от суперпользователя

Отключено/Не сконфигурировано – ограничения определяются системными
параметрами.

Включено – ограничение с установленными правами;

Возможные значения:

«No» – установить ограничение с запретом действия (пользователю не разрешено
выполнять действие);

«Yes» – снять ограничение (пользователь может выполнять действие без какой-
либо аутентификации);

«Auth_self» – пользователь должен ввести свой пароль для аутентификации.
Обратите внимание, этого уровня ограничения недостаточно для большинства
применений в многопользовательских системах, обычно рекомендуется
«Auth_admin»;

«Auth_admin» – пользователь должен ввести пароль администратора при каждом
запросе.
Требуется аутентификация пользователя с правами администратора;

«Auth_self_keep» – подобно «Auth_self», но авторизация сохраняется в течение
короткого периода времени (например, пять минут). Обратите внимание, этого
уровня
ограничения недостаточно для большинства применений в многопользовательских
```

```
системах, обычно рекомендуется «Auth_admin_keep»;

«Auth_admin_keep» — аналогично «Auth_admin», но авторизация сохраняется в
течение
короткого периода времени (например, пять минут);

Примечание: обладание административными правами в контексте PolicyKit
определяются его правилами.
По умолчанию в Альт запрашивается пароль пользователя, находящегося в группе
«wheel».

Опция «Блокировать» — запрещает изменение данной настройки пользователем.
Блокировка политики делает её приоритетнее аналогичной политики для
пользователя.
      </string>
      <string id="org-xfce-thunar-No">No</string>
      <string id="org-xfce-thunar-Yes">Yes</string>
      <string id="org-xfce-thunar-Auth-self">Auth_self</string>
      <string id="org-xfce-thunar-Auth-admin">Auth_admin</string>
      <string id="org-xfce-thunar-Auth-self-keep">Auth_self_keep</string>
      <string id="org-xfce-thunar-Auth-admin-keep">Auth_admin_keep</string>
    </stringTable>
    <presentationTable>
      <presentation id="OrgXfceThunar-pr">
        <dropdownList noSort="true" defaultItem="1"
refId="OrgXfceThunar_setter">Варианты ограничений
        на запуск Thunar от суперпользователя:</dropdownList>
        <checkBox refId="OrgXfceThunar_blocker">Блокировать настройку
ограничений</checkBox>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

3. Создать файл **en-US/MyPolkit.adml**:

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions"
revision="1.0" schemaVersion="1.0">
  <displayName>ALT Xfce policies definitions</displayName>
  <description>This file contains the Xfce service policies definitions used
by ALT operating system.</description>
  <resources>
    <stringTable>
      <string id="org-xfce-thunar">Run Thunar as root</string>
      <string id="org-xfce-thunar_help">This policy grants or restricts
permissions to run Thunar as root

Disabled/Not configured — Permissions are determined by system settings.
Default is «Auth_admin»

Enabled — permission to mount with set rights;

Possible values:

"No" — block permissions (the user is not allowed to perform the action);
```

```
"Yes" – grant permissions (the user can perform the action without any
authentication);

"Auth_self" – The user must enter their password to authenticate.
Note that this permission is not sufficient for most uses on multi-user
systems,
the "Auth_admin" permission is generally recommended;

"Auth_admin" – The user must enter an administrator password on each
request.
Requires user authentication with administrator rights;

"Auth_self_keep" – Similar to "Auth_self", but the authorization is kept for
a short period of time (for example, five minutes). Note that this
permission
is not sufficient for most uses on multi-user systems, the "Auth_admin_keep"
permission is generally recommended;

"Auth_admin_keep" – similar to "Auth_admin", but the authorization
is kept for a short period of time (for example, five minutes);

Note: the possession of administrative rights in the context of PolicyKit
is determined by its rules. By default, Alt asks for the password of the
user in the "wheel" group.

The "Block" option prevents the user from changing this setting.
Blocking a policy makes it a priority over a similar policy for the user.
      </string>
      <string id="org-xfce-thunar-No">No</string>
      <string id="org-xfce-thunar-Yes">Yes</string>
      <string id="org-xfce-thunar-Auth-self">Auth_self</string>
      <string id="org-xfce-thunar-Auth-admin">Auth_admin</string>
      <string id="org-xfce-thunar-Auth-self-keep">Auth_self_keep</string>
      <string id="org-xfce-thunar-Auth-admin-keep">Auth_admin_keep</string>
    </stringTable>
    <presentationTable>
      <presentation id="OrgXfceThunar-pr">
        <dropdownList noSort="true" defaultItem="1"
refId="OrgXfceThunar_setter">Restriction options:</dropdownList>
        <checkBox refId="OrgXfceThunar_blocker">Block</checkBox>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

4. Скопировать обновленные файлы admx/adml на машину с Windows RSAT или GPUI.

   В Windows RSAT:

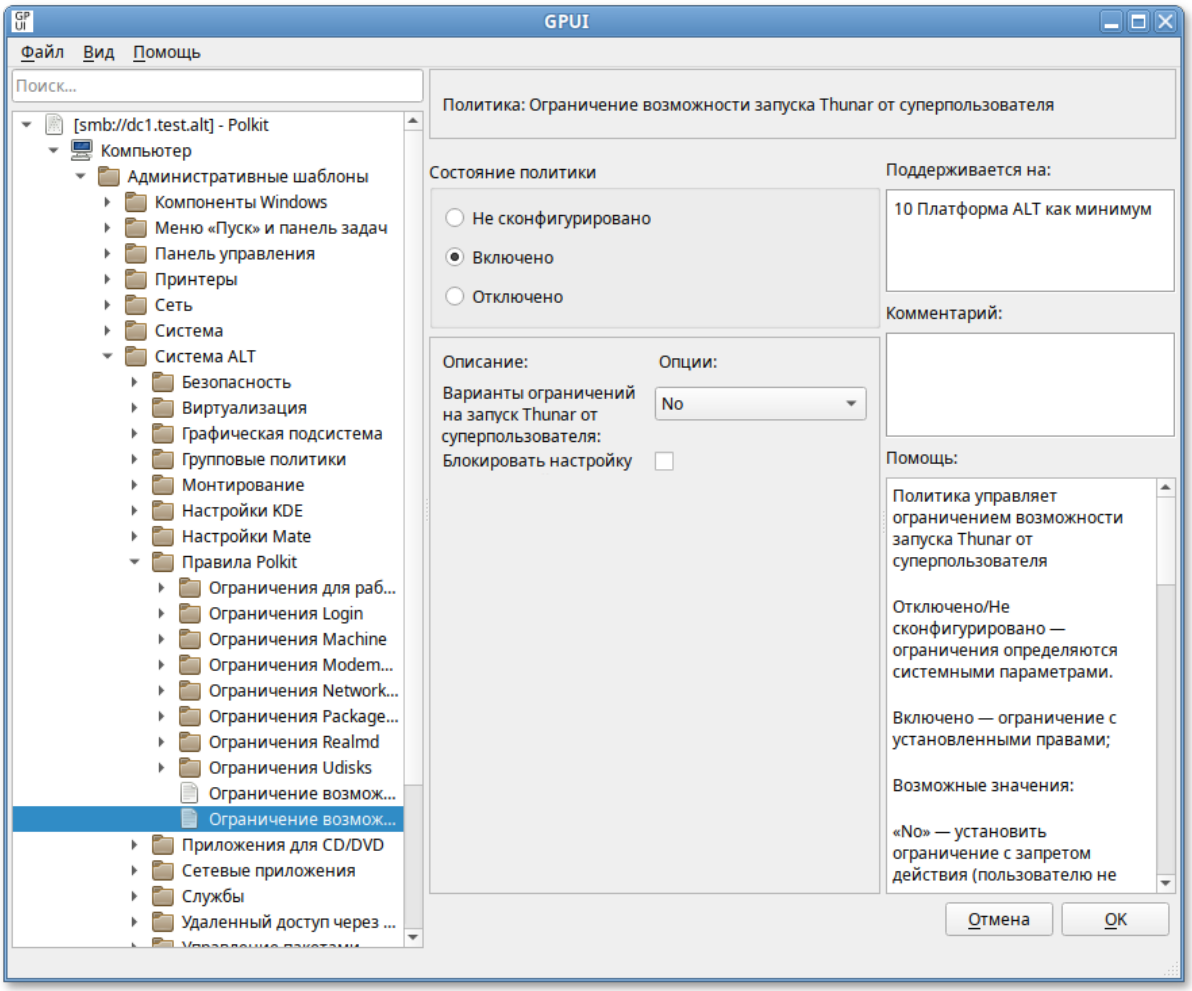
   - файл **MyPolkit.admx** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions**
   - файл **ru-RU/MyPolkit.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\ru-RU**
   - файл **en-US/MyPolkit.adml** в каталог **\\test.alt\sysvol\test.alt\Policies\PolicyDefinitions\en-US**

   Windows RSAT автоматически проверит корректность этих файлов.

В GPUI:

- файл **MyPolkit.admx** в каталог **/usr/share/PolicyDefinitions**
- файл **ru-RU/MyPolkit.adml** в каталог **/usr/share/PolicyDefinitions/ru-RU**
- файл **en-US/MyPolkit.adml** в каталог **/usr/share/PolicyDefinitions/en-US**

5. Проверить корректность кода, открыв редактор групповых политик — GPUI в «Альт» или RSAT в Windows.



6. Если все корректно, скопировать обновленные файлы admx/adml на контроллер домена в сетевой каталог sysvol (**/var/lib/samba/sysvol/<DOMAIN>/Policies/**).

Глава 31. Решение проблем

31.1. Область действия и статус групповой политики

31.2. Наследование групповых политик

31.3. Порядок применения групповых политик

31.4. Замыкание групповой политики

31.5. Диагностика применения GPO на стороне клиента

Прежде чем разбираться, почему групповые политики не применяются как ожидается, необходимо убедиться, что инфраструктура Альт Домен работает штатно. Работа ГП в домене зависит от корректности работы контроллеров домена и репликации между ними.

Следует держать структуру групповых политик как можно более простой и не создавать лишние политик без необходимости. Рекомендуется использовать единую схему именования политик. Имя ГП должно давать однозначное понимание того, для чего она нужна.

31.1. Область действия и статус групповой политики

В каждой ГП есть два независимых раздела с настройками:

- **Компьютер** — параметры, применяемые к компьютеру;
- **Пользователь** — параметры пользователей.

Если параметр политики настраивается в секции **Компьютер**, групповая политика должна быть привязана к OU с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на OU с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном OU с компьютерами или пользователями.

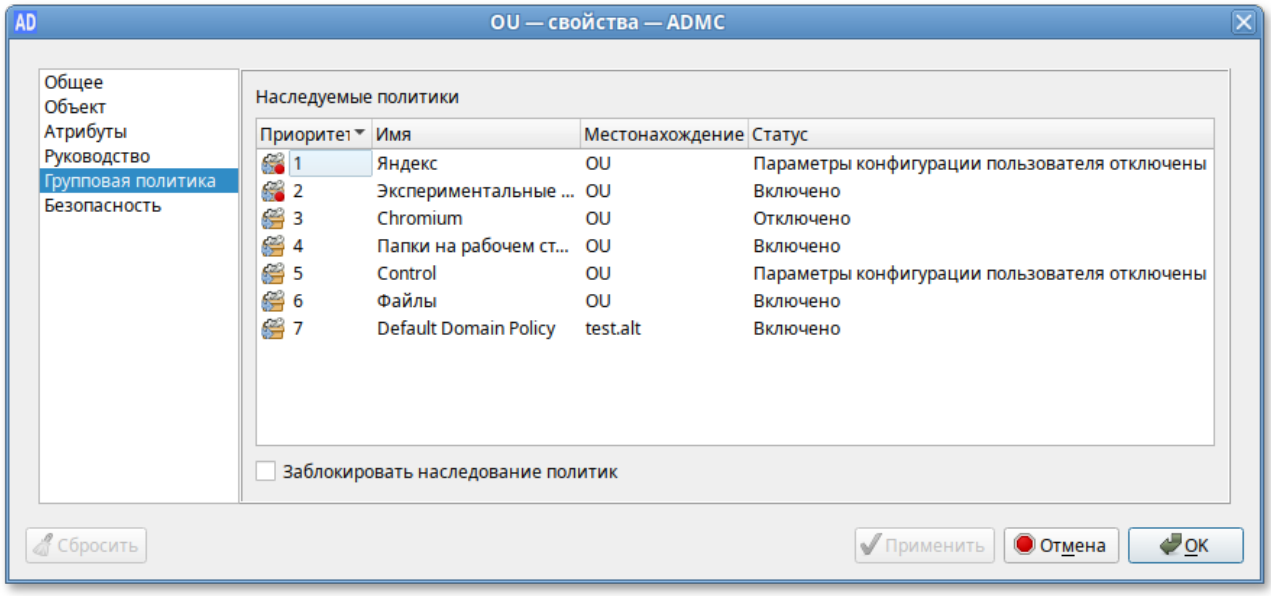
Примечание

Чтобы применить пользовательские настройки к компьютерам, нужно включить политику замыкания (см. Замыкание групповой политики).

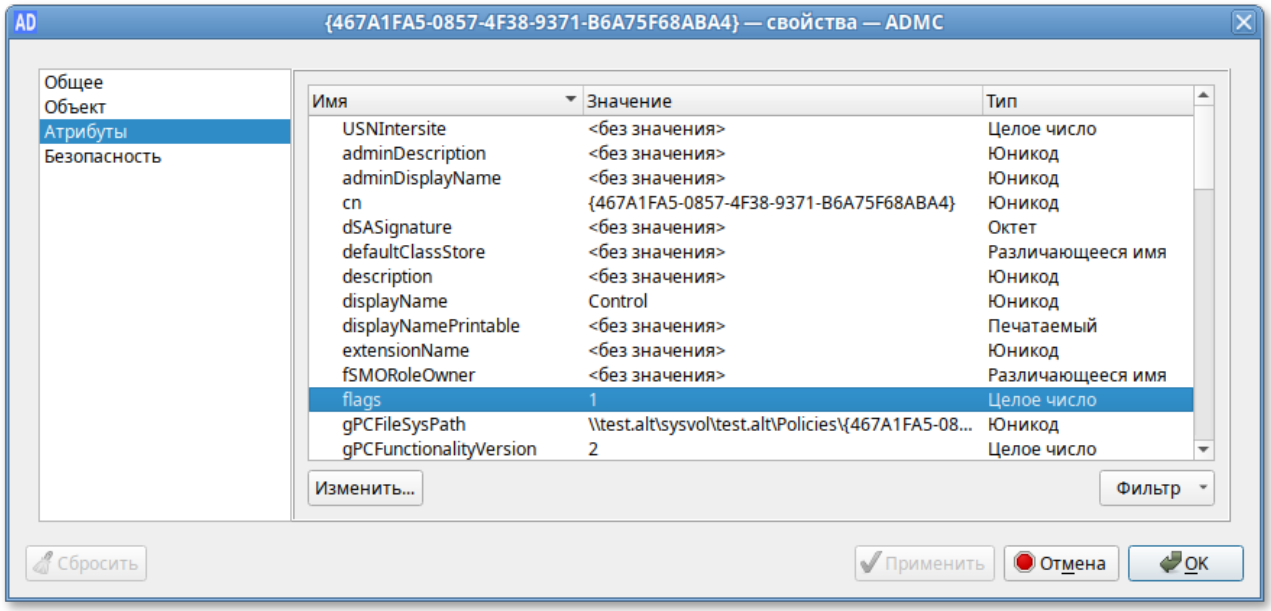
Если ГП настраивает только параметры пользователя или только параметры компьютера, неиспользуемый раздел можно отключить. Это снизит трафик ГП и позволит уменьшить время обработки ГП на клиентах.

Если определенный параметр политики не применяются на клиенте, необходимо проверить область действия (scope) групповой политики.

Статус групповой политики, назначенной на подразделение, можно проверить в ADMC в свойствах этого подразделения на вкладке **Групповая политика**:



Изменить статус групповой политики можно в ADMC в свойствах политики на вкладке **Атрибуты**:

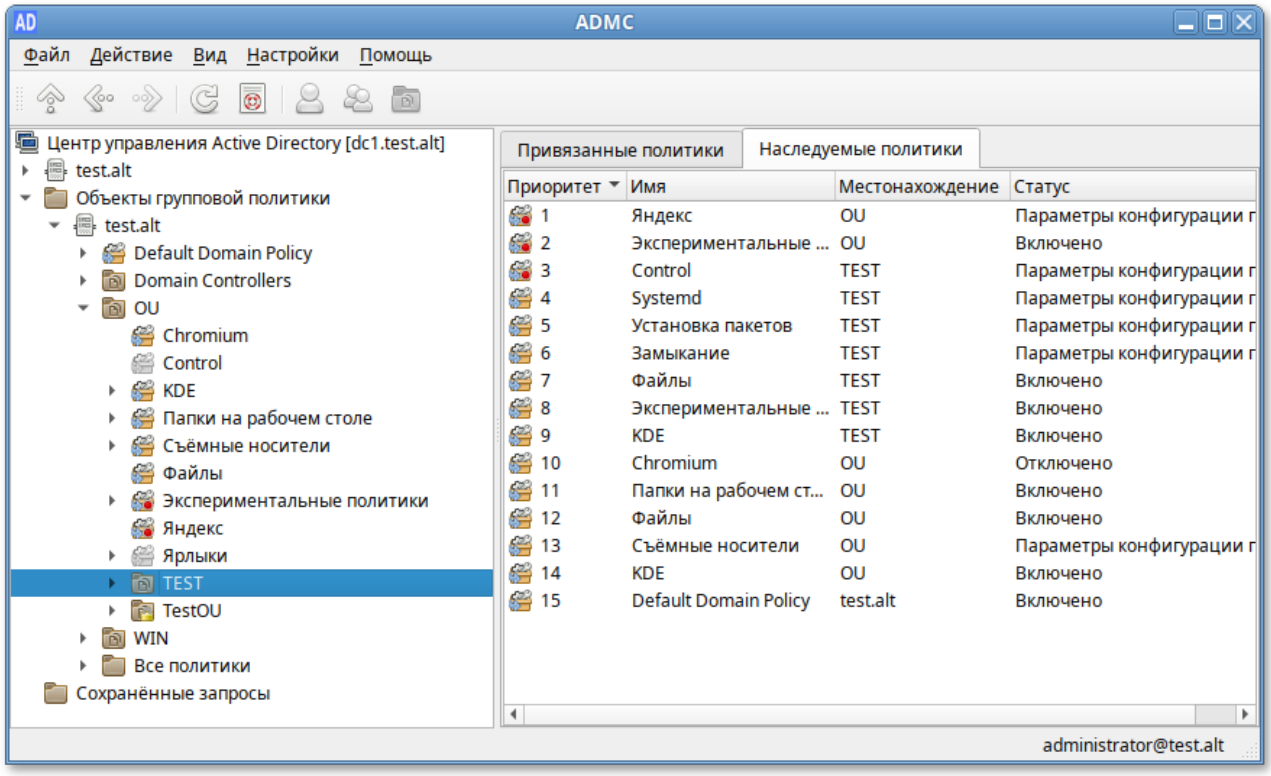


Состояние объекта групповой политики указывается в значении атрибута **`flags`**: объект GPO включён (значение 0, все настройки политики применяются к целевым объектам домена), отключён раздел **`Конфигурация пользователя`** (значение 1, не применяются настройки пользовательских политик), отключён раздел **`Конфигурация компьютера`** (значение 2, не применяются настройки из параметров GPO компьютера), объект GPO полностью отключён (значение 3, все настройки политики не применяются).

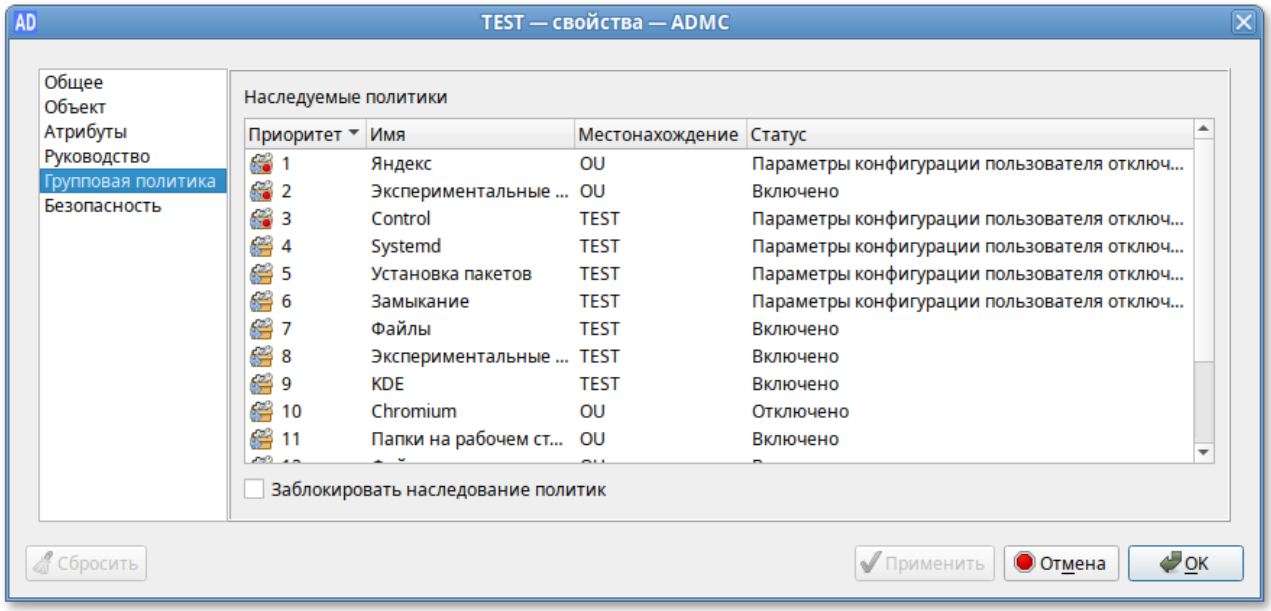
31.2. Наследование групповых политик

По умолчанию политики высокого уровня применяются ко всем вложенным объектам в иерархии домена.

Увидеть какие политики применяются к подразделению и местонахождение политики можно в ADMC при выборе подразделения на вкладке **Наследуемые политики**:



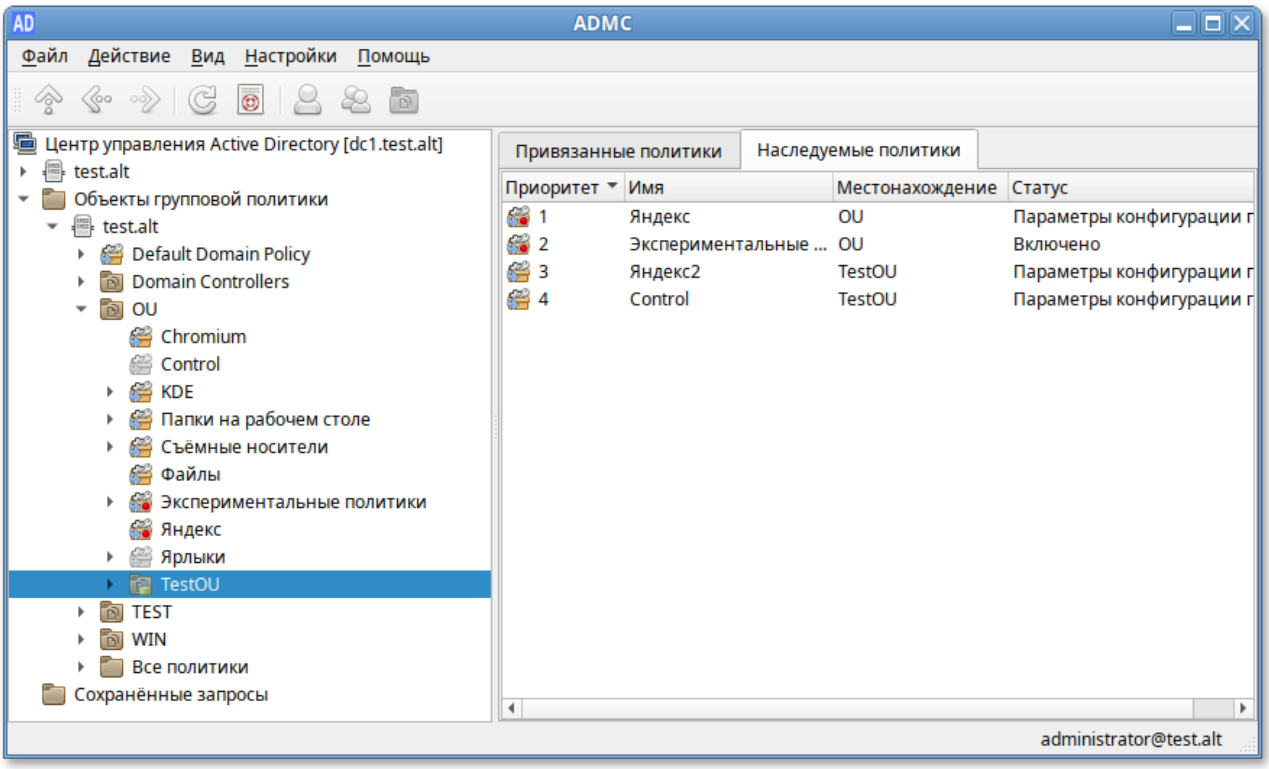
Наследуемые политики также можно увидеть на вкладке **Групповая политика** свойств подразделения:



Каждый объект групповой политики можно настроить на блокирование наследования политик более высокого уровня (см. Блокирование наследования). Таким образом, политика подразделения может блокировать параметры политик домена и сайта. Блокирование наследования предохраняет объекты групповой политики, связанные с доменами или подразделениями родительского уровня, от автоматического наследования на дочернем уровне.

Так как администратор домена может не согласится с тем, что администратор подразделения блокирует параметры политики домена, существует возможность запретить переопределение параметров с помощью отметки **Принудительно**.

Политики подразделения с блокированием наследования:



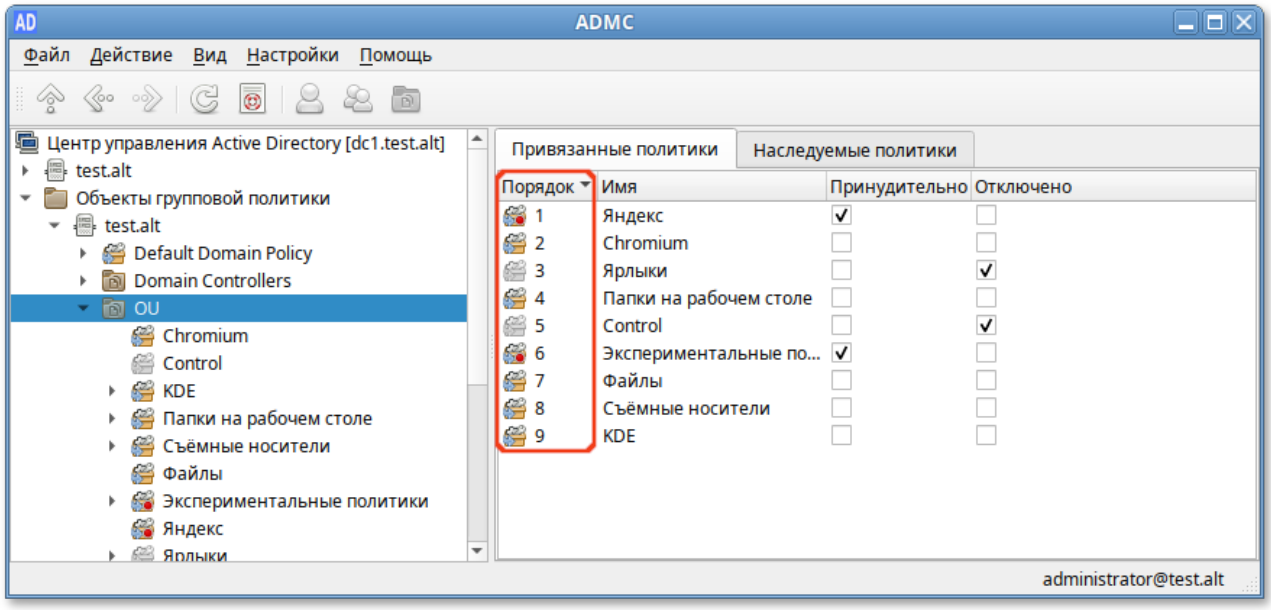
31.3. Порядок применения групповых политик

Групповые политики обрабатываются в следующем порядке:

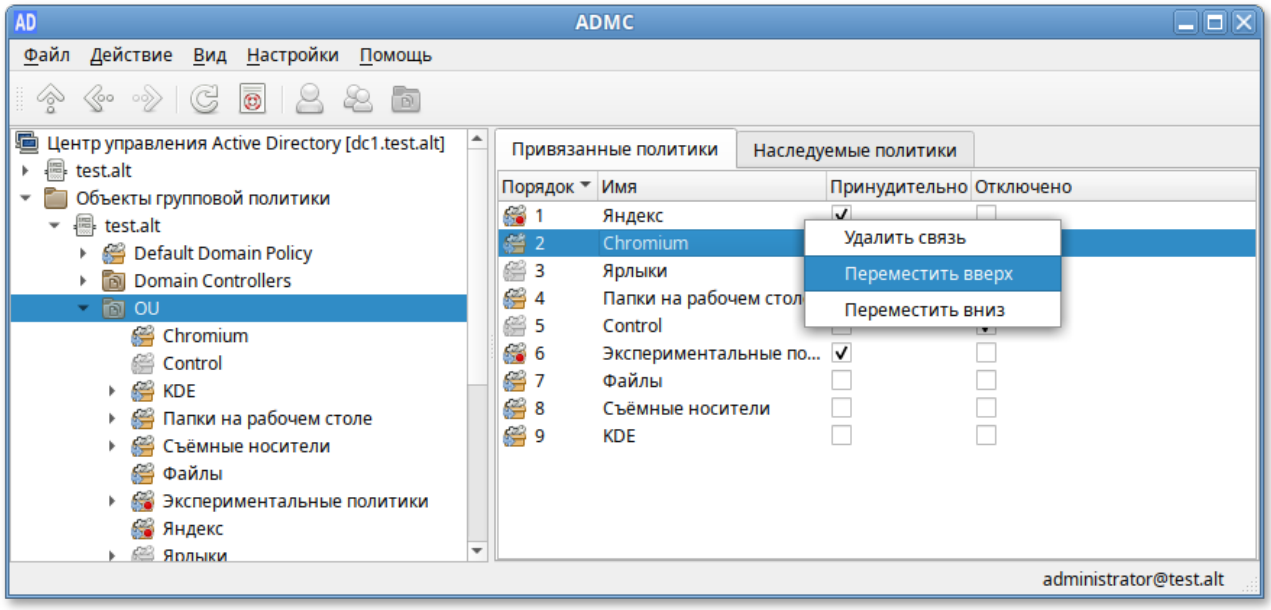
- объект локальной групповой политики;
- объекты групповой политики, связанные с доменом (в рамках возможностей и ограничений поддержки леса доменов в Samba, как набора клиентских компонентов);
- объекты групповой политики, связанные с OU: сначала обрабатываются объекты групповой политики связанные с OU, находящиеся на самом высоком уровне в иерархии Альт Домен, затем объекты групповой политики, связанные с дочерним подразделением и т. д. Последними обрабатываются объекты групповой политики, связанные с OU, в которой находится пользователь или компьютер.

Последние политики имеют наивысший приоритет. Т.е. если параметр включен на уровне политики домена, но на целевом OU данный параметр отключается другой политикой — это означает, что нужный параметр в результате будет отключен на клиенте (выиграет ближайшая политика к объекту в иерархии домена).

Если на OU назначено несколько групповых политик, то они обрабатываются в том порядке, в котором были назначены. Политики обрабатываются в обратном порядке (политика с номером 1 будет обработана последней):



При необходимости этот порядок можно изменить, перетащив политику мышью или выбрав в контекстном меню политики пункт **Переместить вверх** или **Переместить вниз**:



При использовании параметра **Принудительно** у ГП выигрывает та политика, которая находится выше в иерархии домена (например, при включении **Принудительно** у политики Default Domain Policy, она выигрывает у всех других ГП).

У каждого объекта ГП, который привязан к организационному контейнеру AD можно включить или отключить связь (применение политики). Для этого нужно выбрать опцию **Удалить связь**/ **Добавить связь** в меню политики. При отключении связи политика перестает применяться к клиентам, но ссылка на объект ГП не удаляется из иерархии. Активировать данную связь можно в любой момент.

31.4. Замыкание групповой политики

По умолчанию групповая политика применяется к пользователю или компьютеру способом, который зависит от того, где и пользователь, и объекты компьютера находятся в AD. В некоторых случаях может потребоваться применить к пользователям политику в зависимости от расположения объекта компьютера.

На компьютерах, расположенных в организационном подразделении (OU), машинные объекты групповой политики применяются по порядку во время запуска компьютера. Пользовательские объекты групповой политики, пользователей из OU, применяются во время входа, независимо от того, на каком компьютере пользователь входит в систему.

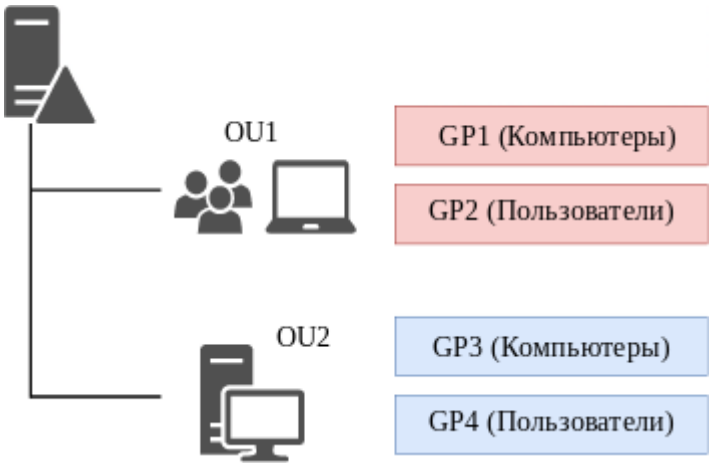
Если пользовательская учётная запись находится в OU, на которое распространяется действие пользовательской политики, то применяться эти настройки будут при входе пользователя в систему независимо от того, в какое OU входит компьютер. Такое поведение может быть нежелательным, например, вполне разумно иметь одни пользовательские настройки для сервера, другие — для локального компьютера.

Политику замыкания можно использовать для применения пользовательских групповых политик в зависимости от того, на каком компьютере пользователь входит в систему.

Эта политика может принимать два значения:

- режим «Слияние» (Merge) — при входе пользователя в систему к компьютеру будут применяться политики основанные на расположении пользователя, а затем политики, привязанные к компьютеру. При возникновении конфликтов между пользовательскими и машинными политиками, машинные политики будут иметь более высокий приоритет;
- режим «Замена» (Replace) — к пользователю будут применяться только политики, назначенные на OU, в котором содержится компьютер, на который пользователь выполнил вход.

В качестве примера рассмотрим домен с двумя организационными подразделениями — OU1 и OU2. В первом находятся объекты учётных записей пользователей и их локальные компьютеры, во втором — объекты серверов.



Если пользователь осуществляет вход в систему на локальном компьютере, то он оказывается под действием политики GP1 локального компьютера (которая была применена при его включении) и политики GP2 пользователя (примененной при входе в систему). Если пользователь осуществляет вход на сервер, то будут действовать политика сервера GP3 и политика пользователя GP2.

Если же включить политику замыкания (см. раздел Политика замыкания), то при входе на сервер будут действовать политика сервера GP3 и политика пользователя GP2+GP4 (в режиме «Слияние») или только GP4 (в режиме «Замена»). При возникновении любых конфликтов настроек между политиками OU пользователя и OU сервера в режиме «Слияние» политика в OU сервера будет иметь более высокий приоритет.

31.5. Диагностика применения GPO на стороне клиента

Для диагностики применения групповых политик на стороне клиента используются утилиты gpoa, gpresult (на машинах с ОС «Альт»), **gpresult** (на машинах Windows).

Для диагностики механизмов применения групповых политик на клиенте можно выполнить команды:

- получить полный отчет о примененных ГП для пользователя и машины:

```
$ gpresult -v
```

- получить и применить настройки для текущей машины:

```
# gpoa --loglevel 0
```

- получить и применить настройки для пользователя:

```
# gpoa --loglevel 0 <имя_пользователя>
```

31.5.1. Коды ошибок

Сообщения, сопутствующие кодам ошибок, могут изменяться (переводиться, исправляться), но сам код уникален для определённой части программы, что позволяет однозначно идентифицировать проблему.

Таблица 31.1. Коды ошибок

Код	Описание	Решение
E00001	Недостаточно прав для запуска программы **gpupdate**	Необходимо повысить уровень привилегий. Может помочь запуск программы от имени администратора
E00002	Программа **gpupdate** не будет запущена из-за предыдущих ошибок	
E00003	Ошибка работы бэкэнда, которая привела к досрочному прекращению обработки групповых политик. Этот код характеризует серьёзные ошибки, которые обрабатываются на самом высоком уровне	Возможно, это ошибка в коде и необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00004	Ошибка во время работы фронтенда	Высокоуровневая ошибка при инициализации фронтенда или во время работы appliers. С большой вероятностью может оказаться ошибкой в коде

Код	Описание	Решение
E00005	Не получилось запустить appliers политик для обновления групповых политик компьютера	Необходимо проверить, что машина всё ещё в домене, демон oddjobd доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00006	Показать список доступных бэкэндов	Необходимо проверить, что машина всё ещё в домене, демон oddjobd доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00007	Невозможно инициализировать бэкэнд Samba в силу неполадок компонентов, связанных с Samba	Необходимо проверить инсталляцию Samba на машине, убедиться, что машина введена в домен и домен доступен
E00008	Невозможно инициализировать бэкэнд no-domain для выполнения процедуры бутстрапа групповых политик	Возможно, было произведено вмешательство в локальную политику или произошёл misconfiguration. Необходимо проверить целостность пакета *local-policy* и настройки домена в Alterator
E00009	Произошла ошибка при попытке запуска **`adp`**	Необходимо обратиться к руководству по устранению неполадок проекта ADP
E00010	Произошёл сбой при попытке получить имя домена Active Directory	Необходимо проверить работу доменной службы имён (DNS), а также доступность доменного LDAP. Для доступа к LDAP необходим работоспособный Kerberos, так что стоит проверить и его конфигурацию
E00011	Во время работы applier с пониженным уровнем привилегий произошла неполадка	Возможно, что в используемой групповой политике заданы параметры, для установки которых требуются права администратора. Это необходимо проверить и исправить объект групповой политики соответственно
E00012	Высокоуровневая ошибка инициализации бэкэнда	Необходимо проверить наличие условий для запуска бэкэнда. В случае с Samba — удостовериться, что машина введена в домен
E00013	У пользователя, запустившего программу, недостаточно прав для обновления настроек машины	Необходимо запустить программу с правами администратора
E00014	Не прошла проверка наличия билета Kerberos. Билет Kerberos нужен для доступа к сервисам домена	Необходимо проверить конфигурацию Kerberos в файле **`/etc/krb5.conf`**. Попытаться получить билет Kerberos вручную
E00015	Запрос на получение имени домена Active Directory через LDAP не прошёл	Необходимо проверить возможность получения Kerberos ticket для машины. Проверить работу DNS и возможность обратиться к доменному LDAP
E00016		

Код	Описание	Решение
	Утилита **wbinfo** не отдаёт SID для пользователя, для которого выполняется обновление групповых политик	Необходимо проверить целостность программы **wbinfo**. Проверить, что машина введена в домен
E00017	Невозможно получить список групповых политик для репликации на используемое имя пользователя	Следует удостовериться, что пользователь для которого происходит попытка получить список групповых политик, существует в домене. Необходимо также удостовериться, что проблема не вызвана misconfiguration домена
E00018	Не получилось прочитать содержимое настройки XDG_DESKTOP_DIR	Необходимо удостовериться, что XDG в системе сконфигурирован корректно и пользователь, для которого вычитывается настройка, существует
E00019	Произошла ошибка во время работы applier для пользователя	Необходимо удостовериться, что это не misconfiguration в используемой GPO. Возможно это ошибка. В таком случае необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00020	Произошла ошибка во время работы applier для пользователя с пониженными привилегиями	Необходимо удостовериться, что это не misconfiguration в используемой GPO. Возможно это ошибка. В таком случае необходимо создать отчет об ошибке, чтобы разработчики узнали о ней
E00021	Не был получен ответ от D-Bus при попытке запустить **gpoa** для текущего пользователя	Следует удостовериться, что D-Bus работает корректно и демон oddjobd запущен. Необходимо удостовериться, что у текущего пользователя достаточно прав для обращения к D-Bus
E00022	Не был получен ответ от D-Bus при попытке запустить **gpoa** для машины	Необходимо удостовериться, что D-Bus работает корректно и демон oddjobd запущен
E00023	Не был получен ответ от D-Bus при попытке запустить **gpoa** для пользователя	Следует удостовериться, что D-Bus работает корректно и демон oddjobd запущен. Необходимо удостовериться, что у текущего пользователя достаточно прав для обращения к D-Bus
E00024	Ошибка во время работы машинного applier	Необходимо проверить настройки applier вручную, чтобы убедиться, что соответствующая часть ОС не поломана
E00025	Ошибка во время инициализации пользовательского applier	Необходимо проверить, что машина является частью домена и контроллер домена доступен. Следует удостовериться, что пользователь существует и что соответствующая часть ОС не поломана
E00026	Ошибка слияния машинной групповой политики	Необходимо очистить кеш gpupdate

Код	Описание	Решение
E00027	Ошибка слияния пользовательской групповой политики	Необходимо очистить кеш gpupdate
E00028	Ошибка слияния машинной части групповой политики	Необходимо очистить кеш gpupdate
E00029	Ошибка слияния пользовательской части групповой политики	Необходимо очистить кеш gpupdate
E00030	Ошибка при запуске процесса с пониженным уровнем привилегий в контексте пользователя	Необходимо проверить наличие домашнего каталога пользователя, для которого выполняется **gpupdate**
E00042	Не входит в возможные значения для control	Ошибка возникает в случае некорректного целочисленного типа данных, прописанного в шаблонах групповых политик (ADMX-файлах)
E00055	Ошибка при запуске **pkcon_runner** синхронно для компьютера	Необходимо проверить наличие в системе и корректность файла **pkcon_runner**
E00056	Ошибка запуска **apt-get update**	Необходимо проверить подключение к сети и корректность репозиториев, отсутствие подключённых дополнительных репозиториев
E00057	Ошибка установки пакета	Необходимо проверить наличие пакета в репозиториях, правильность имени пакета, наличие подключения к сети и наличие в системе пакета *packagekit*
E00058	Ошибка удаления пакета	Вероятно, пакет не установлен в систему или в системе отсутствует пакет *packagekit*
E00059	Не входит в возможные значения для control	Ошибка возникает в случае некорректного строкового типа данных, прописанного в шаблонах групповых политик (ADMX-файлах)
E00060	Ошибка при запуске **pkcon_runner** синхронно для пользователя	Необходимо проверить наличие в системе и корректность файла **pkcon_runner**
E00061	Ошибка при запуске **pkcon_runner** асинхронно для компьютера	Необходимо проверить наличие в системе и корректность файла **pkcon_runner**
E00062	Ошибка при запуске **pkcon_runner** асинхронно для пользователя	Необходимо проверить наличие в системе и корректность файла **pkcon_runner**
E00067	Ошибка создания переменных среды	Необходимо убедиться в наличии переменных окружения: XDG_DATA_DIRS, XDG_RUNTIME_DIR, DBUS_SESSION_BUS_ADDRESS, PATH
E00068	Ошибка выполнения команды **kwriteconfig5**	Необходимо убедиться, что установлен пакет *kf5-kconfig*

31.6. Диагностика проблем при работе с политикой скриптов

На контроллере домена:

- проверить работоспособность загружаемого скрипта в дистрибутиве «Альт»;
- убедиться, что кодировка файла со скриптом — UTF8, без BOM;
- убедиться, что скрипт расположен в каталоге (GPT) применяемого объекта групповой политики (GPO);
- убедиться, что включена групповая политика «Экспериментальные групповые политики» или политика «Управление logon-скриптами» (см. Включение экспериментальных групповых политик);
- убедиться, что целевой компьютер, входит в подразделение (OU), к которому привязан объект групповой политики GPO.

На компьютере пользователя:

- проверить версию *gpupdate* (политики скриптов выполняются с релиза 0.9.11-alt1);
- убедиться, что механизм применения политик (gpupdate) запущен:

```
# gpupdate-setup status
```

- убедиться, что служба скриптов запущена:

```
# systemctl status gpupdate-scripts-run.service
```

- проверить содержимое каталога и права для загруженных скриптов:

```
# ls -Rl /var/cache/gpupdate_scripts_cache/
```

- проверить состояние службы запуска скриптов пользователя (от пользователя):

```
$ systemctl --user status gpupdate-scripts-run-user.service
```

- вывести журнал применения политик:

```
# gpoa --loglevel 0
```

Часть VI. Доверительные отношения (Трасты)

Доверительные отношения (trusts) позволяют аутентифицироваться под пользователями не только текущего домена, но и доверенных.

Содержание

32. Настройка доверия

33. Настройка DNS

34. Создание доверительного отношения

35. Управление пользователями и группами

36. Использование трастов на LINUX-клиентах

37. Удаление доверия

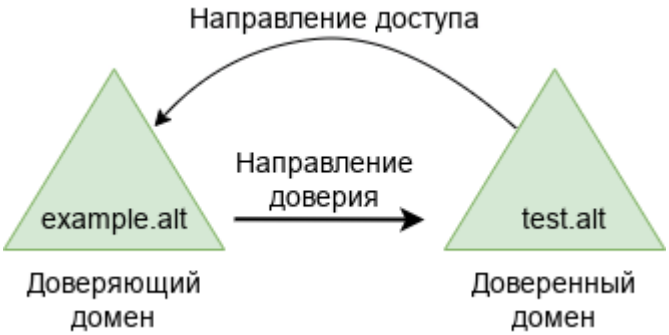
Глава 32. Настройка доверия

32.1. Общие сведения

32.2. Особенности доверительных отношений в Samba

32.1. Общие сведения

Доверительные отношения реализуются в рамках механизма аутентификации. Суть доверительных отношений между двумя доменами сводится к тому, что доверяющий домен (trusting domain) доверяет процесс аутентификации доверенному домену (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене.



Отношения доверия обеспечивают доступ к ресурсам в одном или двух направлениях:

- одностороннее доверие (one-way trust) — позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б, но не наоборот. Домен А доверяет домену Б, но домен Б не доверяет домену А. При создании такого доверия нужно указать направление (входящее или исходящее);

- двустороннее доверие (two-way trust) — позволяет пользователям и группам из домена А получать доступ к ресурсам в домене Б и наоборот. Запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях. Домен А доверяет домену Б, а домен Б доверяет домену А.

Транзитивность определяет, можно ли расширить доверие за пределы двух доменов, для которых оно сформировано:

- транзитивное доверие можно использовать для расширения отношений доверия на другие домены;

- нетранзитивное доверие можно использовать для запрета отношений доверия с другими доменами.

Типы доверия:

- доверие леса (Forest trust) — связывает леса и все их домены (это двухсторонние или односторонние отношения доверия между разными лесами, всегда являющиеся транзитивными);
- внешнее доверие (External trust) — устанавливается между двумя доменами напрямую вне леса (для установки двухстороннего доверия нужно использовать два разнонаправленных доверия, которыми надо связать все требуемые пары доменов).

32.2. Особенности доверительных отношений в Samba

Поддерживается:

- доверие леса (это доверие может быть установлено между двумя Samba-доменами или Samba-доменом и Windows-доменом);
- внешние доверительные отношения (это доверие может быть установлено между двумя Samba-доменами или Samba-доменом и Windows-доменом);
- добавление пользователей и групп доверенного домена в группы доверяющего домена (при этом необходимо использовать SID пользователей и групп, чтобы добавить их в свою группу, имя пользователя или имя группы использовать невозможно).

Особенности и ограничения:

- не применяются правила фильтрации SID;
- не поддерживается выборочная аутентификация (создание таких доверий возможно, но KDC и winbindd всё равно будут их игнорировать);
- нельзя создать доверительные отношения между доменами в одном дереве с одним и тем же пространством имён верхнего уровня. NetBIOS имена доменов должны отличаться (домен MYDOMAIN.WIN и MYDOMAIN.NEW будут иметь одинаковое короткое имя — MYDOMAIN, это приведет к невозможности установки доверительных отношений);
- в RSAT можно увидеть контейнер ***foreignSecurityPrincipal*** для всех добавленных пользователей и групп из доверенного домена. Таким образом Microsoft показывает, что пользователь или группа являются частью доверенного домена;
- Winbind на клиентских машинах не распознаёт доверенные домены, что приводит к проблемам с обновлением паролей учетных записей доверенного домена после их истечения. Чтобы устранить эту проблему, необходимо в секцию **`[global]`** в файла **`smb.conf`** на Linux-клиентах, подключенных через Winbind, добавить опцию:

  ```
  winbind scan trusted domains = yes
  ```

  и перезапустить сервис winbind:

  ```
  # systemctl restart winbind.service
  ```

- при использовании групповой политики (на контроллерах в Win-домене) «Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)» с опцией «требовать сеансовую безопасность NTLMv2» в разделе «Конфигурация компьютера\Конфигурация Windows\Параметры

безопасности\Локальные политики\Параметры безопасности» не строится траст между Win-доменом и Samba-доменом. При включении этой политики после построения траста некорректно работают доверительные отношения между Windows-доменом и Samba-доменом. Не выполняется проверка траста (**samba-tool domain trust validate**) и не выполняется вход на пользователями из доверенного домена на машинах с winbind.

Примечание

После редактирования политики и ее применения в Win-домене необходимо перезапустить сервис samba.

Для управления доверием можно использовать инструмент командной строки **samba-tool**.

Таблица 32.1. Команды управления доверием

Команда	Описание	Примечание
domain trust create <домен>	Создать доверие домена или леса	Можно использовать следующие опции: ***--type=TYPE*** — тип доверия (**external**, **forest**); ***--direction=DIRECTION*** — направление доверия (**incoming**, **outgoing**, **both**); ***--create-location=LOCATION*** — где создать объект доверенного домена (**local**, **both**); ***--quarantined=yes|no*** — применять к доверию специальные правила фильтрации SID (при ***--type=external*** по умолчанию **yes**, при ***--type=forest*** по умолчанию **no**); ***-U USERNAME*** — имя пользователя.
domain trust modify <домен>	Изменить доверие домена или леса	
domain trust delete <домен>	Удалить доверие домена или леса	Можно использовать следующие опции: ***--delete-location=LOCATION*** — где удалить объект доверенного домена (**local**, **both**); ***-U USERNAME*** — имя пользователя.
domain trust list	Вывести список доверительных отношений домена	
domain trust show <домен>	Показать сведения о доверенном домене	
domain trust validate <домен>	Проверить доверие к домену	Можно использовать следующие опции: ***--validate-location=LOCATION*** — где проверить объект доверенного домена (**local**, **both**);

Команда	Описание	Примечание
		-U USERNAME — имя пользователя.

Глава 33. Настройка DNS

33.1. Два домена Samba

33.2. Samba DC и Windows Server с AD

Перед настройкой доверия необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

Примечание

Пересылка — это механизм, который позволяет серверу направлять запросы на разрешение доменных имён на другие DNS-серверы, если он сам не может их обработать.

Пересылка настраивается в конфигурации DNS-сервера в файле **`/etc/bind/options.conf`**:

```
options {
    forwarders { 8.8.8.8; };
};
```

При использовании доверительных отношений, системы в одном домене должны уметь находить ресурсы и аутентифицировать пользователей из другого домена. Для этого им нужно корректно определять IP-адреса ресурсов другого домена. Однако, если один DNS-сервер не знает, как разрешить запросы для другого домена, запросы просто не смогут обрабатываться. Решением является условная пересылка, которая перенаправляет запросы для второго домена на соответствующий DNS-сервер.

Условная пересылка (conditional forwarding) — метод, который позволяет направлять запросы на разные серверы в зависимости от домена.

Условная пересылка указывается в файле **`/etc/bind/options.conf`**:

```
zone "trust.dom" in {
    type forward;
    forwarders { 10.64.224.10; };
};
```

33.1. Два домена Samba

Таблица 33.1. Исходные данные

	Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
Домен Linux	**TEST.ALT**	dc1.test.alt	**192.168.0.132**	ALT Server 10.2	4.19.9
Домен Linux	**EXAMPLE.ALT**	s1.example.alt	**192.168.0.172**	ALT Server 10.2	4.19.9
Выделенный DNS-сервер			**192.168.0.150**	ALT Server 10.2	

33.1.1. Настройка переадресации DNS на DC с BIND9_DLZ

Если используется DNS бэкенд BIND9_DLZ, необходимо добавить информацию о зоне в конец файла **/etc/bind/options.conf**:

- на контроллере домена dc1.test.alt добавить строки:

```
zone "example.alt" {
      type forward;
      forwarders { 192.168.0.172; };
};
```

- на контроллере домена s1.example.alt:

```
zone "test.alt" {
      type forward;
      forwarders { 192.168.0.132; };
};
```

Перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание

Если удалённый DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить проверку DNSSEC на сервере AD. Для этого необходимо в файле **/etc/bind/options.conf** в секцию ***options*** добавить параметр:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

33.1.2. Настройка переадресации DNS на DC с SAMBA_INTERNAL

Если используется DC с DNS бэкенд SAMBA_INTERNAL, самый простой способ заставить работать разрешение имен — настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На каждом контроллере домена:

1. Указать DNS-прокси, как сервер пересылки в файле **/etc/samba/smb.conf** (в параметре ***dns forwarder***). Например:

```
dns forwarder = 192.168.0.150 8.8.8.8
```

2. Перезапустить службу samba:

```
# systemctl restart samba
```

На сервере bind9 отредактировать файл **/etc/bind/options.conf**:

- так как SAMBA_INTERNAL не имеет функционала расширения безопасности DNS, необходимо отключить проверку DNSSEC, для этого в секцию ***options*** добавить параметр:

```
dnssec-validation no;
```

- в конец файла **/etc/bind/options.conf** (или **/etc/bind/ddns.conf**) добавить информацию о зонах:

```
zone "example.alt" {
      type forward;
      forwarders { 192.168.0.172; };
};

zone "test.alt" {
      type forward;
      forwarders { 192.168.0.132; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

33.1.3. Проверка конфигурации DNS

Для проверки настройки следует убедиться, что на обоих контроллерах домена разрешаются SRV-записи:

- на контроллере домена dc1.test.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt has SRV record 0 100 88 s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

- на контроллере домена s1.example.alt:

```
# host -t srv _kerberos._tcp.example.alt
_kerberos._tcp.example.alt has SRV record 0 100 88 s1.example.alt.
# host -t srv _kerberos._tcp.test.alt
_kerberos._tcp.test.alt has SRV record 0 100 88 dc1.test.alt.
```

Проверить возможность получения билета Kerberos:

- на контроллере домена dc1.test.alt:

```
# kinit administrator@EXAMPLE.ALT
Password for administrator@EXAMPLE.ALT:
# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_eFyZ8Tr
Default principal: administrator@EXAMPLE.ALT

Valid starting       Expires              Service principal
27.03.2024 14:14:36  28.03.2024 00:14:36  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 14:14:32
```

- на контроллере домена s1.example.alt:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@TEST.ALT

Valid starting       Expires              Service principal
27.03.2024 15:17:50  28.03.2024 01:17:50  krbtgt/TEST.ALT@TEST.ALT
        renew until 28.03.2024 15:17:46
```

Важно

realm должен быть записан заглавными буквами.

33.2. Samba DC и Windows Server с AD

Таблица 33.2. Исходные данные

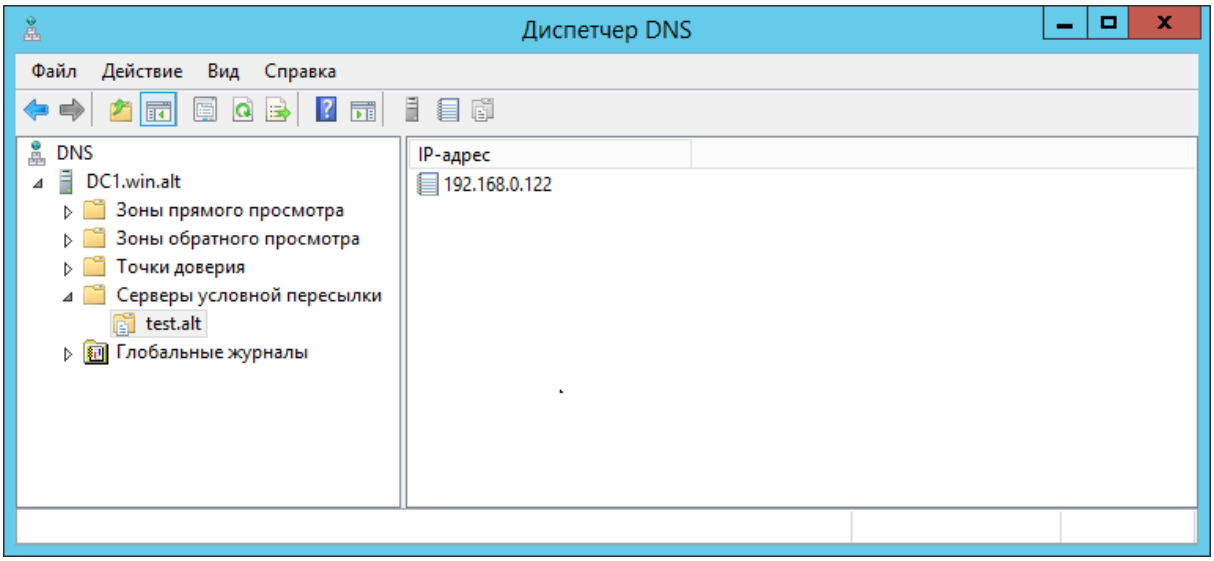
	Имя домена	Контроллер домена	IP-адрес	ОС	Уровень работы домена	Версия Samba
Домен Linux	**TEST.ALT**	dc1.test.alt	**192.168.0.132**	ALT Server 10.2	2012_R2	4.19.9
Домен Windows	**WIN.ALT**	DC1.win.alt	**192.168.0.190**	Windows Server 2012	2012R2	
Выделенный DNS-сервер			**192.168.0.150**	ALT Server 10.2		

33.2.1. Windows Server с AD

На AD сервере создать сервер условной пересылки для зоны Samba домена.

В графическом интерфейсе:

1. Открыть **Диспетчер DNS** (**DNS Manager**).
2. В разделе **Серверы условной пересылки** (**Conditional Forwarders**) добавить новый сервер пересылки, указав FQDN или IP-адрес сервера Samba:



3. Сохранить настройки.

В командной строке:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd test.alt /Forwarder 192.168.0.132
DNS Server 127.0.0.1 created zone test.alt:

Command completed successfully
```

Или выполнить следующую команду в сеансе PowerShell для настройки пересылки DNS:

```
PS C:\Windows\system32> Add-DnsServerConditionalForwarderZone -Name test.alt
-MasterServers 192.168.0.132 -ReplicationScope Forest
```

33.2.2. Samba DC с BIND9_DLZ

Если используется DNS бэкенд BIND9_DLZ, добавить в конец файла **/etc/bind/options.conf** (или **/etc/bind/ddns.conf**) строки:

```
zone "win.alt" {
      type forward;
      forwarders { 192.168.0.190; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

Примечание

Если удалённый DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить проверку DNSSEC на сервере AD. Для этого необходимо в файл **/etc/bind/options.conf** в секцию ***options*** добавить параметр:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

33.2.3. Samba DC с SAMBA_INTERNAL

Если используется DC с DNS бэкенд SAMBA_INTERNAL, самый простой способ заставить работать разрешение имен — настроить DNS-прокси между двумя доменами. DNS-прокси будет перенаправлять запрос между доменами и внешним DNS-серверами. В примере, в качестве DNS-прокси используется отдельный сервер (IP-адрес 192.168.0.150) с настроенным bind9.

На контроллере домена:

- указать DNS-прокси, как сервер пересылки в файле **/etc/samba/smb.conf** (в параметре ***dns forwarder***), например:

```
dns forwarder = 192.168.0.150 8.8.8.8
```

- перезапустить службу samba:

```
# systemctl restart samba
```

На выделенном DNS-сервере:

- отредактировать файл **/etc/bind/options.conf**:
  - так как SAMBA_INTERNAL не имеет функционала расширения безопасности DNS, необходимо отключить проверку DNSSEC, для этого в секцию ***options*** добавить параметр:

```
dnssec-validation no;
```

  - в конец файла добавить информацию о зонах:

```
zone "win.alt" {
      type forward;
      forwarders { 192.168.0.190; };
};
```

- перезапустить службу DNS:

```
# systemctl restart bind.service
```

33.2.4. Проверка конфигурации DNS

Перед настройкой доверия необходимо убедиться, что серверы могут разрешать себя и друг друга.

На Samba DC:

1. Запись отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
# dig +short -t SRV _kerberos._udp.test.alt
0 100 88 dc1.test.alt.
# dig +short -t SRV _ldap._tcp.test.alt
0 100 389 dc1.test.alt.
```

   В выводе команд должен быть отображен список всех серверов.

2. Наличие записей для работы сервисов AD на DNS-сервере Samba:

```
# dig +short -t SRV _kerberos._tcp.dc._msdcs.win.alt
0 100 88 dc1.win.alt.
# dig +short -t SRV _ldap._tcp.dc._msdcs.win.alt
0 100 389 dc1.win.alt.
```

3. Проверить возможность получения билета Kerberos:

```
# kinit administrator@WIN.ALT
Password for administrator@WIN.ALT:
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@WIN.ALT

Valid starting       Expires              Service principal
27.04.2023 17:42:28  28.04.2023 03:42:28  krbtgt/WIN.ALT@WIN.ALT
    renew until 28.04.2023 17:42:25
```

Проверить наличие записей DNS-сервере AD:

1. Запустить утилиту nslookup.exe для поиска служебных записей:

```
C:\> nslookup.exe
> set type=SRV
```

2. Ввести доменное имя для служебных записей Kerberos через UDP и LDAP через TCP:

```
> _kerberos._udp.test.alt
_kerberos._udp.test.alt       SRV service location:
    priority               = 0
    weight                 = 100
    port                   = 88
    svr hostname           = dc1.test.alt
…
test.alt
    primary name server = dc1.test.alt
    responsible mail addr = hostmaster.test.alt
    serial = 7
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
```

```
    expire = 86400 (1 days)
    default TTL = 3600 (1 hours)
> _ldap._tcp.test.alt
_ldap._tcp.test.alt       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 389
    svr hostname            = dc1.test.alt
…
```

Глава 34. Создание доверительного отношения

34.1. Два домена Samba

34.2. Samba AD и Windows Server с AD

34.1. Два домена Samba

На стороне Samba AD для создания доверия используется команда:

```
# samba-tool domain trust create <домен> --type=<тип доверия>
--direction=<направление> --create-location=<место создания> -U <пользователь>
```

Где:

- **<домен>** — имя удалённого домена, с которым создаётся доверие;
- **<тип доверия>** — определяет тип доверия:
  - **external** — используется для внешнего доверия между доменами, не находящимися в одном лесу. Рекомендуется, если для Linux-клиентов используется SSSD;
  - **forest** — используется для создания доверия между лесами доменов, включая все их дочерние домены. Рекомендуется, если для Linux-клиентов используется Winbind;
- **--direction=<направление>** — определяет направление доверия:
  - **incoming** — доверие только со стороны удалённого домена к текущему;
  - **outgoing** — доверие только от текущего домена к удалённому;
  - **both** — двустороннее доверие;
- **--create-location=<место создания>** — указывает место создания доверительного отношения:
  - **local** — объект доверенного домена будет создан только в локальном домене, доверительные отношения будут зарегистрированы и настроены только со стороны текущего домена, без внесения изменений в конфигурацию удаленного домена;
  - **both** — объект доверенного домена будет создан в обоих доменах;
- **-U <пользователь>** — имя пользователя с правами администратора для удалённого домена.

В данном примере на контроллере домена dc1.test.alt необходимо выполнить команду:

```
# samba-tool domain trust create EXAMPLE.ALT  --type=forest \
--direction=both --create-location=both -U administrator@EXAMPLE.ALT

LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
Creating remote TDO.
Remote TDO created.
Setting supported encryption types on remote TDO.
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                  DNS[*.example.alt]
DOM: Status[Enabled]                  DNS[example.alt] Netbios[EXAMPLE]
SID[S-1-5-21-3274802069-598906262-3677769431]
Setup remote forest trust information...
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                  DNS[*.test.alt]
DOM: Status[Enabled]                  DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]
Validating outgoing trust...
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Validating incoming trust...
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Success
```

Важно

Для входа в доверенный домен через SSSD надо использовать тип связи **external**, а не **forest**.

Проверка доверия:

- просмотр доверия с dc1.test.alt:

```
[root@dc1 ~]# samba-tool domain trust show EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
TrustedDomain:

NetbiosName:    EXAMPLE
DnsName:        example.alt
SID:            S-1-5-21-3274802069-598906262-3677769431
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
```

```
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[example.alt]:
TLN: Status[Enabled]                  DNS[*.example.alt]
DOM: Status[Enabled]                  DNS[example.alt] Netbios[EXAMPLE]
SID[S-1-5-21-3274802069-598906262-3677769431]
```

- просмотр доверия с s1.example.alt:

```
[root@s1 ~]# samba-tool domain trust show TEST.ALT
LocalDomain Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
TrustedDomain:

NetbiosName:    TEST
DnsName:        test.alt
SID:            S-1-5-21-1455776928-3410124986-2843404052
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[test.alt]:
TLN: Status[Enabled]                  DNS[*.test.alt]
DOM: Status[Enabled]                  DNS[test.alt] Netbios[TEST]
SID[S-1-5-21-1455776928-3410124986-2843404052]
```

- список трастов:

```
[root@dc1 ~]# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[example.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста, который установлен с этим доменом.

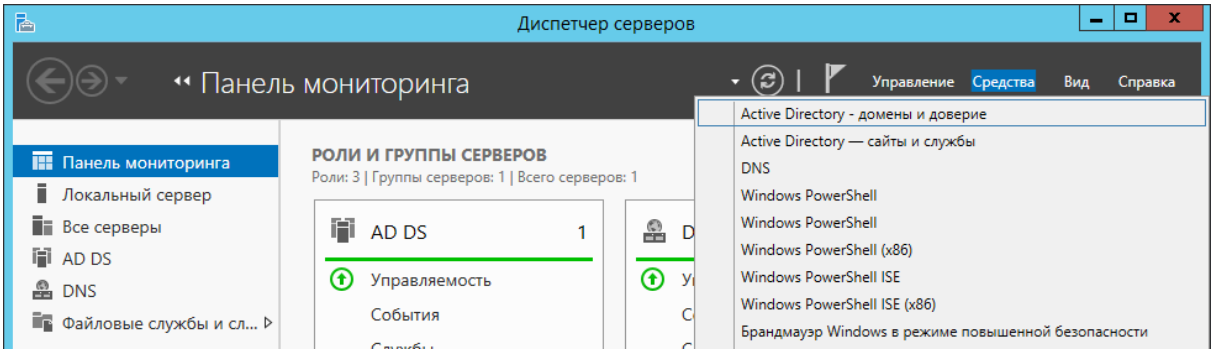
Если после настройки доверия возникли проблемы с доступом пользователей из трастового домен в свой домен, тогда следует проверить, действительно ли установлен траст:

```
[root@dc1 ~]# samba-tool domain trust validate EXAMPLE.ALT
-Uadministrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
LocalTDO Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
OK: LocalValidation: DC[\\s1.example.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\s1.example.alt] CONNECTION[WERR_OK]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc1.test.alt] CONNECTION[WERR_OK]
```

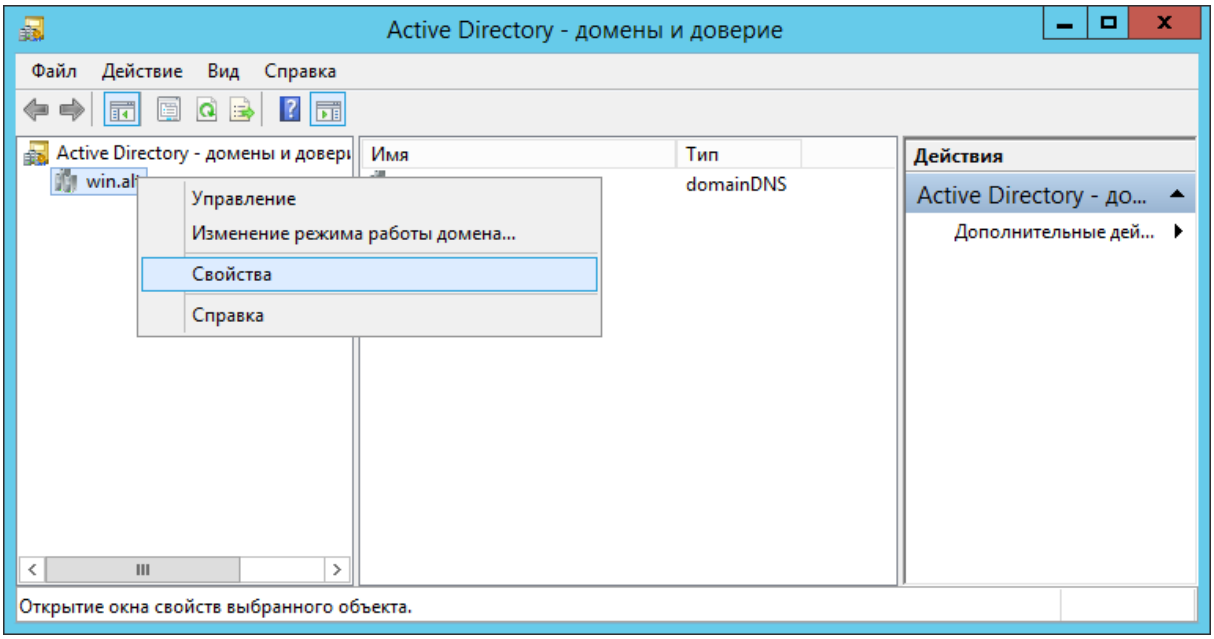
34.2. Samba AD и Windows Server с AD

Настройка на стороне Windows:

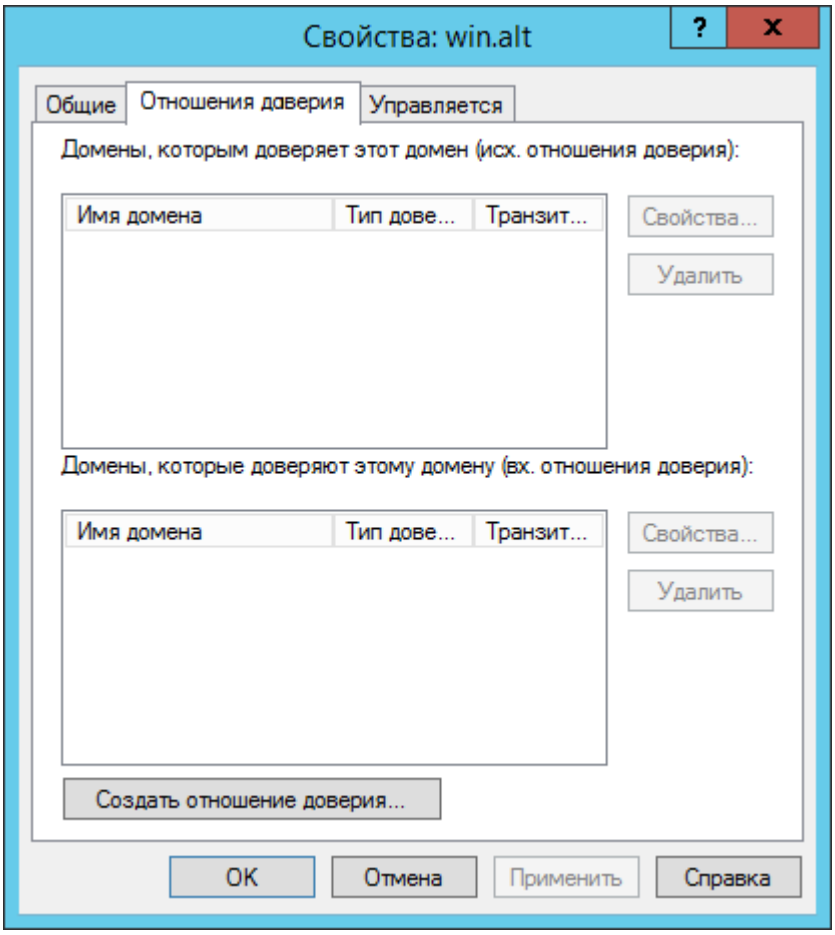
1. Открыть **Диспетчер серверов**, выбрать **Средства** → **Active Directory — Домены и Доверие**:



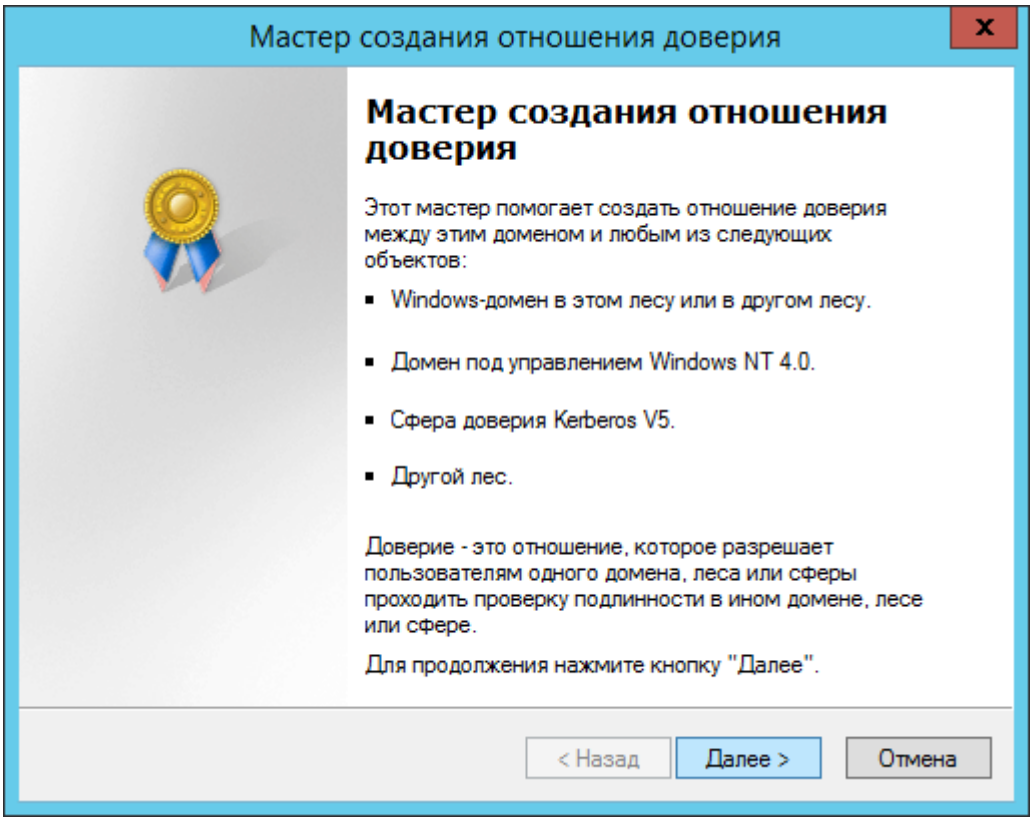
2. В открывшемся окне в контекстном меню домена выбрать пункт **Свойства**:



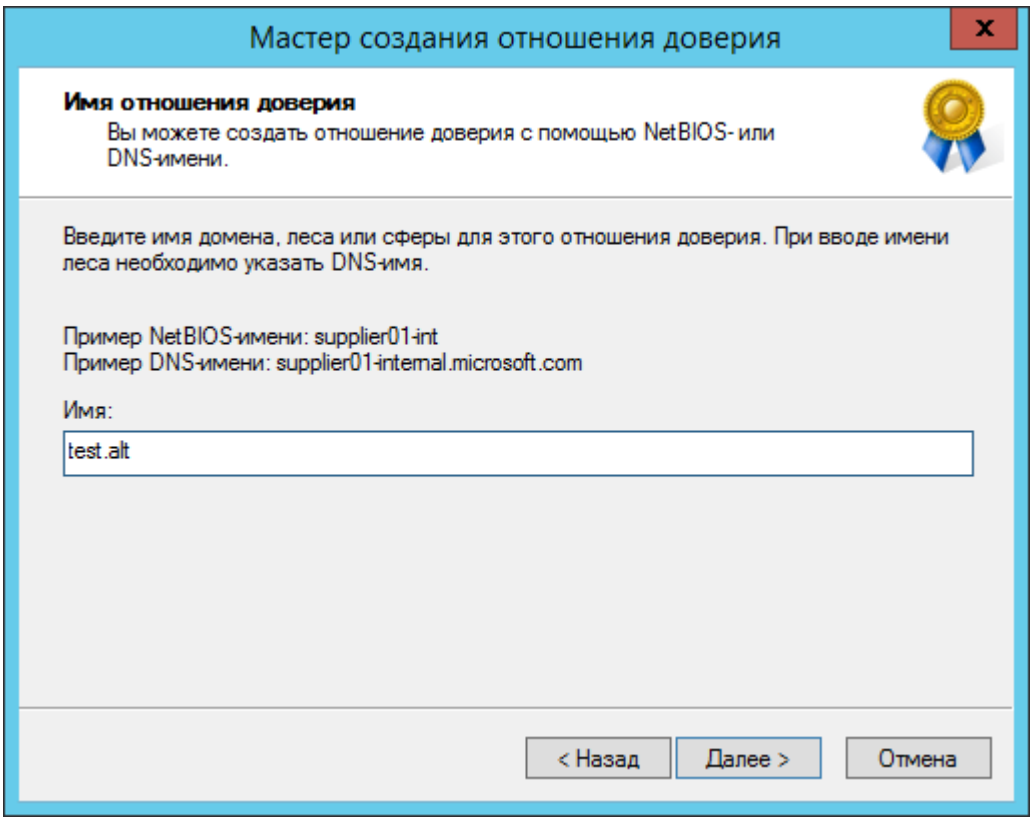
3. Откроется окно свойств домена. Необходимо перейти во вкладку **Отношения доверия** и нажать кнопку **Создать отношение доверия…**:



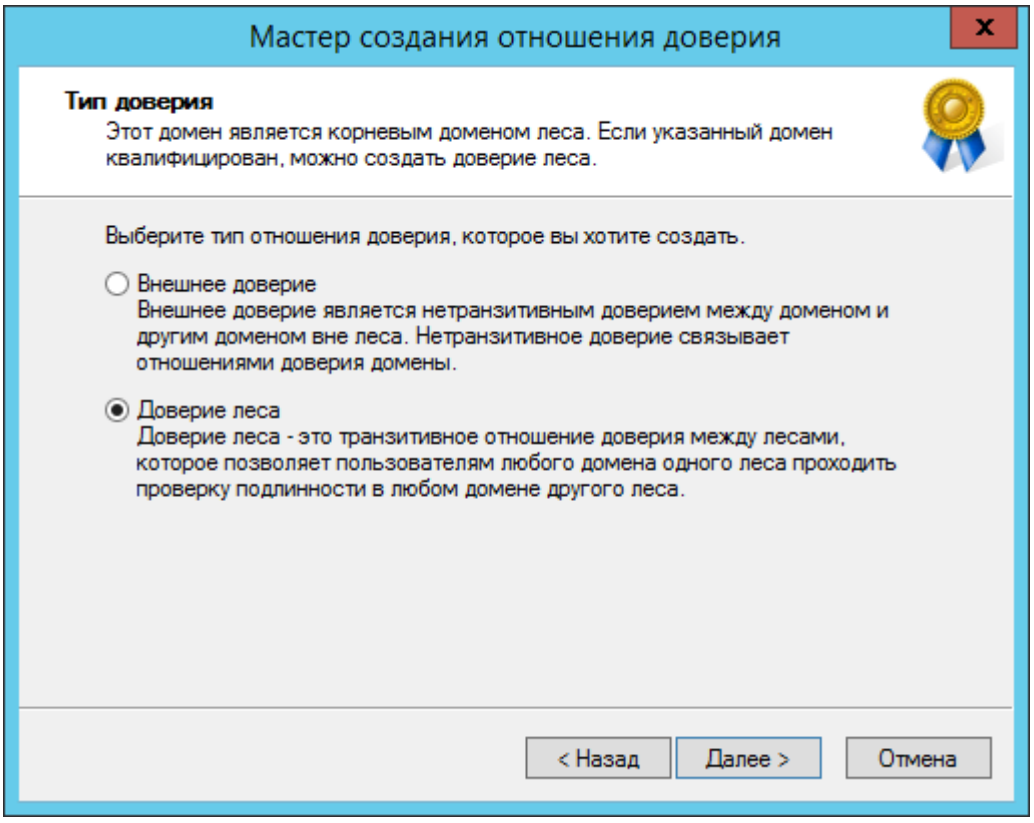
4. Будет запущен **`Мастер создания отношения доверия`**. Для перехода ко второму шагу следует нажать кнопку **`Далее`**:



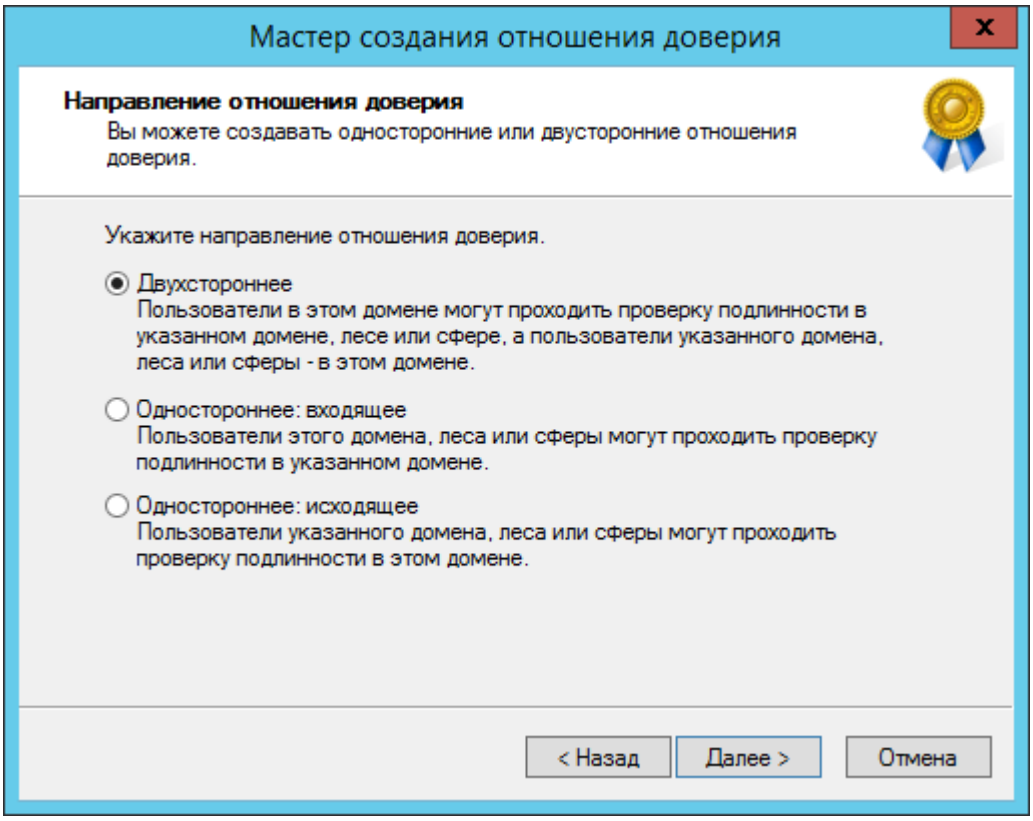
5. На втором шаге создания отношения доверия необходимо ввести имя домена Samba AD (в примере TEST.ALT):



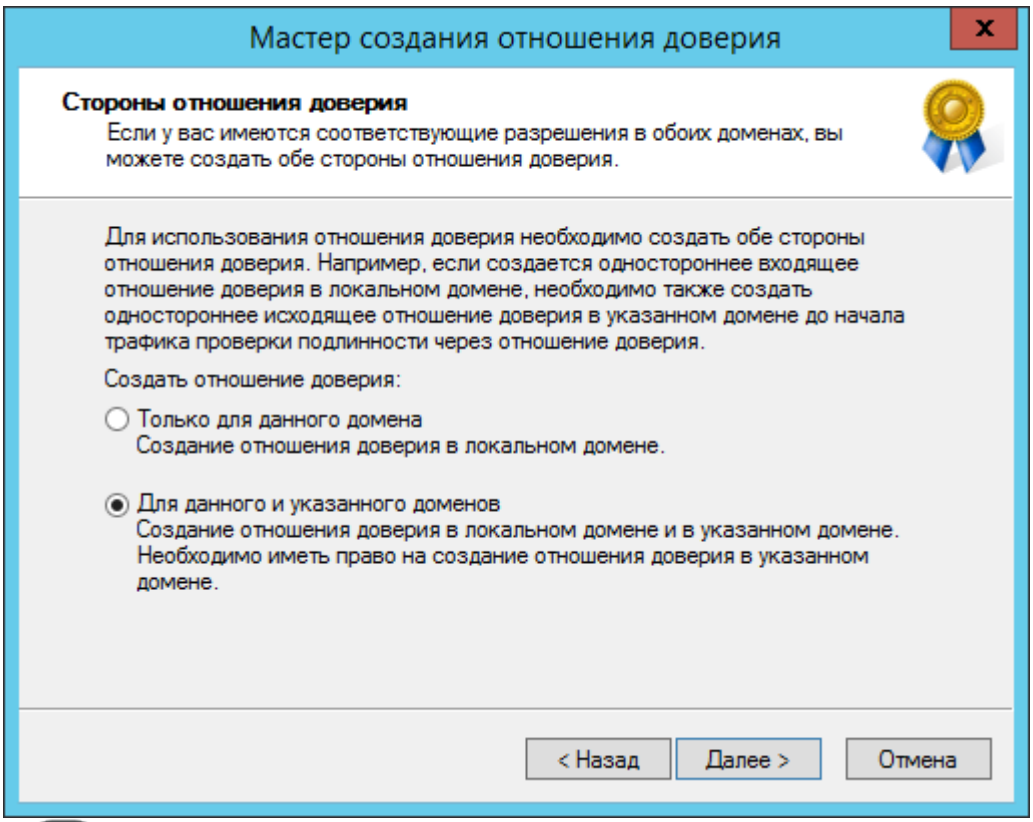
6. На следующем шаге следует выбрать тип доверия:



7. Далее выбирается направление доверия:

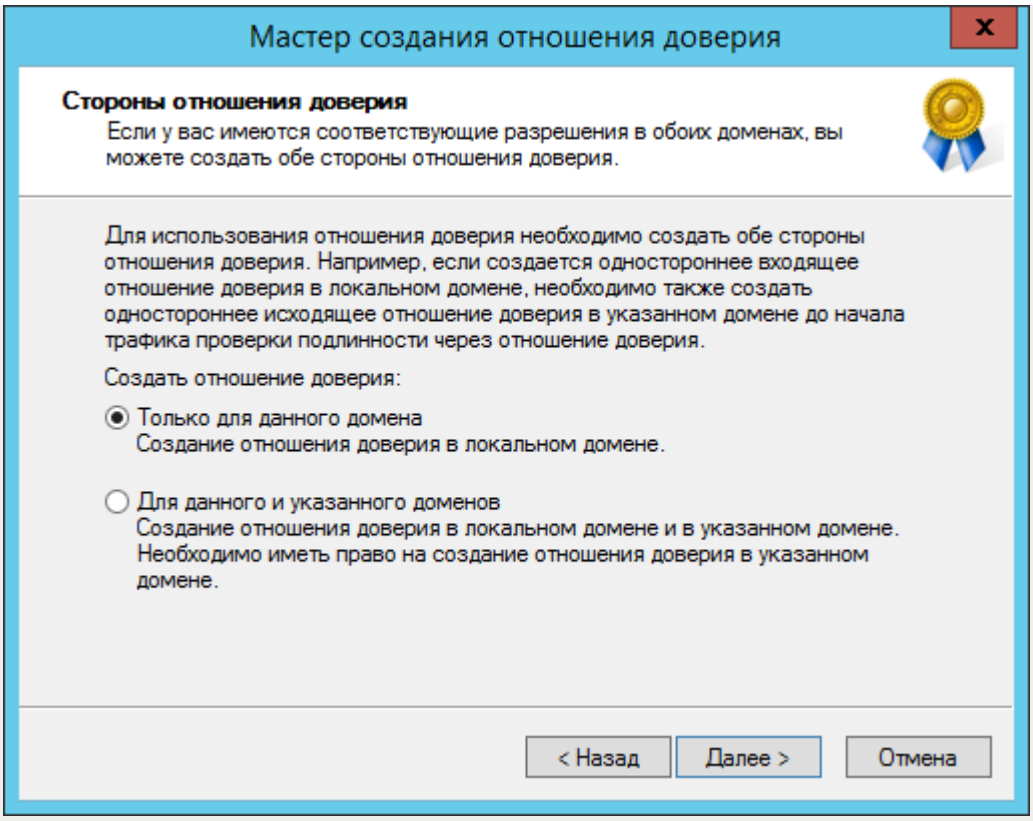


8. В открывшемся окне **`Стороны отношения доверия`** нужно выбрать, на каком из доменов применяется настройка. Если есть права администратора для обоих доменов, можно выбрать пункт **`Для данного и указанного домена`**:

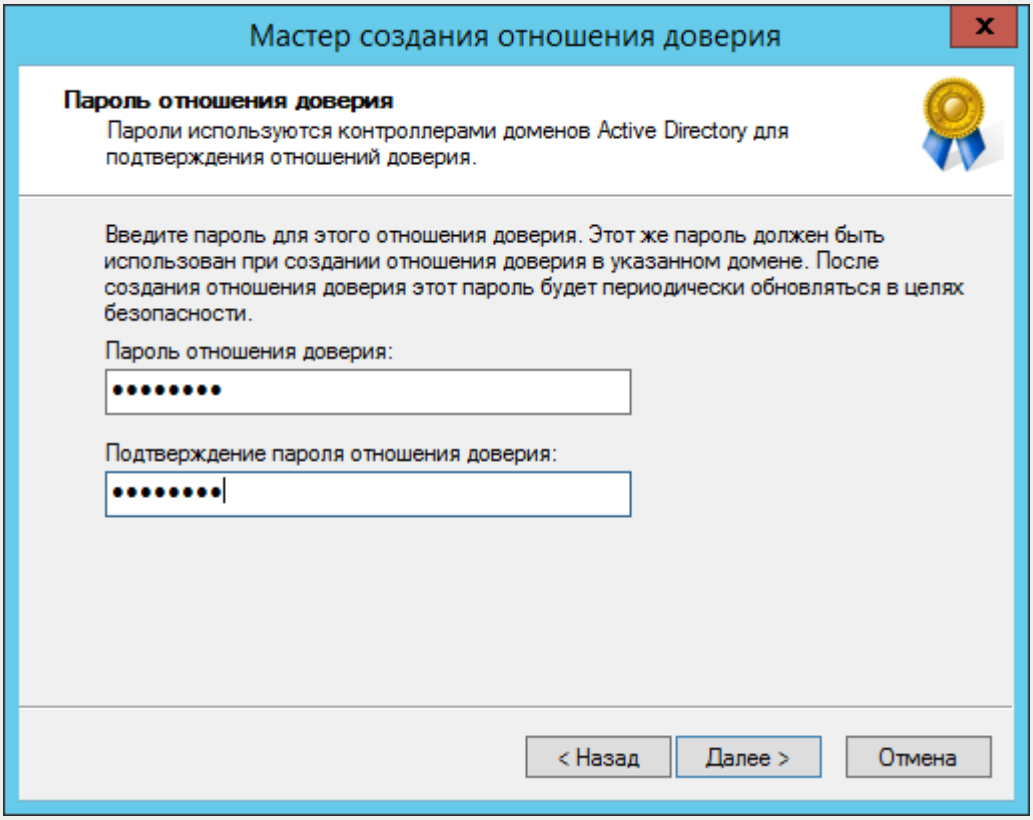


Примечание

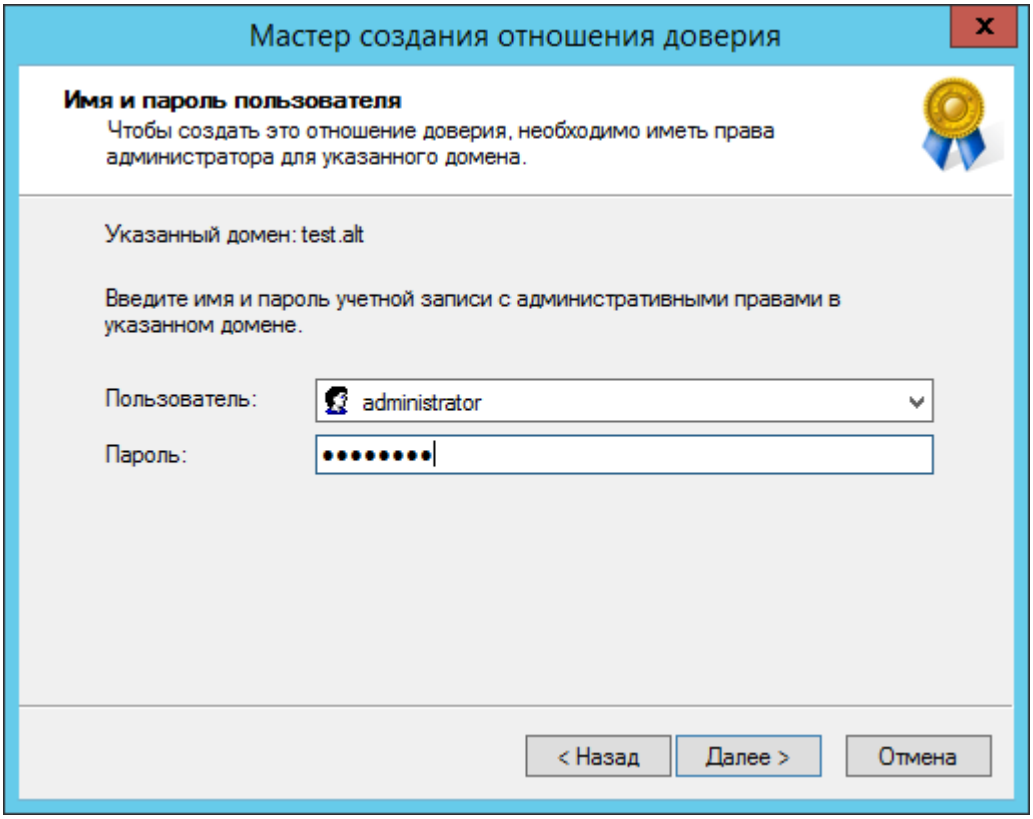
Если выбрать параметр **`Только для данного домена`**:



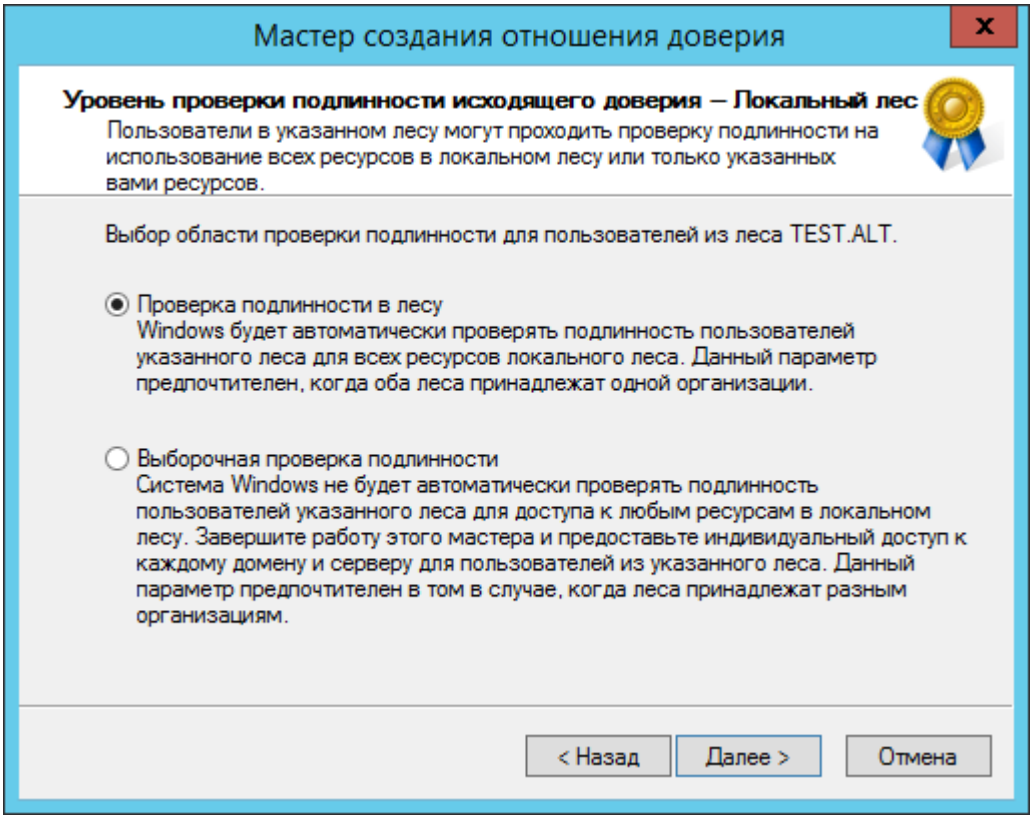
Необходимо задать **`Пароль отношения доверия`** (**`Trust Secret Key`**), который в дальнейшем будет использоваться при создании доверительного отношения на стороне Samba AD:



9. На следующем этапе мастер свяжется с удалённым доменом (если он доступен), и запросит имя и пароль пользователя с правами установки доверительных отношений в домене:

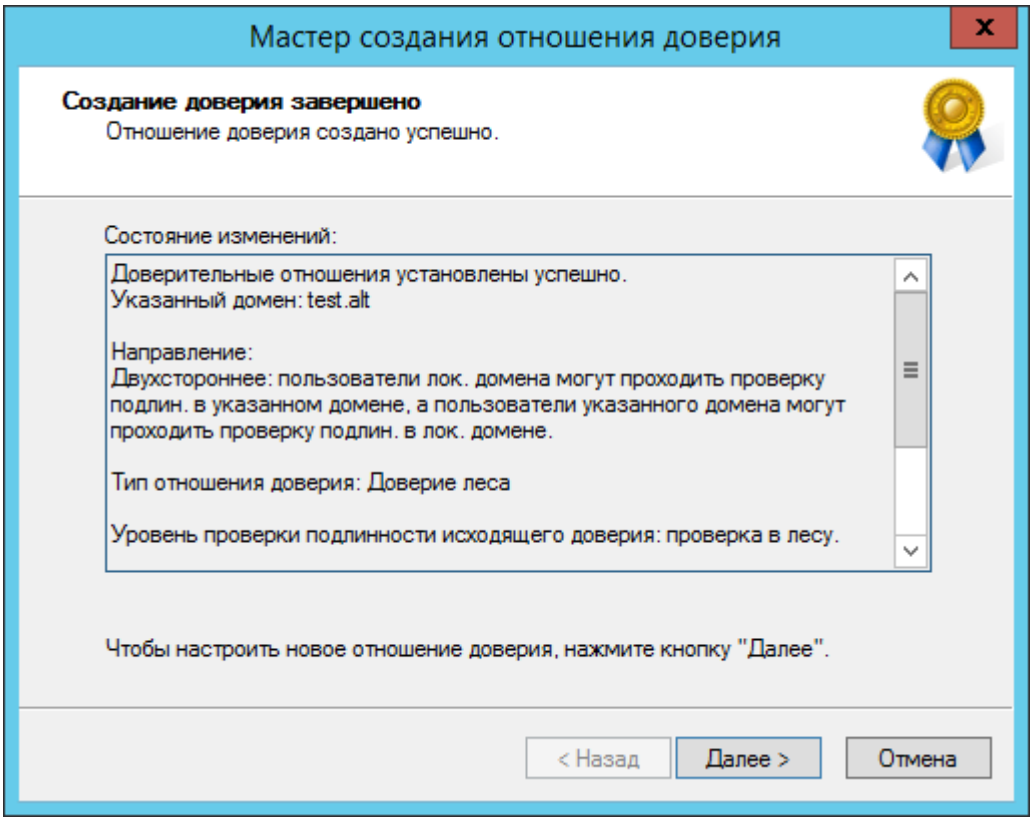


10. На шаге **`Уровень проверки подлинности исходящего доверия — Локальный лес`** следует выбрать **`Проверка подлинности в лесу`**:

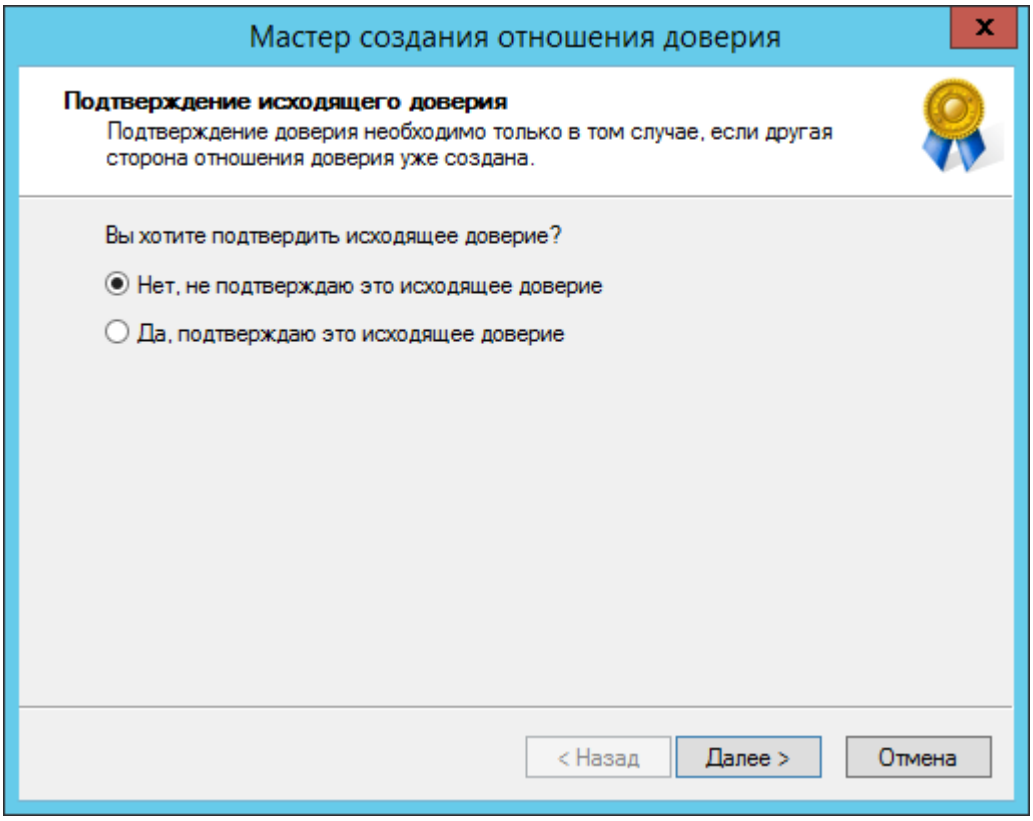


11. На шаге **Уровень проверки подлинности исходящего доверия — Указанный лес** также следует выбрать пункт **Проверка подлинности в лесу**.

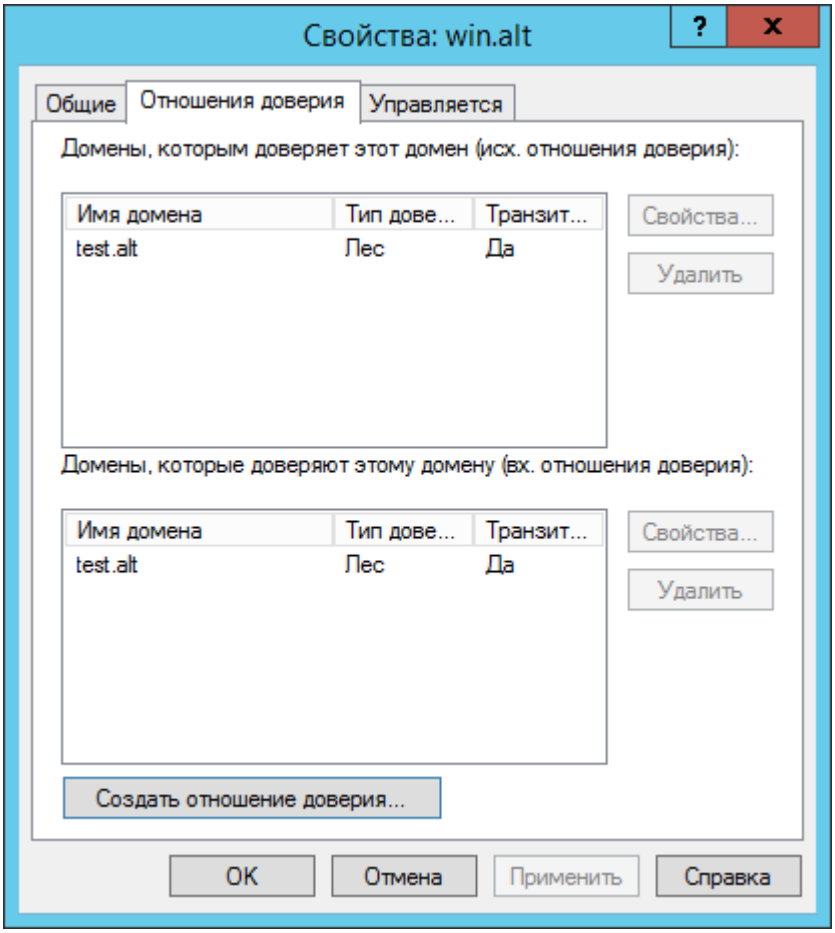
12. В окне **Выбор доверия завершен** мастер выдаст уведомление о том, что готов создать новое отношение доверия, и покажет краткую сводку с выбранными параметрами. Если согласиться с параметрами, то должно появиться уведомление о том, что создание доверия завершено:



13. После нажатия кнопки **Далее** появится окно **Подтверждение исходящего доверия**, а после него **Подтверждение входящего доверия**. Здесь можно оставить выбранным пункт **Нет, не подтверждаю это исходящее/входящее отношение доверие**, так как на стороне Samba DC доверие ещё не создавалось:



14. В результате будут получены двухсторонние доверительные отношения между доменами:



На стороне Samba AD для создания доверия необходимо выполнить команду:

```
# samba-tool domain trust create win.alt --type=forest \
--direction=both --create-location=both -Uadministrator@WIN
```

При появлении запроса необходимо ввести пароль администратора.

Важно

Для входа в доверенный домен через SSSD следует использовать тип связи **external**, а не **forest**.

Если все настроено верно, будет установлено доверие к домену AD:

```
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6,ADS_WEB_SERVICE,DS_8,__unknown_00008000__]
Password for [administrator@WIN]:
RemoteDomain Netbios[WIN] DNS[win.alt]
SID[S-1-5-21-212759798-1661061060-862600140]
Creating local TDO.
Local TDO created
Setting supported encryption types on local TDO.
Setup local forest trust information...
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled]                  DNS[*.win.alt]
DOM: Status[Enabled]                  DNS[win.alt] Netbios[WIN]
SID[S-1-5-21-212759798-1661061060-862600140]
Validating outgoing trust...
OK: LocalValidation: DC[\\DC1.win.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
Validating incoming trust…
OK: RemoteValidation: DC[\\dc1.test.alt] CONNECTION[WERR_OK] TRUST[WEER_OK]
VERIFY_STATUS_RETURNED
Success.
```

В случае использования Trust Secret Key в параметре ***--create-location*** нужно заменить опцию **both** на **local**. Samba DC прежде чем создать доверительные отношения сначала запросит Trust Key (Incoming Trust Password/Outgoing Trust Password), созданный ранее при настройке в Windows:

```
# samba-tool domain trust create win.alt --type=forest \
--direction=both --create-location=local -Uadministrator@WIN

New Incoming Trust Password:
Retype Incoming Trust Password:
New Outgoing Trust Password:
Retype Outgoing Trust Password:
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
RemoteDC Netbios[DC1] DNS[DC1.win.alt] ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,…]
Password for [administrator@WIN]:
…
```

Проверка доверия с dc1.test.alt:

- просмотр доверия:

```
# samba-tool domain trust show WIN.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
TrustedDomain:

NetbiosName:    WIN
DnsName:        win.alt
SID:            S-1-5-21-212759798-1661061060-862600140
Type:           0x2 (UPLEVEL)
Direction:      0x3 (BOTH)
Attributes:     0x8 (FOREST_TRANSITIVE)
PosixOffset:    0x00000000 (0)
kerb_EncTypes:  0x18 (AES128_CTS_HMAC_SHA1_96,AES256_CTS_HMAC_SHA1_96)
Namespaces[2] TDO[win.alt]:
TLN: Status[Enabled]                DNS[*.win.alt]
DOM: Status[Enabled]                DNS[win.alt] Netbios[WIN]
SID[S-1-5-21-212759798-1661061060-862600140]
```

- список трастов:

```
# samba-tool domain trust list
Type[Forest]   Transitive[Yes] Direction[BOTH]     Name[win.alt]
```

В разных доменах могут быть разные результаты. Результат зависит от типа траста, который установлен с этим доменом.

Если после настройки доверия возникли проблемы с доступом пользователей из трастового домен в свой домен, тогда следует проверить, действительно ли установлен траст:

```
# samba-tool domain trust validate win.alt -Uadministrator@WIN
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-3848605173-1839566900-710408900]
LocalTDO Netbios[WIN] DNS[win.alt] SID[S-1-5-21-212759798-1661061060-862600140]
OK: LocalValidation: DC[\\DC1.win.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\DC1.win.alt] CONNECTION[WERR_OK]
RemoteDC Netbios[DC1] DNS[DC1.win.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6,ADS_WEB_SERVICE,DS_8,__unknown_00008000__]
Password for [administrator@WIN]:
OK: RemoteValidation: DC[\\dc2.test.alt] CONNECTION[WERR_OK] TRUST[WERR_OK]
VERIFY_STATUS_RETURNED
OK: RemoteRediscover: DC[\\dc2.test.alt] CONNECTION[WERR_OK]
```

Глава 35. Управление пользователями и группами

35.1. Список пользователей и групп

35.2. Тестирование аутентификации

35.3. Просмотр доверия в Windows

После настройки доверия можно назначать пользователей и группы из доверяющего домена в группу доверенного домена. Так как настроено двустороннее доверие, можно назначать пользователей и группы в обоих направлениях.

Примечание

Предварительно необходимо создать несколько пользователей и групп в обоих доменах (см. Управление пользователями и группами).

35.1. Список пользователей и групп

С помощью команды **wbinfo** нельзя получить список пользователей и групп из доверяющего домена, можно получить список пользователей и групп только из своего домена. Пример получения списка пользователей:

- команды выполняются на контроллере домена dc1.test.alt:

```
# wbinfo -u --domain=EXAMPLE.ALT
# wbinfo -u --domain=TEST.ALT
TEST\administrator
TEST\guest
TEST\krbtgt
TEST\dns-dc1
TEST\ivanov
```

- команды выполняются на контроллере домена s1.example.alt:

```
# wbinfo -u --domain=EXAMPLE.ALT
EXAMPLE\administrator
EXAMPLE\guest
EXAMPLE\krbtgt
EXAMPLE\dns-s1
EXAMPLE\kim
# wbinfo -u --domain=TEST.ALT
```

Для получения списка всех пользователей можно выполнить LDAP-запрос с помощью команды **samba-tool**. Пример получения списка пользователей из обоих доменов на контроллере домена dc1.test.alt:

```
# samba-tool user list -H ldap://s1 -Uadministrator@EXAMPLE.ALT
Password for [administrator@EXAMPLE.ALT]:
dns-s1
krbtgt
Administrator
Guest
kim
# samba-tool user list -H ldap://dc1 -Uadministrator@TEST.ALT
Password for [administrator@TEST.ALT]:
dns-dc1
krbtgt
Guest
Administrator
ivanov
```

Получение дополнительной информации о доменах (в примерах команды выполняются на контроллере домена dc1.test.alt):

- получение списка всех доменов:

```
# wbinfo --all-domains
BUILTIN
TEST
EXAMPLE
```

- вывод основного домена (домен, к которому в данный момент подключена система):

```
# wbinfo --own-domain
TEST
```

- вывод списка доменов, которые находятся в состоянии доверия с текущим доменом:

```
# wbinfo --trusted-domains
BUILTIN
TEST
EXAMPLE
```

- отображение текущего состояния подключения Winbind к различным доменам:

```
# wbinfo --online-status
BUILTIN : active connection
TEST : active connection
EXAMPLE : active connection
```

Получение SID пользователей и групп (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# wbinfo -n TEST\\office
S-1-5-21-1455776928-3410124986-2843404052-1107 SID_DOM_GROUP (2)

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)

# wbinfo -i TEST\\ivanov
TEST.ALT\ivanov:*:3000022:100::/home/TEST.ALT/ivanov:/bin/false

# wbinfo -i EXAMPLE\\kim
EXAMPLE\kim:*:3000020:3000021::/home/EXAMPLE/kim:/bin/false
```

35.2. Тестирование аутентификации

С помощью команды **wbinfo** можно протестировать процесс аутентификации разных пользователей из обоих доменов.

wbinfo попытается авторизовать пользователя. Первой проверкой будет аутентификация по паролю с открытым текстом. Этот тип аутентификации применяется, когда пользователь входит в систему локально (plaintext не означает, что пароль будет отправлен без шифрования, это просто название процесса входа в систему). Вторая проверка — аутентификация по паролю запрос/ответ. Этот тип аутентификации использует NTLM или Kerberos.

Проверка методов аутентификации (в примере команды выполняются на контроллере домена dc1.test.alt):

```
# wbinfo -a TEST\\ivanov
Enter TEST\ivanov's password:
plaintext password authentication succeeded
Enter TEST\ivanov's password:
challenge/response password authentication succeeded


# wbinfo -a EXAMPLE\\kim
Enter EXAMPLE\kim's password:
plaintext password authentication succeeded
Enter EXAMPLE\kim's password:
challenge/response password authentication succeeded
```

Посмотреть какие контроллеры домена отвечают за аутентификацию:

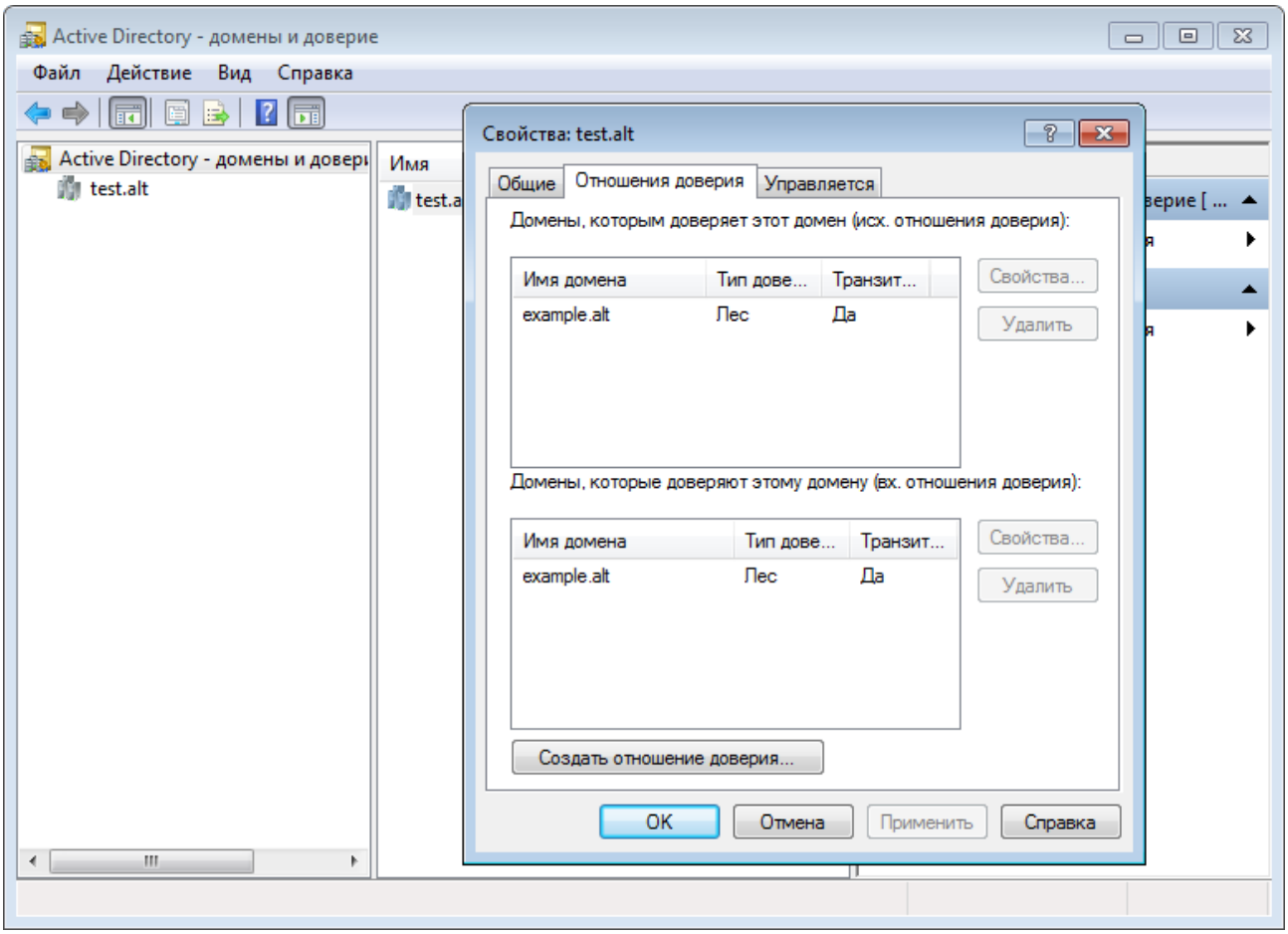
```
# wbinfo --ping-dc
checking the NETLOGON for domain[TEST] dc connection to "dc1.test.alt" succeeded

# wbinfo --ping-dc --domain=EXAMPLE.ALT
checking the NETLOGON for domain[EXAMPLE.ALT] dc connection to "s1.example.alt"
succeeded
```

Назначение пользователей и групп из доверенных доменов в группу доверяющего домена:

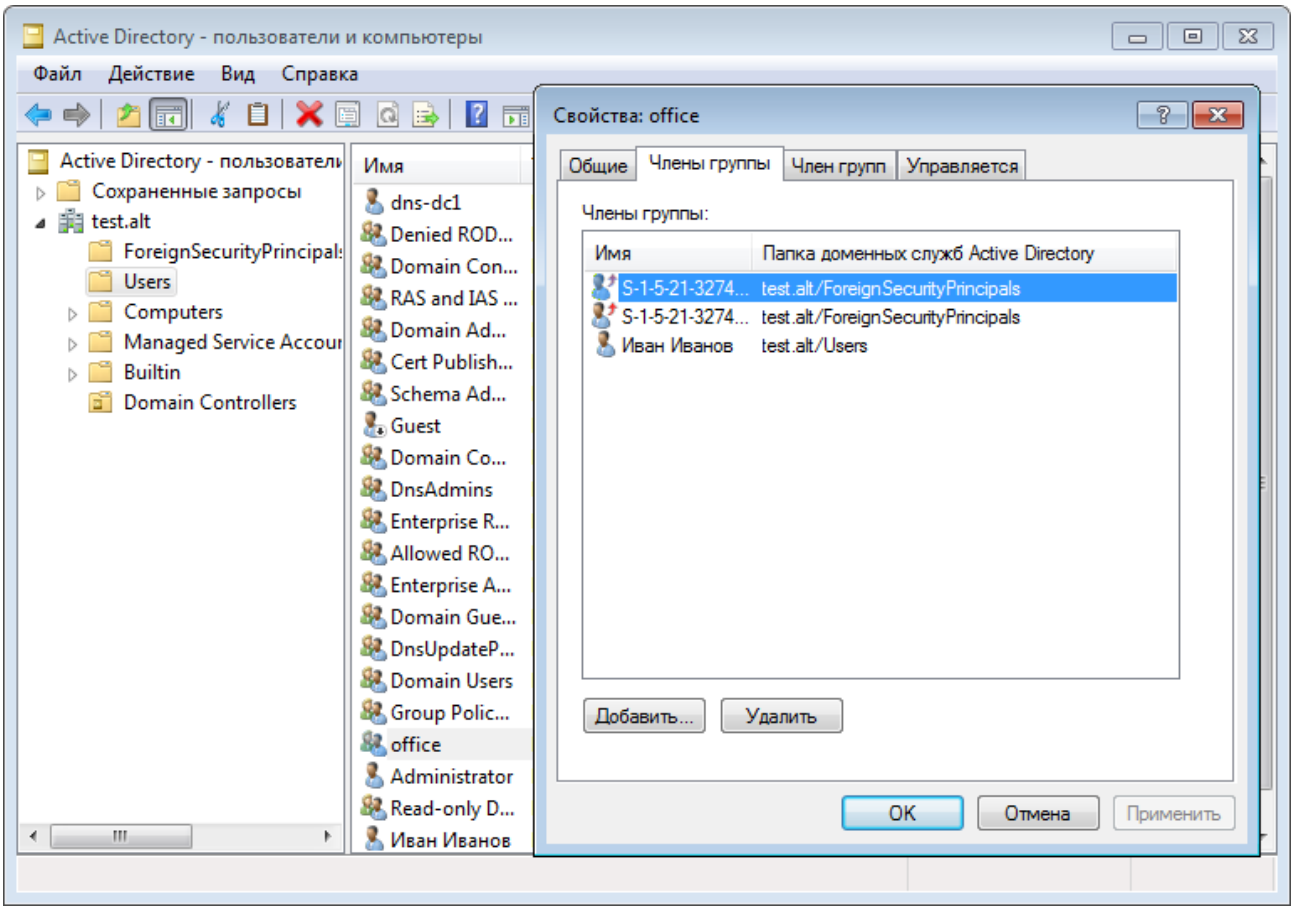
```
# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)

# samba-tool group addmembers office
S-1-5-21-3274802069-598906262-3677769431-1104
Added members to group office

# wbinfo -n EXAMPLE\\office2
S-1-5-21-3274802069-598906262-3677769431-1107 SID_DOM_GROUP (2)

# samba-tool group addmembers office
S-1-5-21-3274802069-598906262-3677769431-1107
Added members to group office

# samba-tool group listmembers office
S-1-5-21-3274802069-598906262-3677769431-1104
ivanov
S-1-5-21-3274802069-598906262-3677769431-1107
```

35.3. Просмотр доверия в Windows

Модуль RSAT (см. Установка административных инструментов (машина Windows)) «Active Directory — домены и доверие» («Active Directory — Domain and Trusts») позволяет проверить состояние отношений доверия между доменами:



В модуле RSAT «Active Directory — пользователи и компьютеры» («Active Directory — Users and Computers») можно просмотреть список пользователей группы:



Глава 36. Использование трастов на LINUX-клиентах

36.1. Настройка Winbind

36.2. Настройка SSSD

Если необходимо использовать пользователей из обоих доменов (установлены двухсторонние доверительные отношения с типом связи **Лес**), то рабочую станцию с ОС Альт следует вводить в домен через Winbind (см. Подключение к домену с использованием Winbind).

36.1. Настройка Winbind

Важно правильно спланировать диапазоны идентификаторов (UID и GID), назначаемых пользователям и группам (см. Планирование и настройка диапазонов идентификаторов UID и GID (Winbind/IDMapping)).

На машине, введённой в домен, необходимо в файле **`smb.conf`** установить ID-маппинг для обоих доменов (backend = rid/tdb).

Пример файла **`smb.conf`** на машине введённой в домен example.alt:

```
[global]
        security = ads
        realm = EXAMPLE.ALT
        workgroup = EXAMPLE
        netbios name = WORK1
        template shell = /bin/bash
```

```
        kerberos method = system keytab
        wins support = no
        winbind use default domain = yes
        winbind enum users = no
        winbind enum groups = no
        template homedir = /home/EXAMPLE.ALT/%U
        winbind refresh tickets = yes
        winbind offline logon = yes
        idmap config * : range = 3000-7999
        idmap config * : backend = tdb

        idmap config EXAMPLE : backend = rid
        idmap config EXAMPLE : range = 10000-999999
        idmap config TEST : backend = rid
        idmap config TEST : range = 1000000-9999999
```

После перезапуска **smbd** и **winbind** можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# net rpc trustdom list -Uadministrator
Password for [EXAMPLE\administrator]:
Trusted domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052

Trusting domains list:

TEST                S-1-5-21-1455776928-3410124986-2843404052
```

С помощью команды **winbind** можно получить информацию о пользователях из обоих доменов и проверить доступность доменов:

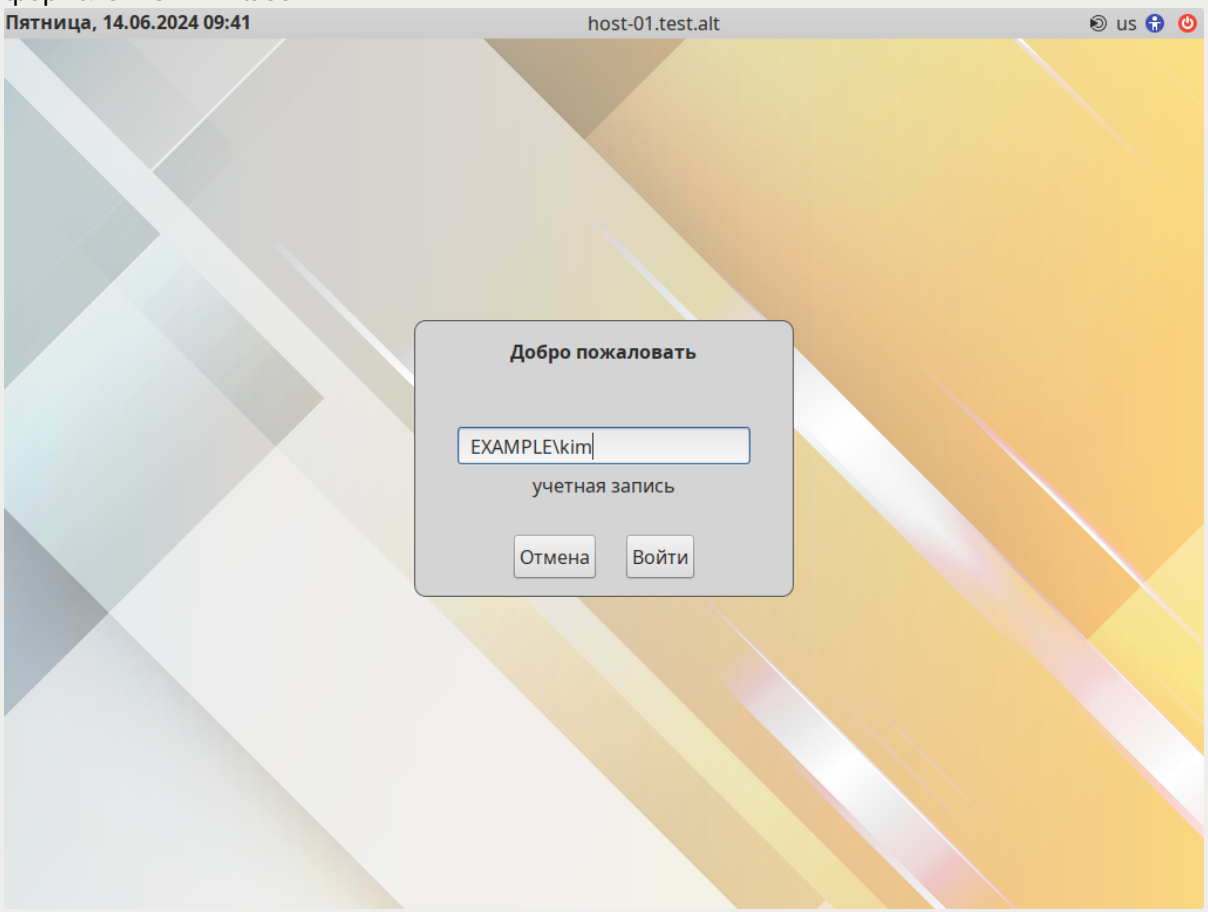
```
# wbinfo -n TEST\\ivanov
S-1-5-21-1455776928-3410124986-2843404052-1105 SID_USER (1)

# wbinfo -n EXAMPLE\\kim
S-1-5-21-3274802069-598906262-3677769431-1104 SID_USER (1)
```

Для проверки доступности пользователей и групп из доверенных доменов можно использовать **getent**:

```
# getent group TEST\\office
TEST\office:*:1001106:

# getent group EXAMPLE\\office2
office2:*:11107:

# getent passwd TEST\\ivanov
TEST\ivanov:*:1001105:1000513::/home/EXAMPLE.ALT/ivanov:/bin/bash

# getent passwd EXAMPLE\\kim
kim:*:11125:10001:Олег Ким:/home/EXAMPLE.ALT/kim:/bin/bash
```

Примечание

Для авторизации в доверенном домене следует вводить учётные данные пользователя в формате DOMAIN\user:



Проверка входа по SSH пользователями из обоих доменов:

```
$ ssh TEST\\ivanov@192.168.0.126
TEST\ivanov@192.168.0.126's password:
[TEST\ivanov@work1 ~]$ exit
выход
Connection to 192.168.0.126 closed.

$ ssh EXAMPLE\\kim@192.168.0.126
EXAMPLE\kim@192.168.0.126's password:
[kim@work1 ~]$ exit
выход
Connection to 192.168.0.126 closed.
```

36.2. Настройка SSSD

Особенности:

- SSSD требует ручного указания настроек для каждого трастового домена в клиентской конфигурации в файле **`/etc/sssd/sssd.conf`**;
- SSSD не поддерживает трасты уровня леса (Forest Trusts), что ограничивает его возможности при работе с многоуровневыми лесами доменов. Однако, для большинства стандартных трастов (External Trust) SSSD может быть применен;

- по умолчанию пул UID/GID для сопоставления SID в SSSD имеет ограниченный размер. Для больших доменов с количеством пользователей более 200 тысяч этот пул необходимо расширять вручную.

  При стандартной конфигурации настраивается 10000 срезов, каждый из которых может содержать до 200000 идентификаторов, начиная от 200000 и до 2000200000.

  Из общего диапазона, размером 2 миллиарда под каждый домен выделяется срез ID размером 200000, каждому домену может соответствовать только один единственный срез.

  Для увеличения размера среза в конфигурации SSSD используются параметры:

  - **ldap_idmap_range_min** — нижняя (включительно) граница диапазона идентификаторов;
  - **ldap_idmap_range_max** — верхняя (не включительно) граница диапазона идентификаторов;
  - **ldap_idmap_range_size** — количество идентификаторов, доступных для каждого среза. Значение должно быть не меньше значения максимального RID пользователя, запланированного для использования на сервере AD.

  Эти параметры позволяют адаптировать пул UID/GID под нужды домена. Однако, увеличивая размер среза, необходимо уменьшать количество срезов, что увеличивает вероятность коллизий (по умолчанию вероятность коллизии одного конкретного домена с другим составляет 1/10000).

На машине введённой в домен необходимо в файл **/etc/sssd/sssd.conf** добавить доверенный домен:

```
[domain/TEST.ALT/EXAMPLE.ALT]
use_fully_qualified_names = false
```

и перезапустить sssd:

```
# systemctl restart sssd
```

После перезапуска **sssd** можно проверить, есть ли возможность просматривать пользователей из обоих доменов:

```
# getent passwd ivanov
ivanov:*:1855401105:1855400513:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash

# getent passwd kim
kim@example.alt:*:829801104:829801104:Виталий Ким:/home/example.alt/kim:/bin/bash
```

С помощью команды **sssctl** можно вывести все домены, с которыми готова взаимодействовать клиентская машина, а также их статусы:

```
# sssctl domain-list
 EXAMPLE.ALT
 TEST.ALT

# sssctl domain-status EXAMPLE.ALT
 Online status: Online

 Active servers:
```

```
AD Global Catalog: s1.example.alt
AD Domain Controller: s1.example.alt

Discovered AD Global Catalog servers:
- s1.example.alt

Discovered AD Domain Controller servers:
- s1.example.alt
```

В случае проблем с авторизацией пользователем из доверенного домена, в **/etc/sssd/sssd.conf** в секцию основного домена можно вписать:

```
krb5_validate = false
```

Глава 37. Удаление доверия

37.1. На стороне Samba

37.2. На стороне Windows Server с AD

37.1. На стороне Samba

Пример удаления доверия на контроллере домена dc1.test.alt:

```
# samba-tool domain trust delete EXAMPLE.ALT -U administrator@EXAMPLE.ALT
LocalDomain Netbios[TEST] DNS[test.alt]
SID[S-1-5-21-1455776928-3410124986-2843404052]
RemoteDC Netbios[S1] DNS[s1.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIMESERV,FULL_SECRET
_DOMAIN_6]
Password for [administrator@EXAMPLE.ALT]:
RemoteDomain Netbios[EXAMPLE] DNS[example.alt]
SID[S-1-5-21-3274802069-598906262-3677769431]
RemoteTDO deleted.
```

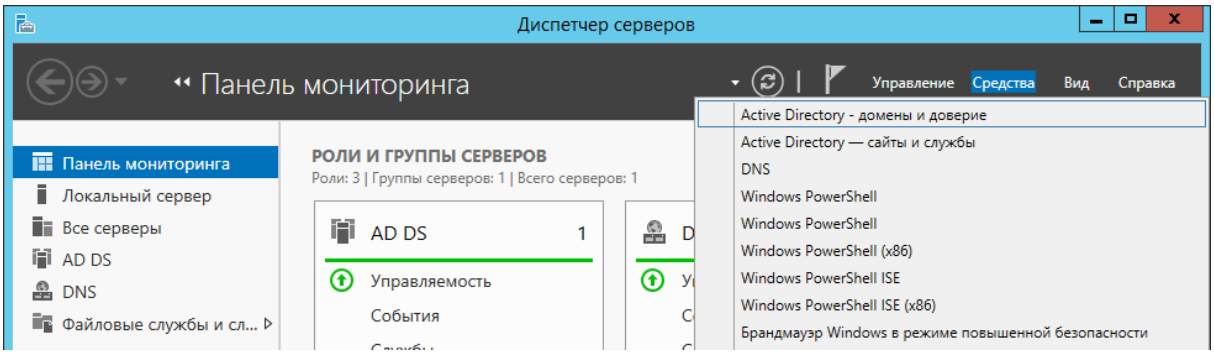
Проверка:

```
# samba-tool domain trust list
```

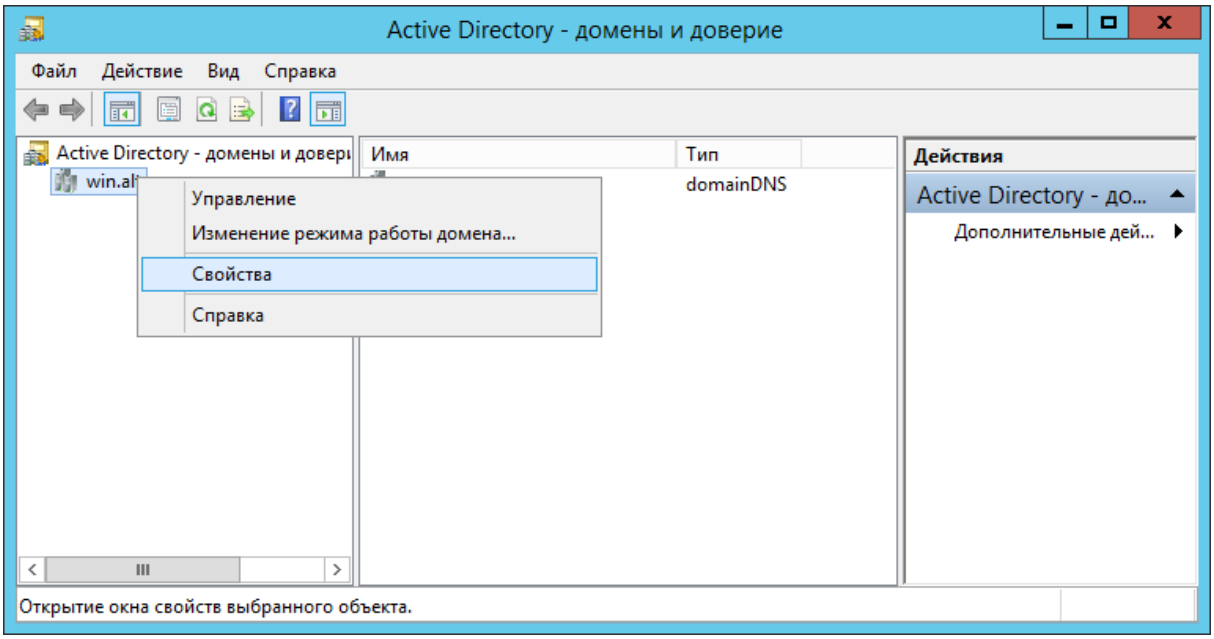
37.2. На стороне Windows Server с AD

Удаление доверия:

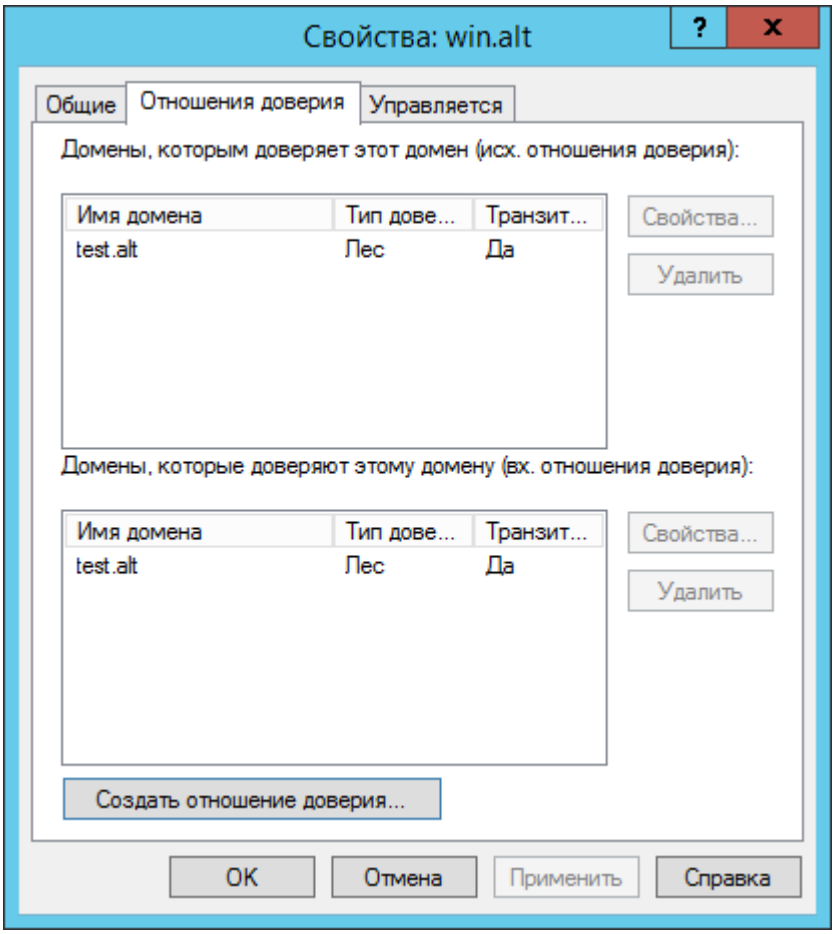
1. Открыть **Диспетчер серверов**, выбрать **Средства** → **Active Directory — Домены и Доверие**:



2. В открывшемся окне в контекстном меню домена выбрать пункт **Свойства**:

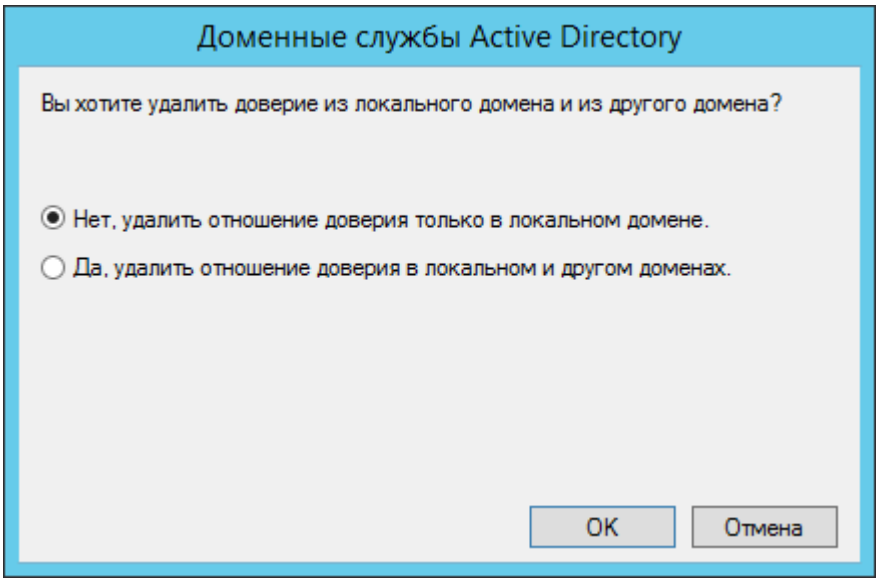


Откроется окно свойств домена. Необходимо перейти во вкладку **`Отношения доверия`** и нажать кнопку **`Создать отношение доверия…`**:



3. В группе **Домены, которым доверяет этот домен (исх. отношения доверия)** или группе **Домены, которые доверяют этому домену (вх. отношения доверия)** выбрать доверие, которое требуется удалить, а затем нажать кнопку **Удалить**.

4. В открывшемся окне выбрать где нужно удалить доверие и нажать кнопку **OK**.



При выборе параметра **Нет, удалить отношение доверия только в локальном домене**, рекомендуется повторить эту процедуру для домена второй стороны. При выборе параметра **Да, удалить отношение доверия в локальном и другом доменах**, необходимо будет ввести учетную запись и пароль администратора для домена второй стороны.

Часть VII. Администрирование домена

Содержание

38. Управление пользователями и группами

39. Администрирование DNS

40. Администрирование сайтов и подсетей

41. Управление парольными политиками

42. Резервное копирование и восстановление домена

43. Роли FSMO

44. Настройка Samba для привязки к определённым интерфейсам

45. Создание keytab-файла

46. Настройка DHCP-сервера для обновления DNS-записей

47. Настройка LDAP через SSL (LDAPS)

48. Аутентификация других сервисов в домене

49. Распределенная файловая система (DFS)

50. Настройка SSSD

51. Samba в режиме файлового сервера

52. Монтирование общих ресурсов samba

53. Журналирование в Samba

54. Усиление безопасности DC

55. Планирование и настройка диапазонов идентификаторов UID и GID (Winbind/IDMapping)

56. Инструменты командной строки

57. Конфигурационные файлы

Глава 38. Управление пользователями и группами

38.1. В ADMC

38.2. С помощью утилиты samba-tool

38.1. В ADMC

Для управления пользователями и группами в Альт Домен можно использовать модуль удалённого управления базой данных конфигурации (ADMC). Подробнее см. Модуль удаленного управления базой данных конфигурации (ADMC).

38.2. С помощью утилиты samba-tool

Для управления пользователями и группами в Альт Домен можно использовать группы подкоманд **user** и **group** утилиты **samba-tool**.

Примечание

Для выполнения команды на удаленном компьютере можно использовать опцию **-H** или **--URL=** с указанием URI LDAP-сервера. Например:

```
# samba-tool user add domainuser Qwerty1 -H ldap://<DC> -Uadministrator
```

По умолчанию в качестве значения опции **-H** передается текущий узел в формате ldap://<имя узла>.

Таблица 38.1. Команды samba-tool для управления пользователями домена

Команда	Описание	Примечание
user add <имя пользователя> [<пароль>] [опции]	Создать нового пользователя	Переданное в команде значение <имя пользователя> интерпретируется как имя учетной записи SAM (значение атрибута sAMaccountName). Оно должно быть уникальным. Некоторые опции: • **--surname** — фамилия пользователя; • **--given-name** — имя пользователя; • **--initials** — инициалы; • **--must-change-at-next-login** — пользователь должен изменить пароль при первом входе в домен; • **--random-password** — сформировать пароль случайным образом; • **--smartcard-required** — требовать наличие смарт-карты при входе в интерактивном режиме; • **--use-username-as-cn** — включить принудительное использование имени пользователя в качестве общего имени (CN); • **--userou** — имя (DN) альтернативного расположения (без domainDN), в котором будет создан пользователь (вместо используемого по умолчанию CN=Users); • **--company** — компания пользователя;

Команда	Описание	Примечание
		--department — подразделение, к которому относится пользователь; **--description** — информация о пользователе; **--mail-address** — адрес электронной почты пользователя; **--rfc2307-from-nss** — включить копирования атрибутов пользователя Unix из диспетчера службы имен (NSS); значение параметра переопределяется в случае явного задания числового идентификатора пользователя (UID), числового идентификатора основной группы пользователя (GID), информации о пользователе (GECOS) или интерпретатора команд, который должен запускаться при входе пользователя в систему (shell); **--nis-domain** — домен службы сетевой информации (NIS) для пользователя (Unix/RFC 2307); **--unix-home** — домашний каталог пользователя (Unix/RFC 2307); **--uid** — имя пользователя (Unix/RFC 2307); **--uid-number** — уникальный числовой идентификатор пользователя (Unix/RFC 2307); **--gid-number** — числовой идентификатор основной группы пользователя (Unix/RFC 2307); **--gecos** — информация о пользователе в поле GECOS (Unix/RFC 2307); **--login-shell** — оболочка (shell), которая должна запускаться при входе в систему пользователя (Unix/RFC 2307)
user create <имя пользователя> [<пароль>] [опции]	Создать нового пользователя	Команда доступна только в целях совместимости. Вместо этой команды рекомендуется использовать команду **samba-tool user add**
user delete <имя пользователя> [опции]	Удалить существующего пользователя	При удалении учетной записи также удаляются все связанные с нею разрешения, права и членства в группах
user disable (<имя пользователя>| --filter <фильтр>) [опции]	Отключить пользовательский аккаунт	Параметры вызова: **--filter** — LDAP-фильтр для поиска объектов в домене
user edit <имя пользователя> [опции]		В опции **--editor=<редактор>** можно указать редактор (по умолчанию *vi*)

Команда	Описание	Примечание
	Редактировать объект пользовательского аккаунта	
user enable (<имя пользователя>| --filter <фильтр>) [опции]	Включить пользовательский аккаунт	Параметры вызова: - **--filter** — LDAP-фильтр для поиска объектов в домене.
user list [опции]	Вывести список пользователей	По умолчанию выводятся sAMAccountNames пользователей. Можно использовать следующие опции: - **--full-dn** — показать различающиеся имена пользователей (CN) вместо sAMAccountNames; - **-b BASE_DN|--base-dn=BASE_DN** — вывести пользователей с указанным базовым DN; - **--hide-expired** — не выводить просроченные учётные записи пользователей; - **--hide-disabled** — не выводить отключенные учётные записи пользователей
user setprimarygroup <имя пользователя> <имя группы> [опции]	Установить основную группу для учётной записи пользователя	
user getgroups <имя пользователя> [опции]	Вывести список групп, в которые входит учётная запись пользователя напрямую	Можно использовать следующие опции: - **--full-dn** — показать в списке вместо имен групп SAM (sAMAccountName) их полные уникальные имена (Distinguished Name, DN)
user show <имя пользователя> [опции]	Вывести атрибуты учетной записи	В опции **--attributes=USER_ATTRS** можно указать разделённый запятыми список атрибутов, значения которых требуется отобразить. Для вывода скрытых атрибутов, их необходимо явно указать в параметре **--attributes**>
user move <имя пользователя> <контейнер> [опции]	Переместить учётную запись пользователя в указанную организационную единицу или контейнер	Имя пользователя указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN, так и без компонента domainDN

Команда	Описание	Примечание
user password [опции]	Изменить пароль текущей учетной записи (пользователя, прошедшего аутентификацию)	Если пароль не передается в открытом виде в значении параметра **--newpassword**, пользователь получит запрос на ввод пароля в командной строке
user rename <имя пользователя> [опции]	Переименовать пользователя и изменить его атрибуты	По умолчанию выводятся sAMAccountNames пользователей. Для удаления атрибута следует использовать пустое значение атрибута. Имя пользователя указывается в команде в формате sAMAccountName. Некоторые опции: - **--surname** — новая фамилия; - **--given-name** — новое имя; - **--initials** — новые инициалы; - **--force-new-cn** — новый CN (вместо использования комбинации имени, инициалов и фамилии); - **--reset-cn** — установить CN на комбинацию имени, инициалов и фамилии по умолчанию; - **--display-name** — новое отображаемое имя; - **--mail-address** — новая электронная почта; - **--samaccountname=SAMACCOUNTNAME** — новое имя для входа (sAMAccountName); - **--upn** — новое основное имя пользователя
user setexpiry (<имя пользователя>| --filter <фильтр>) [опции]	Установить срок действия для учётной записи пользователя	По истечении заданного периода учетная запись отключается; пользователь не может получать доступ к ресурсам домена. При этом сохраняются связанные с учетной записью разрешения, права и членства. Параметры вызова: - **--filter** — LDAP-фильтр для поиска объектов в домене; - **--days** — продолжительность периода в днях; - **--noexpiry** — период действия неограничен
	Установить или сбросить пароль учетной записи пользователя	Если пароль не передается в открытом виде в значении параметра **--newpassword**, пользователь получит запрос на ввод пароля в командной строке.

Команда	Описание	Примечание
user setpassword (<имя пользователя>| --filter <фильтр>) [опции]		Параметры вызова: ▸ **--filter** — LDAP-фильтр для поиска объектов в домене; ▸ **--newpassword** — новый пароль; ▸ **--must-change-at-next-login** — пользователь должен изменить пароль при первом входе в домен; ▸ **--random-password** — сформировать пароль случайным образом; ▸ **--smartcard-required** — требовать наличие смарт-карты при входе в интерактивном режиме
user unlock (<имя пользователя>| --filter <фильтр>) [опции]	Разблокировать учётную запись пользователя в домене	Параметры вызова: ▸ **--filter** — LDAP-фильтр для поиска объектов в домене
user getpassword (<имя пользователя>| --filter <фильтр>) [опции]	Получить атрибуты пароля учётной записи пользователя	Параметры вызова: ▸ **--filter** — LDAP-фильтр для поиска объектов в домене; ▸ **--attributes** — атрибуты (через запятую), которые требуется вывести или передать скрипту, заданному в параметре **--script**. В параметре могут передаваться любые атрибуты, заданные в схеме каталога, а также следующие виртуальные атрибуты: virtualClearTextUTF16, virtualClearTextUTF8, virtualCryptSHA256, virtualCryptSHA512, virtualKerberosSalt, virtualSSHA, virtualSambaGPG, virtualDigest01..29; ▸ **--decrypt-samba-gpg** — дешифровать пароль SambaGPG (должен быть установлен пакет *python3-module-gpg*)
user syncpasswords [--cache-ldb-initialize] [опции]	Синхронизировать пароли всех учётных записей пользователей с помощью дополнительного сценария	Эта команда должна выполняться только на одном контроллере домена (обычно на PDC). В первый раз команда должна выполняться с параметром, обеспечивающим инициализацию кеша: **--cache-ldb-initialize**. Для корректной инициализации кеша требуется передать список атрибутов в параметре **--attributes**

Примечание

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool user add --help
```

Примеры:

- создать пользователя ivanov в подразделении KDE, пользователь должен изменить пароль при следующем входе в систему:

```
# samba-tool user add ivanov --given-name='Иван' \
--surname='Иванов' --mail-address='ivanov@test.alt' \
--userou='OU=KDE' --must-change-at-next-login

New Password:
Retype Password:
User 'ivanov' added successfully
```

- создать пользователя kim со случайным паролем, с указанием удаленного LDAP-сервера, пользователь должен изменить пароль при следующем входе в систему:

```
# samba-tool user add kim --given-name='Виталий' \
--surname='Ким' --mail-address='kim@test.alt' \
--must-change-at-next-login  --random-password \
-H ldap://dc2.test.alt -U administrator

Password for [TEST\administrator]:
User 'kim' added successfully
```

- установить, что срок действия пароля пользователя ivanov никогда не истекает:

```
# samba-tool user setexpiry ivanov --noexpiry

Expiry for user 'ivanov' disabled.
```

- задать 20-дневный период действия (начиная с текущей даты) для учетной записи kim:

```
# samba-tool user setexpiry kim --days=20

Expiry for user 'kim' set to 20 days.
```

- просмотреть список учётных записей пользователей:

```
# samba-tool user list
Guest
ivanov
Administrator
krbtgt
kim
```

- отключить пользователя ivanov:

```
# samba-tool user disable ivanov
```

- включить всех пользователей, почтовый ящик которых начинается на k:

```
# samba-tool user enable --filter=mail=k*
Enabled user 'mail=k*'
```

- изменить пароль пользователя ivanov:

```
# samba-tool user setpassword ivanov

New Password:
Retype Password:
Changed password OK
```

- переместить пользователя kim в подразделение KDE:

```
# samba-tool user move kim 'OU=KDE'

Moved user "kim" into "OU=KDE,DC=test,DC=alt"
```

- получить информацию о пароле пользователя ivanov:

```
# samba-tool user getpassword ivanov \
--attributes=pwdLastSet,virtualClearTextUTF8

dn: CN=Иван Иванов,OU=TEST,DC=test,DC=alt
pwdLastSet: 133628348830281440

Got password OK
```

- удалить пользователя ivanov:

```
# samba-tool user delete ivanov

Deleted user ivanov
```

Предупреждение

Не следует допускать одинаковых имён для пользователя и компьютера, это может привести к коллизиям (например, такого пользователя нельзя добавить в группу). Если компьютер с таким именем заведён, удалить его можно командой: **`pdbedit -x -m имя`**

Примечание

При удалении учетной записи также удаляются все связанные с нею разрешения, права и членства в группах. Если в последствии в домен будет добавлена учетная запись с тем же именем, она не получит разрешения права или членства удаленной записи, так как ей будет присвоен новый идентификатор безопасности (SID).

Учетная запись может быть отключена, например, по следующим причинам:

- достигнуто максимальное количество попыток входа, установленное для учетной записи политикой;
- учетная запись отключена администратором;
- истек период действия учетной записи.

Команда включения учетной записи может использоваться администратором как для восстановления доступа отключенной ранее учетной записи к ресурсам домена, так и для включения группы учетных записей, созданных с разрешениями по умолчанию.

Таблица 38.2. Команды samba-tool для управления группами

Команда	Описание	Примечание
group add <имя группы> [опции]	Создать новую группу	Переданное в команде значение <имя группы> интерпретируется как имя учетной записи SAM (значение атрибута sAMaccountName). Оно должно быть уникальным. Некоторые опции: - **`--groupou`** — имя (DN) альтернативного расположения (без domainDN), в котором будет создана группа (вместо используемого по умолчанию CN=Users); - **`--group-scope`** — область действия, возможные значения: Domain, Global, Universal; - **`--group-type`** — тип группы, возможные значения: Security, Distribution; - **`--description`** — описание группы; - **`--mail-address`** — адрес электронной почты группы; - **`--notes`** — дополнительная информация; - **`--gid-number`** — числовой идентификатор группы Unix/RFC 2307; - **`--nis-domain`** — домен службы сетевой информации (NIS); - **`--special`** — используется для создания группы безопасности с именем Protected Users
group create <имя группы> [опции]	Создать новую группу	Доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду **`samba-tool group add`**
group addmembers <имя группы> (<список участников>|--member-dn=<member-dn>) [опции]	Добавить участников в группу	Команда позволяет добавить в группу одного или нескольких участников (указанных через запятую). В качестве участника группы может выступать учетная запись пользователя, учетная запись компьютера или другая группа, существующая в домене.

Команда	Описание	Примечание
		Некоторые опции: - **--member-dn** — уникальное составное имя (DN) добавляемого в группу нового участника (значение опции **--object-types** игнорируется); - **--object-types** — список типов объектов (через запятую); указанные типы используются в качестве фильтра при выполнении поиска для указанных в команде участников; возможные значения: user, group, computer, serviceaccount, contact, all; значение по умолчанию — user,group,computer; - **--member-base** — базовое уникальное имя (DN) для поиска участников группы; значение по умолчанию — уникальное имя (DN) домена
group delete <имя группы> [опции]	Удалить группу	Операция удаления является необратимой. При удалении группы также удаляются все связанные с нею разрешения и права, а также унаследованные от нее разрешения и права участников.
group edit <имя группы> [опции]	Редактировать объект группы	В опции **--editor=<редактор>** можно указать редактор (по умолчанию *vi*)
group addunixattrs <имя группы> <gidnumber> [опции]	Добавить атрибуты Unix/RFC 2307 для группы	Для использования этих атрибутов для сопоставления UID/GID в конфигурации (**smb.conf**) должен быть задан параметр **idmap_ldp:use rfc2307 = Yes**
group list [опции]	Вывести список групп	По умолчанию выводится список имен учетных записей SAM (sAMAccountName). Можно использовать следующие опции: - **--full-dn** — выводить уникальные имена (DN) вместо sAMAccountNames; - **b BASE_DN|--base-dn=BASE_DN** — выводить в списке только группы с указанным базовым уникальным именем (DN)
group listmembers <имя группы> [опции]	Вывести список участников данной группы	По умолчанию выводятся sAMAccountNames участников. Если sAMAccountName недоступен, будет использоваться CN.

Команда	Описание	Примечание
		Можно использовать следующие опции: - **`--full-dn`** — показать различающиеся имена участников (CN) вместо sAMAccountNames; - **`--hide-expired`** — не выводить членов группы с истекшим сроком действия; - **`--hide-disabled`** — не выводить отключённых членов группы
group move <имя группы> <контейнер> [опции]	Переместить группу в указанную организационную единицу или контейнер	Имя группы указывается в команде в формате sAMAccountName. Имя организационной единицы или контейнера можно указать как полное DN или без компонента domainDN
group removemembers <имя группы> (<список участников>|--member-dn=<member-dn>) [опции]	Удалить участников из группы	Команда позволяет удалить из группы одного или нескольких участников (указанных через запятую). При удалении из группы участник теряет все унаследованные от нее разрешения и права. Некоторые опции: - **`--member-dn`** — уникальное составное имя (DN) удаляемого из группы участника (значение опции **`--object-types`** игнорируется); - **`--object-types`** — список типов объектов (через запятую); указанные типы используются в качестве фильтра при выполнении поиска для указанных в команде участников; возможные значения: user, group, computer, serviceaccount, contact, all; значение по умолчанию — user,group,computer; - **`--member-base`** — базовое уникальное имя (DN) для поиска участников группы; значение по умолчанию — уникальное имя (DN) домена
group show <имя группы> [опции]	Вывести группу и её атрибуты	В опции **`--attributes=USER_ATTRS`** можно указать список атрибутов (через запятую)
group stats [опции]	Показать статистику для общих групп и членства в группах	В результате выполнения команды выводятся следующие сведения: - общее количество групп; - общее количество участников (без учета вложенности); - среднее количество участников в группе;

Команда	Описание	Примечание
		▸максимальное количество участников в группе; ▸медианное количество участников в группе; ▸распределение участников по группам с точки зрения количественного состава
group rename <имя группы> [опции]	Переименовать группу и изменить её атрибуты	Для удаления атрибута следует использовать пустое значение атрибута. Имя группы указывается в команде в формате sAMAccountName. Можно использовать следующие опции: ▸**--force-new-cn=NEW_CN** — новый CN (вместо использования sAMAccountName); ▸**--reset-cn** — установить CN равным sAMAccountName; ▸**--mail-address=MAIL_ADDRESS** — новая электронная почта; ▸**--samaccountname=SAMACCOUNTNAME** — новое имя для входа (sAMAccountName)

Примечание

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool group add --help
```

В группу могут входить учетные записи пользователей и компьютеров, а также другие группы. Такое объединение объектов в рамках одной сущности упрощает работу с ними, включая выполнение задач по управлению безопасностью и системному администрированию.

Группы также могут использоваться для создания списков рассылки (группы рассылки). Для этого при вызове команды создания группы должна быть передана опция **--group-type=Distribution**.

Группы располагаются в подразделениях (OU). Область действия (scope) группы определяет место группы в дереве доменов.

Примеры:

▸добавить группу безопасности:

```
# samba-tool group add office --description='Simple group'
Added group office
```

▸добавить новую группу рассылки с указанием удалённого LDAP-сервера:

```
# samba-tool group add manager --group-type=Distribution \
 -H ldap://dc2.test.alt -U administrator

Added group manager
```

- добавить новую группу в соответствии с RFC 2307 в домен NIS samdom с GID 12345:

```
# samba-tool group add mygroup --nis-domain=samdom --gid-number=12345
Added group mygroup
```

- удалить группу:

```
# samba-tool group delete office
Deleted group office
```

- добавить пользователя ivanov в группу «Domain Users»:

```
# samba-tool group addmembers "Domain Users" ivanov
```

- добавить в группу mygroup пользователей kim, ivanov и группу manager:

```
# samba-tool group addmembers mygroup manager,kim,ivanov
```

- удалить пользователя ivanov из группы «Domain Users»:

```
# samba-tool group removemembers "Domain Users" ivanov
```

- переместить группу manager в подразделение OU:

```
# samba-tool group move manager 'OU=OU'
Moved group "manager" into "OU=OU,DC=test,DC=alt"
```

- вывести список пользователей группы «Domain Users»:

```
# samba-tool group listmembers "Domain Users"
```

- получить определённые атрибуты группы manager:

```
# samba-tool group show manager --attributes=member,objectGUID
dn: CN=test2,CN=Users,DC=test,DC=alt
objectGUID: 2f708ea2-f42c-4344-af22-bc243301c777
member: CN=Иван Иванов,OU=KDE,DC=test,DC=alt
```

- получить общую информацию о группах и их участниках:

```
# samba-tool group stats

Group membership statistics*
--------------------------------------------------
Total groups: 48
Total memberships: 32
Average members per group: 0.67
Max members: 8 (Denied RODC Password Replication Group)
Median members per group: 0.0
```

```
Members        Number of Groups
-----------------------------------------------
          0-1  42
          2-4  5
          5-9  1

* Note this does not include nested group membership
```

В Альт Домен поддерживается работа с группой безопасности «Protected Users» («Защищенные пользователи»). В данную группу должны включаться только учетные записи пользователей. После добавления в группу в отношении учетной записи начинают действовать следующие ограничения:

- недоступна аутентификация по протоколу NTLM;
- пользователю не выдаются и от пользователя не принимаются билеты Kerberos с использованием алгоритма шифрования RC4 (используется алгоритм AES);
- максимальный период действия билета — 4 часа;
- недоступно неограниченное и ограниченное делегирование Kerberos.

Примечание

Группа «Защищенные пользователи» доступна только при функциональном уровне домена Windows Server 2012 R2.

Для создания группы безопасности «Защищенные пользователи» следует создать группу «Protected Users» с указанием опции **`--special`**:

```
# samba-tool group add 'Protected Users' --special
```

Глава 39. Администрирование DNS

39.1. DNS-записи при вводе машины в домен

39.2. Утилита samba-tool

39.3. Утилита nsupdate

39.4. Оснастка DNS в RSAT

39.5. Динамическое обновление DNS-записей

39.6. Обновление IP-адресов вручную

39.7. Известные проблемы

Для связывания доменных имен с IP-адресами используются A-записи (для IPv4) и AAAA-записи (для IPv6), которые создаются при настройке DNS и содержат соответствующий IP-адрес узла. PTR-записи применяются для обратного разрешения, связывая IP-адреса с доменными именами в обеих версиях протокола, и создаются в зоне обратного DNS.

В процессе эксплуатации IP-адреса узла могут меняться (из-за перезагрузки устройства, изменений в конфигурации сети или обновления через DHCP). В таких случаях необходимо обновить соответствующие DNS-записи, чтобы сохранить корректное разрешение имен и обеспечить работу служб аутентификации, таких как Kerberos или LDAP, для успешной проверки подлинности пользователей. Это обновление может выполняться автоматически как со стороны DHCP-сервера, так и со стороны клиента домена. DHCP-сервер может обновлять записи в DNS при изменении IP-адресов, в то время как клиент домена может обновлять записи через такие службы, как Winbind и SSSD, а также через встроенные функции операционных систем (на Windows-клиенте). Возможно также ручное обновление записей администраторами.

39.1. DNS-записи при вводе машины в домен

При вводе машины в домен в DNS-записи на DNS-сервере прописывается текущий IP-адрес машины.

Например, если машина с именем work.test.alt вводится в домен и имеет IP-адрес 192.168.0.55 (независимо от того, получен ли он статически или через DHCP), то на DNS-сервере будет создана (или обновлена) запись:

```
work.test.alt. IN A 192.168.0.55
```

Эта запись будет храниться в DNS-зоне прямого просмотра домена и использоваться для разрешения имени work.test.alt в IP-адрес 192.168.0.55.

PTR DNS-запись автоматически не создается, даже если существует обратная зона в базе данных AD. Для её создания необходимо на клиенте включить необходимые настройки для обновления PTR DNS-записей (то есть в дальнейшем вместо обновления запись будет зарегистрирована). В противном случае запись нужно будет создать вручную:

```
$ samba-tool dns add dc1.test.alt 0.168.192.in-addr.arpa 55 PTR work.test.alt -U
administrator
Password for [TEST\administrator]:
Record added successfully
```

При этом будет создана DNS-запись:

```
55.0.168.192.in-addr.arpa. 3600 IN PTR work.test.alt.
```

Проверить наличие записи можно, выполнив команду:

```
$ host -t PTR 192.168.0.55 dc1.test.alt
Using domain server:
Name: dc1.test.alt
Address: 192.168.0.132#53
Aliases:

55.0.168.192.in-addr.arpa domain name pointer work.test.alt.
```

Примечание

Обратная зона создается так:

```
$ samba-tool dns zonecreate dc1.test.alt 0.168.192.in-addr.arpa -U
administrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

39.2. Утилита samba-tool

Для администрирования службы доменных имен (DNS) в Альт Домен можно использовать подкоманду dns утилиты **samba-tool**.

39.2.1. Работа с DNS-записями

Таблица 39.1. Команды управления DNS-записями samba-tool

Команда	Описание	Примечание
dns add <сервер> <зона> <имя> <A|AAAA|PTR|CNAME|NS|MX|SRV|TXT> <данные>	Добавить новую запись	Параметры вызова: - сервер — IP-адрес или доменное имя DNS-сервера; - зона — зона DNS; - имя — имя DNS-записи; - тип добавляемой записи с данными
dns delete <сервер> <зона> <имя> <A|AAAA|PTR|CNAME|NS|MX|SRV|TXT> <данные>	Удалить DNS-запись	
dns edit <сервер> <зона> <имя> <A|AAAA|PTR|CNAME|NS|MX|SOA|SRV|TXT> <текущие данные> <новые данные>	Изменить DNS-запись	Дополнительно для изменения доступен тип записи SOA (Start of Authority), являющейся начальной записью зоны, со следующими данными (порядок пунктов в списке ниже соответствует порядку следования параметров в строке): - nameserver — доменное имя DNS-сервера, на котором хранятся другие DNS-записи; - email — адрес электронной почты администратора зоны (вместо @ указывается точка, например для адреса user@test.alt указывается значение user.test.alt); - serial — серийный номер файла зоны, представляющий собой номер версии записи SOA; увеличивается при каждом изменении значения записи и служит сигналом другим DNS-серверам о том, что требуется обновить данные; - refresh — интервал для запроса изменений;

Команда	Описание	Примечание
		▸retry — интервал для повторных попыток запроса данных в случае неудачи; ▸expire — время, в течение которого обновленные данные могут быть применены на других DNS-серверах; ▸minimum-ttl — время хранения в кеше информации о зоне
dns cleanup <сервер> <имя узла> [опции]	Очистить DNS-записи указанного DNS-узла	Во многих случаях данная подкоманда только устанавливает значение true в атрибуте dNSTombstoned DNS-записей. После этого при запросе таких записей информация о них возвращаться не будет, но в базе данных могут оставаться соответствующие им записи-заполнители
dns query <сервер> <зона> <имя> <A|AAAA|PTR|CNAME|NS|MX|SOA|SRV|TXT|ALL> [опции]	Вывести информацию о DNS-записях	Можно использовать следующие опции: ▸**--authority** — поиск по записям полномочного DNS-сервера (значение по умолчанию); ▸**--cache** — поиск по записям в кеше; ▸**--glue** — поиск по связующим (glue) записям; ▸**--root** — поиск по корневым ссылкам DNS-сервера; ▸**--additional** — вывод списка дополнительных записей; ▸**--no-children** — исключение вывода дочерних записей; ▸**--only-children** — вывод только дочерних записей

Возможные типы записей и данные:

- A <IPv4-адрес> — IPv4-адрес для связи с именем домена;
- AAAA <IPv6-адрес> — IPv6-адрес для связи с именем домена;
- PTR <FQDN> — полное доменное имя (FQDN) для связи с IP-адресом домена;
- CNAME <FQDN> — полное доменное имя (FQDN) для создания псевдонима;
- NS <FQDN> — полное доменное имя (FQDN) сервера, выполняющего роль сервера имен;
- MX <FQDN> <приоритет> — полное доменное имя (FQDN) и приоритет почтового сервера;
- SRV <FQDN> <порт> <приоритет> <вес> — полное доменное имя (FQDN) сервера, на котором доступна определенная служба, порт для доступа к службе, приоритет и относительный вес на случай, если существует несколько записей с одинаковым приоритетом;
- TXT "'string1' 'string2' …" — информация о домене в текстовом формате (string).

Примечание

Полный список параметров каждой команды можно увидеть в справке, например:

```
$ samba-tool dns add --help
```

Примечание

При использовании команды **samba-tool dns** указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примеры:

- добавить запись типа A:

```
$ samba-tool dns add 192.168.0.132 test.alt \
DC2 A 192.168.0.133 -Uadministrator

Password for [TEST\administrator]:
Record added successfully
```

- добавить запись типа PTR для обратной зоны 192.168.0.0/24:

```
$ samba-tool dns add dc1.test.alt 0.168.192.in-addr.arpa \
55 PTR demo.test.alt -U administrator

Password for [TEST\administrator]:
Record added successfully
```

- удалить запись типа A:

```
$ samba-tool dns delete dc1.test.alt test.alt \
DC2 A 192.168.0.133 -U administrator

Password for [TEST\administrator]:
Record deleted successfully
```

- изменить запись типа A:

```
$ samba-tool dns update dc1.test.alt test.alt DC2 \
A 192.168.0.133 192.168.0.149 -U administrator

Password for [TEST\administrator]:
Record updated succefully
```

- изменить адрес электронной почты администратора в записи типа SOA:

```
$ samba-tool dns update dc1.test.alt test.alt @ SOA \
"dc1.test.alt admin.test.alt 63 900 600 86400 3600" \
"dc1.test.alt new.test.alt 64 900 600 86400 3600" \
-U administrator

Password for [TEST\administrator]:
Record updated succefully
```

- вывести все DNS-записи для указанной зоны:

```
$ samba-tool dns query dc1.test.alt 0.168.192.in-addr.arpa \
@ ALL -U administrator
```

39.2.2. Работа с DNS-зонами

Таблица 39.2. Команды samba-tool для управления зонами DNS

Команда	Описание	Примечание
dns zonecreate <сервер> <зона> [опции]	Создать зону DNS	Дополнительно с помощью параметра **--client-version** можно указать версию DNS-клиента. Возможные значения: w2k, dotnet, longhorn (по умолчанию)
dns zonedelete <сервер> <зона> [опции]	Удалить зону DNS	
dns zoneinfo <сервер> <зона> [опции]	Вывести информацию о зоне DNS	
dns zonelist <сервер> [опции]	Вывести список зон DNS	Можно использовать следующие опции: - **--client-version** — версия DNS-клиента. Возможные значения: w2k, dotnet, longhorn (по умолчанию); - **--primary** — получение списка первичных зон DNS (по умолчанию); - **--secondary** — получение списка вторичных зон DNS; - **--cache** — получение списка зон DNS из кеша; - **--auto** — получение списка автоматически созданных зон DNS; - **--reverse** — получение списка обратных зон DNS; - **--ds** — получение списка зон DNS, интегрированных с доменом; - **--non-ds** — получение списка зон DNS без интеграции с доменом
dns zoneoptions <сервер> <зона> [опции]		

Команда	Описание	Примечание
	Изменить настройки очистки от устаревших записей для зоны DNS	Можно использовать следующие опции: ▸**--client-version** — версия DNS-клиента. Возможные значения: w2k, dotnet, longhorn (по умолчанию); ▸**--mark-old-records-static=YYYY-MM-DD** — записи старше указанной даты становятся статическими (их временные метки становятся нулевыми); ▸**--mark-records-static-regex=REGEXP** — записи, соответствующие заданному регулярному выражению, становятся статическими; ▸**-n|--dry-run** — запуск в тестовом режиме для проверки корректности заданных параметров; фактически изменения не вносятся; ▸**--aging** — признак необходимости очистки от устаревших записей: 0 — очистка отключена (по умолчанию), 1 — очистка включена; ▸**--norefreshinterval=[0-87600]** — интервал блокировки для зоны с включенной очисткой в часах; если параметр равен нулю, используется значение по умолчанию (168 часов, одна неделя); ▸**--refreshinterval=[0-87600]** — интервал обновления для зоны с включенной очисткой в часах; если параметр равен нулю, используется значение по умолчанию (168 часов, одна неделя)

Примечание

Полный список параметров каждой команды можно увидеть в справке, например:

```
$ samba-tool dns zoneoptions --help
```

Примечание

При использовании команды **samba-tool dns** указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Примеры:

▸создать обратную зону /24:

```
$ samba-tool dns zonecreate 192.168.0.132 \
0.168.192.in-addr.arpa -U administrator
```

- вывести информацию об обратной зоне DNS:

```
$ samba-tool dns zoneinfo dc1.test.alt \
0.168.192.in-addr.arpa -U administrator
```

- включить очистку с интервалом обновления 5 лет:

```
$ samba-tool dns zoneoptions dc1.test.alt \
test.alt --aging=1 --refreshinterval=43800 -U administrator
```

Примечание

Чтобы очистка работала, в файле **smb.conf** хотя бы на одном контроллере домена должен быть задан параметр **dns zone scavenging = yes**.

39.2.3. Получение информации о DNS-серверах

Таблица 39.3. Команды samba-tool для получения информации о DNS-серверах

Команда	Описание	Примечание
dns serverinfo <сервер> [опции]	Вывести информацию о DNS-сервере	Дополнительно с помощью параметра **--client-version** можно указать версию DNS-клиента. Возможные значения: w2k, dotnet, longhorn (по умолчанию)
dns roothints <сервер> [<имя>] [опции]	Вывести информацию о корневых серверах DNS	

Примечание

Полный список параметров каждой команды можно увидеть в справке, например:

```
$ samba-tool dns roothints --help
```

Примеры:

- вывести информацию о DNS-сервере:

```
$ samba-tool dns serverinfo dc1.test.alt -U administrator
```

- вывести информацию об обратной зоне DNS:

```
$ samba-tool dns zoneinfo dc1.test.alt \
0.168.192.in-addr.arpa -U administrator
```

Данная команда возвращает структуру DNS_RPC_SERVER_INFO, содержащую информацию о состоянии и конфигурации DNS-сервера, в формате, соответствующем версии DNS-клиента.

- вывести информацию о корневых серверах DNS:

```
$ samba-tool dns roothints dc1.test.alt -U administrator
```

39.3. Утилита nsupdate

Утилита **nsupdate** используется для отправки запросов на обновление динамического DNS серверу имен в соответствии со стандартом RFC 2136. С ее помощью можно добавлять или удалять записи ресурсов из зоны без необходимости правки зонного файла вручную. Один запрос на обновление может содержать запросы на добавление или удаление нескольких записей ресурсов.

Синтаксис команды **nsupdate**:

```
nsupdate [-dDi] [-L level] [-l][-g | -o | -y keyname:secret | -k keyfile] [-v] [-
V] [-P] [-T] [-4 | -6] [filename]
```

Таблица 39.4. Опции команды nsupdate

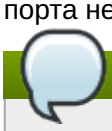
Ключ	Описание
-4	Использовать только IPv4
-6	Использовать только IPv6
-d	Включить режим отладки
-D	Включить дополнительный режим отладки
-i	Принудительно включить интерактивный режим, даже если стандартный ввод не является терминалом
-k keyfile	Позволяет указать файл, содержащий ключ аутентификации TSIG. Файлы могут быть в двух форматах: один файл, содержащий оператор ключа named.conf-format, который может быть автоматически сгенерирован ddns-confgen; или пара файлов, имена которых имеют формат K{name}.+157.+{random}.key и K{name}.+157.+{random}.private, которые могут быть сгенерированы dnssec-keygen. Параметр **-k** также может использоваться для указания ключа SIG(0), используемого для аутентификации запросов на обновление Dynamic DNS. В этом случае указанный ключ не является ключом HMAC-MD5
-l	Установить режим локального хоста. Адрес сервера будет установлен на localhost (отключая сервер, чтобы адрес сервера не мог быть переопределен). Подключения к локальному серверу используют ключ TSIG, найденный в **/var/run/named/session.key**, который автоматически генерируется named, если какая-либо локальная первичная зона установила update-policy на local. Расположение этого файла ключа можно переопределить с помощью опции **-k**
-L level	Установить уровень отладки ведения журнала. Если 0, ведение журнала отключено

Ключ	Описание
-p port	Установить порт для подключения к серверу имен. Значение по умолчанию — 53
-P	Вывести список частных типов записей ресурсов BIND, формат которых понимает nsupdate
-r udpretries	Установить количество повторных попыток UDP. Значение по умолчанию — 3. Если 0, выполняется только один запрос на обновление
-t timeout	Установить максимальное время, которое может занять запрос на обновление, прежде чем он будет прерван. Значение по умолчанию — 300 секунд. Если 0, тайм-аут отключен
-T	Вывести список стандартных типов записей ресурсов IANA, формат которых понимает nsupdate. nsupdate завершает работу после вывода списков. Параметр **-T** можно комбинировать с параметром **-P**. Другие типы можно ввести с помощью TYPEXXXXX, где XXXXX — это десятичное значение типа без начальных нулей. Rdata, если они присутствуют, анализируются с использованием формата UNKNOWN rdata (<обратная косая черта> <хеш> <пробел> <длина> <пробел> <шестнадцатеричная строка>)
-u udptimeout	Задать интервал повтора UDP. Значение по умолчанию — 3 секунды. Если равно 0, интервал вычисляется из интервала тайм-аута и количества повторов UDP
-v	Указывает, что TCP следует использовать даже для небольших запросов на обновление. По умолчанию nsupdate использует UDP для отправки запросов на обновление на сервер имен, если только они не слишком велики для того, чтобы поместиться в запрос UDP, в этом случае используется TCP. TCP может быть предпочтительнее, когда выполняется пакет запросов на обновление
-V	Вывести номер версии
-y [hmac:]keyname:secret	Задает буквальный ключ аутентификации TSIG. keyname — имя ключа, а secret — общий секрет в кодировке base64. hmac — имя алгоритма ключа; допустимые варианты: hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-sha384 или hmac-sha512. Если hmac не указан, по умолчанию используется hmac-md5 или, если MD5 отключен, hmac-sha256. **Примечание** Использование опции **-y** не рекомендуется, поскольку общий секрет предоставляется как аргумент командной строки в виде открытого текста.

nsupdate считывает входные данные из **filename** или стандартного ввода. Каждая команда предоставляется ровно в одной строке ввода. Некоторые команды предназначены для административных целей; другие — это либо инструкции по обновлению, либо проверки предварительных условий содержимого зоны. Эти проверки устанавливают условия, что некоторое имя или набор записей ресурсов (RRset) либо существует, либо отсутствует в зоне. Эти условия должны быть выполнены, чтобы весь запрос на обновление был успешным. Обновления отклоняются, если тесты на предварительные условия не пройдены.

Каждый запрос на обновление состоит из нуля или более предварительных условий и нуля или более обновлений. Это позволяет соответствующим образом аутентифицированному запросу на обновление продолжить работу, если некоторые указанные записи ресурсов либо присутствуют, либо отсутствуют в зоне. Пустая строка ввода (или команда **send**) приводит к отправке накопленных команд как одного запроса на обновление Dynamic DNS на сервер имен.

Таблица 39.5. Форматы команд и их значения

Команда	Описание
server servername port	Отправить все динамические запросы на обновление на сервер имен servername. Если не указано ни одного оператора сервера, nsupdate отправляет обновления на основной сервер правильной зоны. Поле MNAME записи SOA этой зоны определяет основной сервер для этой зоны. port — это номер порта на servername, куда отправляются динамические запросы на обновление. Если номер порта не указан, используется номер порта DNS по умолчанию 53.  **Примечание** Эта команда не действует, если используется GSS-TSIG
local address port	Отправить все динамические запросы на обновление, используя локальный адрес. Если локальный оператор не указан, **nsupdate** отправляет обновления, используя адрес и порт, выбранные системой. port также может использоваться для принудительного поступления запросов с определенного порта. Если номер порта не указан, система назначает его
zone zonename	Указывает, что все обновления должны быть сделаны в зоне zonename. Если оператор zone не указан, **nsupdate** пытается определить правильную зону для обновления на основе остальной части ввода
class classname	Указывает класс по умолчанию. Если класс не указан, класс по умолчанию — IN
ttl seconds	Указывает время жизни по умолчанию в секундах для добавляемых записей. Значение none очищает TTL по умолчанию
key hmac:keyname secret	Указывает, что все обновления должны быть подписаны TSIG с использованием пары keyname-secret. Если указан hmac, он устанавливает используемый алгоритм подписи. Значение по умолчанию — hmac-md5; если MD5 отключен, то по умолчанию используется hmac-sha256. Команда key переопределяет любой ключ, указанный в командной строке с помощью **-y** или **-k**
gsstsig	Эта команда использует GSS-TSIG для подписи обновлений. Это эквивалентно указанию **-g** в командной строке

Команда	Описание
oldgsstsig	Эта команда использует версию GSS-TSIG для Windows 2000 для подписи обновлений. Это эквивалентно указанию **-o** в командной строке
realm [realm_name]	При использовании GSS-TSIG эта команда указывает использование realm_name вместо realm по умолчанию в krb5.conf. Если realm не указан, сохраненная realm очищается
check-names [yes_or_no]	Включить или выключить обработку check-names для добавляемых записей. Check-names не влияет на предварительные условия или удаляемые записи. По умолчанию обработка check-names включена. Если обработка check-names завершается неудачей, запись не добавляется в сообщение UPDATE
prereq nxdomain domain-name	Эта команда требует, чтобы не существовало ни одной записи ресурса любого типа с именем domain-name
prereq yxdomain domain-name	Эта команда требует, чтобы существовал domain-name (как минимум одна запись ресурса любого типа)
prereq nxrrset domain-name class type	Эта команда требует, чтобы не существовало ни одной записи ресурса указанного типа, класса и domain-name. Если class не указан, предполагается IN (Интернет)
prereq yxrrset domain-name class type	Для этой команды требуется, чтобы существовала запись ресурса указанного типа, класса и доменного имени. Если class не указан, предполагается IN (Интернет)
prereq yxrrset domain-name class type data	С помощью этой команды данные из каждого набора предварительных условий этой формы, имеющих общий тип, класс и доменное имя, объединяются для формирования набора RR. Этот набор RR должен точно соответствовать набору RR, существующих в зоне с указанным типом, классом и доменным именем. Данные записываются в стандартном текстовом представлении RDATA записи ресурса
update delete domain-name ttl class type data	Удалить все записи ресурсов с именем domain-name. Если указаны type и data, удаляются только соответствующие записи ресурсов. Если class не указан, предполагается класс Internet. TTL игнорируется и допускается только для совместимости
update add domain-name ttl class type data	Добавить новую запись ресурса с указанным ttl, class и data
show	Отобразить текущее сообщение, содержащее все предварительные условия и обновления, указанные с момента последней отправки
send	Отправить текущее сообщение (эквивалентно вводу пустой строки)
answer	Отобразить ответ
debug	Включить отладку
version	Вывести номер версии
help	Вывести список команд

Примечание

Строки, начинающиеся с точки с запятой (;), являются комментариями и игнорируются.

При использовании утилиты **nsupdate** для динамического обновления DNS-записей в доменных средах AD, необходимо использовать механизм аутентификации GSS-TSIG, который использует Kerberos-билет для аутентификации машины в домене. Kerberos-билет используется при обновлении DNS-записей с помощью **nsupdate** с флагом **-g**.

Перед выполнением команды **nsupdate -g** необходимо получить Kerberos-билет для машинного аккаунта с помощью команды:

```
# kinit -k 'MACHINENAME$'
```

Примечание

Имя машинного аккаунта можно узнать, используя команду **hostname -s**. В команде **kinit** имя машинного аккаунта нужно указывать в верхнем регистре со знаком $, например:

```
# hostname -s
comp01
# kinit -k 'COMP01$'
```

В следующих примерах показано использование команды **nsupdate** для добавления и удаления записей ресурсов из зоны test.alt.

- удалить записи A для oldhost.test.alt и добавить запись A для newhost.test.alt с IP-адресом 192.168.0.195:

```
# nsupdate -g
> update delete oldhost.test.alt A
> update add newhost.test.alt 86400 A 192.168.0.195
> send
```

Новая запись будет имеет TTL 1 день (86400 секунд).

- указать предварительное условие перед обновлением DNS-сервера:

```
# nsupdate -g
> prereq nxdomain nickname.test.alt
> update add nickname.test.alt 86400 CNAME somehost.test.alt
> send
```

Предварительное условие позволяет серверу имен проверить, нет ли записей о ресурсах любого типа для nickname.test.alt. Если в зоне есть записи ресурсов, запрос на обновление не выполняется. Если этого имени не существует, добавляется CNAME.

39.4. Оснастка DNS в RSAT

Оснастка DNS в RSAT позволяет администраторам Windows удаленно управлять DNS-записями через графический интерфейс. С его помощью можно добавлять, удалять и изменять DNS-записи.

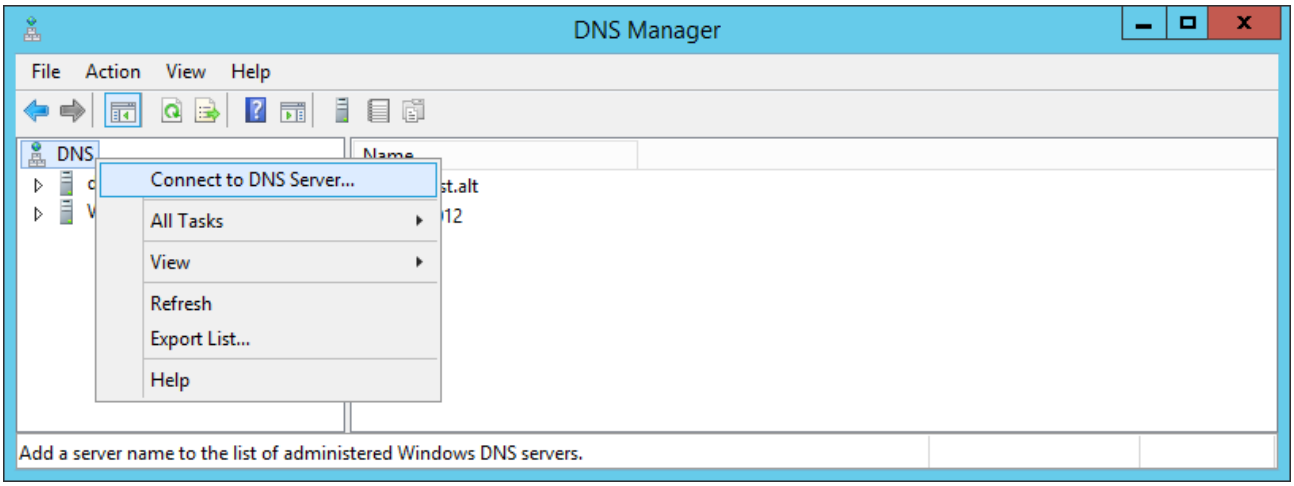
Примечание

Для возможности администрирования DNS с клиента Windows должна быть установлена оснастка DNS MMC (см. Установка административных инструментов (машина Windows)).

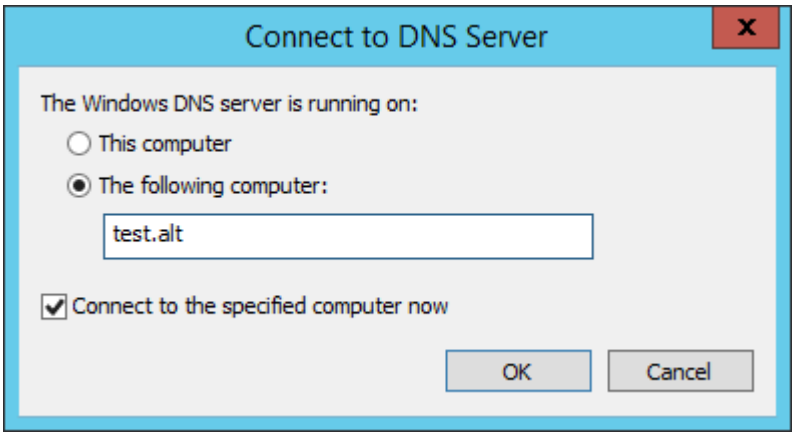
Существуют следующие известные проблемы если используется внутренний сервер DNS:

- очистка еще не реализована. Возвращается сообщение об ошибке «This function is not supported on this system»;
- условные пересылки еще не реализованы. Возвращается то же сообщение об ошибке, что и выше;
- пересылку DNS можно изменить только в **`smb.conf`**, а не через оснастку MMC;
- создание статических записей. Когда создается статическая запись, она имеет временную метку и опцию «Delete this record when it becomes stale». В Windows AD статические записи имеют «статическую» временную метку и не могут быть случайно удалены.

Для подключения к своему DNS-серверу в оснастке DNS необходимо в контекстном меню **DNS** выбрать пункт **Connect to DNS Server…**:



В открывшемся окне следует выбрать пункт **`The following computer`**, ввести в поле имя домена (также можно использовать IP-адрес или FQDN), установить отметку **`Connect to the special computer now`** и нажать кнопку **`OK`**:

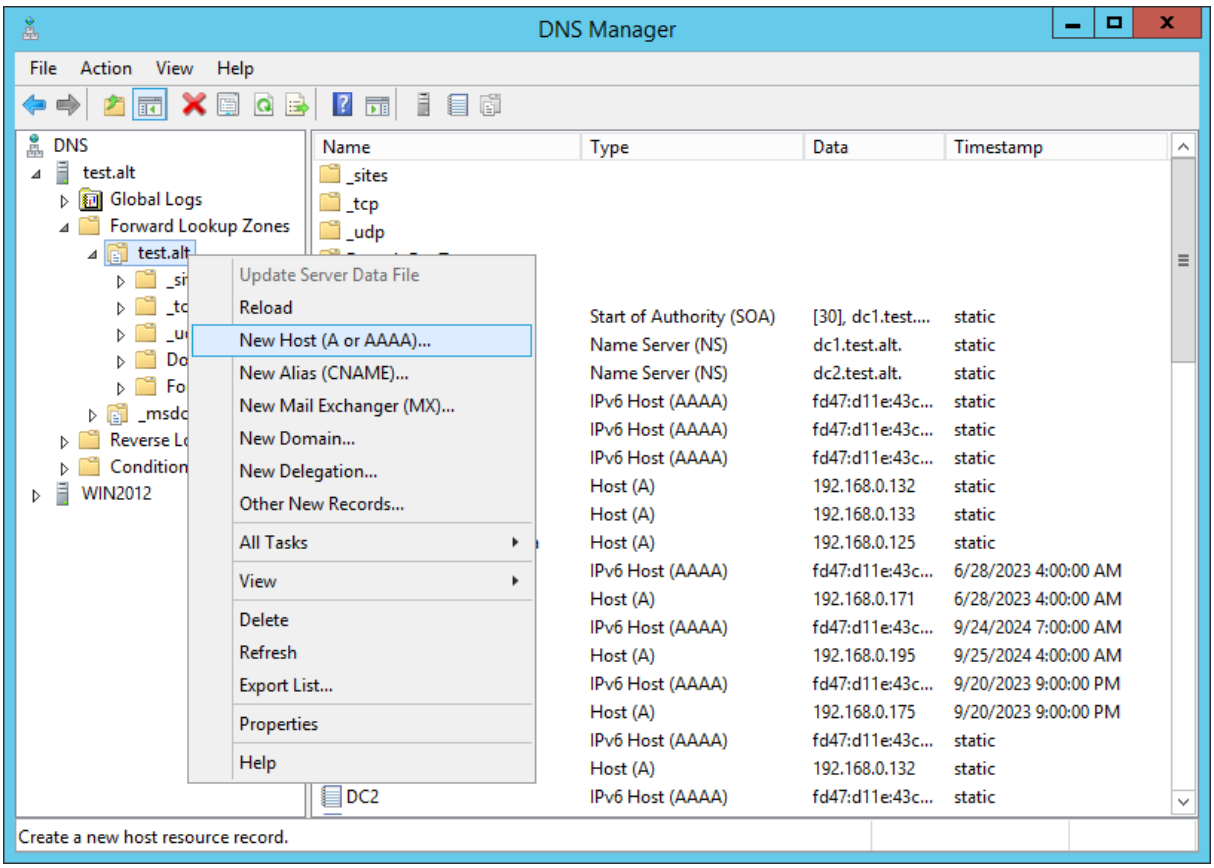


39.4.1. Работа с DNS-записями

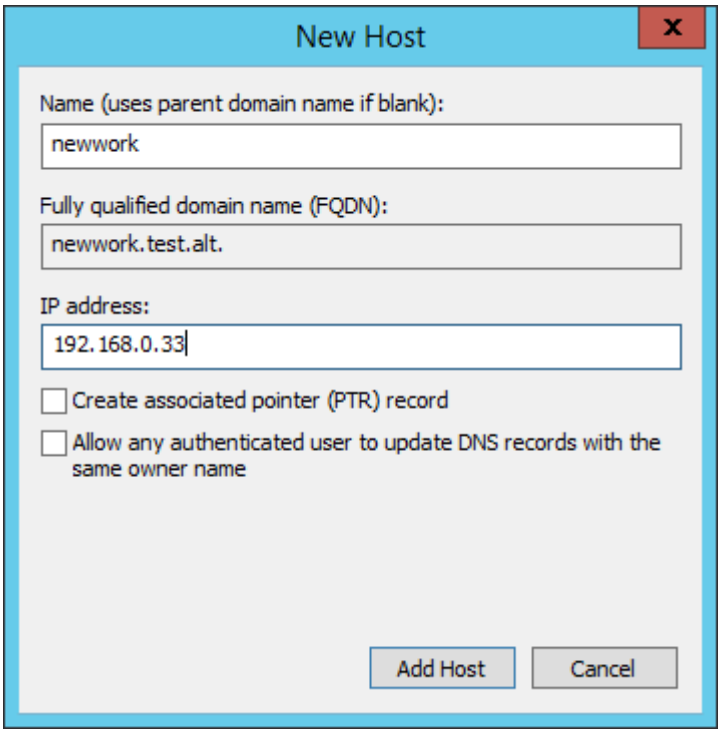
Чтобы добавить новую запись необходимо:

1. Перейти в зону, в которую нужно добавить новую запись.

2. В контекстном меню зоны выбрать тип записи:

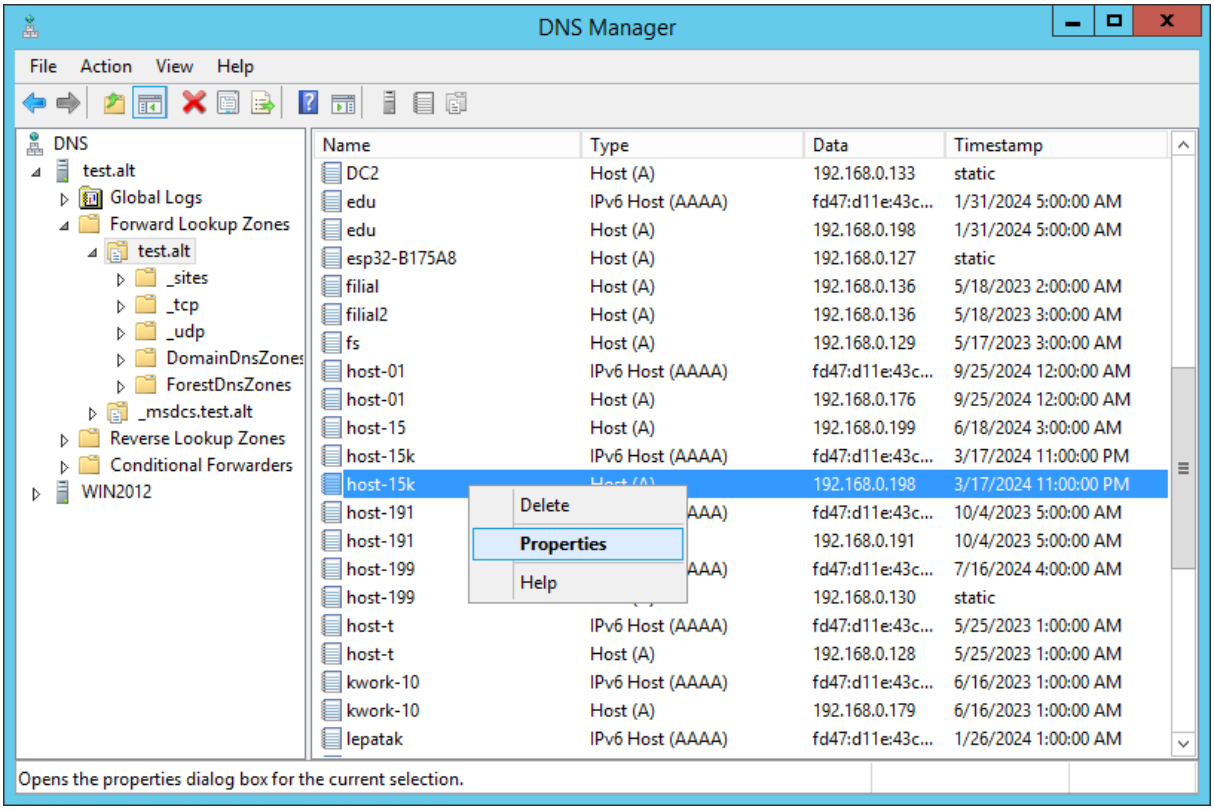


3. Заполнить поля и сохранить запись, нажав кнопку **`Add Host`**:

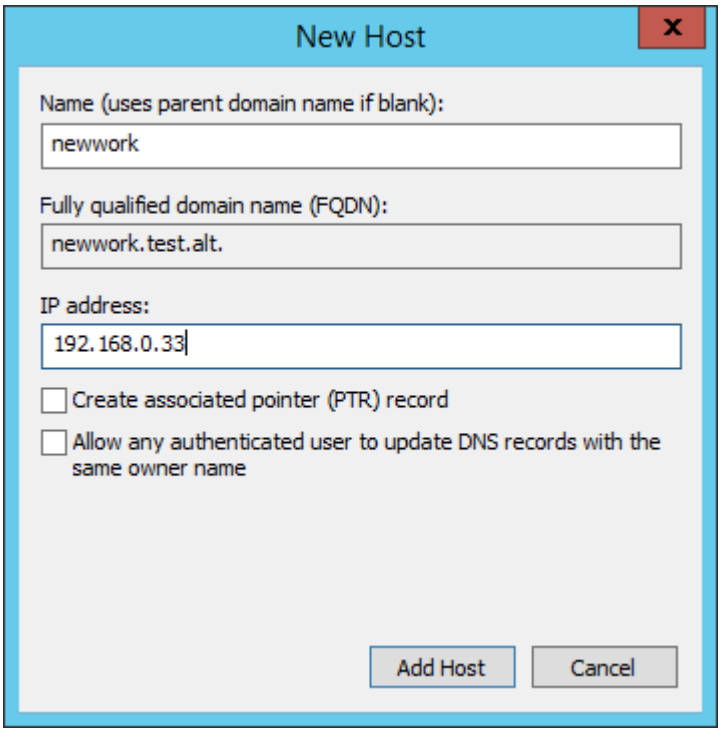


Для обновления существующей записи необходимо:

1. Перейти в зону, содержащую запись, которую нужно изменить.
2. В контекстном меню записи выбрать пункт **Properties**:



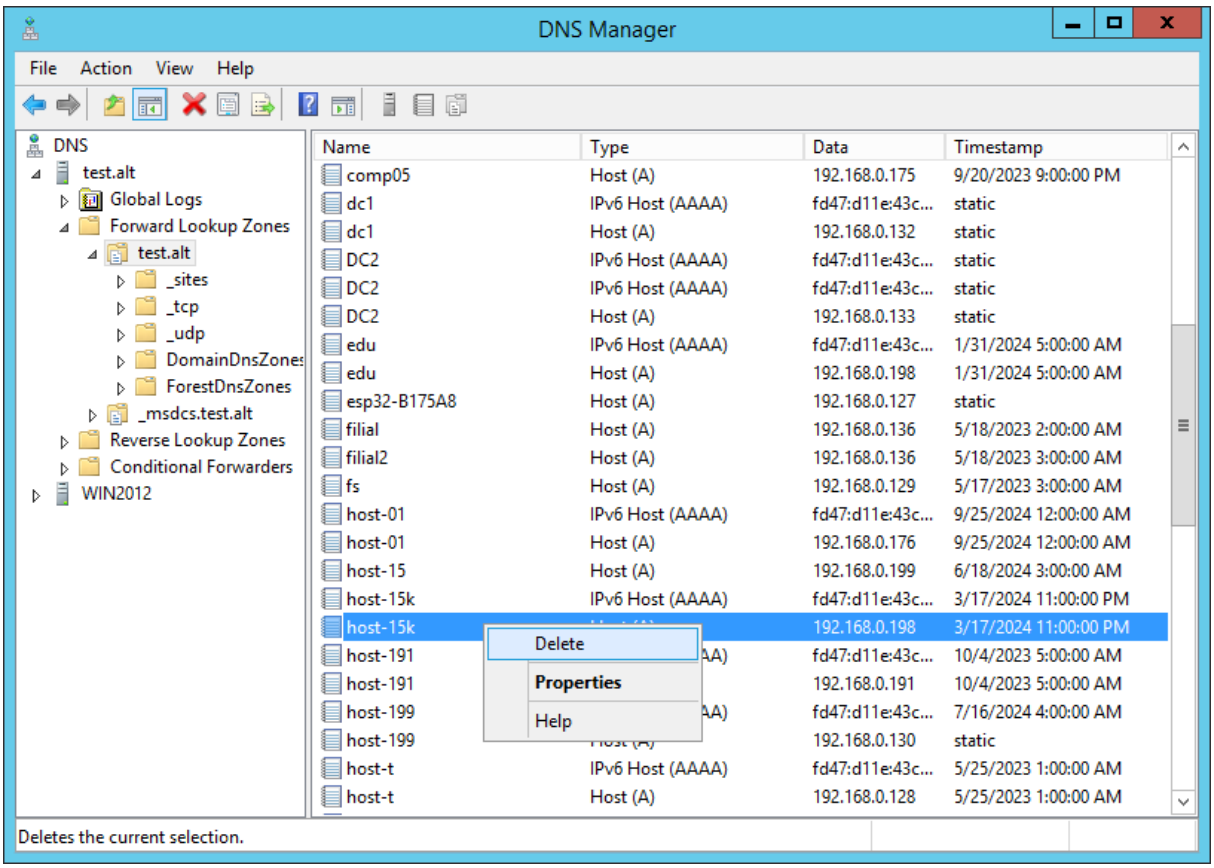
3. Отредактировать запись и сохранить изменения, нажав кнопку **`Apply`**:



Для удаления записи необходимо:

1. Перейти в зону, содержащую запись, которую нужно удалить.

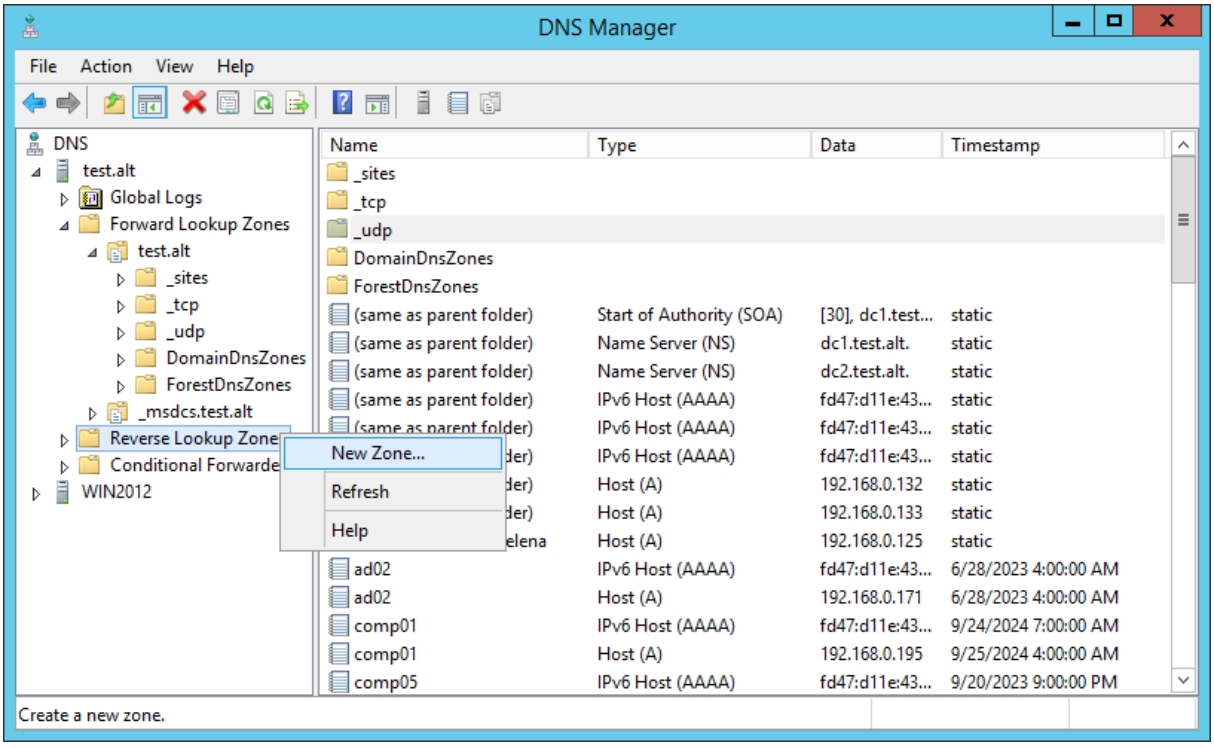
2. В контекстном меню записи выбрать пункт **Delete**:



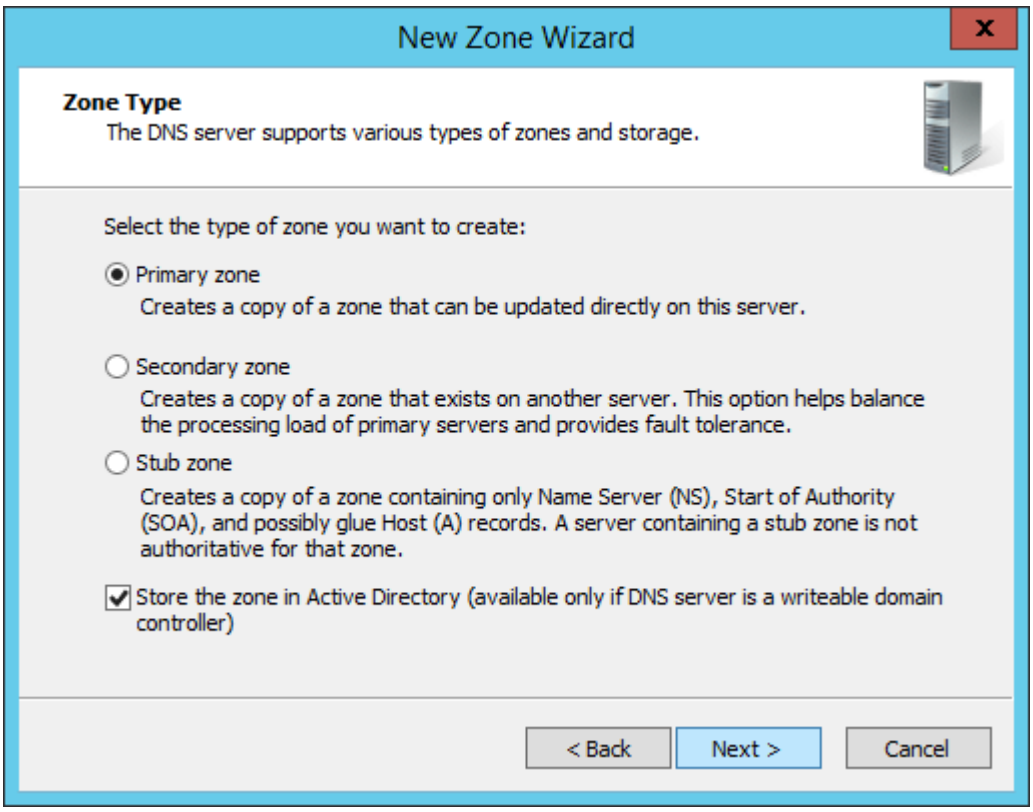
39.4.2. Работа с DNS-зонами

В качестве примера рассмотрено добавление зоны обратного просмотра:

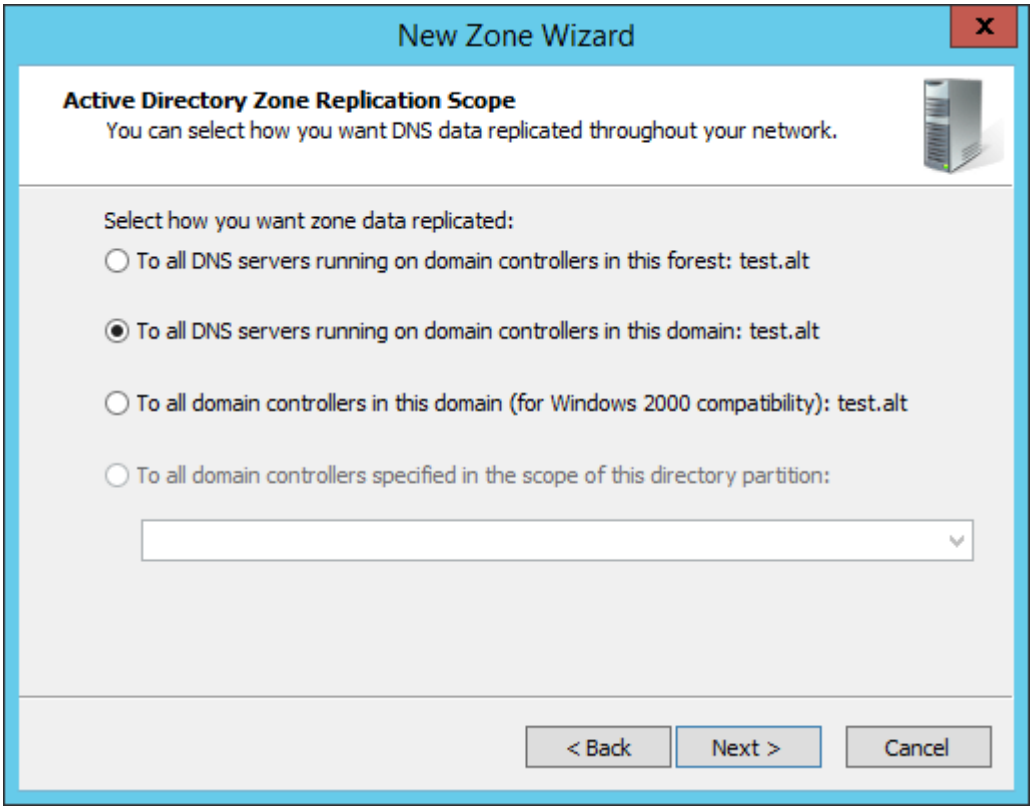
1. В контекстном меню зоны обратного просмотра (**`Reverse Lookup Zones`**) выбрать пункт **New Zone…**:



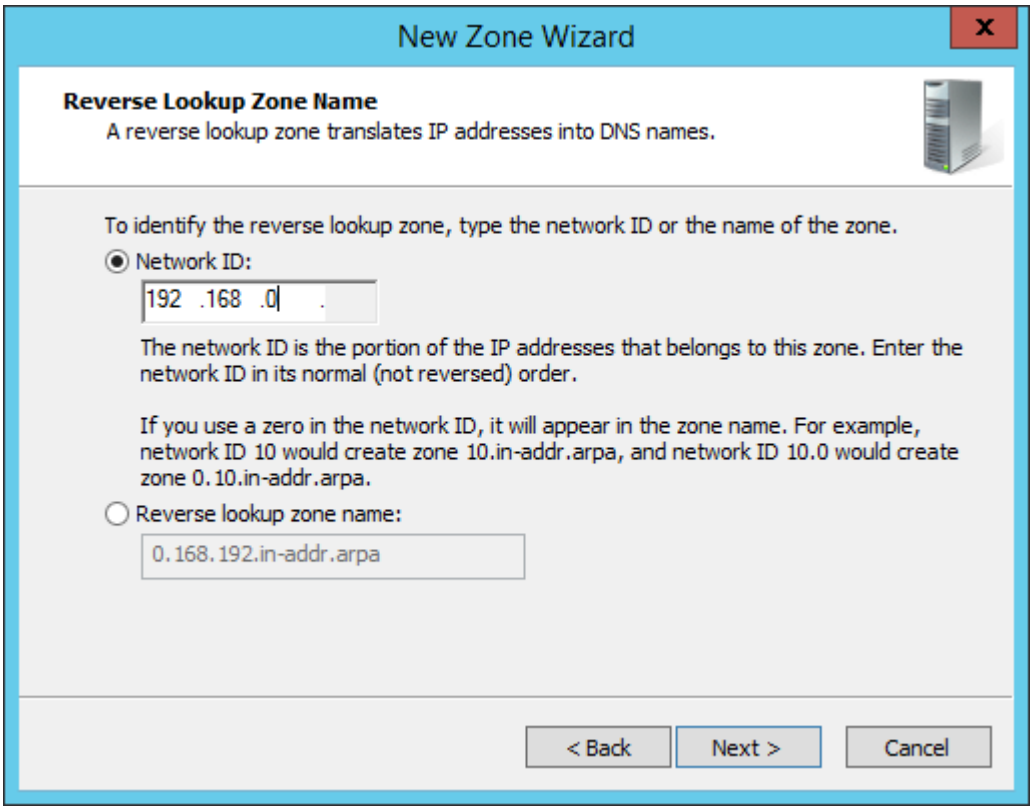
2. На втором шаге мастера создания новой зоны выбрать **`Primary zone`** и установить отметку в пункте **`Store the zone in Active Directory`**:



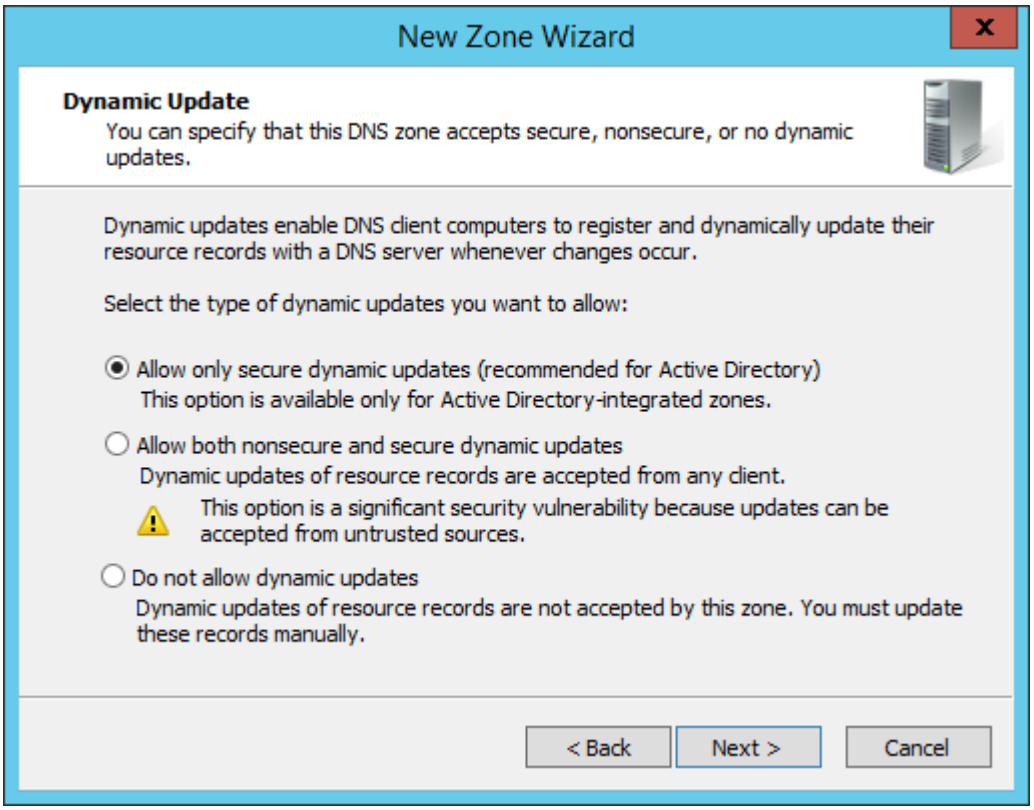
3. На следующем шаге мастера указать область репликации зоны:



4. Указать имя зоны обратного просмотра:



5. Включить динамическое обновление:

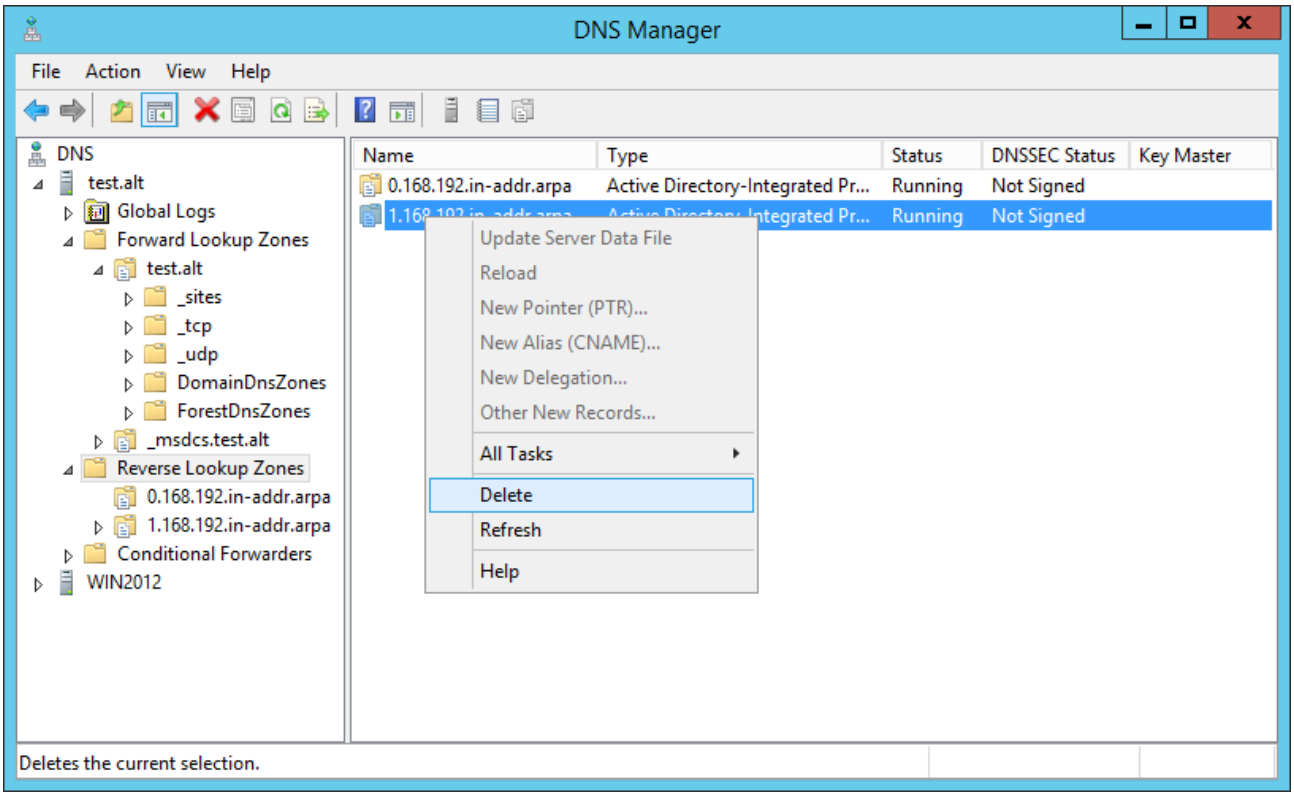


6. Завершить работу мастера.

Примечание

Новая зона будет активна сразу, без перезапуска Samba или BIND.

Для удаления зоны следует в контекстном меню зоны выбрать пункт **`Delete`**:



39.5. Динамическое обновление DNS-записей

Используются следующие механизмы обновления DNS-записей:

- *На стороне DHCP*. Динамическое обновление DNS-записей часто осуществляется с помощью DHCP-серверов. В частности, такие системы как ISC DHCP и Kea DHCP могут автоматически обновлять записи на DNS-сервере при выдаче нового IP-адреса клиенту.
- *На стороне клиента*. В доменных средах с использованием Linux-клиентов для взаимодействия с AD могут использоваться службы Winbind и SSSD для обновления DNS-записей. На Windows-клиентах обновление происходит через встроенные функции операционных систем. Кроме того, обновление записей может быть выполнено вручную администраторами.

39.5.1. На стороне клиента

39.5.1.1. SSSD

Включить обновление IP-адресов службой sssd можно несколькими способами:

- отредактировав файл **`/etc/sssd/sssd.conf`**;
- в модуле ЦУС **Аутентификация**;
- применением control;

- групповыми политиками.

39.5.1.1.1. Настройка через файл /etc/sssd/sssd.conf

В файл конфигурации службы SSSD (**/etc/sssd/sssd.conf**) в секцию с параметрами домена можно добавить опции, приведенные в табл. Параметры настройки автоматического обновления DNS. Например:

```
[domain/TEST.ALT]
.....
#Включить обновление прямых записей (A/AAAA записей)
dyndns_update = true

#Включить обновление обратных записей (PTR записей)
dyndns_update_ptr = true
#Задать интервал обновления в секундах.
#По умолчанию – 86400 (24 часа), обновление выполняется раз в сутки.
#Если интервал равен 0, то обновление выполняется только один раз при запуске
службы SSSD.
#Если интервал менее 60 секунд, то обновление выполняется раз в 60 секунд.
#Если адрес после предыдущего обновления не изменялся – обновление не
выполняется.
dyndns_refresh_interval = 60
```

Примечание

Чтобы загрузить новые параметры конфигурации необходимо перезапустить службу SSSD:

```
# systemctl restart sssd
```

Таблица 39.6. Параметры настройки автоматического обновления DNS

Параметр	Описание	Значение по умолчанию
dyndns_update	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) IP-адресом клиента через SSSD. Соответственно, администратору AD требуется только разрешить защищённые обновления для зоны DNS. Для обновления будет использован IP-адрес LDAP-соединения AD, если с помощью параметра «dyndns_iface» не указано иное	true
dyndns_ttl	Значение TTL, которое применяется при обновлении DNS-записи клиента. Если **dyndns_update** имеет значение **false**, этот параметр не имеет никакого эффекта. Если администратором установлено значение TTL на стороне сервера, оно будет переопределено этим параметром	3600 (секунд)

Параметр	Описание	Значение по умолчанию
dyndns_iface	Позволяет указать интерфейс или список интерфейсов, IP-адреса которых должны использоваться для динамических обновлений DNS. Специальное значение «*» подразумевает, что следует использовать IP-адреса всех интерфейсов. Если **dyndns_update** имеет значение **false**, этот параметр не имеет никакого эффекта	IP-адреса интерфейса, который используется для подключения LDAP AD
dyndns_refresh_interval	Определяет как часто внутреннему серверу следует выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при переходе внутреннего сервера в сетевой режим. Этот параметр применим только в том случае, если для параметра **dyndns_update** установлено значение **true**. Следует обратить внимание, что наименьшее допустимое значение составляет 60 секунд: если будет указано меньшее значение, параметр примет наименьшее допустимое значение (60 секунд)	86400 (24 часа)
dyndns_update_ptr	Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента. Применимо, только если параметр **dyndns_update** имеет значение **true**. Следует обратить внимание, что параметр **dyndns_update_per_family** не применяется для обновлений записей PTR. Эти обновления всегда отправляются отдельно	true
dyndns_force_tcp	Должна ли утилита **nsupdate** по умолчанию использовать TCP для обмена данными с сервером DNS	false (разрешить **nsupdate** выбрать протокол)
dyndns_auth	Следует ли утилите **nsupdate** использовать проверку подлинности GSS-TSIG для защищённых обновлений сервера DNS. Незащищённые отправления можно отправлять, установив этот параметр в значение **none**	GSS-TSIG
dyndns_auth_ptr	Следует ли утилите **nsupdate** использовать проверку подлинности GSS-TSIG для защищённых обновлений PTR сервера DNS. Незащищённые отправления можно отправлять, установив этот параметр в значение **none**	То же, что и **dyndns_auth**
dyndns_server		none (разрешить **nsupdate** выбрать сервер)

Параметр	Описание	Значение по умолчанию
	Сервер DNS, который следует использовать для выполнения обновления DNS. В большинстве конфигураций рекомендуется не устанавливать значение для этого параметра. Установка этого параметра имеет смысл для сред, в которых сервер DNS отличается от сервера данных идентификации. Следует обратить внимание, что этот параметр используется только для резервной попытки, которая выполняется если предыдущая попытка с использованием автоматически определённых параметров завершилась неудачей	
dyndns_update_per_family	По умолчанию обновление DNS выполняется за два шага: обновление IPv4, а затем обновление IPv6. В некоторых случаях может быть желательно выполнить обновление IPv4 и IPv6 за один шаг	true

39.5.1.1.2. Настройка через ЦУС

Некоторые настройки автоматического обновления DNS для SSSD можно настроить в модуле ЦУС **Аутентификация**. Подробнее см. Настройки SSSD в ЦУС.

39.5.1.1.3. При помощи механизма control

Список всех возможных настроек автоматического обновления DNS для SSSD с помощью control можно получить, выполнив команду:

```
# control | grep sssd-dyndns
sssd-dyndns-refresh-interval unknown         (disabled INTERVAL)
sssd-dyndns-ttl unknown         (disabled TTL)
sssd-dyndns-update unknown         (disabled enabled default)
sssd-dyndns-update-ptr unknown         (disabled enabled default)
```

Таблица 39.7. control для настройки автоматического обновления DNS для SSSD

control	Опция в файле /etc/sssd/sssd.conf	Описание
sssd-dyndns-refresh-interval	**dyndns_refresh_interval**	Определяет как часто серверная часть должна выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при подключении серверной части к сети. Этот параметр применим только в том случае, если для параметра **dyndns_update** установлено значение **true**.

control	Опция в файле /etc/sssd/sssd.conf	Описание
		Доступные режимы: - **INTERVAL** — задать интервал; - **disabled** — установить значение по умолчанию (86400); - **unknown**
sssd-dyndns-ttl	**dyndns_ttl**	Срок жизни, применяемый к DNS-записи клиента при ее обновлении. Если **dyndns_update** имеет значение **false**, этот параметр не имеет никакого эффекта. Доступные режимы: - **TTL** — задать TTL; - **disabled** — установить значение по умолчанию (3600); - **unknown**
sssd-dyndns-update	**dyndns_update**	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD. Доступные режимы: - **enabled** — автоматическое обновление DNS-записи клиента через SSSD включено; - **disabled** — автоматическое обновление DNS-записи клиента через SSSD отключено; - **default** — настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете; - **unknown**
sssd-dyndns-update-ptr	**dyndns_update_ptr**	Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента. Применимо, только если параметр **dyndns_update** имеет значение **true**. Доступные режимы: - **enabled** — автоматическое обновление DNS-записи обратной зоны через SSSD включено; - **disabled** — автоматическое обновление DNS-записи обратной зоны через SSSD отключено;

control	Опция в файле / etc/sssd/sssd.conf	Описание
		▹**default** — настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете; ▹**unknown**

Например, чтобы SSSD автоматически обновлял на сервере DNS AD IP-адрес клиента, необходимо включить **control sssd-dyndns-update**:

```
# control sssd-dyndns-update enabled
```

и перезапустить службу SSSD:

```
# systemctl restart sssd
```

Проверка:

```
# control sssd-dyndns-update
enabled
```

39.5.1.1.4. При помощи групповых политик

С помощью групповых политик в Альт Домен можно централизованно управлять настройками обновления DNS-записей на всех клиентах в сети. В настоящее время с помощью групповых политик можно сконфигурировать параметры **dyndns_update** и **dyndns_update_ptr**. Подробнее см. Групповые политики control (раздел **SSSD опции**).

39.5.1.2. Samba Winbind

Samba Winbind не поддерживает возможность динамического обновления DNS-записей. Для обхода этой проблемы был разработана утилита, реализующая динамическое обновление адресов на DNS-сервере при использовании Winbind в качестве клиента домена — **winbind-dnsupdate**.

Для возможности работы с программой необходимо установить пакет *samba-winbind-dnsupdate*:

```
# apt-get install samba-winbind-dnsupdate
```

И активировать и запустить таймер, который в свою очередь запускает сервис:

```
# systemctl enable --now winbind-dnsupdate.timer
```

Основным функционалом **winbind-dnsupdate** является обновление IPv4 (A), IPv6 (AAAA) и соответствующих PTR DNS-записей. Для обновления DNS-записей **winbind-dnsupdate** использует файл **/etc/resolv.conf**.

Синтаксис команды **winbind-dnsupdate**:

```
winbind-dnsupdate [опции]
```

При запуске без параметров скрипт обновляет A запись.

Таблица 39.8. Опции команды winbind-dnsupdate

Ключ	Описание
-h, --help	Вывести справку о команде
-v, --version	Вывести версию
-a, --all	Включить обновление всех записей (IPv4, IPv6, PTR)
-6, --update-ipv6	Включить обновление IPv6 (AAAA) записей
-d, --daemon	Отправлять логи в journald
-t, --ttl <time>	Задать TTL («время жизни», указывает, как долго настройки DNS должны храниться в кеше, прежде чем они будут автоматически обновлены)
--allow-ipv4-ptr-update	Включить обновление обратной DNS-записи IPv4 (A) PTR
--allow-ipv6-ptr-update	Включить обновление обратной DNS-записи IPv6 (AAAA) PTR
--enable-dconf	Включить чтение параметров из dconf

Пример запуска скрипта **`winbind-dnsupdate`**:

```
# winbind-dnsupdate -a
[INFO]: Hostname: comp01.test.alt.
[INFO]: Check winbind status.
[INFO]: Winbind is running. Continue.
[INFO]: Trying to get the site name.
[INFO]: Site: Default-First-Site-Name.
[INFO]: Get host credentials.
[INFO]: Retrieving host credentials successfully.
[INFO]: Trying to get a list of domain controllers in site.
[INFO]: Success.
[INFO]: Trying to find an available DNS server.
[INFO]: Checking the availability of DNS server on dc1.test.alt..
[INFO]: DNS server on dc1.test.alt. available.
[INFO]: Update IPv4.
[INFO]: Trying to get IPv4 address of a domain controller.
[INFO]: Successful. DC info:
[INFO]: Domain controller name: dc1.test.alt.
[INFO]: Domain controller IPv4: 192.168.0.132.
[INFO]: Trying parse connection interface name.
[INFO]: Successful. Intraface name: enp0s3.
[INFO]: Checking the existence of A record.
[INFO]: IPv4 record exists.
[INFO]: Checking whether the IPv4 records needs to be updated.
[INFO]: Current IPv4 address: 192.168.0.195.
[INFO]: IPv4 address in DNS server: 192.168.0.195.
[INFO]: The IPv4 address of interface enp0s3 has not been changed.
[INFO]: The update IPv4 was skipped.
[INFO]: IPv4 update was successful.
[INFO]: The update was successful.
[INFO]: Destroy host credential.
```

В пакете вместе со скриптом предоставляются systemd сервис и таймер. Таймер запускает systemd сервис для обновления DNS-записи через 5 минут после загрузки системы и затем каждый час. Просмотреть параметры таймера можно, выполнив команду:

```
# systemctl cat winbind-dnsupdate.timer
# /lib/systemd/system/winbind-dnsupdate.timer
[Unit]
Description=Update dns record Daily and on boot

[Timer]
OnBootSec=5min
OnUnitActiveSec=60min

[Install]
WantedBy=timers.target
```

Чтобы изменить частоту запуска systemd сервиса, необходимо отредактировать настройки таймера:

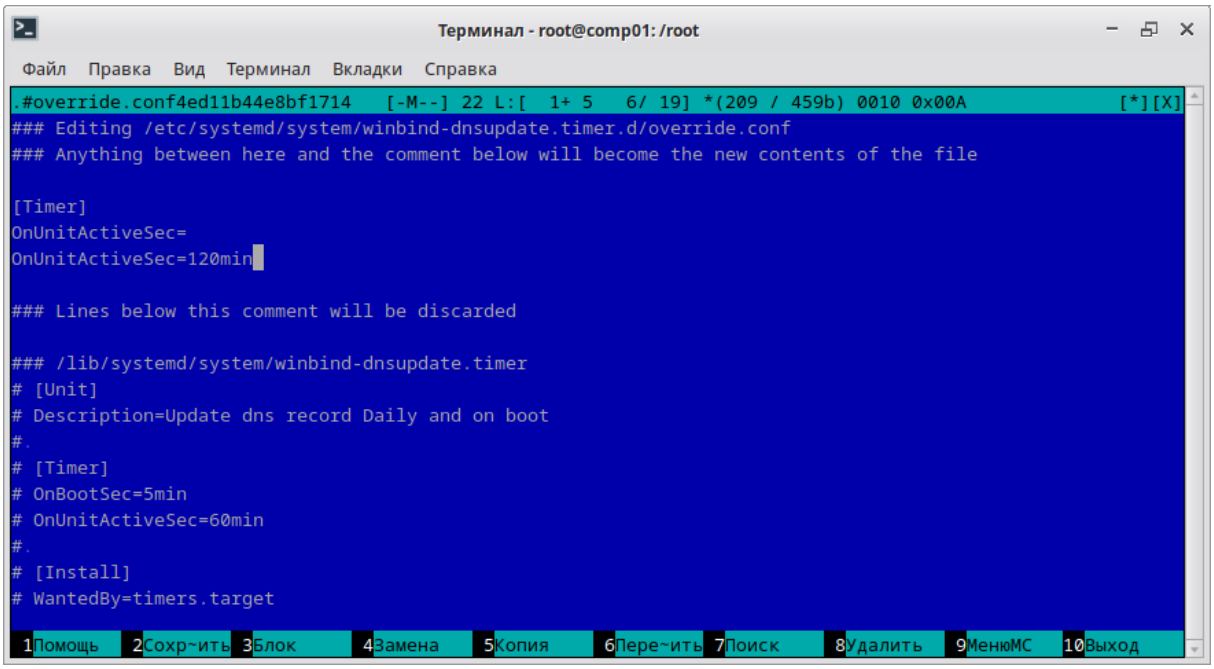
1. Выполнить команду:

   ```
   # systemctl edit winbind-dnsupdate.timer
   ```

2. Добавить следующие строки после строки ***Anything between here and the comment below will become the new contents of the file***:

   ```
   [Timer]
   OnUnitActiveSec=
   OnUnitActiveSec=120min
   ```

   OnUnitActiveSec= очистит предыдущее определение (60min), а ***OnUnitActiveSec=120min*** установит новое значение (120min).

3. Сохранить внесённые изменения.

4. Перезагрузить таймер для применения изменений:

   ```
   # systemctl daemon-reload
   ```

Примечание

Команда:

```
# systemctl edit winbind-dnsupdate.timer
```

открывает текстовый редактор с конфигурацией winbind-dnsupdate.timer, куда можно внести изменения. Этот подход позволяет создавать или изменять так называемые «дополнения» (overrides) для systemd сервиса, не изменяя оригинальный файл сервиса, который находится в **/usr/lib/systemd/system/**. Это важно, потому что оригинальные файлы могут быть перезаписаны при обновлении пакетов.

При выполнении этой команды создаётся каталог **/etc/systemd/system/winbind-dnsupdate.timer.d/**, в котором, после сохранения изменений, появляется файл **override.conf**. В этом файле можно задать новые параметры или изменить существующие параметры сервиса.

Параметрами **winbind-dnsupdate** можно управлять с помощью групповых политик (см. Опции Winbind DNSupdate).

39.5.1.3. Windows клиент

В Windows клиенты автоматически обновляют DNS-записи, такие как A и PTR, при изменении IP-адресов или имени компьютера. Этот процесс инициируется службой DHCP-клиента, которая отправляет обновления на DNS-сервер. Обновления происходят каждые 24 часа (по умолчанию) или могут быть инициированы вручную командой **ipconfig /registerdns**. Для DHCP-клиентов DHCP-сервер может выполнять эти обновления от имени клиента, что снижает необходимость ручного администрирования.

39.6. Обновление IP-адресов вручную

Для обновления IP-адресов вручную существует несколько способов:

- с помощью команды **samba-tool** (см. Утилита samba-tool);
- с помощью утилиты **nsupdate** (см. Утилита nsupdate);
- оснастка DNS в RSAT (см. Оснастка DNS в RSAT).

39.7. Известные проблемы

39.7.1. Неверные права DNS-записей машины в домене

При вводе машины в домен вызывается утилита **system-auth**, которая в свою очередь использует команду **net ads join**. В рамках данной команды выполняется присоединение к домену с использованием Kerberos-аутентификации и не производится обновление DNS. После успешного присоединения машина регистрирует свою DNS-запись с помощью команды **net ads dns register** также используя Kerberos-аутентификацию.

Если машины уже введены в домен или используется старая версия *alterator-auth* (до версии 0.44.10-alt1), то у машин не будет прав на обновление своих DNS-записей. Это происходит потому, что во время создания DNS-записи в доменном DNS **system-auth** использует билет администратора, и в результате владельцем записи становится он, а не машина, что впоследствии не позволяет машине обновить свою DNS-запись.

Примечание

Имеются ввиду записи вида:

```
DC=host1,DC=test.alt,CN=MicrosoftDNS,DC=DomainDnsZones,DC=test,DC=alt
```

Исправление в пакете *alterator-auth* версии 0.44.10-alt1 работает только для машин, которые не были ранее введены в домен с текущим именем (то есть, если машинная учётная запись создаётся впервые). Если машина уже была добавлена в домен, но для неё используется новое имя, то будет создана новая учётная запись, и проблема с правами на обновление DNS-записей будет решена. Однако, если машина повторно вводится в домен с тем же именем, это не устранит проблему.

Примечание

При вводе машины в домен с новым именем необходимо убедиться, что очищены кеши SSSD и Winbind, а также удален старый keytab-файл.

В случае с уже введёнными в домен машинами можно воспользоваться скриптом https://altlinux.space/alt-domain/samba-allow-nsupdate на контроллере домена (предварительно получив билет администратора). Этот скрипт позволяет задать необходимые права как для всех машин в домене или OU, так и для произвольного списка машин в домене. Примеры:

- разрешить самостоятельное обновление для машин, находящихся в контейнере «Computers»:

```
# samba_allow_nsupdate --domain-dns="test.alt" --computers-base-
dn="CN=Computers,DC=test,DC=alt"
Domain: test.alt
Domain DN: DC=test,DC=alt
Computers search base DN: CN=Computers,DC=test,DC=alt
Action: allow
Selected computers list:
DC1$
WS2$
WS$
WS3$
Allow self nsupdate for this computers list? (Y/n):
DC1$                    S-1-5-21-3099202228-3607437695-3279060739-1000  DONE
WS2$                    S-1-5-21-3099202228-3607437695-3279060739-1113  DONE
WS$                     S-1-5-21-3099202228-3607437695-3279060739-1107  DONE
WS3$                    S-1-5-21-3099202228-3607437695-3279060739-1127  DONE
```

- разрешить самостоятельное обновление для произвольного списка машин в домене (в примере для WS, WS2):

```
# samba_allow_nsupdate --action=allow WS$ WS2$ --computers-base-
dn="DC=test,DC=alt" --domain-dns="test.alt"
Domain: test.alt
Domain DN: DC=test,DC=alt
Computers search base DN: DC=test,DC=alt
Action: allow
Selected computers list:
WS$
WS2$
Allow self nsupdate for this computers list? (Y/n):
WS$                     S-1-5-21-3099202228-3607437695-3279060739-1107   DONE
WS2$                    S-1-5-21-3099202228-3607437695-3279060739-1113   DONE
```

Другие решения:

- воспользоваться RSAT оснасткой DNS на Windows машине и задать необходимые права вручную;
- в той же оснастке DNS для всего DNS домена дать права на запись группе «Domain Computers» (не рекомендуется);
- воспользоваться инструментом **samba-tool dsacl**.

Глава 40. Администрирование сайтов и подсетей

40.1. Утилита samba-tool

40.1. Утилита samba-tool

Для администрирования сайтов и подсетей в Альт Домен можно использовать подкоманду sites утилиты **samba-tool**.

Примечание

Для выполнения команды на удаленном компьютере можно использовать опцию **-H** или **--URL=** с указанием URI LDAP-сервера. Например:

```
# samba-tool sites list -H ldap://<DC> -Uadministrator
```

По умолчанию в качестве значения опции **-H** передается текущий узел в формате ldap://<имя узла>.

Таблица 40.1. Команды управления сайтами samba-tool

Команда	Описание	Примечание
sites create <сайт> [опции]	Добавить новый сайт	В качестве аргумента (***сайт***) ожидается общее имя (CN) сайта.

Команда	Описание	Примечание
		После создания сайта в него могут быть добавлены контроллеры домена, например, путём передачи имени сайта в параметре **`--site=SITE`** при выполнении операции присоединения (см. Присоединение к домену в роли контроллера домена)
sites list [опции]	Вывести список сайтов	Подкоманда поддерживает два формата представления информации о сайтах: • без дополнительных параметров — список общих имен (CN) сайтов; • с параметром **`--json`** — вывод подробной информации о каждом сайте в формате JSON
sites remove <сайт> [опции]	Удалить сайт	В качестве аргумента (***`сайт`***) ожидается общее имя (CN) сайта
sites subnet <подкоманда>	Подкоманды управления подсетью	См. Команды управления подсетями samba-tool
sites view <сайт> [опции]	Вывести информацию об отдельном сайте	В качестве аргумента (***`сайт`***) ожидается общее имя (CN) сайта. Подкоманда выводит тот же набор атрибутов сайта, что и подкоманда **`samba-tool sites list --json`**

Таблица 40.2. Команды управления подсетями samba-tool

Команда	Описание	Примечание
sites subnet create <подсеть> <сайт> [опции]	Создать новую подсеть	Параметры вызова: • подсеть — IP-адрес и маска подсети; • сайт — сайт, за которым будет закреплена подсеть
sites subnet list <сайт> [опции]	Вывести список подсетей сайта	В качестве аргумента (***`сайт`***) ожидается общее имя (CN) сайта. Подкоманда поддерживает два формата представления информации о подсетях: • без дополнительных параметров — список общих имен (CN) подсетей; • с параметром **`--json`** — вывод подробной информации о каждой подсети в формате JSON

Команда	Описание	Примечание
sites subnet remove <подсеть> [опции]	Удалить подсеть	В качестве аргумента (***подсеть***) ожидается общее имя (CN) существующей подсети
sites subnet set-site <подсеть> <сайт> [опции]	Закрепить подсеть за сайтом	Параметры вызова: ▸подсеть — IP-адрес и маска подсети; ▸сайт — сайт, за которым будет закреплена подсеть
sites subnet view <подсеть> [опции]	Просмотр сведений о подсети	В качестве аргумента (***подсеть***) ожидается общее имя (CN) существующей подсети. Подкоманда выводит тот же набор атрибутов подсети, что и подкоманда **`samba-tool subnet list --json`**

Примечание

Полный список параметров каждой команды можно увидеть в справке, например:

```
$ samba-tool sites subnet view --help
```

Примеры:

- получить список сайтов в формате JSON:

```
# samba-tool sites list --json
{
"Default-First-Site-Name": {
"cn": "Default-First-Site-Name",
"distinguishedName": "CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt",
"dn": "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt",
"instanceType": 4,
"name": "Default-First-Site-Name",
"objectCategory": "CN=Site,CN=Schema,CN=Configuration,DC=test,DC=alt",
"objectClass": [
    "top",
    "site"
],
"objectGUID": "4dbdb4a9-ebe9-4ff8-a047-40da60136056",
"showInAdvancedViewOnly": true,
"systemFlags": 1107296256
}
}
```

- получить информацию о сайте:

```
# samba-tool sites view Default-First-Site-Name
```

- создать сайт:

```
# samba-tool sites create newSite
Site newSite created !
```

- создать подсеть:

```
# samba-tool sites subnet create 192.168.10.0/24 newSite
Subnet 192.168.10.0/24 created !
```

- получить список подсетей для сайта newSite с подробной информацией в JSON:

```
# samba-tool sites subnet list newSite --json
{
  "192.168.10.0/24": {
    "cn": "192.168.10.0/24",
    "distinguishedName":
"CN=192.168.10.0/24,CN=Subnets,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "dn":
"CN=192.168.10.0/24,CN=Subnets,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "instanceType": 4,
    "name": "192.168.10.0/24",
    "objectCategory": "CN=Subnet,CN=Schema,CN=Configuration,DC=test,DC=alt",
    "objectClass": [
      "top",
      "subnet"
    ],
    "objectGUID": "5ebde1f9-5369-4673-a10a-b9c10310d137",
    "showInAdvancedViewOnly": true,
    "siteObject": "CN=newSite,CN=Sites,CN=Configuration,DC=test,DC=alt",
    "systemFlags": 1073741824
  }
}
```

- закрепить подсеть 192.168.10.0/24 за сайтом newSite:

```
# samba-tool sites subnet set-site 192.168.10.0/24 newSite
Subnet 192.168.10.0/24 shifted to site newSite
```

- удалить подсеть:

```
# samba-tool sites subnet remove 192.168.10.0/24
```

Глава 41. Управление парольными политиками

41.1. Глобальные парольные политики

41.2. Объекты настроек паролей (PSO)

В Альт Домен настройки пароля позволяют настроить:

- минимальные требования к длине и сложности пароля;
- длину истории паролей: предотвращает повторное использование пользователем предыдущего пароля;

- минимальный и максимальный срок действия пароля: как часто пользователь может/должен менять свой пароль;
- блокировку учетной записи: пороговое значение неудачных попыток входа в систему перед блокировкой учетной записи пользователя и продолжительность блокировки.

Для управления настройками паролей используется подкоманда **passwordsettings** утилиты **samba-tool**.

Управление политиками паролей домена производится на контроллере домена.

41.1. Глобальные парольные политики

Для просмотра текущих параметров политик паролей используется команда:

```
# samba-tool domain passwordsettings show
```

Например:

```
# samba-tool domain passwordsettings show
Password information for domain 'DC=test,DC=alt'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Команда изменения параметра политик паролей:

```
# samba-tool domain passwordsettings set <параметр>
```

Возможные параметры:

- ***--complexity=on|off|default*** — должен ли пароль отвечать требованиям сложности (по умолчанию **on**);
- ***--store-plaintext=on|off|default*** — хранить пароли используя обратимое шифрование (по умолчанию **off**);
- ***--history-length=целое число|default*** — число хранимых предыдущих паролей пользователей (требование неповторяемости паролей) (по умолчанию **24**);
- ***--min-pwd-length=целое число|default*** — минимальное количество символов в пароле (по умолчанию **7**);
- ***--min-pwd-age=целое число|default*** — минимальный срок действия пароля (по умолчанию **1**);
- ***--max-pwd-age=целое число|default*** — максимальный срок действия пароля (по умолчанию **43**);

- ***--account-lockout-duration=целое число|default*** — интервал времени (в минутах), в течение которого возможность аутентификации для пользователя, превысившего количество попыток входа, будет заблокирована (по умолчанию **30**);
- ***--account-lockout-threshold=целое число|default*** — допустимое количество неудачных попыток ввода пароля перед блокировкой учетной записи (по умолчанию **0** — никогда не блокировать);
- ***--reset-account-lockout=целое число|default*** — интервал времени (в минутах), по истечении которого записанное количество попыток начинается заново (по умолчанию **30**).

Изменить минимальную длину пароля и количество неудачных попыток входа в систему:

```
# samba-tool domain passwordsettings set \
--min-pwd-length=7 --account-lockout-threshold=3

Minimum password length changed!
Account lockout threshold changed!
All changes applied successfully!
```

Примечание

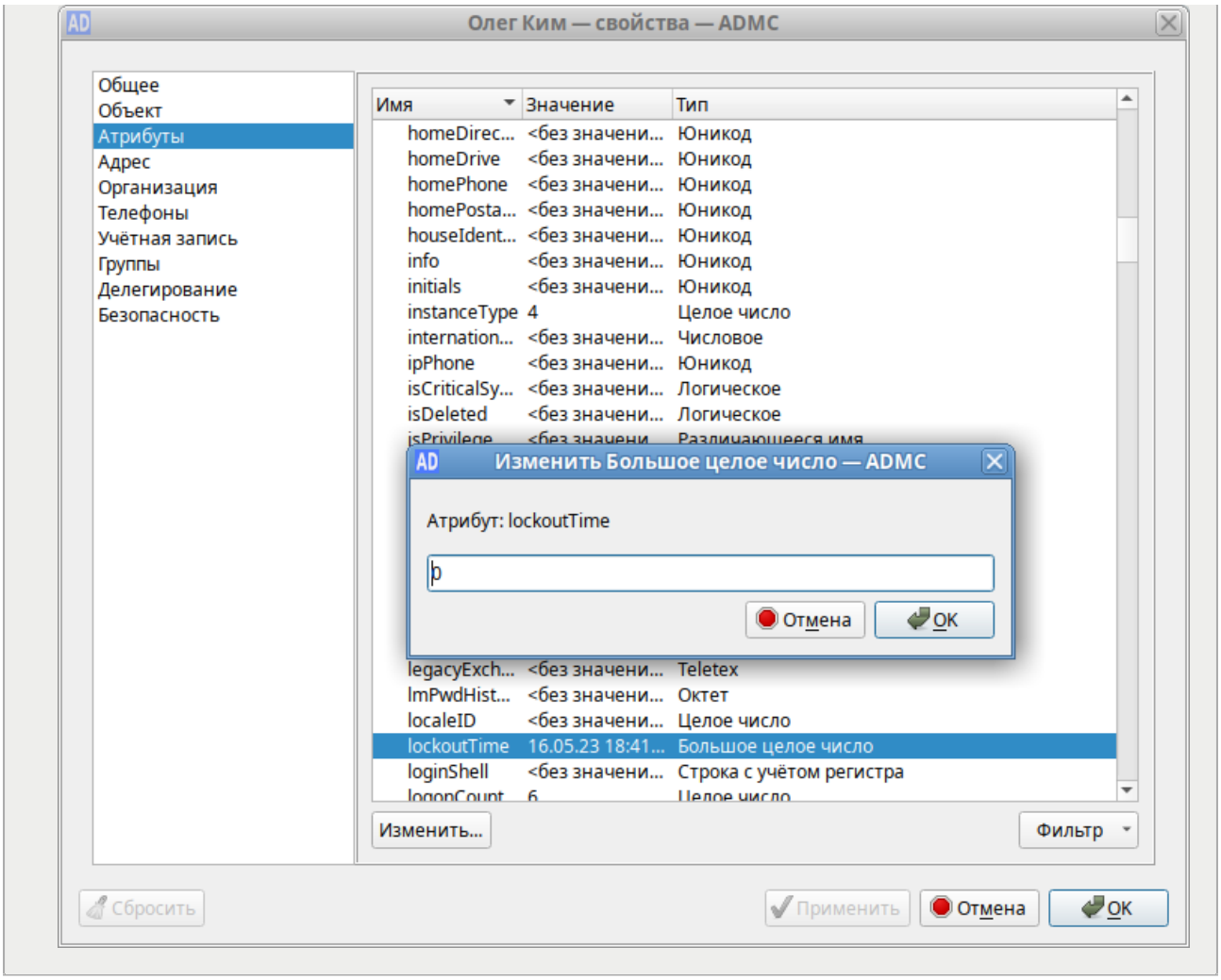
Определить, была ли учётная запись пользователя заблокирована после нескольких неудачных попыток входа в систему можно, просмотрев параметры учётной записи. Если ***badPwdCount*** достиг своего порога и для пользователя существует параметр ***lockoutTime*** значит учётная запись была заблокирована после нескольких неудачных попыток входа в систему:

```
# samba-tool user show ivanov
…
badPwdCount: 3
badPasswordTime: 133560395216186060
lockoutTime: 133560395216186060
…
```

Чтобы разблокировать пользователя, необходимо отредактировать объект учётной записи пользователя, установив для атрибута ***lockoutTime*** значение 0:

```
# samba-tool user edit ivanov
Modified User 'ivanov' successfully

# samba-tool user show ivanov
…
badPasswordTime: 133560395216186060
lockoutTime: 0
…
```

Разблокировать пользователя также можно в модуле удалённого управления базой данных конфигурации (ADMC) (подробнее см. Модуль удаленного управления базой данных конфигурации (ADMC)):



41.2. Объекты настроек паролей (PSO)

Объекты настроек паролей (Password Settings Object, PSO) позволяют администраторам Альт Домен переопределять параметры политики паролей домена и настраивать более точные параметры паролей для конкретных пользователей или групп пользователей. Например, для определённых пользователей можно установить требование минимальной длины пароля, ослабить ограничения сложности для других пользователей и т.д. PSO могут применяться к группам или к отдельным пользователям.

При создании объект PSO сохраняется в LDAP по пути

```
CN=<имя парольной политики>,CN=Password Settings Container,CN=System,DC=<domain>.
```

К одному и тому же пользователю может применяться множество различных PSO (напрямую или через группы). Если несколько PSO применяются к одному и тому же пользователю, в основном вступает в силу PSO с наименьшим приоритетом. Однако PSO, которые применяются непосредственно к пользователю, всегда превосходят PSO, унаследованные через членство в группе.

Если для пользователя не создано правила, будет применяться правило по умолчанию.

Примечание

Необходимо одновременно настраивать политику паролей для всех остальных пользователей, иначе есть риск снижения производительности при настройке PSO и применении их к пользователям. Например:

```
# samba-tool domain passwordsettings pso create PwPolicyAdmins 1 --min-pwd-length=16
# samba-tool domain passwordsettings pso apply PwPolicyAdmins "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyUsers 3 --min-pwd-length=8
# samba-tool domain passwordsettings pso apply PwPolicyUsers "domain admins"
# samba-tool domain passwordsettings pso create PwPolicyService 2 --min-pwd-length=24
# samba-tool domain passwordsettings pso apply PwPolicyService "domain admins"
```

Если объектов PSO вообще нет, производительность не снижается.

Расчет PSO включает в себя расчет членства пользователя в группах, что является довольно дорогостоящим расчетом. Если PSO применяется непосредственно к пользователю (а не к группе), то дорогостоящие групповые вычисления пропускаются. Однако применение PSO непосредственно к пользователям делает управление PSO более сложным по сравнению с применением PSO к группам.

41.2.1. В ADMC

Для управления объектами настроек паролей в Альт Домен можно использовать модуль удалённого управления базой данных конфигурации (ADMC). Подробнее см. Управление объектами парольных настроек.

41.2.2. С помощью samba-tool

Для работы с объектами PSO используется подкоманда **pso** утилиты **samba-tool**.

Команда изменения PSO:

```
# samba-tool domain passwordsettings pso <подкоманда>
```

Доступные подкоманды:

- **apply** — применить политику паролей PSO к пользователю или группе;
- **create** — создать новый объект настроек пароля (PSO);
- **delete** — удалить объект настроек пароля (PSO);
- **list** — вывести список всех объектов настроек пароля (PSO);
- **set** — изменить объект настроек пароля (PSO);
- **show** — показать детали объекта настроек пароля;

- **show-user** — отобразить настройки пароля, которые применяются к пользователю;
- **unapply** — обновить PSO, чтобы он больше не применялся к пользователю или группе.

Для создания нового объекта PSO используется команда:

```
# samba-tool domain passwordsettings pso create <pso-name> <precedence> [options]
```

Подкоманда создает новую парольную политику с указанным именем (<pso-name>). Имя должно быть уникальным на уровне домена.

При создании политики может быть задан ее приоритет (<precedence>), который будет учитываться в том случае, если к пользователю или группе пользователей применяются несколько политик. Чем меньше значение параметра ***precedence***, тем выше приоритет.

В качестве аргументов передаются атрибуты парольной политики с требуемыми значениями.

Примечание

Для создания политики требуется передать новое значение хотя бы для одного атрибута.

Для применения атрибутов, заданных в объекте PSO, к определенному пользователю или группе используется команда:

```
# samba-tool domain passwordsettings pso apply <pso-name> <user-or-group-name>
[options]
```

Подкоманда обеспечивает применение атрибутов парольной политики (PSO) с указанным именем (<pso-name>) к указанному пользователю или группе пользователей (<user-or-group-name>).

Пример создания и назначения парольной политики:

1. Создать парольную политику:

```
# samba-tool domain passwordsettings pso create PwPolicyUser 1 --min-pwd-
length=10
Not all password policy options have been specified.
For unspecified options, the current domain password settings will be used
as the default values.
PSO successfully created: CN=PwPolicyUser,CN=Password Settings
Container,CN=System,DC=test,DC=alt
Password information for PSO 'PwPolicyUser'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

2. Назначить созданную политику пользователю ivanov:

```
# samba-tool domain passwordsettings pso apply PwPolicyUser ivanov
The following PSO settings apply to user 'ivanov'.

Password information for PSO 'PwPolicyUser'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 10
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30

Note: PSO applies directly to user (any group PSOs are overridden)
```

Чтобы увидеть, какой PSO действует для данного пользователя, используется команда **`samba-tool pso show-user`**:

```
# samba-tool domain passwordsettings pso show-user kim
No PSO applies to user 'kim'. The default domain settings apply.
Refer to 'samba-tool domain passwordsettings show'.
```

Для получения списка всех объектов PSO в домене используется команда:

```
# samba-tool domain passwordsettings pso list [options]
```

Эта подкоманда выводит список всех парольных политик (PSO), доступных в домене, в виде таблицы со столбцами **`Precedence`** и **`PSO name`**.

Глава 42. Резервное копирование и восстановление домена

42.1. Резервное копирование и восстановление из резервной копии

42.2. Восстановление произвольного контроллера домена после фатального сбоя

42.1. Резервное копирование и восстановление из резервной копии

Инструменты резервного копирования и восстановления позволяют пересоздать домен при возникновении проблем, делающих невозможной его дальнейшую полноценную эксплуатацию.

Примером такой проблемы может служить изменение или удаление какого-либо объекта или группы объектов в базе данных службы каталогов, приводящее к неработоспособности одного из доменных сервисов. Подобное изменение реплицируется на все контроллеры домена. То есть для восстановления работоспособности такого сервиса недостаточно выполнить повторное присоединение к домену какого-либо отдельного контроллера, так как он получит копию базы данных с вызвавшим проблему изменением. В этом случае при наличии резервной копии домена без внесенного «проблемного» изменения она может быть использована для восстановления.

В процессе восстановления создается новый контроллер домена с базой данных из резервной копии. Существующие контроллеры домена должны быть остановлены и заново присоединены к нему.

Примечание

Механизм восстановления из резервной копии не должен использоваться для восстановления работоспособности отдельно взятого контроллера домена в случае возникновения на нем локальной проблемы, не затрагивающей работу всего домена. В этом случае достаточно провести диагностику и устранить проблему на контроллере домена, а затем выполнить повторное присоединение к домену для получения актуальной копии базы данных службы каталогов (см. раздел Восстановление произвольного контроллера домена после фатального сбоя).

Если контроллер домена используется и в качестве файлового сервера (что не рекомендуется), потребуется также создать отдельные резервные копии этих данных.

Поддерживаются следующие виды резервного копирования:

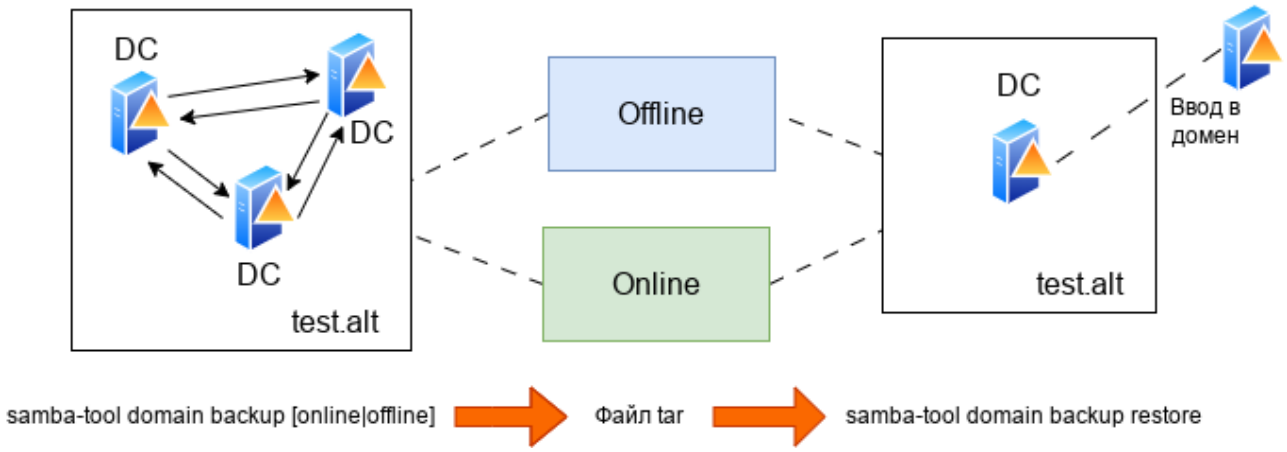
- *Online* (онлайн-режим) — выполняется клонирование работающей базы данных DC. По функциональности это похоже на присоединение нового контроллера домена к сети;
- *Offline* (автономный режим) — резервные копии Samba создаются в том виде, в котором они появляются на диске. Сюда входят метаданные репликации, которые являются локальными для этого конкретного контроллера домена и которые не включаются в резервные копии в онлайн-режиме. Такую резервную копию также можно создать, когда контроллер домена находится в автономном режиме (т.е. процесс samba фактически не запущен);
- *Rename* (режим с переименованием) — создаётся файл резервной копии с переименованным доменом (предназначен только для временной замены).

Резервные копии можно создать, используя команду **`samba-tool domain backup`**. При этом будет создан файл резервной копии **`.tar.bz2`**, который будет содержать полную резервную копию домена (на основе данного контроллера домена). Этот файл резервной копии можно использовать для восстановления домена с помощью команды **`samba-tool domain backup restore`**.

Примечание

Следует иметь в виду, что файл резервной копии — это резервная копия домена, а не контроллера домена. Восстановление файла резервной копии создаст новый контроллер домена с информацией о домене. Чтобы восстановить последующие контроллеры домена, необходимо присоединить данные контроллеры домена к восстановленному контроллеру домена.

42.1.1. Создание резервной копии в онлайн/офлайн режимах



42.1.1.1. Создание резервной копии в онлайн-режиме

В онлайн-режиме (*online*) формируется набор файлов с актуальными данными службы каталогов, не привязанными к состоянию конкретного контроллера домена.

Данный вид резервного копирования подходит в том случае, если требуется оперативно получить работоспособную долгосрочную или постоянную замену вышедшему из строя домену без детального изучения причин возникновения проблем в работе службы каталогов.

Для создания резервной копии в онлайн-режиме используется команда:

```
# samba-tool domain backup online \
 --targetdir=<output-dir> \
 --server=<DC-server> -UAdministrator
```

Эту команду можно запустить как локально на контроллере домена, так и удалённо на другом узле. При удалённом запуске рекомендуется указать параметр **`--configfile`**, чтобы в резервную копию были включены правильные настройки **`smb.conf`** (т.к. локальный файл **`smb.conf`** может не существовать или его настройки могут отличаться от настроек контроллера домена).

Примечание

Перед созданием файла резервной копии рекомендуется запустить команду **`samba-tool dbcheck`** и исправить все ошибки, о которых она сообщает.

Примечание

Вся секретная информация домена будет включена в файл резервной копии.

Пример создания резервной копии в онлайн-режиме на контроллере домена:

```
# mkdir /var/samba-backup-online
# samba-tool domain backup online --targetdir=/var/samba-backup-online --
server=dc1 -UAdministrator

Password for [TEST\Administrator]:
workgroup is TEST
realm is test.alt
Looking up IPv4 addresses
Looking up IPv6 addresses
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
A Kerberos configuration suitable for Samba AD has been generated at /var/samba-
backup-online/tmpxqc6dwts/private/krb5.conf
Merge the contents of this file with your system krb5.conf or replace it with
this one. Do not create a symlink!
…
Creating backup file /var/samba-backup-online/samba-backup-
test.alt-2024-06-04T16-15-49.475857.tar.bz2...
```

42.1.1.2. Создание резервной копии в автономном режиме

В автономном режиме (*offline*) создается резервная копия локальных файлов контроллера домена, на котором запускается команда резервного копирования.

Данный вид резервного копирования оптимален для изучения причин возникновения проблем в работе службы каталогов, так как в этом режиме в резервную копию включаются дополнительные данные, как правило, не подлежащие реплицированию. В больших доменах на создание такой резервной копии требуется меньше времени, поскольку исключаются временные затраты на передачу данных из базы данных службы каталогов по сети и запись их на локальный диск. Однако следует учитывать, что при копировании базы данных с диска потенциально повышается риск попадания в резервную копию ошибочных данных.

Примечание

Отличия автономного резервного копирования от онлайн-режима:

- резервную копию можно создать, даже если контроллер домена в данный момент не работает;
- резервная копия включает нереплицированные атрибуты, которые не сохраняются в онлайн-резервной копии;
- в копию попадают необработанные файлы базы данных, что может привести к тому, что какие-либо скрытые проблемы в БД сохранятся в резервной копии.

Для создания автономной резервной копии используется команда:

```
# samba-tool domain backup offline --targetdir=<output-dir>
```

Примечание

Несмотря на то, что данный тип резервного копирования называется автономным, контроллеру домена не нужно быть в автономном режиме при выполнении этой команды. Инструмент просто выполняет резервное копирование локальных файлов и имеет достаточную блокировку, чтобы гарантировать безопасное создание резервной копии.

Пример создания автономной резервной копии на контроллере домена:

```
# mkdir /var/samba-backup-offline
# samba-tool domain backup offline --targetdir=/var/samba-backup-offline

running backup on dirs: /var/lib/samba/private /var/lib/samba /etc/samba
Starting transaction on /var/lib/samba/private/secrets
Starting transaction on /var/lib/samba/private/sam.ldb
   backing up /var/lib/samba/private/sam.ldb

…
   adding misc file etc/lmhosts
   adding misc file etc/smb.conf
Backup succeeded.
```

42.1.1.3. Восстановление домена из резервной копии

Для восстановления домена из резервной копии необходимо выполнить следующие шаги:

1. Остановить службу каталогов (**samba**) на всех контроллерах домена. Этот шаг можно пропустить если используется переименованная резервная копия.
2. Выполнить команду **samba-tool domain backup restore**, с требуемыми параметрами для восстановления базы данных домена на одном новом контроллере домена.
3. Запустить **samba** на новом контроллере домена.
4. Повторно добавить старые контроллеры домена в сеть, присоединив их к восстановленному контроллеру домена, например, выполнив команду:

```
samba-tool domain join <dns-realm> DC --server=<restored-dc>
```

5. Если используется переименованная резервная копия, также потребуется перенастроить сетевые устройства, так чтобы трафик перенаправлялся в восстановленный домен, а не в неисправный/исходный домен.

Примечание

Из файла резервной копии восстанавливается весь домен, а не конкретный контроллера домена. Шаг с командой **samba-tool domain backup restore** выполняется только один раз, при этом домен воссоздается на одном контроллере домена. Затем все старые контроллеры домена должны быть повторно присоединены к восстановленному контроллеру домена.

Этап восстановления из файла резервной копии аналогичен разворачиванию домена, который выполнялся при первой настройке сети Samba, за исключением того, что резервная копия содержит в себе все объекты базы данных, которые были добавлены с момента создания домена. Как и при создании нового домена, при запуске команды восстановления домена потребуется указать новый контроллер домена. Этот контроллер домена не должен был существовать ранее в сети Samba.

Команда восстановления домена из резервной копии:

```
# samba-tool domain backup restore --backup-file=<tar-file> \
 --newservername=<DC-name> \
 --targetdir=<new-samba-dir>
```

где

- tar-file — файл резервной копии;
- DC-name — новый контроллер домена;
- new-samba-dir — каталог, куда будут восстановлены все файлы службы каталогов (smb.conf, sam.ldb и т. п.).

Следует обратить внимание, что указанный целевой каталог должен быть пустым (или не должен существовать). Не рекомендуется восстанавливать базу данных домена в место установки по умолчанию (например, в каталог **/var/lib/samba**). Вместо этого рекомендуется восстановить базу данных домена в другой целевой каталог, а затем, при запуске samba, использовать параметр **-s** (или **--configfile**), например:

```
# samba -s <targetdir>/etc/smb.conf
```

Указание восстановленного **smb.conf** гарантирует, что Samba будет использовать правильные файлы базы данных.

Восстановленный контроллер домена будет добавлен в сайт 'Default-First-Site-Name'. Если он не существует в базе данных, он будет создан. Указать альтернативный сайт для добавления восстановленного контроллера домена можно с помощью параметра **--site**.

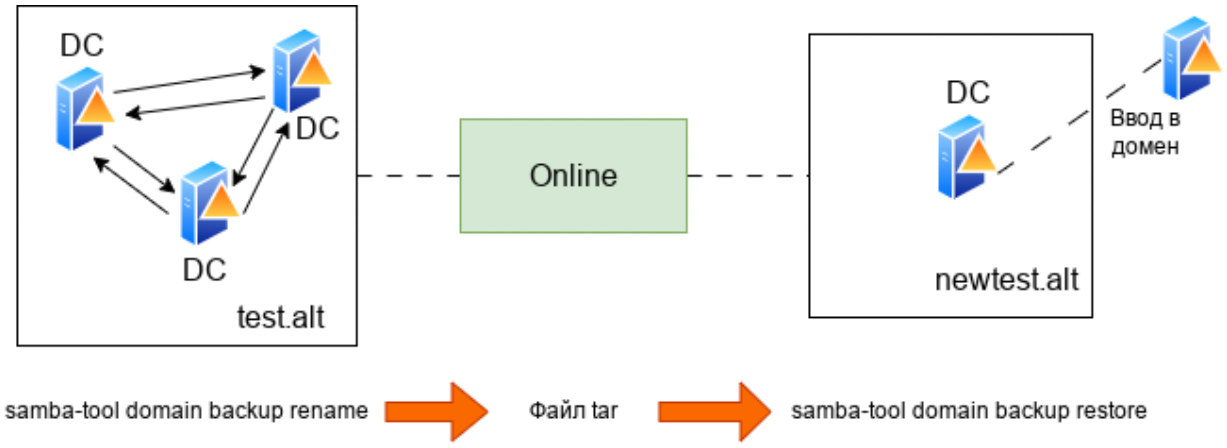
Перед запуском службы каталогов на восстановленном контроллере домена следует еще раз проверить правильность восстановленных настроек **smb.conf**.

Пример восстановления данных из резервной копии:

```
# mkdir /var/lib/samba/new
# samba-tool domain backup restore \
 --backup-file=/home/user/samba-backup-
test.alt-2024-06-04T16-15-49.475857.tar.bz2 \
 --newservername=newdc  --targetdir=/var/lib/samba/new

Adding new DC to site 'Default-First-Site-Name'
Updating basic smb.conf settings...
…
Backup file successfully restored to /var/lib/samba/new
Please check the smb.conf settings are correct before starting samba.
```

42.1.2. Переименованная резервная копия

Процедура создания резервной копии и восстановления из неё в режиме переименования:



В режиме с переименованием (*rename*) формируется набор файлов с актуальными данными службы каталогов, не привязанными к состоянию конкретного контроллера домена, с переименованием домена.

Данный вид резервного копирования позволяет с минимальными усилиями временно подменить вышедший из строя домен таким образом, чтобы обеспечить работоспособность ключевых сетевых сервисов службы каталогов и иметь возможность детально исследовать причины возникновения проблем в существующем домене.

Создание резервной копии в режиме переименования может применяться для:

- запуска временного альтернативного домена на случай катастрофического отказа основного домена. На альтернативный/переименованный домен можно переключиться с минимальными усилиями. Затем можно запустить два домена одновременно, не мешая друг другу (переименованный/альтернативный домен будет предоставлять основные сетевые службы Samba, в это же время на исходных контроллерах домена можно устранять неполадки);
- создания реалистичного лабораторного домена: домен переименовывается и удаляются конфиденциальные данные (на данный момент только самые важные), чтобы создать предпроизводственную среду для тестирования.

При клонировании базы данных службы каталогов в нее вносятся изменения, обеспечивающие использование другого NetBIOS-имени и другой области DNS в новом домене. Изменяются следующие объекты:

- все DN-имена;
- объект раздела домена и его NetBIOS-имя;
- объекты зоны DNS, а также атрибуты dnsRoot.

Примечание

Модифицируется только клонированный домен — исходный домен вообще не затрагивается.

Объекты, которые не меняются:

- userPrincipalName (UPN) по-прежнему будет использовать user@old-realm. Если при выполнении команды резервного копирования с переименованием домена использовался параметр ***--keep-dns-realm***, пользователи могут использовать для входа в домен свои полные UPN-имена. В противном случае они могут использовать имена в формате user@new-realm (при условии, что конфигурация Kerberos корректно обрабатывает новую область);
- объекты групповой политики: атрибуты объекта групповой политики (gPCFileSysPath и gPLink) вообще не обновляются, файлы в sysvol сохраняются с прежним именем области в путях (например, sysvol/test.alt/Policies). Каталог для файлов политик в sysvol по умолчанию создается с новым именем области (например, sysvol/newtest.alt/Policies).

Примечание

Обновление объектов групповой политики для обработки изменения имени домена — нетривиальный процесс. Лучший способ справиться с долгосрочным переименованием домена — вручную экспортировать файлы ГП, а затем повторно импортировать их. В краткосрочной перспективе переименованный домен сможет продолжать использовать объекты групповой политики, относящиеся к старой области.

Переименование домена выполняется в два этапа:

- создание переименованной резервной копии домена: команда **`samba-tool domain backup rename`** делает клон работающей базы данных DC, в процессе клонирования переименовывает домен и создаёт файл резервной копии;
- восстановление резервной копии домена: команда **`samba-tool domain backup restore`** из файла резервной копии формирует файлы, необходимые для запуска нового контроллера домена Samba.

42.1.2.1. Создание переименованной резервной копии

Команда для создания переименованной резервной копии:

```
# samba-tool domain backup rename <new-domain-netbios> \
 <newdomain-dns-realm> --server=<dc-to-backup> \
 --targetdir=<output-dir> --no-secrets -UAdministrator
```

где

- new-domain-netbios — новое имя NETBIOS;
- newdomain-dns-realm — новая область DNS;
- output-dir — каталог, куда будет записан сгенерированный файл резервной копии.

Предупреждение

Параметр **`--no-secrets`** исключает из резервной копии конфиденциальную информацию о паролях (например, такие атрибуты, как ***`unicodePwd`***, ***`lmPwdHistory`*** и т. д.) для всех пользователей в домене. При этом, файл резервной копии по-прежнему содержит конфиденциальную информацию, такую как имена учётных записей пользователей.

В результате выполнения команды формируется файл резервной копии **`/var/samba-backup-rename/samba-backup-newtest.alt-<timestamp>.tar.bz2`**.

В случае, если команда создания резервной копии запускается на узле, который будет использоваться в качестве нового контроллера домена (он должен быть подключён к рабочему домену), рекомендуется иметь файл **`smb.conf`**, максимально соответствующий производственному контроллеру домена, и передать его команде резервного копирования (с помощью параметра **`--configfile=smb.conf`**). Это гарантирует, что резервная копия будет содержать **`smb.conf`**, точно соответствующий домену.

Пример создания переименованной резервной копии на контроллере домена:

```
# mkdir /var/samba-backup-rename
# samba-tool domain backup rename NEWTEST newtest.alt --server=dc1 \
 --targetdir=/var/samba-backup-rename --no-secrets -UAdministrator

New realm for backed up domain: newtest.alt
New base DN for backed up domain: DC=newtest,DC=alt
New domain NetBIOS name: NEWTEST
Password for [TEST\Administrator]:
Provisioning the new (renamed) domain...
…
```

Если команда создания резервной копии запускается на другом узле, (например, на рабочем контроллере домена), необходимо скопировать сгенерированный файл резервной копии на узел, который будет использоваться в качестве нового контроллера домена.

42.1.2.2. Восстановление данных из резервной копии

Файл резервной копии **/var/samba-backup-rename/samba-backup-newtest.alt-<timestamp>.tar.bz2** может использоваться для восстановления клонированной и переименованной базы данных на диске. В восстановленном домене будет только один новый контроллер домена с именем, указанными с помощью опции ***--newservername***. В последующем к нему могут быть присоединены другие контроллеры домена. Для указания нового каталога для размещения всех файлов службы каталогов (smb.conf, sam.ldb и т. п.) может использоваться опция ***--targetdir***.

Команда восстановления домена из резервной копии:

```
# samba-tool domain backup restore \
 --backup-file=<tar-file> \
 --newservername=<DC-name> \
 --targetdir=<new-samba-dir>
```

где

- tar-file — файл резервной копии;
- DC-name — новый контроллер домена;
- new-samba-dir — каталог, куда будут восстановлены все файлы службы каталогов (smb.conf, sam.ldb и т. п.).

Пример восстановления домена из переименованной резервной копии:

```
# mkdir /var/lib/samba/newtest
# samba-tool domain backup restore \
 --targetdir=/var/lib/samba/newtest \
 --newservername=NEWDC1 \
 --backup-file=/home/user/samba-backup-
newtest.alt.alt-2024-04-17T20-09-56.883910.tar.bz2
```

Примечание

Целевой каталог должен быть пустым (или не должен существовать). Не рекомендуется восстанавливать базу данных домена в место установки по умолчанию (например, в каталог **/var/lib/samba/**). Однако можно указать подкаталог (например, **/var/lib/samba/newtest/**).

Примечание

Новый контроллер домена не может использовать то же имя сервера, что и контроллер домена в исходной сети.

42.1.2.3. Сброс пароля

Во время резервного копирования/восстановления пароль для учётной записи администратора сбрасывается на случайно сгенерированный пароль. Для его изменения можно просто обновить базу данных на локальном диске, выполнив команду:

```
# samba-tool user setpassword Administrator \
 --newpassword=<пароль> -H /var/lib/samba/newtest/private/sam.ldb
```

Для тестирования аутентификации пользователей можно либо добавить дополнительные «тестовые» учётные записи пользователей/машин, либо «командовать» некоторыми учётными записями, скопированными из рабочего домена. Для учётных записей, скопированных из рабочего домена, не будут установлены пароли, поэтому на этом этапе также можно сбросить пароли для выбранных учётных записей. Или можно сделать это позже, когда служба каталогов действительно запустится на новом контроллере домена.

42.1.2.4. Запуск Samba

Перед запуском службы каталогов на новом контроллере домена, рекомендуется проверить корректность настроек в восстановленном файле **smb.conf** (например, **/var/lib/samba/newtest/etc/smb.conf**) и в файле **/etc/krb5.conf**, и при необходимости вручную внести в них изменения.

При запуске службы каталогов необходимо указать восстановленный **smb.conf** (это гарантирует, что Samba загрузит правильные файлы базы данных для нового домена). Например:

```
# samba -s /var/lib/samba/newtest/etc/smb.conf
```

При первом запуске службы каталогов могут быть зарегистрированы ошибки DNS. Это связано с тем, что **samba_dnsupdate** запускается автоматически и добавляет записи DNS для нового домена.

После запуска **samba** можно проверить правильность работы нового контроллера домена, например, выполнив команду:

```
# ldbsearch -H ldap://NEWDC1 -UAdministrator
```

42.1.2.5. Обновление подсетей сайта

Новый домен будет содержать все сайты рабочего домена, но ни один из рабочих контроллеров домена. Однако подсети, которые используют эти сайты, скорее всего, больше не будут иметь смысла для экспериментального домена.

42.1.3. Рекомендуемая стратегия

Восстановление файла резервной копии имеет несколько неудобств:

- необходимость использовать другой каталог для установки по умолчанию;
- необходимо указать имя сервера DC, отличное от того, что было ранее в сети.

Свести эти неудобства к минимуму можно, используя временный сервер (или виртуальную машину) для восстановления контроллера домена. В этом случае процесс восстановления работоспособности домена состоит из следующих шагов:

- выполнить восстановление из файла резервной копии на временный контроллер домена и запустить службу каталогов;

- повторно по одному присоединить существующие контроллеры домена к временному контроллеру домена (во время присоединения можно повторно использовать одно и то же имя сервера и место установки по умолчанию);
- после присоединения всех существующих контроллеров домена к восстановленному домену, можно удалить временный контроллер домена (например, с помощью команды **samba-tool domain demote**).

В этом случае новая сеть контроллеров домена будет полностью повторять существующую.

Примечание

Пример разворачивания домена (SAMBA_INTERNAL) из резервной копии на ВМ:

1. Подготовить узел:
   - установить пакет *task-samba-dc* (или *task-samba-dc-mitkrb5*):

     ```
     # apt-get install task-samba-dc
     ```

   - остановить конфликтующие службы:

     ```
     # for service in smb nmb krb5kdc slapd bind; do systemctl disable
     $service; systemctl stop $service; done
     ```

   - очистить базы и конфигурацию Samba:

     ```
     # rm -f /etc/samba/smb.conf
     # rm -rf /var/lib/samba/*
     # rm -rf /var/cache/samba
     ```

2. Скопировать файл резервной копии на ВМ и выполнить восстановление домена из файла резервной копии:

   ```
   # samba-tool domain backup restore \
    --backup-file=/home/user/samba-backup-
   test.alt-2024-04-17T20-09-56.883910.tar.bz2 \
    --newservername=newdc  --targetdir=/var/lib/samba

   Adding new DC to site 'Default-First-Site-Name'
   Updating basic smb.conf settings...
   …
   Backup file successfully restored to /var/lib/samba
   Please check the smb.conf settings are correct before starting samba.
   ```

3. Скопировать файл **smb.conf** из каталога **/var/lib/samba/etc/** в **/etc/samba/**:

   ```
   # cp /var/lib/samba/etc/smb.conf /etc/samba/
   ```

4. Запустить службу каталогов:

   ```
   # systemctl enable --now samba
   ```

5. Заменить файл **/etc/krb5.conf** файлом из каталога **/var/lib/samba/private/**:

```
# cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

6. Проверить работоспособность домена (см. Проверка работоспособности домена):

```
# samba-tool domain info 127.0.0.1
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : newdc.test.alt
DC netbios name  : NEWDC
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name

# smbclient -L localhost -Uadministrator
Password for [TEST\administrator]:

Sharename       Type      Comment
---------       ----      -------
sysvol          Disk
netlogon        Disk
share           Disk      Commonplace
Free            Disk
IPC$            IPC       IPC Service (Samba 4.19.9)
SMB1 disabled -- no workgroup available

# host -t SRV _kerberos._udp.test.alt.
_kerberos._udp.test.alt has SRV record 0 100 88 newdc.test.alt.
```

42.1.4. Отладочная информация

Если команды резервного копирования или восстановления завершится с ошибкой, то они могут оставить после себя временный каталог (указанный в параметре **`--targetdir`**). Это может помочь понять, почему произошел сбой. Необходимо удалить этот каталог перед повторным запуском команды восстановления.

Создание резервной копии:

- резервное копирование следует запускать от имени пользователя root. Резервное копирование в онлайн-режиме может быть успешным и для пользователя без полномочий root, но при попытке восстановить данные из такой резервной копии могут возникнуть проблемы;

- для резервных копий, выполненных в онлайн-режиме или в режиме переименования, следует проверить правильность используемых учётных данных и сведений о сервере, например:

```
# ldbsearch -H ldap://<server> -UAdministrator
```

- чтобы узнать больше информации о причине сбоя можно увеличить уровень журналирования. Например, добавить в команду параметр **`--debug=3`**;

- работа команд, для выполнения резервного копирования резервного копирования в онлайн-режиме или в режиме переименования, очень похожа на присоединение к контроллеру домена. Если известно, что присоединение к контроллеру домена в вашей сети не удается, то эти команды также вероятно не будут работать. Сообщения «Committing SAM database» и «Cloned domain <domain>», говорят о том, что часть резервного копирования, подобная присоединению, скорее всего, выполнена успешно;

- инструменты резервного копирования не работают напрямую с контроллером домена Windows (в основном простое резервное копирование файлов sysvol не удается из-за блокировки службы DFSR). Если используется смешанный домен контроллера домена, следует создать резервную копию контроллера домена Samba, а не контроллера домена Windows. Если используется домен Windows, можно на время резервного копирования на контроллере домена остановить службу DFSR «Репликация DFS».

Восстановление из резервной копии:

- команду восстановления необходимо запускать от имени пользователя root;

- имя, указанное в параметре **`--newservername`**, не должно существовать в исходном домене. В противном случае будет получена ошибка:

```
Adding CN=NEWDC,OU=Domain Controllers,DC=test,DC=alt
ERROR(ldb): uncaught exception - Entry CN=NEWDC,OU=Domain
Controllers,DC=test,DC=alt already exists
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/__init__.py", line 186, in
_run
    return self.run(*args, **kwargs)
  File "/usr/lib64/samba-dc/python3.9/samba/netcmd/domain_backup.py", line
562, in run
    ctx.join_add_objects(specified_sid=dom_sid(str(sid)))
  File "/usr/lib64/samba-dc/python3.9/samba/join.py", line 674, in
join_add_objects
    ctx.samdb.add(rec, controls=controls)
```

- если команда резервного копирования выполнялась локально на контроллере домена, то файл резервной копии должен содержать файл **`smb.conf`** контроллера домена. Однако **`smb.conf`** в файле резервной копии может содержать конфигурацию «интерфейсов», которая не соответствует IP-адресам на контроллере домена, на котором разворачиваются данные из резервной копии. Избежать этой проблемы можно, указав аргумент **`--host-ip`** во время восстановления (это имеет значение только на переименованных резервных копий).

42.2. Восстановление произвольного контроллера домена после фатального сбоя

Служба каталогов использует единую распределенную базу данных, которая хранит сведения обо всех сетевых ресурсах домена. Каждый контроллер домена работает с локальной копией этой базы данных. Синхронизацию изменений между такими локальными копиями обеспечивает механизм репликации. При выполнении на существующем контроллере домена команды **`samba-tool domain join DC`** локальная копия базы данных полностью перезаписывается актуальной копией распределенной базы данных (происходит процесс «повторного ввода» контроллера в домен).

Возможны ситуации, когда в работе отдельного контроллера домена возникают неполадки или он полностью выходит из строя, при этом остальная часть домена продолжает функционировать корректно. Например, это может быть вызвано ошибками в нереплицируемой части локальной копии базы данных на контроллере или некорректной репликацией изменений с других контроллеров. То есть ошибки не распространяются по домену через механизм репликации и носят локальный характер.

Алгоритм восстановления контроллера домена под тем же именем, если в результате каких либо технических проблем он пришел в неработоспособное состояние:

1. Вывести контроллер домена из эксплуатации, путём удаления всей информации о нём. Для этого на любом работающем контроллере домена выполнить команду:

   ```
   # samba-tool domain demote --remove-other-dead-server=dc2 -UAdministrator
   ```

   где dc2 — имя (hostname) не функционирующего контроллера домена.

2. На узле, который будет заменой вышедшего из строя контроллера домена, выполнить следующие действия:

   - в файле **/etc/krb5.conf** указать опции **default_realm = TEST.ALT** и **dns_lookup_realm = false**;
   - остановить все зависимые службы:

     ```
     # for service in samba smb nmb krb5kdc slapd bind; do systemctl disable
     $service; systemctl stop $service; done
     ```

   - очистить всю конфигурацию Samba:

     ```
     # rm -f /etc/samba/smb.conf
     # rm -rf /var/lib/samba
     # rm -rf /var/cache/samba
     # mkdir -p /var/lib/samba/sysvol
     ```

   - ввести узел в домен как дополнительный контроллер домена:

     ```
     # samba-tool domain join test.alt DC --dns-backend=SAMBA_INTERNAL
     -Uadministrator --realm=test.alt
     ```

   - запустить samba и обновить dns:

     ```
     # systemctl enable --now samba
     # samba_dnsupdate --use-samba-tool --verbose
     ```

Важно

На других контроллерах домена в выводе команды **samba-tool drs showrepl** в секции неисправного DC некоторое время будет присутствовать сообщение WERR_GEN_FAILURE:

```
…
DC=DomainDnsZones,DC=test,DC=alt
  Default-First-Site-Name\DC2 via RPC
    DSA object GUID: b78f2c9d-5c62-4497-a5e1-4fc85aedf1cb
    Last attempt @ Wed Apr 24 07:51:24 2024 MSK failed, result 31
(WERR_GEN_FAILURE)
    28 consecutive failure(s).
    Last success @ NTTIME(0)

DC=ForestDnsZones,DC=test,DC=alt
  Default-First-Site-Name\DC2 via RPC
    DSA object GUID: b78f2c9d-5c62-4497-a5e1-4fc85aedf1cb
    Last attempt @ Wed Apr 24 07:51:24 2024 MSK failed, result 31
(WERR_GEN_FAILURE)
    28 consecutive failure(s).
    Last success @ NTTIME(0)
…
```

Это нормально, и через некоторое время после полной репликации оно исчезнет. Репликация может занять до нескольких часов.

Глава 43. Роли FSMO

43.1. Семь ролей FSMO

43.2. Просмотр и передача ролей FSMO

FSMO, или Flexible single-master operations (операции с одним исполнителем) — это операции, выполняемые контроллерами домена, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах одного домена или леса доменов. Различные типы FSMO могут выполняться как на одном, так и на нескольких контроллерах домена. Выполнение FSMO сервером называют ролью сервера, а сами сервера — хозяевами операций.

Альт Домен — это центральный репозиторий, в котором хранятся все объекты и соответствующие им атрибуты. Это иерархическая база данных с поддержкой нескольких источников. Большинство операций в Альт Домен можно выполнять на любом контроллере домена. Служба репликации Альт Домен скопирует изменения на остальные контроллеры домена, обеспечив идентичность базы Альт Домен на всех контроллерах одного домена. Один из способов разрешения конфликтов заключается в том, что сохраняются изменения, внесенные последними. Изменения, внесенные остальными контроллерами домена, игнорируются.

Однако существует несколько операций (например, изменение схемы Альт Домен), при которых конфликты недопустимы. В Альт Домен некоторые обновления выполняются на одном специальном контроллере домена, а затем реплицируются на все остальные. Альт Домен использует роли, назначенные контроллерам домена, для этих специальных задач. Так как роль не привязана к одному контроллеру домена, она называется ролью FSMO.

В настоящее время существует семь ролей FSMO с разными областями действия:

- *Эмулятор PDC/PDC Emulator* (один на домен);
- *Хозяин RID/RID Master* (один на домен);

- *Хозяин схемы/Schema Master* (один на лес);
- *Хозяин именования доменов/Domain Naming Master* (один на лес);
- *Хозяин инфраструктуры/Infrastructure Master* (один на домен);
- *Хозяин зоны DNS домена/Domain DNS Zone Master role* (один на домен);
- *Хозяин зоны DNS леса/Forest DNS Zone Master role* (один на лес).

43.1. Семь ролей FSMO

Ниже описаны роли FSMO, их функции и требования к доступности. Эти сведения позволяют определить последствия, когда контроллер домена, владеющий этой ролью, находится в автономном режиме.

43.1.1. Эмулятор PDC

Владелец роли эмулятора PDC отвечает за следующие задачи в домене:

- является сервером точного времени для клиентов в домене. Для аутентификации Kerberos необходима точная синхронизация времени. Эмулятор PDC корневого домена в лесу является по умолчанию сервером точного времени для эмуляторов PDC в дочерних доменах;
- изменения паролей, внесенные другими контроллерами домена в домене, реплицируются преимущественно в эмулятор PDC. В случае недоступности эмулятора PDC информация об изменении пароля всё равно распространится по домену, просто произойдет это несколько медленнее;
- выполняет все функции, предоставляемые PDC в стиле NT4;
- обрабатывает блокировки учетных записей. Сбои аутентификации на любом контроллере домена в домене, вызванные неправильным паролем, перенаправляются в эмулятор PDC до того, как сообщение о сбое из-за неправильного пароля будет передано пользователю. При успешной аутентификации учётной записи сразу после неудачной попытки, о ней уведомляется эмулятор PDC и сбрасывает счетчик неудачных попыток в ноль;
- консоль управления групповыми политиками по умолчанию соединяется с эмулятором PDC, и изменения политик происходят на нем же. Если эмулятор PDC недоступен, то будет нужно указать редактору, к какому контроллеру домена подключиться;
- в больших средах контроллер домена, которому принадлежит роль эмулятора PDC, может иметь высокую загрузку ЦП из-за сквозной аутентификации, смены пароля и синхронизации времени.

На каждый домен приходится один эмулятор PDC.

Этот контроллер домена должен, по возможности, быть доступен всегда, потому что для Kerberos требуется точное время на всех машинах в домене. Если клиенты настроены на использование другого источника времени и в сети нет клиентов до Windows 2000, временное отсутствие может быть менее критичным.

Для поиска эмулятора PDC можно использовать команду **`host`**:

```
# host -t SRV _ldap._tcp.pdc._msdcs.<домен>
```

Например:

```
# host -t SRV _ldap._tcp.pdc._msdcs.test.alt
_ldap._tcp.pdc._msdcs.test.alt has SRV record 0 100 389 dc1.test.alt.
```

43.1.2. Хозяин RID

Владелец роли FSMO хозяина RID отвечает за обработку запросов пула RID от всех DC в домене. Он также отвечает за перемещение объектов в другой домен и удаление их из домена.

Все объекты безопасности, например, учётные записи и группы пользователей/компьютеров имеют уникальный идентификатор безопасности (SID). SID объектов содержит идентификатор безопасности (SID) домена, одинаковый для всех объектов в домене, и относительный идентификатор (RID), уникальный для каждого идентификатора безопасности субъекта безопасности, созданного в домене.

Каждому контроллеру домена в домене выделяется пул относительных идентификаторов RID, которые разрешено назначать созданным субъектам безопасности. По умолчанию это диапазон из 500 уникальных RID для всего домена, назначаемых хозяином RID каждому контроллеру домена. Если объект безопасности создается на контроллере домена, то RID берется из этого пула, что гарантирует его уникальность в домене. Если выделенный пул RID контроллера домена оказывается ниже порогового значения (ниже 50 %), контроллер домена выполняет запрос дополнительных идентификаторов RID к хозяину RID в домене. Хозяин RID в домене отвечает на запрос, извлекая идентификаторы RID из невыделенного пула RID домена и назначая их пулу запрашивающего контроллера домена.

На каждый домен приходится один хозяин RID.

Этот контроллер домена должен быть активен, при создании нового контроллера домена в домене, чтобы назначить ему пул RID. Также хозяин RID должен быть доступен, когда существующие контроллеры домена обновляют свой резервный пул RID.

С другой стороны, если хозяин RID находится в автономном режиме, то на каждом контроллере домена можно создавать новые объекты безопасности, пока локальный пул RID не станет пустым. Если пулы RID на всех контроллерах домена опустеют, создание дополнительных объектов станет невозможно. Пока хозяин RID домена находится в автономном режиме невозможно присоединиться к дополнительным контроллерам домена,

43.1.3. Хозяин схемы

Контроллер домена, обладающий ролью хозяина схемы, является единственным в лесу AD, кому разрешено обновлять схему каталога. После завершения обновления изменения реплицируются на все другие контроллеры домена в лесу.

Схема каталога (контекст именования схемы) или LDAP://cn=schema,cn=configuration,dc=<домен> существует на всех контроллерах домена. Обновления выполняются только на хозяине схемы. После завершения обновления схема реплицируется из хозяина схемы во все остальные контроллеры домена каталога.

В каждом лесу есть один хозяин схемы.

Контроллер домена, обладающий ролью хозяина схемы, должен быть подключен к сети при выполнении обновлений схемы.

43.1.4. Хозяин именования доменов

Хозяин именования доменов отвечает за внесение изменений в пространство доменных имен в масштабах леса. Только этот контроллер домена может добавлять или удалять домены, доверительные отношения с внешними каталогами и разделами приложений в/из леса.

Информация об именах доменов хранится в разделе «Контекст именования конфигурации» в CN=Partitions,CN=Configuration,DC=<домен>. Этот раздел существует на всех контроллерах домена, но обновляется только на хозяине именования доменов.

На каждый лес приходится один хозяин именования доменов.

Контроллер домена, обладающий ролью хозяина именования доменов, должен быть подключен к сети, когда устанавливаются доверительные отношения с внешними каталогами и доменами, а разделы приложений добавляются или удаляются из леса.

43.1.5. Хозяин инфраструктуры

Контроллер домена, которому принадлежит роль хозяина инфраструктуры, отвечает за обновление идентификатора безопасности (SID) и различающегося имени объекта в ссылке на междоменный объект. Это используется, например, если пользователь из одного домена добавляется в группу безопасности другого домена.

На каждый домен приходится один хозяин инфраструктуры.

Если контроллер домена, обладающий ролью хозяина инфраструктуры, временно отключен, междоменные изменения невозможны.

43.1.6. Хозяин зоны DNS домена

Контроллер домена, которому принадлежит роль хозяина зоны DNS домена, отвечает за координацию добавления или удаления любых зон DNS, интегрированных в AD, на контроллерах домена с DNS-серверами, на которых размещен домен.

На каждый домен приходится один хозяин зоны DNS домена.

43.1.7. Хозяин зоны DNS леса

Контроллер домена, которому принадлежит роль хозяина зоны DNS леса, отвечает за координацию добавления или удаления записей всего леса на DNS-серверах, на которых размещена зона DNS верхнего уровня. Эти записи содержат имена серверов глобального каталога (GC).

На каждый домен приходится один хозяин зоны DNS леса.

43.2. Просмотр и передача ролей FSMO

По возможности следует передавать роли FSMO штатным образом и не использовать принудительную передачу (захват роли). Для штатной передачи роли требуется, чтобы контроллер домена, которому в данный момент принадлежит роль, работал и был подключен к сети. В этом случае при передаче роли старый контроллер домена узнает, что он больше не владеет ролью.

Если контроллер домена сломан (например, из-за аппаратного дефекта) и больше никогда не будет возвращён в сеть, можно использовать принудительную передачу (захватить роль на оставшемся контроллере домена). Если старый контроллер домена будет снова подключён к сети, это вызовет конфликты и приведет к неконсистентному AD (т.к. старый контроллер домена не заметит изменения и по-прежнему будет считать себя владельцем роли).

Роли FSMO можно передавать с помощью инструмента командной строки **samba-tool** или в модуле удалённого управления базой данных конфигурации (ADMC) (подробнее см. Модуль удаленного управления базой данных конфигурации (ADMC)).

43.2.1. ADMC

См. раздел Прсмотр и передача ролей FSMO

43.2.2. Инструмент samba-tool

43.2.2.1. Просмотр текущих владельцев

Операция просмотра списка владельцев ролей FSMO доступна всем пользователям.

Просмотр текущего состояния (команда выполняется на контроллере домена):

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

43.2.2.2. Передача роли

Операция передачи роли FSMO доступна пользователям со следующими полномочиями:

- передача ролей уровня леса — администраторы леса (члены группы Enterprise Admins);
- передача ролей уровня домена — администраторы домена (члены группы Domain Admins);
- передача роли владельца схемы каталога — администраторы схемы (члены группы Schema Admins).

Для штатной передачи роли необходимо на контроллере домена, который должен стать новым владельцем роли, выполнить команду:

```
# samba-tool fsmo transfer --role=<роль>
```

Список возможных ролей:

- rid — хозяин RID (RidAllocationMasterRole);
- pdc — эмулятор PDC (PdcEmulationMasterRole);
- infrastructure — хозяин инфраструктуры (InfrastructureMasterRole);
- schema — хозяин схемы (SchemaMasterRole);
- naming — хозяин именования доменов (DomainNamingMasterRole);
- domaindns — хозяин зоны DNS домена (DomainDnsZonesMasterRole);
- forestdns — хозяин зоны DNS домена (ForestDnsZonesMasterRole);
- all — все роли.

Пример штатной передачи роли (команда выполняется на DC2):

```
# samba-tool fsmo transfer --role=infrastructure
FSMO transfer of 'infrastructure' role successful
```

Проверка:

```
# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

43.2.2.3. Захват роли FSMO

Операция захвата роли FSMO доступна пользователям со следующими полномочиями:

- захват ролей уровня леса — администраторы леса (члены группы Enterprise Admins);
- захват ролей уровня домена — администраторы домена (члены группы Domain Admins);
- захват роли владельца схемы каталога — администраторы схемы (члены группы Schema Admins).

Для принудительной передачи роли (если контроллер домена вышел из строя) необходимо на контроллере домена, который должен стать новым владельцем роли, выполнить команду:

```
# samba-tool fsmo seize --role=<роль>
```

Список возможных ролей:

- rid — хозяин RID (RidAllocationMasterRole);
- pdc — эмулятор PDC (PdcEmulationMasterRole);
- infrastructure — хозяин инфраструктуры (InfrastructureMasterRole);
- schema — хозяин схемы (SchemaMasterRole);
- naming — хозяин именования доменов (DomainNamingMasterRole);
- domaindns — хозяин зоны DNS домена (DomainDnsZonesMasterRole);
- forestdns — хозяин зоны DNS домена (ForestDnsZonesMasterRole);
- all — все роли.

Важно

Если роль была передана принудительно, старый контроллер домена больше никогда не должен подключаться к сети!

Примечание

При передаче ролей *domaindns* и *forestdns* необходимо предоставить аутентификацию.

Примечание

В ранних версиях **samba-tool** была ошибка, не позволявшая захватить роль *naming*:

```
# samba-tool fsmo seize --role=naming
ERROR (ldb): uncaught exception – Failed FSMO transfer: WERR_BADFILE
```

В этом случае необходимо использовать «ещё более принудительную передачу»:

```
# samba-tool fsmo seize --force --role=naming
```

Глава 44. Настройка Samba для привязки к определённым интерфейсам

Если на сервере настроено несколько сетевых интерфейсов, можно настроить Samba для привязки только к определенным интерфейсам.

Например, для того чтобы привязать все службы Samba к устройству enp0s3 и loopback (lo) необходимо добавить следующие параметры в раздел ***[global]*** файла **smb.conf**:

```
bind interfaces only = yes
interfaces = lo enp0s3
```

и перезапустить службу Samba:

```
# systemctl restart samba.service
```

В параметре **`interfaces`** вместо имён интерфейсов можно указывать IP-адреса.

Примечание

Некоторые утилиты подключаются к петлевому IP-адресу, если имя хоста не указано. Поэтому всегда нужно указывать Samba прослушивать петлевые (lo) устройства.

Глава 45. Создание keytab-файла

45.1. Назначение и формат SPN

45.2. Создание SPN и генерация keytab с помощью samba-tool

45.1. Назначение и формат SPN

SPN (Service Principal Name) — уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account). Это позволяет клиентским приложением аутентифицироваться в роли сервиса даже не зная имени пользователя.

До того как аутентификация Kerberos сможет использовать SPN для аутентификации сервиса, SPN должен быть привязан к учётной записи, которая будет использоваться для входа. К учётной записи может быть привязано несколько SPN. SPN может быть привязан только к одной учетной записи. Если учетная запись, привязанная к SPN, изменяется, то необходимо заново выполнить привязку.

Можно иметь столько SPN, сколько необходимо. Когда клиент хочет воспользоваться сервисом, он находит экземпляр сервиса и составляет SPN для этого экземпляра, далее использует этот SPN для аутентификации. Если клиент не может найти правильный SPN, он не сможет запросить билет службы.

SPN состоит из двух обязательных элементов и двух дополнительных элементов:

```
<service class>/<host>:<port>/<service name>
```

Элементы SPN:

- service class (обязательный элемент) — строка, указывающая на класс, к которому относится сервис (например: HTTP, www, ldap и т. п.);
- host (обязательный элемент) — имя компьютера, на котором работает сервис; это может быть полное доменное имя (FQDN) или NetBIOS-имя;

- port — номер порта; может использоваться в том случае, если несколько экземпляров сервиса одного класса работают на одном узле; не требуется указывать, если экземпляр сервиса один и работает на стандартном для своего класса порту;

- service name — имя реплицируемого сервиса, которое позволяет идентифицировать предоставляемые сервисом данные или обслуживаемый сервисом домен; в качестве имени могут использоваться DN-имя или objectGUID объекта службы каталогов, DNS-имя домена (если сервис реализует определенную службу на уровне всего домена), DNS-имя записи SRV или MX.

Примечание

Если клиент не может найти правильный SPN, он не сможет запросить билет службы. Поэтому формирование SPN было глобально нормализовано:

- для файлового сервера могут использоваться следующие SPN (их можно добавить столько, сколько нужно):
  - HOST/fileserver.test.alt
  - HOST/fileserver
  - HOST/fileserver@TEST.ALT
  - CIFS/fileserver.test.alt
- для веб-сервера (подробнее см. Настройка аутентификации для веб-сервера):
  - HTTP/web.test.alt
- для прокси-сервера:
  - HTTP/proxy.test.alt
- на практике можно сопоставить SPN с IP-адресом, но это не рекомендуется:
  - HOST/192.168.0.129@TEST.ALT

Keytab-файл — это файл содержащий пары Kerberos принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля. Если пароль принципала изменится, то keytab-файл необходимо будет сгенерировать заново.

Важно

Каждый кто имеет разрешения на чтения keytab-файла может воспользоваться любыми ключами в нем. Чтобы предотвратить нежелательное использование, необходимо ограничивать права доступа при создании keytab-файла.

45.2. Создание SPN и генерация keytab с помощью samba-tool

Добавить имена SPN для пользователя можно с помощью команды **samba-tool spn add**:

```
# samba-tool spn add host/fdqn@KerberosRealm <sAMAccount name>
```

После добавления SPN можно сгенерировать keytab, выполнив команду:

```
# samba-tool domain exportkeytab <имя>.keytab --principal=[<sAMAccount name> |
<SPN>]
```

В результате выполнения этой команды будет создан keytab-файл **<имя>.keytab**, содержащий UPN или SPN, в зависимости от того, что было указано в параметре ***--principal***.

Получить дополнительную информацию можно на справочной странице samba-tool (8) (**man samba-tool**).

Примечание

В команде нужно использовать или <sAMAccount name> или <SPN>, но не оба параметра сразу.

Пример:

- привязать к пользователю SPN:

```
# samba-tool spn add HTTP/test.alt webauth
```

- создать keytab:

```
# samba-tool domain exportkeytab /tmp/web.keytab --principal=HTTP/test.alt
Export one principal to /tmp/keytab
```

- проверка:

```
# klist -ke /tmp/web.keytab
Keytab name: FILE:/tmp/web.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 HTTP/test.alt@TEST.ALT (DEPRECATED:arcfour-hmac)
```

Можно также проверить авторизацию в домене по имени SPN с помощью keytab-файла. Для этого на контроллере домена получить билет Kerberos:

```
# kinit administrator@TEST.ALT
Password for administrator@TEST.ALT:
```

И выполнить команду:

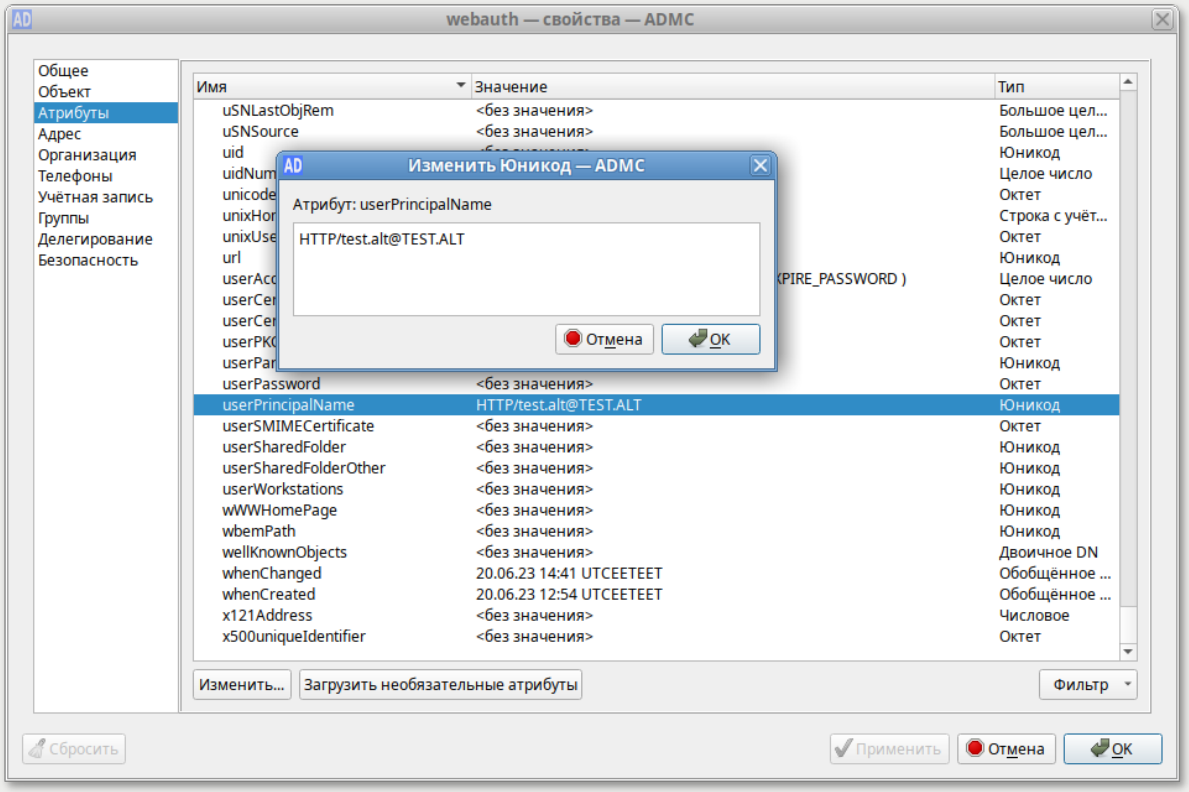
```
# kinit -5 -V -k -t /tmp/web.keytab HTTP/test.alt
Using default cache: /tmp/krb5cc_0
Using principal: HTTP/test.alt@TEST.ALT
Using keytab: /tmp/web.keytab
Authenticated to Kerberos v5
```

Примечание

Если при проверке авторизации возникает ошибка:

```
kinit: Client not found in Kerberos database while getting initial
credentials
```

Необходимо в ADMC (см. Модуль удаленного управления базой данных конфигурации (ADMC)) изменить для пользователя webauth значение параметра ***userPrincipalName*** на значение **servicePrincipalName + REALM** (в данном примере нужно поменять webauth на HTTP/test.alt@TEST.ALT):



И заново экспортировать keytab-файл.

Для получения списка идентификаторов SPN, привязанных к учетной записи, используется команда:

```
# samba-tool spn list <user> [options]
```

В качестве аргумента передается имя учетной записи SAM (значение атрибута sAMaccountName).

Команда удаления идентификатора SPN, привязанного к учетной записи пользователя:

```
# samba-tool spn delete <name> <user> [options]
```

В качестве аргументов передаются значение SPN (name) и имя учетной записи SAM (значение атрибута sAMaccountName).

Глава 46. Настройка DHCP-сервера для обновления DNS-записей

46.1. Настройка DHCP-сервера

46.2. Настройка переключения DHCP

В этом разделе описана настройка DHCP-сервера для автоматического обновления DNS-записей Samba в домене.

Предварительные условия:

- DHCP-сервер устанавливается на одном из контроллеров домена;
- созданы все необходимые обратные зоны;
- если используется Bind9, Bind9_dlz должен быть установлен и должен работать на контроллере домена, на котором выполняется данная настройка.

Описание имеющейся сети:

- Realm: TEST.ALT
- Подсеть: 192.168.0.0
- Маска сети: 255.255.255.0
- Широковещательный адрес: 192.168.0.255
- Шлюз по умолчанию: 192.168.0.1
- Имя домена: test.alt
- DNS-сервера: 192.168.0.132, 192.168.0.133
- Netbios-сервера: 192.168.0.132, 192.168.0.133
- Ntp-сервера: 192.168.0.132, 192.168.0.133
- Диапазон арендуемых IP-адресов: 192.168.0.150 192.168.0.200

46.1. Настройка DHCP-сервера

Все действия, указанные ниже, выполняются на узле dc1.test.alt (192.168.0.132), если не указано иное.

Создать пользователя (в примере dhcpduser), от имени которого будут производится обновления DNS-записей:

```
# samba-tool user create dhcpduser \
  --description="Пользователь для обновления TSIG-GSSAPI DNS через DHCP-сервер" \
  --random-password
User 'dhcpduser' added successfully
```

Установить срок действия пароля (бессрочный) для созданного пользователя и добавить его в группу DnsAdmins:

```
# samba-tool user setexpiry dhcpduser --noexpiry
Expiry for user 'dhcpduser' disabled.
# samba-tool group addmembers DnsAdmins dhcpduser
Added members to group DnsAdmins
```

Экспортировать файл keytab, чтобы пользователь мог аутентифицироваться через Kerberos:

```
# samba-tool domain exportkeytab --principal=dhcpduser@TEST.ALT /etc/dhcp/
dhcpduser.keytab
Export one principal to /etc/dhcp/dhcpduser.keytab
# chown dhcpd:dhcp /etc/dhcp/dhcpduser.keytab
# chmod 400 /etc/dhcp/dhcpduser.keytab
```

Примечание

Параметр *dhcpd:dhcp* указывает пользователя и группу, от имени которых работает DHCP-сервер.

Создать скрипт, который будет выполнять обновления (файл **/usr/local/bin/dhcp-dyndns.sh**):

```
#!/bin/bash
#
# This script is for secure DDNS updates on Samba,
# it can also add the 'macAddress' to the Computers object.
#
# Version: 0.9.6
#

#############################################################################
#                                                                           #
#    You can optionally add the 'macAddress' to the Computers object.       #
#    Add 'dhcpduser' to the 'Domain Admins' group if used                   #
#    Change the next line to 'yes' to make this happen                      #
Add_macAddress='no'
#                                                                           #
#############################################################################

keytab=/etc/dhcp/dhcpduser.keytab

usage()
{
  cat <<-EOF
  USAGE:
    $(basename "$0") add ip-address dhcid|mac-address hostname
    $(basename "$0") delete ip-address dhcid|mac-address
  EOF
}

_KERBEROS()
{
  # get current time as a number
  test=$(date +%d'-'%m'-'%y' '%H':'%M':'%S)
  # Note: there have been problems with this
  # check that 'date' returns something like

  # Check for valid kerberos ticket
  #logger "${test} [dyndns] : Running check for valid kerberos ticket"
  klist -c "${KRB5CCNAME}" -s
  ret="$?"
  if [ $ret -ne 0 ]
```

```
  then
    logger "${test} [dyndns] : Getting new ticket, old one has expired"
    kinit -F -k -t $keytab "${SETPRINCIPAL}"
    ret="$?"
    if [ $ret -ne 0 ]
    then
      logger "${test} [dyndns] : dhcpd kinit for dynamic DNS failed"
      exit 1
    fi
  fi
}

rev_zone_info()
{
  local RevZone="$1"
  local IP="$2"
  local rzoneip
  rzoneip="${RevZone%.in-addr.arpa}"
  local rzonenum
  rzonenum=$(echo "$rzoneip" |  tr '.' '\n')
  declare -a words
  for n in $rzonenum
  do
    words+=("$n")
  done
  local numwords="${#words[@]}"

  unset ZoneIP
  unset RZIP
  unset IP2add

  case "$numwords" in
    1)
      # single ip rev zone '192'
      ZoneIP=$(echo "${IP}" | awk -F '.' '{print $1}')
      RZIP="${rzoneip}"
      IP2add=$(echo "${IP}" | awk -F '.' '{print $4"."$3"."$2}')
      ;;
    2)
      # double ip rev zone '168.192'
      ZoneIP=$(echo "${IP}" | awk -F '.' '{print $1"."$2}')
      RZIP=$(echo "${rzoneip}" | awk -F '.' '{print $2"."$1}')
      IP2add=$(echo "${IP}" | awk -F '.' '{print $4"."$3}')
      ;;
    3)
      # triple ip rev zone '0.168.192'
      ZoneIP=$(echo "${IP}" | awk -F '.' '{print $1"."$2"."$3}')
      RZIP=$(echo "${rzoneip}" | awk -F '.' '{print $3"."$2"."$1}')
      IP2add=$(echo "${IP}" | awk -F '.' '{print $4}')
      ;;
    *)
      # should never happen
      exit 1
      ;;
  esac
}

BINDIR=$(samba -b | grep 'BINDIR' | grep -v 'SBINDIR' | awk '{print $NF}')
[[ -z $BINDIR ]] && printf "Cannot find the 'samba' binary, is it installed ?\
```

```
\nOr is your path set correctly ?\\n"
WBINFO="$BINDIR/wbinfo"

SAMBATOOL=$(command -v samba-tool)
[[ -z $SAMBATOOL ]] && printf "Cannot find the 'samba-tool' binary, is it
installed ?\\nOr is your path set correctly ?\\n"

MINVER=$($SAMBATOOL -V | grep -o '[0-9]*' | tr '\n' ' ' | awk '{print $2}')
if [ "$MINVER" -gt '14' ]
then
  KTYPE="--use-kerberos=required"
else
  KTYPE="-k yes"
fi

# DHCP Server hostname
Server=$(hostname -s)

# DNS domain
domain=$(hostname -d)
if [ -z "${domain}" ]
then
  logger "Cannot obtain domain name, is DNS set up correctly?"
  logger "Cannot continue... Exiting."
  exit 1
fi

# Samba realm
REALM="${domain^^}"

# krbcc ticket cache
export KRB5CCNAME="/tmp/dhcp-dyndns.cc"

# Kerberos principal
SETPRINCIPAL="dhcpduser@${REALM}"
# Kerberos keytab as above
# krbcc ticket cache : /tmp/dhcp-dyndns.cc
TESTUSER="$($WBINFO -u | grep 'dhcpduser')"
if [ -z "${TESTUSER}" ]
then
  logger "No AD dhcp user exists, need to create it first.. exiting."
  logger "you can do this by typing the following commands"
  logger "kinit Administrator@${REALM}"
  logger "$SAMBATOOL user create dhcpduser --random-password --
description='Unprivileged user for DNS updates via DHCP server'"
  logger "$SAMBATOOL user setexpiry dhcpduser --noexpiry"
  logger "$SAMBATOOL group addmembers DnsAdmins dhcpduser"
  exit 1
fi

# Check for Kerberos keytab
if [ ! -f "$keytab" ]
then
  logger "Required keytab $keytab not found, it needs to be created."
  logger "Use the following commands as root"
  logger "$SAMBATOOL domain exportkeytab --principal=${SETPRINCIPAL} $keytab"
  logger "chown XXXX:XXXX $keytab"
  logger "Replace 'XXXX:XXXX' with the user & group that dhcpd runs as on your
distro"
```

```
  logger "chmod 400 $keytab"
  exit 1
fi

# Variables supplied by dhcpd.conf
action="$1"
ip="$2"
DHCID="$3"
name="${4%%.*}"

# Exit if no ip address
if [ -z "${ip}" ]
then
  usage
  exit 1
fi

# Exit if no computer name supplied, unless the action is 'delete'
if [ -z "${name}" ]
then
  if [ "${action}" = "delete" ]
  then
    name=$(host -t PTR "${ip}" | awk '{print $NF}' | awk -F '.' '{print $1}')
  else
    usage
    exit 1
  fi
fi

# exit if name contains a space
case ${name} in
  *\ * )
    logger "Invalid hostname '${name}' ...Exiting"
    exit
    ;;
esac

# if you want computers with a hostname that starts with 'dhcp' in AD
# comment the following block of code.
if [[ $name == dhcp* ]]
then
  logger "not updating DNS record in AD, invalid name"
  exit 0
fi

## update ##
case "${action}" in
  add)
    _KERBEROS
    count=0
    # does host have an existing 'A' record ?
    mapfile -t A_REC < <($SAMBATOOL dns query "${Server}" "${domain}" "${name}" A
"$KTYPE" 2>/dev/null | grep 'A:' | awk '{print $2}')
    if [ "${#A_REC[@]}" -eq 0 ]
    then
      # no A record to delete
      result1=0
      $SAMBATOOL dns add "${Server}" "${domain}" "${name}" A "${ip}" "$KTYPE"
      result2="$?"
```

```
    elif [ "${#A_REC[@]}" -gt 1 ]
    then
      for i in "${A_REC[@]}"
      do
        $SAMBATOOL dns delete "${Server}" "${domain}" "${name}" A "${i}" "$KTYPE"
      done
      # all A records deleted
      result1=0
      $SAMBATOOL dns add "${Server}" "${domain}" "${name}" A "${ip}" "$KTYPE"
      result2="$?"
    elif [ "${#A_REC[@]}" -eq 1 ]
    then
      # turn array into a variable
      VAR_A_REC="${A_REC[*]}"
      if [ "$VAR_A_REC" = "${ip}" ]
      then
        # Correct A record exists, do nothing
        logger "Correct 'A' record exists, not updating."
        result1=0
        result2=0
        count=$((count+1))
      elif [ "$VAR_A_REC" != "${ip}" ]
      then
        # Wrong A record exists
        logger "'A' record changed, updating record."
        $SAMBATOOL dns delete "${Server}" "${domain}" "${name}" A "${VAR_A_REC}"
"$KTYPE"
        result1="$?"
        $SAMBATOOL dns add "${Server}" "${domain}" "${name}" A "${ip}" "$KTYPE"
        result2="$?"
      fi
    fi

    # get existing reverse zones (if any)
    ReverseZones=$($SAMBATOOL dns zonelist "${Server}" "$KTYPE" --reverse | grep
'pszZoneName' | awk '{print $NF}')
    if [ -z "$ReverseZones" ]; then
      logger "No reverse zone found, not updating"
      result3='0'
      result4='0'
      count=$((count+1))
    else
      for revzone in $ReverseZones
      do
        rev_zone_info "$revzone" "${ip}"
        if [[ ${ip} = $ZoneIP* ]] && [ "$ZoneIP" = "$RZIP" ]
        then
          # does host have an existing 'PTR' record ?
          PTR_REC=$($SAMBATOOL dns query "${Server}" "${revzone}" "${IP2add}" PTR
"$KTYPE" 2>/dev/null | grep 'PTR:' | awk '{print $2}' | awk -F '.' '{print $1}')
          if [[ -z $PTR_REC ]]
          then
            # no PTR record to delete
            result3=0
            $SAMBATOOL dns add "${Server}" "${revzone}" "${IP2add}" PTR "$
{name}"."${domain}" "$KTYPE"
            result4="$?"
            break
          elif [ "$PTR_REC" = "${name}" ]
```

```
          then
            # Correct PTR record exists, do nothing
            logger "Correct 'PTR' record exists, not updating."
            result3=0
            result4=0
            count=$((count+1))
            break
          elif [ "$PTR_REC" != "${name}" ]
          then
            # Wrong PTR record exists
            # points to wrong host
            logger "'PTR' record changed, updating record."
            $SAMBATOOL dns delete "${Server}" "${revzone}" "${IP2add}" PTR "$
{PTR_REC}"."${domain}" "$KTYPE"
            result3="$?"
            $SAMBATOOL dns add "${Server}" "${revzone}" "${IP2add}" PTR "$
{name}"."${domain}" "$KTYPE"
            result4="$?"
            break
          fi
        else
          continue
        fi
      done
    fi
    ;;
  delete)
    _KERBEROS

    count=0
    $SAMBATOOL dns delete "${Server}" "${domain}" "${name}" A "${ip}" "$KTYPE"
    result1="$?"
    # get existing reverse zones (if any)
    ReverseZones=$($SAMBATOOL dns zonelist "${Server}" --reverse "$KTYPE" | grep
'pszZoneName' | awk '{print $NF}')
    if [ -z "$ReverseZones" ]
    then
      logger "No reverse zone found, not updating"
      result2='0'
      count=$((count+1))
    else
      for revzone in $ReverseZones
      do
        rev_zone_info "$revzone" "${ip}"
        if [[ ${ip} = $ZoneIP* ]] && [ "$ZoneIP" = "$RZIP" ]
        then
          host -t PTR "${ip}" > /dev/null 2>&1
          ret="$?"
          if [ $ret -eq 0 ]
          then
            $SAMBATOOL dns delete "${Server}" "${revzone}" "${IP2add}" PTR "$
{name}"."${domain}" "$KTYPE"
            result2="$?"
          else
            result2='0'
            count=$((count+1))
          fi
          break
        else
```

```
          continue
        fi
      done
    fi
    result3='0'
    result4='0'
    ;;
        *)
    logger "Invalid action specified"
    exit 103
  ;;
esac

result="${result1}:${result2}:${result3}:${result4}"

if [ "$count" -eq 0 ]
then
  if [ "${result}" != "0:0:0:0" ]
  then
    logger "DHCP-DNS $action failed: ${result}"
    exit 1
  else
    logger "DHCP-DNS $action succeeded"
  fi
fi

if [ "$Add_macAddress" != 'no' ]
then
  if [ -n "$DHCID" ]
  then
    Computer_Object=$(ldbsearch "$KTYPE" -H ldap://"$Server"
"(&(objectclass=computer)(objectclass=ieee802Device)(cn=$name))" | grep -v '#' |
grep -v 'ref:')
    if [ -z "$Computer_Object" ]
    then
      # Computer object not found with the 'ieee802Device' objectclass, does the
computer actually exist, it should.
      Computer_Object=$(ldbsearch "$KTYPE" -H ldap://"$Server"
"(&(objectclass=computer)(cn=$name))" | grep -v '#' | grep -v 'ref:')
      if [ -z "$Computer_Object" ]
      then
        logger "Computer '$name' not found. Exiting."
        exit 68
      else
        DN=$(echo "$Computer_Object" | grep 'dn:')
        objldif="$DN
changetype: modify
add: objectclass
objectclass: ieee802Device"

        attrldif="$DN
changetype: modify
add: macAddress
macAddress: $DHCID"

        # add the ldif
        echo "$objldif" | ldbmodify "$KTYPE" -H ldap://"$Server"
        ret="$?"
        if [ $ret -ne 0 ]
```

```
        then
          logger "Error modifying Computer objectclass $name in AD."
          exit "${ret}"
        fi
        sleep 2
        echo "$attrldif" | ldbmodify "$KTYPE" -H ldap://"$Server"
        ret="$?"
        if [ "$ret" -ne 0 ]; then
          logger "Error modifying Computer attribute $name in AD."
          exit "${ret}"
        fi
        unset objldif
        unset attrldif
        logger "Successfully modified Computer $name in AD"
      fi
  else
    DN=$(echo "$Computer_Object" | grep 'dn:')
    attrldif="$DN
changetype: modify
replace: macAddress
macAddress: $DHCID"

    echo "$attrldif" | ldbmodify "$KTYPE" -H ldap://"$Server"
    ret="$?"
    if [ "$ret" -ne 0 ]
    then
      logger "Error modifying Computer attribute $name in AD."
      exit "${ret}"
    fi
      unset attrldif
      logger "Successfully modified Computer $name in AD"
    fi
  fi
fi

exit 0
```

Примечание

Если нужно сохранять MAC-адреса узлов в AD, следует заменить строку:

```
Add_macAddress='no'
```

на:

```
Add_macAddress='yes'
```

Следует обратить внимание, что необходимо предоставить права администратора домена пользователю обновления DNS.

Установить права для скрипта:

```
# chmod 755 /usr/local/bin/dhcp-dyndns.sh
```

Создать резервную копию исходного файла конфигурации:

```
# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.orig
```

Внести изменения в файл конфигурации **/etc/dhcp/dhcpd.conf**:

```
authoritative;
ddns-update-style none;

subnet 192.168.0.0 netmask 255.255.255.0 {
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.0.255;
        option time-offset 0;
        option routers 192.168.0.1;
        option domain-name-servers 192.168.0.132, 192.168.0.133;
        option ntp-servers 192.168.0.132, 192.168.0.133;
        option domain-name "test.alt";
        default-lease-time 3600;
        pool {
             max-lease-time 1800; #30 минут
             range 192.168.0.150 192.168.0.200;
             }
}

on commit {
set noname = concat("dhcp-", binary-to-ascii(10, 8, "-", leased-address));
set ClientIP = binary-to-ascii(10, 8, ".", leased-address);
set ClientDHCID = concat (
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,1,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,2,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,3,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,4,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,5,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,6,1))),2)
);
set ClientName = pick-first-value(option host-name, config-option host-name,
client-name, noname);
log(concat("Commit: IP: ", ClientIP, " DHCID: ", ClientDHCID, " Name: ",
ClientName));
execute("/usr/local/bin/dhcp-dyndns.sh", "add", ClientIP, ClientDHCID,
ClientName);
}

on release {
set ClientIP = binary-to-ascii(10, 8, ".", leased-address);
set ClientDHCID = concat (
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,1,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,2,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,3,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,4,1))),2),
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,5,1))),2),
```

```
":",
suffix (concat ("0", binary-to-ascii (16, 8, "", substring(hardware,6,1))),2)
);
log(concat("Release: IP: ", ClientIP));
execute("/usr/local/bin/dhcp-dyndns.sh", "delete", ClientIP, ClientDHCID);
}

on expiry {
set ClientIP = binary-to-ascii(10, 8, ".", leased-address);
# cannot get a ClientMac here, apparently this only works when actually receiving
a packet
log(concat("Expired: IP: ", ClientIP));
# cannot get a ClientName here, for some reason that always fails
# however the dhcp update script will obtain the short hostname.
execute("/usr/local/bin/dhcp-dyndns.sh", "delete", ClientIP, "", "0");
}
```

Отключить chroot для DHCP-сервера:

```
# control dhcpd-chroot disabled
```

Перезапустить DHCP-сервер:

```
# systemctl restart dhcpd
```

Теперь если на клиенте изменить сетевую конфигурацию со статического IP-адреса, на получение IP-адреса от DHCP-сервера, в журнале на сервере можно будет увидеть следующее:

```
dhcpd[7817]: DHCPDISCOVER from 08:00:27:99:a6:1f via enp0s3
dhcpd[7817]: DHCPOFFER on 192.168.0.150 to 08:00:27:99:a6:1f (host-199) via
enp0s3
dhcpd[7817]: Commit: IP: 192.168.0.150 DHCID: 08:00:27:99:a6:1f Name: host-199
dhcpd[7817]: execute_statement argv[0] = /usr/local/bin/dhcp-dyndns.sh
dhcpd[7817]: execute_statement argv[1] = add
dhcpd[7817]: execute_statement argv[2] = 192.168.0.150
dhcpd[7817]: execute_statement argv[3] = 08:00:27:99:a6:1f
dhcpd[7817]: execute_statement argv[4] = host-199
dhcpd[8228]: 17-07-24 08:55:31 [dyndns] : Getting new ticket, old one has expired
dhcpd[8236]: 'A' record changed, updating record.
dhcpd[8237]: Record deleted successfully
dhcpd[8240]: Record added successfully
dhcpd[8268]: Record added successfully
dhcpd[8271]: DHCP-DNS add succeeded
dhcpd[7817]: DHCPREQUEST for 192.168.0.125 (192.168.0.132) from 08:00:27:99:a6:1f
(host-199) via enp0s3
dhcpd[7817]: DHCPACK on 192.168.0.150 to 08:00:27:99:a6:1f (host-199) via enp0s3
```

Клиента можно найти как в прямой, так и в обратной зонах:

```
# host host-199
host-199.test.alt has address 192.168.0.150
host-199.test.alt has IPv6 address fd47:d11e:43c1:0:a00:27ff:fe99:a61f
# host 192.168.0.150
150.0.168.192.in-addr.arpa domain name pointer host-199.test.alt.
```

46.2. Настройка переключения DHCP

Для обеспечения отказоустойчивости, следует на втором контроллере домена также поднять DHCP-сервер.

Связь между двумя DHCP-серверами осуществляется через интерфейс прикладного программирования управления объектами (OMAPI). Этот API контролирует работу протокола переключения DHCP. Этот API будет настроен на следующих шагах.

На ведущем (master) DHCP-сервере необходимо сгенерировать случайный ключ OMAPI:

```
# tsig-keygen -a hmac-md5 omapi_key
key "omapi_key" {
    algorithm hmac-md5;
    secret "KKkAspinSr/nXYXhAv7CTQ==";
};
```

Как на ведущем, так и на ведомом устройстве должен быть настроен специальный раздел, путём добавления следующих строк в файл **/etc/dhcp/dhcpd.conf**:

```
omapi-port 7911;
omapi-key omapi_key;
key "omapi_key" {
    algorithm hmac-md5;
    secret "Секретный_ключ";
};
```

«Секретный_ключ» следует заменить на ключ, полученный на предыдущем шаге.

Для настройки аварийного переключения на первом сервере в файл **/etc/dhcp/dhcpd.conf** перед разделом subnet следует добавить строки:

```
omapi-port 7911;
omapi-key omapi_key;
key "omapi_key" {
    algorithm hmac-md5;
    secret "KKkAspinSr/nXYXhAv7CTQ==";
};

failover peer "dhcp-failover" {
  primary;
  address dc1.test.alt; # Полное DNS-имя основного DHCP-сервера
  port 847;
  peer address dc2.test.alt; # Полное DNS-имя имя резервного DHCP-сервера
  peer port 647;
  max-response-delay 60;
  max-unacked-updates 10;
  mclt 3600;
  split 128;
  load balance max seconds 3;
}
```

И добавить ссылку на подсеть/пул, которые будут выполнять аварийное переключение в раздел pool:

```
pool {
    failover peer "dhcp-failover"; # Add for failover
    max-lease-time 1800; #30 минут
    range 192.168.0.150 192.168.0.200;
    }
```

На втором DC выполнить следующие действия:

1. Скопировать скрипт и keytab-файл с первого DC на второй:

```
# scp dc1:/usr/local/bin/dhcp-dyndns.sh /usr/local/bin/
# scp dc1:/etc/dhcp/dhcpduser.keytab /etc/dhcp/
# chown dhcpd:dhcp /etc/dhcp/dhcpduser.keytab
```

Примечание

Для возможности копирования файлов должно быть настроено беспарольное взаимодействие между rootами контроллеров домена (см. Настройка беспарольного доступа по ssh).

2. Создать резервную копию исходного файла конфигурации DHCP-сервера и скопировать файл конфигурации с первого сервера:

```
# cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.orig
# scp dc1:/etc/dhcp/dhcpd.conf /etc/dhcp/
```

3. В файле **/etc/dhcp/dhcpd.conf** внести изменения в раздел «failover peer "dhcp-failover"»:

```
failover peer "dhcp-failover" {
  secondary;
  address dc2.test.alt; # Полное DNS-имя имя резервного DHCP-сервера
  port 647;
  peer address dc1.test.alt; # Полное DNS-имя основного DHCP-сервера
  peer port 847;
  max-response-delay 60;
  max-unacked-updates 10;
  load balance max seconds 3;
}
```

4. Отключить chroot для DHCP-сервера:

```
# control dhcpd-chroot disabled
```

Примечание

> Параметр ***split*** должен быть установлен только на ведущем DHCP-сервере. Этот параметр управляет балансировкой нагрузки двух серверов. Параметр может принимать значения от 0 до 255. Если установлено значение «255», основной сервер, если он не отключен (по какой-либо причине), будет отвечать на все запросы DHCP. Если установить значение «128», то оба DHCP-сервера будут использоваться одинаково. Подробности смотрите на man-странице dhcpd.conf.

Далее следует перезапустить оба DHCP-сервера:

```
# systemctl restart dhcpd
```

В системном журнале на обоих серверах должны появиться записи вида:

```
dhcpd[7879]: failover peer dhcp-failover: peer moves from recover-done to normal
dhcpd[7879]: failover peer dhcp-failover: Both servers normal
```

Если OMAPI работает правильно, можно проверить переход на другой ресурс, остановив основной сервер.

Глава 47. Настройка LDAP через SSL (LDAPS)

47.1. Параметры smb.conf для LDAPS

47.2. Ограничение шифров TLS

47.3. Использование автоматически сгенерированного самоподписанного сертификата Samba

47.4. Использование пользовательского самоподписанного сертификата

47.5. Использование доверенного сертификата

47.6. Проверка сертификата

Альт Домен использует LDAP (Lightweight Directory Access Protocol) для доступа на чтение и запись. По умолчанию соединения LDAP не зашифрованы. Для защиты трафика LDAP можно использовать SSL/TLS. Ниже описано, как включить LDAPS, установив сертификат в Samba.

Ограничения:

- закрытый ключ должен быть доступен без парольной фразы, т. е. он не должен быть зашифрован!
- файлы, которые использует Samba, должны быть в формате PEM (DER с кодировкой Base64). Содержимое сертификата может быть заключено, например, между

  ```
  -----BEGIN CERTIFICATE-----
  ```

  и

  ```
  -----END CERTIFICATE-----
  ```

- при использовании промежуточных сертификатов их следует добавлять в файл **cert.pem** после сертификата сервера.

47.1. Параметры smb.conf для LDAPS

LDAPS управляется параметрами ***tls**** в файле **smb.conf** (подробнее см. **man smb.conf**).

Параметры ***tls**** задаются в разделе [global] файла **smb.conf**. После внесения изменений в файл **smb.conf** необходимо перезапустить Samba.

47.2. Ограничение шифров TLS

Опция ***tls priority*** позволяет задать строку приоритета шифра GnuTLS и, таким образом, отключить устаревшие шифры.

GnuTLS управляет тем, какие шифры включены по умолчанию, но SSLv3 дополнительно отключен.

В данном примере предполагается, что библиотека отключает SSLv3, а также дополнительно отключает TLS 1.0 и 1.1:

```
tls priority = NORMAL:-VERS-TLS1.0:-VERS-TLS1.1
```

47.3. Использование автоматически сгенерированного самоподписанного сертификата Samba

При первом запуске Samba создает закрытый ключ, самоподписанный сертификат и сертификат CA:

```
/var/lib/samba/private/tls/ca.pem
/var/lib/samba/private/tls/cert.pem
/var/lib/samba/private/tls/key.pem
```

Сертификаты действительны в течение 700 дней после создания.

По умолчанию TLS включен (***tls enabled = yes***), используются указанные выше файлы, которые соответствуют следующим параметрам **smb.conf**:

```
tls enabled  = yes
tls keyfile  = tls/key.pem
tls certfile = tls/cert.pem
tls cafile   = tls/ca.pem
```

47.4. Использование пользовательского самоподписанного сертификата

Для создания пользовательского самоподписанного сертификата можно выполнить следующие действия:

1. Перейти в каталог, в котором будет сохранен ключ и сертификат:

```
# cd /var/lib/samba/private/tls/
```

2. Создать закрытый ключ (2048 бит) и самоподписанный сертификат, действительный в течение 1 года. Важно при запросе **Common Name** ввести полное доменное имя контроллера домена, для которого создается сертификат:

```
#
openssl req -newkey rsa:2048 -keyout myKey.pem -nodes -x509 -days 365 -out
myCert.pem

Generating a RSA private key
.....................+++++
...........+++++
writing new private key to 'myKey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (e.g., your name or your server's hostname) []:dc1.test.alt
Email Address []:
```

3. Ограничить права на закрытый ключ:

```
# chmod 600 myKey.pem
```

4. В файле **smb.conf** указать следующие параметры:

```
tls enabled = yes
tls keyfile = tls/myKey.pem
tls certfile = tls/myCert.pem
tls cafile =
```

5. Перезапустить Samba.

47.5. Использование доверенного сертификата

Если планируется использовать доверенный сертификат, следует выполнить следующие действия:

1. Перейти в каталог, в котором будут созданы ключ и сертификат:

```
# cd /var/lib/samba/private/tls/
```

2. Создать ключ сервера:

```
# openssl genrsa -out myKey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.....................................................................
..................+++++
e is 65537 (0x010001)
```

3. Сгенерировать запрос на сертификат (CSR). Важно при запросе **`Common Name`** ввести полное доменное имя контроллера домена, для которого создается сертификат:

```
# openssl req -new -key myKey.pem -out myCSR.pem

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (e.g., your name or your server's hostname) []:dc1.test.alt
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

4. Получить доверенный сертификат от CA, используя CSR (**`myCSR.pem`**).

5. Сохранить доверенный сертификат (в примере **`myCert.pem`**) в каталоге с ключом сервера. Если CA требует промежуточные сертификаты, файл с промежуточными сертификатами следует также сохранить в том же каталоге, что и другие файлы (например, **`myIntermediate.pem`**).

6. Добавить следующие параметры в файл **`smb.conf`**:

```
tls enabled  = yes
tls keyfile  = tls/myKey.pem
tls certfile = tls/myCert.pem
tls cafile   = tls/myIntermediate.pem
```

7. Перезапустить Samba.

47.6. Проверка сертификата

Просмотреть данные сертификата можно, выполнив команду:

```
# openssl x509 -in /var/lib/samba/private/tls/myCert.pem -noout -text

Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number:
            32:9d:8f:2f:95:46:59:8d:9d:56:1c:da:14:b1:03:0c:82:ed:96:d0
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RU, CN = dc1.test.alt
        Validity
            Not Before: Jan  8 16:24:09 2025 GMT
            Not After : Jan  8 16:24:09 2026 GMT
        Subject: C = RU, CN = dc1.test.alt
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                .....{.....}.....
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                45:2E:E1:87:EE:54:77:E1:88:86:C6:48:DB:99:E6:EA:36:CA:D5:79
            X509v3 Authority Key Identifier:
                keyid:45:2E:E1:87:EE:54:77:E1:88:86:C6:48:DB:99:E6:EA:36:CA:D5:79

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         .....{.....}.....
```

Локальная проверка сертификата:

```
# openssl verify /var/lib/samba/private/tls/myCert.pem
C = RU, CN = dc1.test.alt
error 18 at 0 depth lookup: self signed certificate
OK
```

Если в файле **smb.conf** указан файл CA, следует использовать следующую команду:

```
# openssl verify /var/lib/samba/private/tls/myCert.pem -CAfile /path/to/ca-file.pem
```

Проверка сертификата удаленно (через TCP):

```
# openssl s_client -showcerts -connect dc1.test.alt:636
CONNECTED(00000003)
depth=0 C = RU, CN = dc1.test.alt
verify error:num=18:self signed certificate
verify return:1
depth=0 C = RU, CN = dc1.test.alt
verify return:1
---
Certificate chain
 0 s:C = RU, CN = dc1.test.alt
   i:C = RU, CN = dc1.test.alt
-----BEGIN CERTIFICATE-----
.....{.....}.....
-----END CERTIFICATE-----
---
Server certificate
subject=C = RU, CN = dc1.test.alt
```

```
issuer=C = RU, CN = dc1.test.alt

---
No client certificate CA names sent
Requested Signature Algorithms: RSA+SHA256:RSA-PSS+SHA256:RSA-
PSS+SHA256:ECDSA+SHA256:Ed25519:RSA+SHA384:RSA-PSS+SHA384:RSA-
PSS+SHA384:ECDSA+SHA384:Ed448:RSA+SHA512:RSA-PSS+SHA512:RSA-
PSS+SHA512:ECDSA+SHA512:RSA+SHA1:ECDSA+SHA1
Shared Requested Signature Algorithms: RSA+SHA256:RSA-PSS+SHA256:RSA-
PSS+SHA256:ECDSA+SHA256:Ed25519:RSA+SHA384:RSA-PSS+SHA384:RSA-
PSS+SHA384:ECDSA+SHA384:Ed448:RSA+SHA512:RSA-PSS+SHA512:RSA-
PSS+SHA512:ECDSA+SHA512
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1437 bytes and written 424 bytes
Verification error: self signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self signed certificate)
---
```

Выйти из s_client можно, нажав [Ctrl]+[C].

Если в файле **smb.conf** указан файл CA, следует использовать следующую команду:

```
# openssl s_client -showcerts -connect localhost:636 -CAfile /path/to/ca-file.pem
```

Глава 48. Аутентификация других сервисов в домене

48.1. Настройка аутентификации Kerberos для веб-сервера Apache

48.2. Настройка аутентификации Kerberos для веб-сервера Nginx

48.3. Настройка браузеров для SSO

В данном разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте. В качестве веб-сервера используется отдельный сервер (web.test.alt, IP-адрес 192.168.0.150), введенный в домен.

Примечание

Веб-сервер может быть присоединен или не присоединен к домену, это не имеет значения.

Для работы требуется наличие прямой и обратной записей DNS для веб-сервера.

Если в качестве веб-сервера используется не DC, следует добавить A-запись для веб-сервера:

```
$  samba-tool dns add dc1.test.alt test.alt web A 192.168.0.150 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

где dc1.test.alt — имя контроллера домена.

Добавить зону обратного просмотра для подсети 192.168.0.0/24, в которой располагается веб-сервер:

```
$ samba-tool dns zonecreate dc1.test.alt 0.168.192.in-addr.arpa -Uadministrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

Если требуется более одной обратной зоны (при использовании нескольких подсетей), следует запустить приведенную выше команду еще раз, но с данными для другой подсети.

Обратная зона работает напрямую без перезапуска Samba или BIND.

Добавить зону обратного просмотра для веб-сервера:

```
$ samba-tool dns add dc1.test.alt 0.168.192.in-addr.arpa 150 PTR web.test.alt
```

48.1. Настройка аутентификации Kerberos для веб-сервера Apache

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Apache2.

48.1.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт (подробнее см. Создание keytab-файла). Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для создания SPN на контроллере домена выполнить команды:

```
# samba-tool user add --random-password webauth
# samba-tool user setexpiry webauth --noexpiry
# samba-tool spn add HTTP/web.test.alt webauth
```

Создать Kerberos keytab-файл для Apache2:

```
# samba-tool domain exportkeytab /tmp/httpd.keytab --principal=HTTP/
web.test.alt@TEST.ALT
Export one principal to /tmp/httpd.keytab
```

Перенести полученный файл keytab на веб-сервер в каталог **/etc/httpd2/conf/**, установить права на него, так чтобы Apache мог читать, но не изменять keytab-файл:

```
# chown apache2:apache2 /etc/httpd2/conf/httpd.keytab
# chmod 0440 /etc/httpd2/conf/httpd.keytab
```

48.1.2. Настройка Apache2

На веб-сервере установить пакет *apache2-mod_auth_gssapi* и включить необходимые модули:

```
# apt-get install apache2-mod_auth_gssapi
# a2enmod auth_gssapi
# a2enmod authn_core
# a2enmod authz_user
# service httpd2 condreload
```

Добавить в конфигурацию Apache строки:

```
<Location "/login.html">
        AuthType GSSAPI
        AuthName "GSSAPI Login"
        #GssapiBasicAuth On
        GssapiCredStore keytab:/etc/httpd2/conf/httpd.keytab
        GssapiAllowedMech krb5
        Require valid-user
</Location>
```

Перезапустить Apache:

```
# systemctl restart httpd2
```

48.1.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу http://<полное_доменное_имя_веб-сервера>.

На рабочей станции, введённой в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41  krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt/login.html
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Authentication required!</title>
</head>

<body>
<h1>Authentication required!</h1>
…
<h2>Error 401</h2>
<address>
  <a href="/">web.test.alt</a><br />
  <span>Apache/2.4.57 (Unix) mod_auth_gssapi/1.6.3 OpenSSL/1.1.1u</span>
</address>
</body>
</html>
```

Содержимое страницы не доступно.

48.2. Настройка аутентификации Kerberos для веб-сервера Nginx

В этом разделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Nginx.

48.2.1. Создание keytab-файла

Подробнее см. Создание keytab-файла.

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт (таким образом, фактическое имя сервера, на которое указывает CNAME, является полным). Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для этого на контроллере домена:

```
# samba-tool user add --random-password nginxauth
# samba-tool user setexpiry nginxauth --noexpiry
# samba-tool spn add HTTP/web.test.alt nginxauth
```

Создать Kerberos keytab-файл для Nginx:

```
# samba-tool domain exportkeytab /tmp/nginx.keytab --principal=HTTP/
web.test.alt@TEST.ALT
Export one principal to /tmp/nginx.keytab
```

48.2.2. Настройка Nginx

Для работы прозрачной доменной аутентификации (SSO) в Nginx необходимо установить пакеты *nginx* и *nginx-spnego*:

```
# apt-get install nginx nginx-spnego
```

Модуль SPNEGO для Nginx — это программный компонент для возможности прохождения аутентификации (Single Sign-On или SSO) через сервер LDAP.

Включить модуль http_auth_spnego:

```
# ln -s /etc/nginx/modules-available.d/http_auth_spnego.conf /etc/nginx/modules-enabled.d/
```

Перенести полученный на контроллере домене файл keytab на веб-сервер в каталог **`/etc/nginx`**. Установить права на файл keytab:

```
# chmod 644 /etc/nginx/nginx.keytab
```

Nginx должен иметь права на чтение keytab-файла, но не на его изменение.

Настроить аутентификацию в секции **`server`** файла конфигурации сайта:

```
server {
    …
    location /
    {
        root /var/www/html;
        auth_gss on;
        auth_gss_realm TEST.ALT; #имя Kerberos области
        auth_gss_keytab /etc/nginx/nginx.keytab; #путь к keytab-файлу
        auth_gss_service_name HTTP/web.test.alt; #имя используемого SPN
        auth_gss_allow_basic_fallback off;
    }
}
```

Описание опций:

- ***`auth_gss`*** — включение/отключение аутентификации;
- ***`auth_gss_keytab`*** — абсолютный путь к файлу keytab, содержащему учётные данные службы;
- ***`auth_gss_realm`*** — имя области Kerberos;
- ***`auth_gss_service_name`*** — имя субъекта-службы, используемое при получении учетных данных;
- ***`auth_gss_allow_basic_fallback`*** — включить/отключить базовую аутентификацию. При включённой базовой аутентификации (по умолчанию), если SSO не проходит (машина не в домене) разрешает обычный ввод логина и пароля. Если используется SPNEGO без SSL, рекомендуется отключить базовую аутентификацию, так как в этом случае пароль будет отправлен в виде открытого текста.

Перезапустить nginx:

```
# systemctl restart nginx
```

Если нужно авторизовать только определенный набор пользователей, можно использовать параметр ***`auth_gss_authorized_principal`***. Можно указывать несколько записей, по одной на строку:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal <username2>@<realm>
```

Список пользователей также можно указать с помощью шаблона регулярного выражения в параметре ***auth_gss_authorized_principal_regex***. Этот параметр можно использовать вместе с параметром ***auth_gss_authorized_principal***:

```
auth_gss_authorized_principal <username>@<realm>
auth_gss_authorized_principal_regex ^(<username>)/(<group>)@<realm>$
```

48.2.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу http://<полное_доменное_имя_веб-сервера>.

На рабочей станции, введённой в домен, получить билет Kerberos:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
$ klist
Ticket cache: KEYRING:persistent:500:krb_ccache_5VitJSL
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
28.04.2023 15:54:41  29.04.2023 01:54:41  krbtgt/TEST.ALT@TEST.ALT
    renew until 05.05.2023 15:54:38
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt
<html><body><h1>It works!</h1></body></html>
```

Получено содержимое страницы.

Удалить билеты Kerberos:

```
$ kdestroy
$ klist
```

Попытаться прочитать содержимое сайта, используя аутентификацию Kerberos:

```
$ curl --negotiate -u : http://web.test.alt
<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>
```

Содержимое страницы не доступно.

48.3. Настройка браузеров для SSO

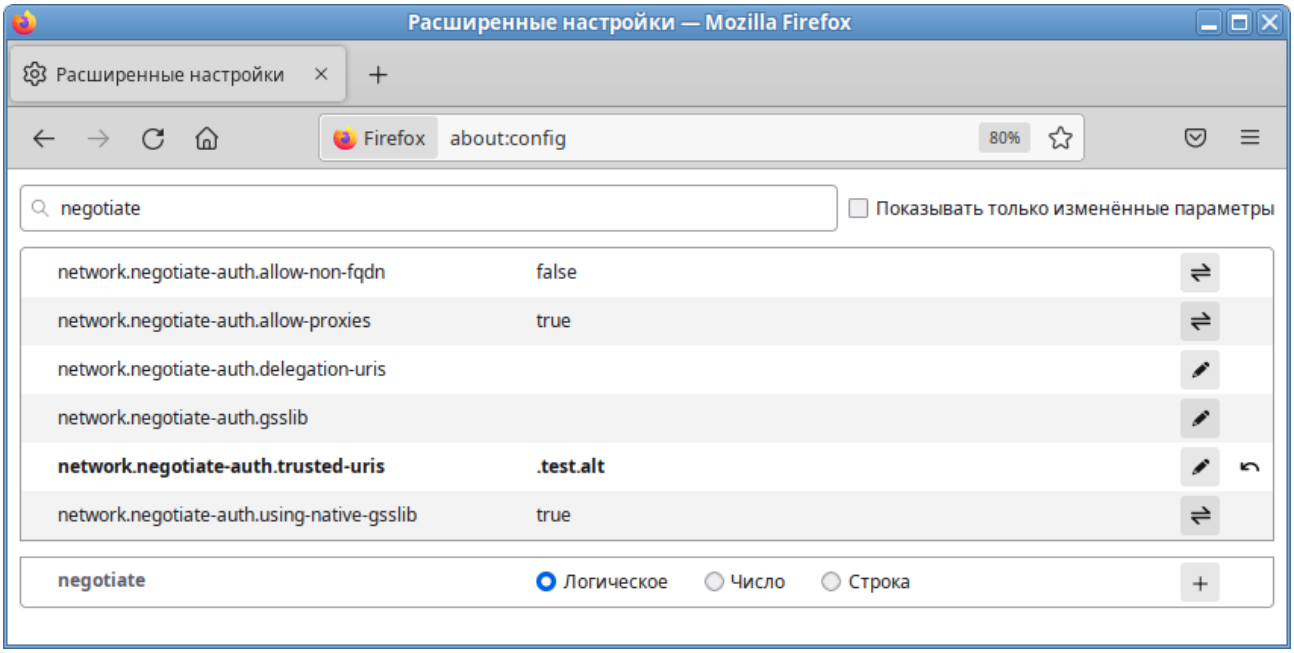
Предварительно необходимо ввести компьютер в домен (см. Подключение к домену) и убедиться, что доменный пользователь получает билет Kerberos.

Для работы SSO в браузерах необходимо произвести некоторые настройки.

48.3.1. Настройка Mozilla Firefox

Порядок действий:

1. В адресной строке ввести **about:config**, чтобы отобразить список текущих параметров конфигурации (необходимо будет нажать кнопку **`Принять риск и продолжить`**).
2. В поле **`Фильтр`** ввести **negotiate**, чтобы ограничить список параметров.
3. Выбрать параметр ***`network.negotiate-auth.trusted-uris`***.
4. Указать в этом параметре имя Kerberos области (realm), включая предшествующую точку (.). Если нужно добавить несколько доменов, их необходимо указать через запятую.



В ряде случаев может потребоваться отредактировать еще несколько параметров:

- параметр ***`network.automatic-ntlm-auth.trusted-uris`*** выставить в Kerberos realm: **.test.alt**;
- параметр ***`network.negotiate-auth.delegation-uris`*** выставить в Kerberos realm: **.test.alt**;
- параметр ***`network.automatic-ntlm-auth.allow-non-fqdn`*** выставить в: **true**;
- параметр ***`network.negotiate-auth.allow-non-fqdn`*** выставить в: **true**;

Вместо выставления этих параметров можно создать файл **`/usr/lib64/firefox/browser/defaults/preferences/prefs.js`** со следующим содержимым:

```
pref("network.negotiate-auth.trusted-uris",".test.alt");
pref("network.automatic-ntlm-auth.trusted-uris",".test.alt");
pref("network.automatic-ntlm-auth.allow-non-fqdn","true");
pref("network.negotiate-auth.allow-non-fqdn","true");
pref("network.negotiate-auth.delegation-uris",".test.alt");
```

Эти параметры могут быть распространены через групповые политики для Firefox:

- параметр ***network.negotiate-auth.trusted-uris*** — политика **SPNEGO**;
- параметр ***network.automatic-ntlm-auth.trusted-uris*** — политика **NTLM**;
- параметр ***network.negotiate-auth.delegation-uris*** — политика **Делегированная авторизация**;
- параметр ***network.automatic-ntlm-auth.allow-non-fqdn*** — политика **Разрешить неполное доменное имя (Non FQDN)**;
- параметр ***network.negotiate-auth.allow-non-fqdn*** — политика **Разрешить неполное доменное имя (Non FQDN)**;

Подробнее см. Управление политиками браузера Firefox.

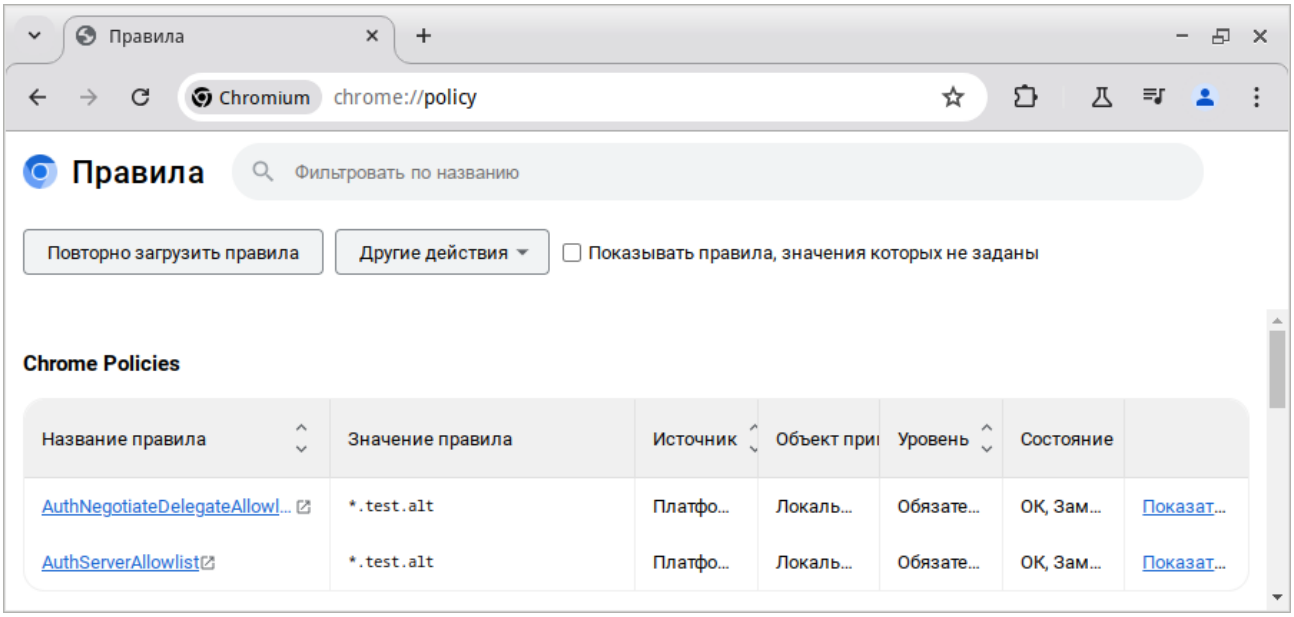
48.3.2. Настройка Chromium

В файл **/etc/chromium/policies/managed/policies.json** добавить строки:

```
{
    "AuthServerAllowlist": "*.test.alt",
    "AuthNegotiateDelegateAllowlist": "*.test.alt"
}
```

где .test.alt — имя Kerberos области (realm).

Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для Chromium можно проверить, указав в адресной строке URL: **chrome://policy**.



Эти параметры могут быть распространены через групповые политики для Chromium: **Список разрешенных серверов для аутентификации** (**Разрешить аутентификацию на серверах из списка**) и **Список разрешенных серверов для делегирования прав по протоколу Kerberos** (**Разрешить делегирование прав по протоколу Kerberos на серверах**). Подробнее см. Управление политиками браузера Chromium.

Примечание

Для проверки работы аутентификации без изменения настроек браузера можно запустить браузер из командной строки, выполнив команду:

```
$ chromium-browser --auth-server-whitelist="*.test.alt"
```

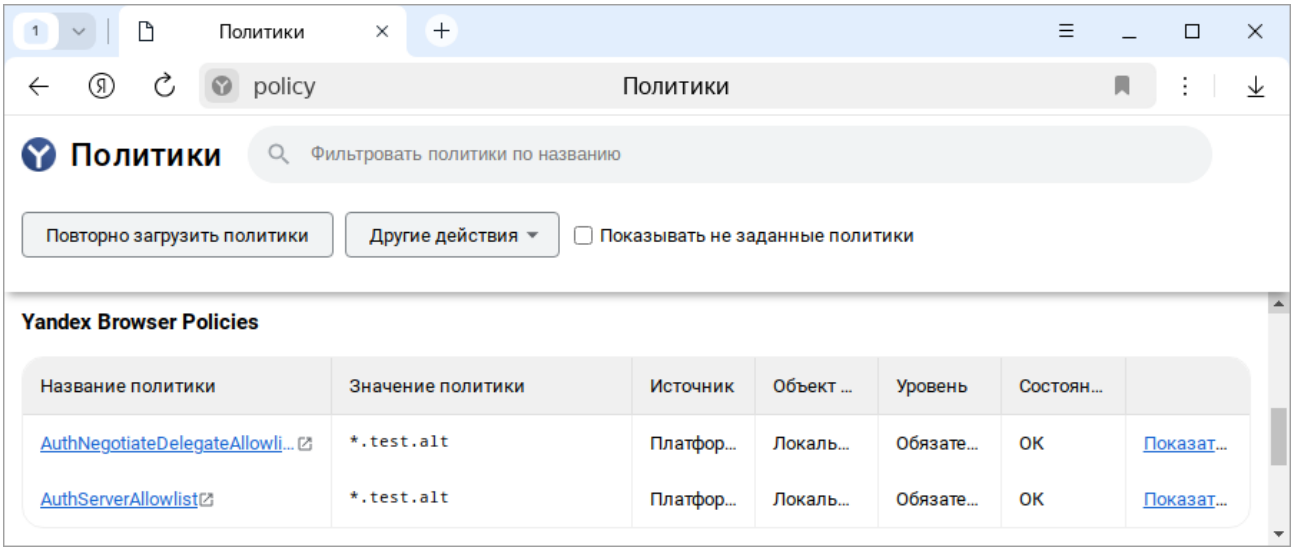
48.3.3. Настройка «Яндекс.Браузера»

В файл **/etc/opt/yandex/browser/policies/managed/policies.json** добавить строки:

```
{
    "AuthServerAllowlist": "*.test.alt",
    "AuthNegotiateDelegateAllowlist": "*.test.alt"
}
```

Где .test.alt — имя Kerberos области (realm).

Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: **browser://policy**.



Эти параметры могут быть распространены через групповые политики для «Яндекс.Браузера»: политики **Разрешить аутентификацию на серверах из списка** и **Разрешить делегирование прав по протоколу Kerberos на серверах**. Подробнее см. Управление политиками «Яндекс.Браузера».

Глава 49. Распределенная файловая система (DFS)

49.1. Пространство DFS-имен

49.2. Настройка DFS на сервере Samba

Распределенная файловая система (Distributed File System, DFS) — серверная технология Microsoft, предназначенная для упрощения доступа к общим файловым ресурсам, распределенным по сети. С помощью DFS можно объединять в единую логическую структуру файловые ресурсы, физически находящиеся на различных серверах, а также производить между ними репликацию. Функционал DFS образуют две составляющих: пространство DFS-имен — DFS-N (DFS-Namespace) и механизм репликации — DFS-R (DFS-Replication).

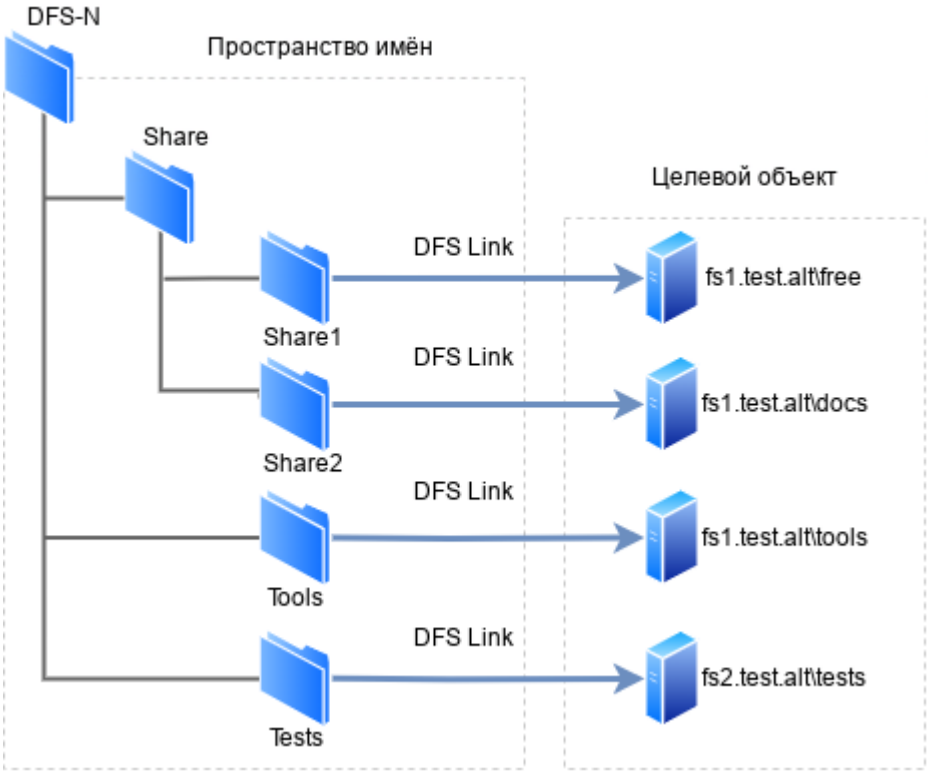
Samba поддерживает DFS-N, но пока не поддерживает DFS-R.

49.1. Пространство DFS-имен

Пространство DFS-имен — это единый виртуальный каталог, содержащий ссылки на общие каталоги, расположенные на разных файловых серверах. Пространство имен состоит из корня (root), ссылок (folders) и целевых объектов (folder targets). Пространство имен DFS может быть двух типов: автономное (Stand-alone) и доменное (Domain-based).

Автономный вариант работает на одном сервере и приводит к тому, что имена DFS содержат имя этого сервера, они выглядят как общие ресурсы, предоставляемые этим сервером (можно создать распределенную файловую систему не используя доменные службы).

При доменном варианте имена DFS содержат только имя домена, а не имя какого-либо конкретного сервера (имя сервера пространства имен скрыто от пользователей, проще замена сервера пространства имен или перенос пространства имен на другой сервер).



Корень пространства имен (Namespace root) — это базовая точка, от которой начинается отсчёт пространства имён. В зависимости от типа корень доступен по адресу \\ServerName\RootName (Stand-alone) или \\DomainName\RootName (Domain-based).

Сервер пространства имен (Namespace server) — физический сервер, на котором содержится пространство имён DFS.

Каталог — ссылка в пространстве имен DFS, указывающая на целевой объект. Каталоги без конечных объектов (например, каталог Share) образуют структуру и иерархию в пространстве имен, а каталоги с целевыми объектами (например, каталог Share1) предоставляют пользователям доступ к фактическому содержимому.

Целевой объект (Folder targets) — ссылка на общий файловый ресурс, находящийся на определенном файловом сервере. Одна ссылка может указывать как на один, так и на несколько целевых объектов.

49.2. Настройка DFS на сервере Samba

Прежде, чем перейти к добавлению пространства имен, необходимо создать хотя бы один сетевой каталог на любом из серверов, добавленных в домен.

Сервер Samba можно сделать сервером DFS, задав логический параметр ***host msdfs*** в файле **/etc/samba/smb.conf**. Корень DFS назначается с помощью логического параметра ***root msdfs***. Если для этого параметра установлено значение **yes**, Samba будет воспринимать открытый для общего доступа ресурс как корневой DFS. Ссылки DFS, указываемые в открытом для доступа каталоге, имеют вид: **msdfs:serverA\shareA,serverB\shareB** и т.д. Корневой каталог DFS в Samba содержит ссылки DFS в виде символических ссылок,

Для создания нового пространства имён необходимо выполнить следующие действия:

- создать каталог, в котором будут настроены ссылки DFS на другие серверы в сети (в примере **/media/dfsroot**):

```
# mkdir /media/dfsroot
```

- в файл **/etc/samba/smb.conf** в секцию **[global]** добавить параметр:

```
host msdfs = yes
```

  и добавить секцию **[dfs]**, с указанием корня:

```
[dfs]
        path = /media/dfsroot
        msdfs root = yes
```

- в каталоге **/media/dfsroot** настроить ссылки DFS на общие ресурсы в сети:

```
# cd /media/dfsroot
# ln -s msdfs:dc1.test.alt\\free linka
# ln -s msdfs:web.test.alt\\tests linkb
```

- Перезапустить samba:

```
# systemctl restart samba
```

- дерево DFS теперь доступно по адресу //test.alt/dfs/. При доступе к ссылкам linka или linkb (которые отображаются для клиента как каталоги) пользователи напрямую переходят к соответствующим общим ресурсам в сети. Проверка:

```
$ smbclient //test.alt/dfs/linka -U 'ivanov'
Password for [TEST\ivanov]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon May 22 10:13:28 2023
  ..                                  D        0  Mon May 22 10:13:06 2023
  dc.txt                              N        5  Mon May 22 15:57:14 2023

        48254668 blocks of size 1024. 40859796 blocks available
smb: \> exit
```

Примечание

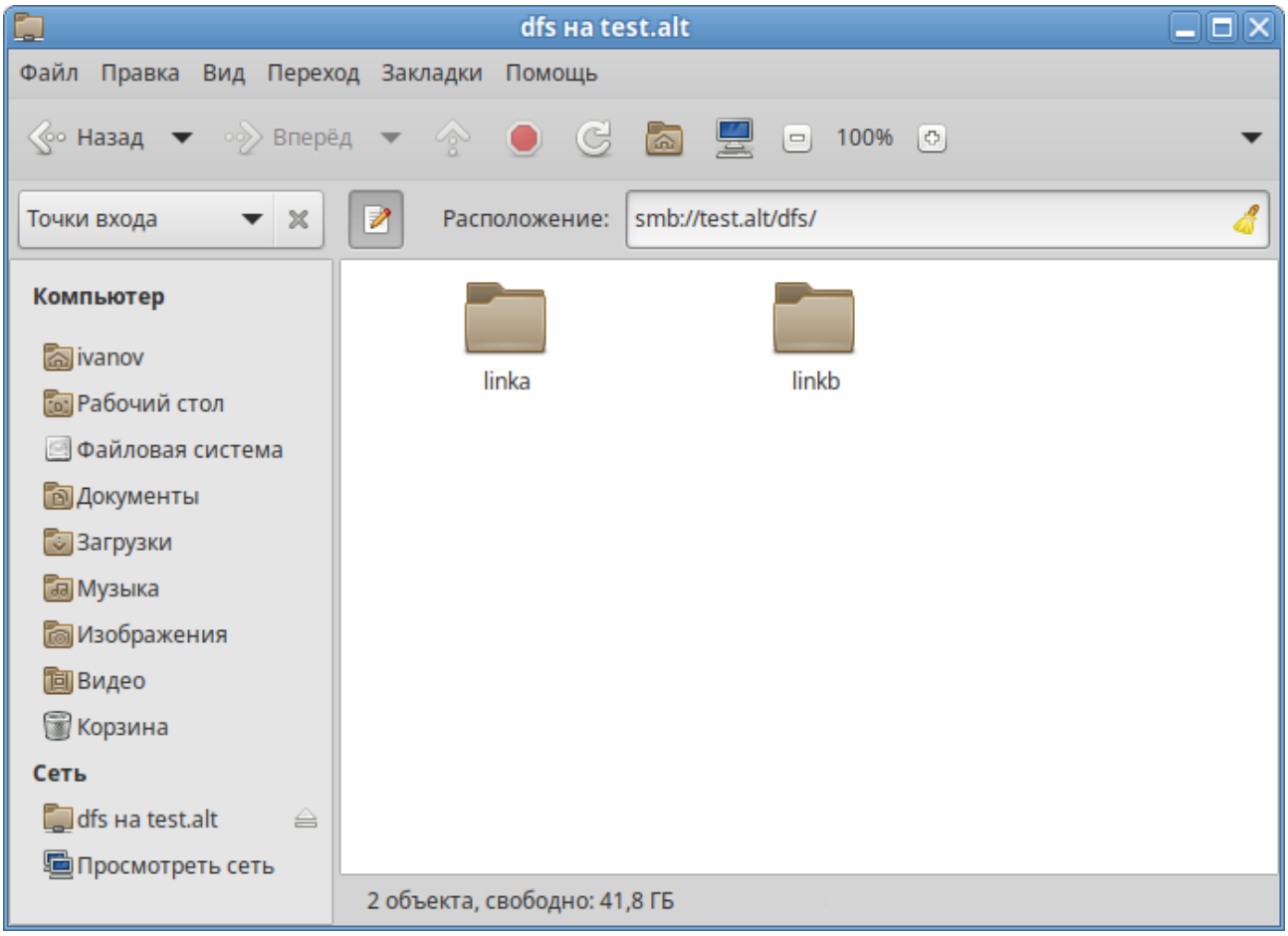
Для доступа к ресурсам DFS по имени домена с использованием аутентификации Kerberos необходимо добавить к имени сервера псевдоним — имя домена. Это можно сделать, выполнив на контроллере домена команду:

```
# samba-tool spn add cifs/cifs/<имя_домена> <имя_сервера>$
```

Например:

```
# samba-tool spn add cifs/test.alt dc1$
```

Подключиться к данному пространству можно, набрав в адресной строке следующий адрес: smb://<имя_домена>/<имя_пространства_имен>:



Глава 50. Настройка SSSD

50.1. Журналирование SSSD

50.2. Настройки SSSD в ЦУС

50.3. Включение автономной аутентификации

50.1. Журналирование SSSD

50.1.1. Файлы журналов SSSD

Каждая служба SSSD записывает логи в свой собственный файл журнала в каталоге **/var/log/sssd/**. Например, для машины в домене test.alt, файлы журналов SSSD могут выглядеть следующим образом:

```
# ls -l /var/log/sssd/
итого 1660
-rw------- 1 _sssd _sssd       0 мая 18 12:55 gpo_child.log
-rw------- 1 _sssd _sssd       0 мая 18 12:55 krb5_child.log
-rw------- 1 _sssd _sssd       0 мая 18 12:54 ldap_child.log
-rw------- 1 root  root      261 июн 19 10:10 sssd_ifp.log
-rw------- 1 root  root     3955 июн 19 09:34 sssd.log
```

```
-rw------- 1 _sssd _sssd 1677605 июн 19 11:18 sssd_nss.log
-rw------- 1 _sssd _sssd    1134 июн 19 09:34 sssd_pac.log
-rw------- 1 _sssd _sssd    3067 июн 19 09:34 sssd_pam.log
-rw------- 1 _sssd _sssd       0 мая 18 12:54 sssd_TEST.ALT.log
```

krb5_child.log

Файл журнала для недолговечного вспомогательного процесса, участвующего в аутентификации Kerberos.

ldap_child.log

Файл журнала для недолговечного вспомогательного процесса, участвующего в получении билета Kerberos для связи с сервером LDAP.

sssd_<domain.name>.log

Для каждого раздела [domain] в файле **sssd.conf** служба SSSD записывает информацию о взаимодействии с LDAP-сервером в отдельный файл журнала.

sssd.log

Файл журнала для мониторинга SSSD и связи его с ответчиком и внутренними процессами.

sssd_ifp.log

Файл журнала для ответчика InfoPipe, который предоставляет общедоступный интерфейс D-Bus, доступный через системную шину.

sssd_nss.log

Файл журнала для ответчика Name Services Switch (NSS), который извлекает информацию о пользователях и группах.

sssd_pac.log

Файл журнала для ответчика Microsoft Privilege Attribute Certificate (PAC), который собирает PAC из билетов AD Kerberos и извлекает информацию о пользователях AD из PAC, что позволяет избежать её запроса непосредственно из AD.

sssd_pam.log

Файл журнала для ответчика Pluggable Authentication Module (PAM).

sssd_ssh.log

Файл журнала для процесса ответчика SSH.

50.1.2. Уровни журналирования SSSD

Таблица 50.1. Уровни журналирования SSSD

Уровень	Описание
0, 0x0010	**Фатальные ошибки**. Ошибки, которые не позволяют запустить службу SSSD или вызывает завершение работы сервиса
1, 0x0020	

Уровень	Описание
	Критические ошибки. Ошибки, которые не завершают работу службы SSSD, но как минимум одна из основных функций не работает должным образом
2, 0x0040	**Серьёзные ошибки**. Ошибки, сообщающие о том, что определенный запрос или операция завершились неудачно. *Это уровень журналирования по умолчанию*
3, 0x0080	**Незначительные ошибки**. Ошибки, которые могут стать причиной ошибок второго уровня (ошибок при выполнении действий)
4, 0x0100	**Настройки конфигурации**
5, 0x0200	**Данные функций**
6, 0x0400	Сообщения трассировки для функций **действий**
7, 0x1000	Сообщения трассировки для функций **внутреннего управления**
8, 0x2000	Содержимое переменных **внутренних функций**
9, 0x4000	Информация **трассировки крайне низкого уровня**
9, 0x20000	**Быстродействие и статистические данные**. Из-за способа обработки запросов на внутреннем уровне, записанное в журнал время выполнения запроса может быть больше, чем оно было на самом деле
10, 0x10000	Информация **трассировки libldb** ещё более низкого уровня. Практически никогда не требуется

Установка уровня журнала также включает все уровни ниже него. Например, установка уровня журнала на 6 также включает уровни с 0 по 5.

Чтобы вести журнал для необходимых уровней журналирования, указанных в представлении битовых масок, следует просто сложить их номера. Например, чтобы вести журнал для фатальных, критических, серьёзных ошибок и для данных функций, следует использовать значение **`0x0270`**.

50.1.3. Настройка уровня журналирования для SSSD в файле `sssd.conf`

Чтобы включить подробное журналирование, сохраняющееся при перезапуске службы SSSD, следует добавить опцию ***`debug_level=<целое_число>`*** в каждую секцию файла **`/etc/sssd/sssd.conf`**. Где значение *<целое_число>* — число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень *6* является хорошей отправной точкой для отладки проблем.

Пример настройки уровня журналирования в файле **`/etc/sssd/sssd.conf`**:

```
[sssd]
debug_level = 6
config_file_version = 2
services = nss, pam

[domain/TEST.ALT]
debug_level = 6
id_provider = ad
…

[nss]
```

```
debug_level = 6

[pam]
debug_level = 6
```

Чтобы загрузить новые параметры конфигурации необходимо перезапустить службу SSSD:

```
# systemctl restart sssd
```

50.1.4. Настройка уровня журналирования для SSSD с помощью команды sssctl

Изменить уровень журналирования службы SSSD можно с помощью команды **`sssctl debug-level <целое_число>`**. Где значение *<целое_число>* — число от 0 до 10. Уровни до 3 регистрируют крупные сбои, а уровни начиная с 8 и выше предоставляют большое количество подробных сообщений журнала. Уровень *6* является хорошей отправной точкой для отладки проблем.

Просмотр текущего уровня журналирования:

```
# sssctl debug-level
sssd                        0x0070
nss                         0x0070
pam                         0x0070
pac                         0x0070
domain/TEST.ALT             0x0070
```

Установка нового уровня журналирования:

```
# sssctl debug-level 6
# sssctl debug-level
sssd                        0x07f0
nss                         0x07f0
pam                         0x07f0
pac                         0x07f0
domain/TEST.ALT             0x07f0
```

Примечание

Уровень журналирования, заданный с помощью команды **`sssctl debug-level`** будет действовать до перезапуска службы sssd.

50.2. Настройки SSSD в ЦУС

Некоторые параметры SSSD можно установить в модуле ЦУС **Аутентификация**. В окне модуля **Аутентификация** следует нажать кнопку **`Настройка SSSD…`** откроется окно настроек SSSD:

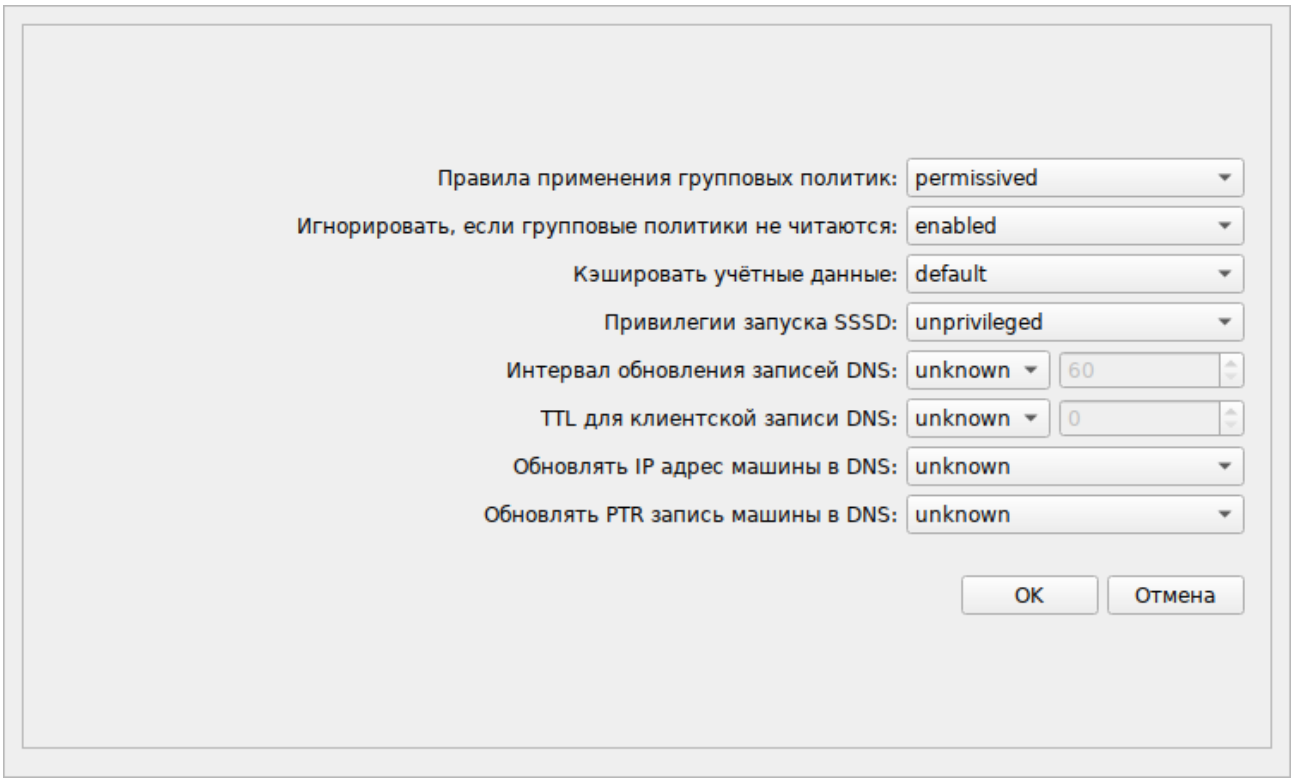


Таблица 50.2. Настройки SSSD в Alterator

Настройка	Опция в файле `/etc/sssd/sssd.conf`	Описание
Правила применения групповых политик	**`ad_gpo_access_control`**	Определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках Active Directory (GPO). Доступные режимы: ▸ **`enforced`** (принудительный режим) — правила управления доступом в SSSD, основанные на GPO, выполняются, ведётся логирование; ▸ **`permissived`** (разрешающий режим) — правила управления доступом в SSSD, основанные на GPO, не выполняются, ведётся только логирование. Такой режим необходим администратору, чтобы оценить, как срабатывают новые правила; ▸ **`disabled`** (отключить) — правила управления доступом в SSSD, основанные на GPO, не логируются и не выполняются; ▸ **`default`** (по умолчанию) — настройка контроля доступом в SSSD, основанная на GPO, сброшена на значение по умолчанию в пакете

Настройка	Опция в файле / `etc/sssd/sssd.conf`	Описание
Игнорировать, если групповые политики не читаются	**`ad_gpo_ignore_unreadable`**	Определяет будут ли проигнорированы правила управления доступом в SSSD основанные на групповых политиках, если недоступен какой-либо шаблон (GPT) объекта групповой политики (GPO). Доступные режимы: ▸**`enabled`** (включить) — игнорировать правила управления доступом через групповые политики, если шаблоны групповых политик не доступны для SSSD; ▸**`disabled`** (отключить) — запретить доступ пользователям SSSD AD, которым назначены групповые политики, если шаблоны групповых политик не доступны; ▸**`default`** (по умолчанию) — настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете
Кешировать учётные данные	**`cache-credentials`**	Определяет, будут ли учётные данные удалённых пользователей сохраняться в локальном кеше SSSD. Доступные режимы: ▸**`enabled`** (включить) — сохранение в локальном кеше SSSD учётных данных пользователей включено; ▸**`disabled`** (отключить) — сохранение в локальном кеше SSSD учётных данных пользователей отключено; ▸**`default`** (по умолчанию) — настройка сохранения в локальном кеше SSSD учётных данных пользователей сброшена на значение по умолчанию в пакете
Привилегии запуска SSSD	**`sssd-drop-privileges`**	Позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root). Доступные режимы: ▸**`privileged`** (привилегированный) — служба SSSD запущена от имени привилегированного суперпользователя (root); ▸**`unprivileged`** (непривилегированный) — служба SSSD запущена от имени непривилегированного пользователя (_sssd);

Настройка	Опция в файле / `etc/sssd/sssd.conf`	Описание
		▸**`default`** (по умолчанию) — режим привилегий службы SSSD задан по умолчанию в пакете
Интервал обновления записей DNS	**`dyndns_refresh_interval`**	Определяет как часто серверная часть должна выполнять периодическое обновление DNS в дополнение к автоматическому обновлению, выполняемому при подключении серверной части к сети. Этот параметр применим только в том случае, если для параметра **`dyndns_update`** установлено значение **`true`**. Доступные режимы: ▸**`enabled`** (включить) — задать интервал; ▸**`disabled`** (отключить) — установить значение по умолчанию (86400); ▸**`unknown`**
TTL для клиентской записи DNS	**`dyndns_ttl`**	Срок жизни, применяемый к DNS-записи клиента при ее обновлении. Если **`dyndns_update`** имеет значение **`false`**, этот параметр не имеет никакого эффекта. Доступные режимы: ▸**`enabled`** (включить) — задать TTL; ▸**`disabled`** (отключить) — установить значение по умолчанию (3600); ▸**`unknown`**
Обновлять IP-адрес машины в DNS	**`dyndns_update`**	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) с IP-адресом клиента через SSSD. Доступные режимы: ▸**`enabled`** (включить) — автоматическое обновление DNS-записи клиента через SSSD включено; ▸**`disabled`** (отключить) — автоматическое обновление DNS-записи клиента через SSSD отключено; ▸**`default`** (по умолчанию) — настройка автоматического обновления DNS-записи клиента через SSSD задана по умолчанию в пакете; ▸**`unknown`**

Настройка	Опция в файле /etc/sssd/sssd.conf	Описание
Обновлять PTR-запись машины в DNS-записей	**dyndns_update_ptr**	Определяет будет ли обновляться клиентская PTR-запись (защищенная с помощью GSS-TSIG) при обновлении DNS-записей клиента. Применимо, только если параметр **dyndns_update** имеет значение **true**. Доступные режимы: - **enabled** (включить) — автоматическое обновление DNS-записи обратной зоны через SSSD включено; - **disabled** (отключить) — автоматическое обновление DNS-записи обратной зоны через SSSD отключено; - **default** (по умолчанию) — настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете; - **unknown**

50.3. Включение автономной аутентификации

По умолчанию SSSD не кеширует учетные данные пользователей. При обработке запросов на аутентификацию SSSD всегда обращается к поставщику идентификационных данных. Если провайдер недоступен, аутентификация пользователя не проходит.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кеширование учетных данных, установив параметр ***cache_credentials*** в значение **true** в разделе домена (в файле **/etc/sssd/sssd.conf**).

Дополнительно можно использовать параметр ***offline_credentials_expiration*** в разделе [pam], чтобы установить ограничение по времени (в днях), в течение которого пользователи смогут аутентифицироваться в автономном режиме с момента последнего успешного входа.

Пример настройки возможности автономной аутентификации пользователей в течение 5 дней с момента последнего успешного входа:

```
[pam]
offline_credentials_expiration = 5
[domain/TEST.ALT]
cache_credentials = true
```

Для включения/отключения кеширования учетных данных можно использовать **control sssd-cache-credentials**. Например:

- просмотреть текущее значение:

```
# control sssd-cache-credentials
default
```

- включить кеширование учетных данных:

```
# control sssd-cache-credentials enabled
default
```

- отключить кеширование учетных данных:

```
# control sssd-cache-credentials disabled
default
```

Примечание

Данные настройки можно применить с помощью механизма групповых политик control. Подробнее см. Групповые политики control.

Глава 51. Samba в режиме файлового сервера

Samba можно настроить как файловый сервер. Samba также можно настроить как сервер печати для совместного доступа к принтеру.

Примечание

Не рекомендуется размещать файловый сервер на контроллере домена. Файловый сервер должен быть присоединён к домену, но не являться DC.

Каждый раздел в файле конфигурации (кроме раздела [global]) описывает общий ресурс. Название раздела — это имя общего ресурса. Параметры в разделе определяют свойства общего ресурса.

Общий ресурс состоит из каталога, к которому предоставляется доступ, а также описания прав доступа, которые предоставляются пользователю.

Разделы — это либо общие файловые ресурсы, либо службы печати. Разделам может быть назначен гостевой доступ, в этом случае для доступа к ним не требуется пароль (для определения прав доступа используется специальная гостевая учетная запись). Для доступа к разделам, к которым запрещен гостевой доступ, потребуется пароль.

Примечание

Вне домена Samba использует отдельную от системной базу данных пользователей. Для добавления в нее служит отдельная утилита **smbpasswd**. Для работы в доменной среде необходимости добавлять пользователей в эту базу нет. Достаточно ввести ПК в домен, используя winbind или sssd.

В файле конфигурации есть три специальных раздела: [global], [homes] и [printers]:

Раздел [global]

Параметры в этом разделе применяются к серверу в целом или являются значениями по умолчанию для разделов, и могут быть переопределены в разделе.

Раздел [homes]

Используется для подключения домашних каталогов пользователей. При каждом обращении Samba сначала ищет имя запрошенного ресурса в списке общих ресурсов, и если имя не найдено проверяет наличие в конфигурации секции [homes]. Если такая секция есть, то имя трактуется как имя пользователя (макрос %S).

```
[homes]
comment = Home Directories
browseable = no
writable = yes
valid users = %S
#можно переназначить путь до домашнего каталога, указав path
#path = /opt/smbhome/%S
```

Раздел [printers]

Если в файле конфигурации имеется раздел [printers], пользователи могут подключаться к любому принтеру, указанному в файле **/etc/printcap** локального хоста. Как правило, в файле **/etc/printcap** содержатся те принтеры, что настроены в CUPS.

Примечание

Флаг ***browseable*** для домашних каталогов будет унаследован от глобального флага ***browseable***, а не флага ***browseable*** раздела [homes]. Таким образом, установка browseable = no в разделе [homes] скроет общий ресурс [homes], но сделает видимыми все автоматические домашние каталоги.

Описание некоторых параметров:

- ***browseable*** — определяет, отображается ли этот общий ресурс в списке доступных общих ресурсов в сетевом окружении и в списке просмотра (по умолчанию: browseable = yes);
- ***path*** — указывает каталог, к которому должен быть предоставлен доступ;
- ***read only*** — если для этого параметра задано значение «yes», то пользователи службы не могут создавать или изменять файлы в каталоге (по умолчанию: read only = yes);
- ***writable*** — инвертированный синоним для ***read only*** (по умолчанию: writeable = no);
- ***write list*** — список пользователей, которым будет предоставлен доступ для чтения и записи. Если пользователь находится в этом списке, ему будет предоставлен доступ для записи, независимо от того, какой параметр установлен для параметра ***read only***. Список может включать имена групп с использованием синтаксиса @group;

Примечание

Особенности написания имен групп:

- в случае, если в названии группы есть пробел, необходимо использовать кавычки, например, @"Domain users";

- в случае, если работа происходит в мультидоменной среде, следует принудительно указывать домен, например, @"TEST\Domain users";
- несколько значений разделяются запятой, например, write list = @"TEST\Domain users", @it, @NEW\buh

- ***read list*** — список пользователей, которым будет предоставлен доступ только для чтения. Если пользователь находится в этом списке, ему не будет предоставлен доступ для записи, независимо от того, какой параметр установлен для параметра ***read only***. Список может включать имена групп;
- ***guest ok*** — если этот параметр имеет значение «yes», то для подключения к ресурсу не требуется пароль (по умолчанию: guest ok = no);
- ***guest only*** — разрешить только гостевые соединения к общему ресурсу (по умолчанию: guest only = no);
- ***printable*** — если этот параметр имеет значение «yes», то клиенты могут открывать, писать и ставить задания в очередь печати (по умолчанию: printable = no);
- ***valid users*** — список пользователей (групп), которым разрешен доступ к сервису;
- ***force group*** — принудительное изменение группы на создаваемые файлы/каталоги;
- ***force create mode*** — принудительная установка указанных атрибутов на файлы;
- ***force directory mode*** — принудительная установка указанных атрибутов на каталоги.

Примечание

После редактирования файла **/etc/samba/smb.conf**, следует запустить команду **testparm** для проверки файла на синтаксические ошибки:

```
# testparm /etc/samba/smb.conf
```

И, в случае отсутствия ошибок, перезапустить службы smb и nmb, чтобы изменения вступили в силу:

```
# systemctl restart smb
# systemctl restart nmb
```

Пример настройки:

```
[Sales]
comment = Sales documents
path = /opt/sales
writable = yes
read list = @sales, @sales-ro
write list = @sales
force group = sales
force create mode = 666
force directory mode = 775
```

Примечание

Пример создания каталога для ресурса общего доступа:

```
# mkdir /opt/sales
# chown -R root:"TEST.ALT\\Domain Users" /opt/sales
# chmod -R 2775 /opt/sales
```

Если нужно скрыть общие ресурсы или файлы, недоступные пользователю в связи отсутствием прав, можно воспользоваться следующими параметрами:

- ***access based share enum = yes*** — включает фильтрацию списка общих ресурсов (верхний уровень) в зависимости от прав пользователя. Пользователь будет только те ресурсы, к которым у него есть хотя бы минимальный доступ;
- ***hide unreadable = yes*** — скрывает файлы/каталоги внутри общего ресурса, если у пользователя нет прав на их чтение;
- ***hide unwriteable files = yes*** — скрывает файлы/каталоги общего ресурса, в которые у пользователя нет прав на запись.

Примечание

Эти опции не заменяют настройку прав, а только управляют видимостью.

Просмотр ресурсов, доступных доменному пользователю ivanov, с использованием активного Kerberos билета:

1. Получить билет, если он еще не получен:

```
$ kinit ivanov
Password for ivanov@TEST.ALT:
```

2. Сделать запрос на получение списка ресурсов, используя «прозрачную» аутентификацию:

```
$ smbclient -k -L //fs-server.test.alt/
WARNING: The option -k|--kerberos is deprecated!

Sharename       Type      Comment
---------       ----      -------
print$          Disk      Printer Drivers
free            Disk
Sales           Disk      Sales documents
IPC$            IPC       IPC Service (Samba 4.19.9-alt5)
ivanov          Disk      Home Directories
SMB1 disabled -- no workgroup available
```

или:

```
$ smbclient --use-kerberos=required --use-krb5-ccache=CCACHE -L //fs-
server.test.alt/

Sharename       Type      Comment
---------       ----      -------
print$          Disk      Printer Drivers
free            Disk
Sales           Disk      Sales documents
IPC$            IPC       IPC Service (Samba 4.19.9-alt5)
ivanov          Disk      Home Directories
SMB1 disabled -- no workgroup available
```

Примечание

Для ознакомления с прочими возможностями, читайте руководство по smb.conf. Для этого используйте команду **man smb.conf**.

Глава 52. Монтирование общих ресурсов samba

52.1. Подключение с использованием gio

52.2. Подключение с использованием pam_mount

52.3. Подключение с использованием Autofs

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

52.1. Подключение с использованием gio

Примечание

Способ актуален для дистрибутивов, использующих gio (например, Simply Linux, Альт Рабочая станция).

Недостаток подключения общих ресурсов с использованием gio — необходимо открыть ресурс в файловом менеджере (**Caja**, **Pcmanfm**). Однако можно открывать любые ресурсы на любых серверах, входящие в домен.

Процедура монтирования общих ресурсов с использованием gio:

- 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:

```
# control fusermount public
```

- войти под доменным пользователем;
- открыть ресурс в файловом менеджере (например, по адресу smb://server/sysvol). Ресурс будет смонтирован по пути **/var/run/<uid_пользователя>/gvfs** или **/var/run/user/<uid_пользователя>/gvfs/smb-share:server=сервер,share=ресурс**;
- другой вариант (полезно для скриптов в автозапуске):

```
gio mount smb://server/sysvol/
```

Примечание

Если необходимо открывать что-то с ресурса в WINE, в winecfg следует добавить диск с путём **/var/run/uid_пользователя/gvfs**.

52.2. Подключение с использованием pam_mount

При подключении общих ресурсов с использованием pam_mount сетевой ресурс подключается с заданного сервера автоматически при каждом входе доменным пользователем.

Процедура монтирования общих ресурсов с использованием pam_mount:

- установить пакеты *pam_mount* и *cifs-utils*:

```
# apt-get install pam_mount cifs-utils
```

Важно

Для того чтобы файловые ресурсы, подключенные с помощью pam_mount, корректно отключались при завершении сеанса, следует установить пакет *systemd-settings-enable-kill-user-processes* и перезагрузить систему:

```
# apt-get install systemd-settings-enable-kill-user-processes
```

- прописать pam_mount в схему аутентификации по умолчанию. Для этого в конец файла **/etc/pam.d/system-auth** добавить строки:

```
session         [success=1 default=ignore] pam_succeed_if.so  service =
systemd-user quiet
session         optional        pam_mount.so disable_interactive
```

- установить правило монтирования ресурса в файле **/etc/security/pam_mount.conf.xml** (перед тегом <cifsmount>):

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

где

- uid="10000-2000200000" — диапазон присваиваемых для доменных пользователей UID (подходит для Winbind и для SSSD);
- server="dc1.test.alt" — имя сервера с ресурсом;
- path="sysvol" — имя файлового ресурса;
- mountpoint="**~/share**" — путь монтирования в домашней папке пользователя.

Опционально можно добавить:

- sgrp="group_name" — имя группы, при членстве пользователя в которой, папка будет примонтирована.

Параметр ***sec=krb5i*** более безопасный, но требует больше вычислительных ресурсов. Вместо него можно указать ***sec=krb5***.

Предупреждение

В параметре ***server*** необходимо указывать настоящее имя сервера, а не имя домена.

Предупреждение

По умолчанию для монтирования используется smb версии 1.0, если он отключен, то необходимо указать в параметрах версию 2 или 3:

```
<volume uid="10000-2000200000" fstype="cifs" server="dc1.test.alt"
path="sysvol" mountpoint="~/share"
options="sec=krb5i,vers=2.0,cruid=%(USERUID),nounix,uid=%(USERUID),gid=%
(USERGID),file_mode=0664,dir_mode=0775" />
```

Для проверки можно попробовать смонтировать ресурс в сессии:

```
# mount.cifs //dc1.test.alt/sysvol /mnt/ -o vers=2.0,user=ivanov
```

Доступность ресурса можно также проверить с помощью команды **smbclient**, например:

```
# smbclient -L dc1.test.alt -U ivanov -m SMB2
```

52.3. Подключение с использованием Autofs

При подключении общих ресурсов с использованием AutoFS заданный ресурс подключается автоматически при каждом обращении пользователя и отключается после определенного времени бездействия (определяется конфигурацией AutoFS).

Принцип работы:

- задаётся каталог, в котором будет происходить подключение, например, **/mnt/auto/**;
- при необходимости обратиться к сетевой файловой системе, следует обратиться к каталогу с именем этой ФС в этом каталоге, например, **/mnt/auto/server/share/**;
- при обращении будет произведена попытка смонтировать соответствующий сетевой ресурс;
- при отсутствии обращения, после заданного таймаута, сетевой ресурс будет отмонтирован.

AutoFS использует для конфигурирования шаблоны **/etc/auto***. Основной шаблон называется **auto.master**, он может указывать на один или несколько других шаблонов для конкретных типов носителей. Пример содержимого файла **/etc/auto.master**:

```
# Format of this file:
# mountpoint map options
# For details of the format look at autofs(8).
/mnt/auto       /etc/auto.tab   -t 5
/mnt/net        /etc/auto.avahi -t 120
```

Первое значение в каждой строке определяет базовый каталог, в который носители будут монтироваться, второе значение — файл конфигурации или скрипт, который будет использован.

Примечание

Параметр ***-t*** (***--timeout***) устанавливает количество секунд, после истечения которых каталоги будут размонтированы. Значение 0 отключает таймаут. Значения параметра по умолчанию задаются в файле **/etc/autofs.conf**.

Базовый каталог будет создан, если он не существует. Он станет точкой монтирования, отображающей в себе динамически подключаемые носители, что означает, что существующее содержимое базового каталога будет недоступно пока autofs работает.

Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя:

1. Добавить в **/etc/auto.master** строку:

   ```
   /mnt/samba /etc/auto.smb -t 120
   ```

   Здесь **/mnt/samba** — каталог, в котором будут подключаться сетевые файловые системы, **/etc/auto.smb** — стандартный скрипт, входящий в состав пакета autofs, 120 — таймаут подключения при отсутствии обращения.

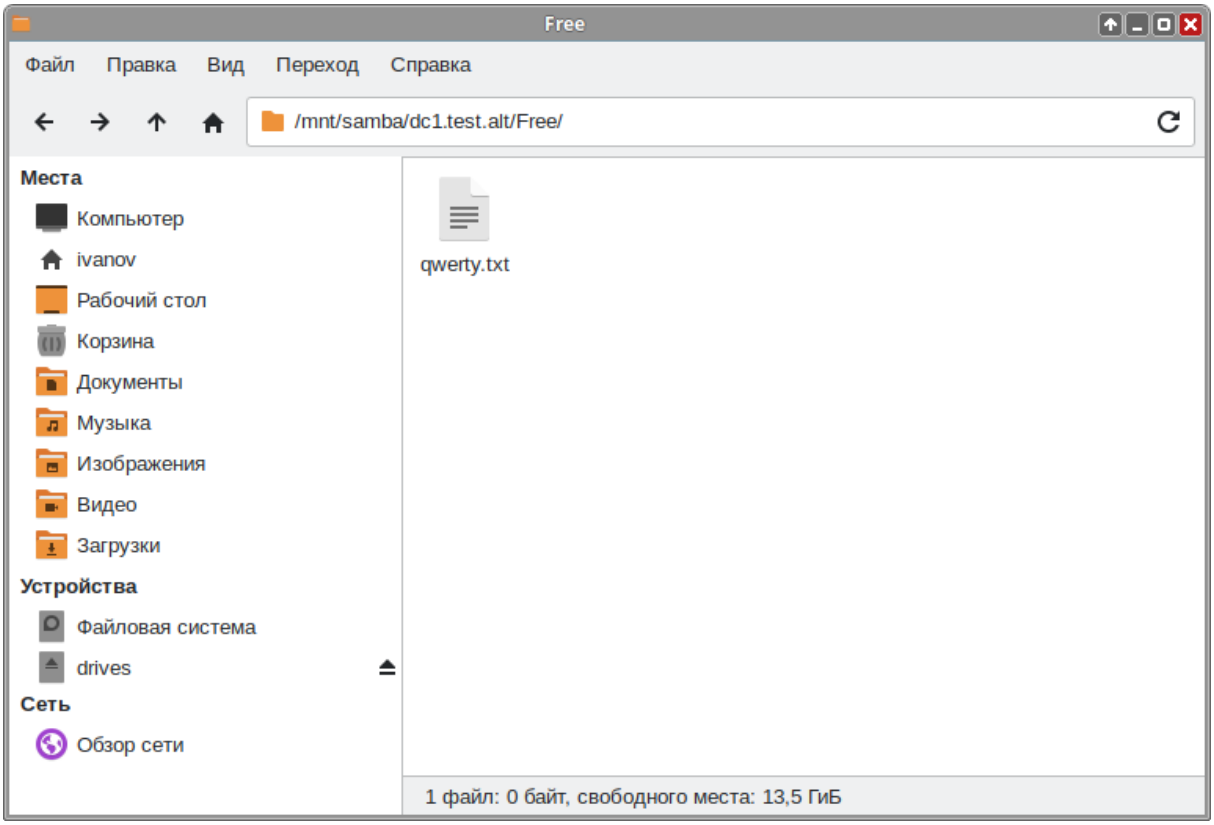
2. Включить и запустить сервис **autofs**:

   ```
   # systemctl enable --now autofs
   ```

3. Для автоматического подключения ресурсов достаточно обратиться к ресурсу по имени хоста, например:

```
$ ls /mnt/samba/<имя_хоста>
```

   или в диспетчере файлов:



Пример настройки автоматического подключения сетевых файловых ресурсов Windows (Samba) при входе пользователя в систему для дистрибутивов с KDE (Альт Рабочая станция К, Альт Образование):

1. Установить пакет *kde5-autofs-shares*:

```
# apt-get install kde5-autofs-shares
```

2. Добавить в **`/etc/auto.master`** строку:

```
/mnt/samba /etc/auto.smb -t 120
```

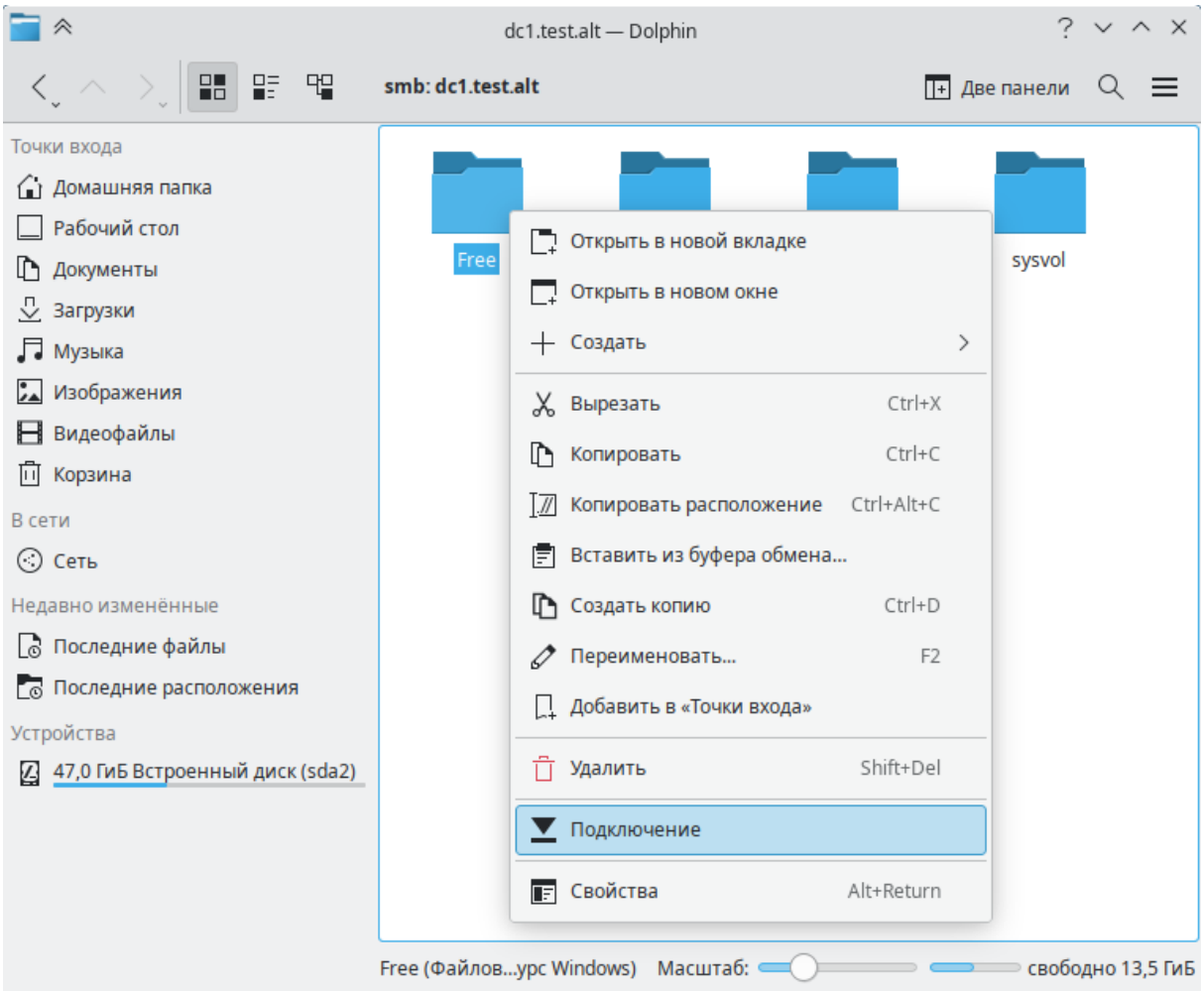
   Здесь **`/mnt/samba`** — каталог, в котором будут подключаться сетевые файловые системы, **`/etc/auto.smb`** — скрипт, входящий в состав пакета *autofs*, 120 — таймаут подключения при отсутствии обращения.

3. Включить и запустить сервис **autofs**:

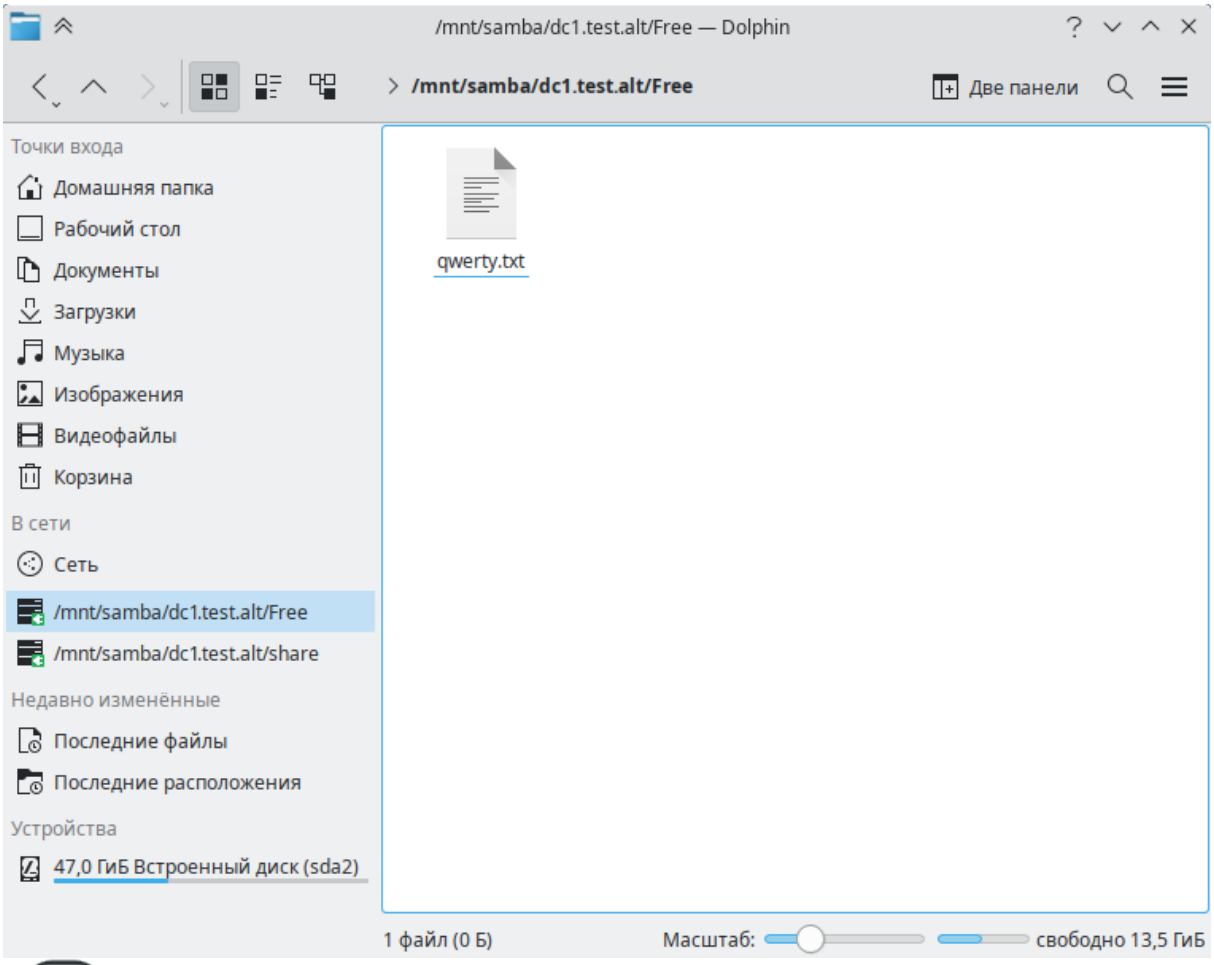
```
# systemctl enable --now autofs
```

4. В диспетчере файлов **Dolphin** по адресу smb://test.alt (**Сеть** → **Общие папки Samba**) найти нужный ресурс Windows (Samba).

5. В контекстном меню подключаемого ресурса выбрать пункт **Подключение**:



Данный ресурс будет подключаться автоматически при входе в систему:



Примечание

Список ресурсов для подключения хранится в файле **`~/.autofs.shares`**.

Важно

Данный способ работает только для ресурсов с гостевым доступом или ресурсов с авторизацией Kerberos.

Глава 53. Журналирование в Samba

53.1. Настройка бэкендов

53.2. Настройка файлов журнала

53.3. Уровни журналирования

53.4. Настройка ведения журнала аудита

53.5. Интерпретация журналов аудита JSON

Сервер Samba позволяет гибко настраивать журналирование для выявления возможных проблем в работе службы каталогов, а также мониторинга событий, связанных с аутентификацией, авторизацией и внесением изменений в базу данных службы.

Файлы журналов службы Samba по умолчанию находятся в каталоге **/var/log/samba/**.

53.1. Настройка бэкендов

На сервере Samba одновременно может вестись журналирование с использованием нескольких бэкендов. При этом для каждого из них может быть задан свой уровень журналирования.

Установить бэкенд для Samba можно, используя параметр ***log file***, который задается в разделе ***[global]*** файла **/etc/samba/smb.conf**. Параметр представляет собой список бэкэндов, разделенных пробелом, в формате:

```
logging = backend1[:option][@loglevel] backendN[:option][@loglevel]
```

Где:

- ***backend*** — один из доступных бэкендов:
  - syslog — запись в системный журнал;
  - file — запись в файл, указанный в параметре ***log file***, либо в стандартные файлы журналов Samba в каталоге **/var/log/samba/**;
  - systemd — запись в журнал systemd;
  - lttng — трассировка с использованием инструментов фреймворка LTTng;
  - gpfs — аудит файлов в кластерной файловой системе GPFS;
  - ringbuf — запись в кольцевой буфер (ring buffer). Для задания размера буфера поддерживается необязательный аргумент size в формате:

    ```
    logging = ringbuf:size=NBYTES
    ```

    (значение по умолчанию — 1 МБ).

    Данный вариант логирования может быть полезен при анализе ошибок, которые связаны с временными эффектами и не могут быть воспроизведены при записи логов в файлы с указанием высоких уровней отладки;
- ***[:option]*** — дополнительные опции, специфичные для указанного бэкенда;
- ***[@loglevel]*** — уровень журналирования. Если для бэкенда данный параметр не установлен, в бэкенд отправляются все сообщения. Параметр ***log level*** определяет общие уровни журнала, а указанные здесь уровни определяют, что отправляется на отдельные бэкенды.

Примечание

Если параметр ***logging*** задан, то его значение переопределяет значения параметров ***syslog*** и ***syslog only***.

По умолчанию параметр ***logging*** не задан.

Пример задания параметра ***logging***:

```
logging = syslog@1 file
```

53.2. Настройка файлов журнала

Параметр ***log file*** в разделе ***[global]*** файла **/etc/samba/smb.conf** позволяет переопределить файл журнала Samba.

Параметр ***log file*** использует стандартные подстановки, что позволят иметь отдельные файлы журналов для различных сущностей и объектов, обслуживаемых Samba.

Примеры подстановок:

- ***%m*** — NetBIOS-имя клиентской машины. Этот параметр недоступен, когда Samba прослушивает порт 445, поскольку клиенты больше не отправляют эту информацию. Для возможности использования этой подстановки следует установить в разделе ***[global]*** параметр:

  ```
  smbports = 139
  ```

- ***%M*** — интернет-имя клиентской машины;
- ***%I*** — IP-адрес клиентской машины;
- ***%i*** — локальный IP-адрес, с которым установил соединение клиент;
- ***%T*** — текущие дата и время;
- ***%U*** — имя пользователя сессии.

Примечание

Получить полный список подстановок можно в разделе VARIABLE SUBSTITUTIONS на справочной странице smb.conf(5) (**man smb.conf**).

Например, для создания отдельного файла журнала для каждого подключенного узла с именем в формате <NetBIOS_name>.log в каталоге **/var/log/samba/** следует задать параметр следующим образом:

```
log file = /var/log/samba/%m.log
```

Параметр ***max log size*** в разделе ***[global]*** файла **/etc/samba/smb.conf** определяет максимальный размер файла журнала. Значение параметра задается в килобайтах. Samba периодически проверяет размер файла журнала и, если он превышен, переименовывает файл, добавляя расширение .old и создает новый файл.

Указание значения 0 для параметра ***max log size*** означает отсутствие ограничений. Значение по умолчанию 5000.

Пример установки ограничения максимального размера файла журнала в 1 МБ:

```
max log size = 1000
```

Примечание

В процессе ротации Samba перезаписывает архивированный ранее файл.

53.3. Уровни журналирования

Установить уровень журналирования для Samba можно, используя параметр ***log level*** файла **/etc/samba/smb.conf**. Для разных классов отладки можно указывать разные уровни журналирования и отдельные файлы журналов.

Уровень журналирования задается в виде целого числа в диапазоне от 0 до 10, где 0 соответствует отключению вывода отладочной информации, а 10 — обеспечивает вывод полной отладочной информации об ошибках и проблемах, которые могут возникать в процессе работы Samba. Оптимальным для получения отладочной информации является уровень 3. Уровни выше 3 предназначены преимущественно для выявления внутренних ошибок Samba. Их использование может привести к существенному снижению производительности сервера.

В таблице Классы отладки приведено описание доступных классов отладки.

Таблица 53.1. Классы отладки

Класс отладки	Описание
all	Включает все сообщения отладки и подходит для общего мониторинга системы
tdb	Отвечает за отладку работы с TDB (Trivial Database). TDB — это простая встраиваемая база данных, используемая Samba для хранения различных данных, таких как сессии, аутентификационные данные, метаданные файлов и другие внутренние структуры
printdrivers	Используется для отладки драйверов печати. Этот класс полезен для отладки и анализа работы с принтерами, включая загрузку, установку и настройку драйверов
lanman	Предназначен для отладки протоколов LAN Manager, что может быть полезно при работе с устаревшими системами или приложениями
smb	Предназначен для регистрации вызовов по протоколу SMB
rpc_parse	Включает информацию об обработке RPC-сообщений. Может использоваться при анализе репликации

Класс отладки	Описание
rpc_srv	Включает информацию о регистрации конечных точек RPC
rpc_cli	Предназначен для регистрации информации, связанной с работой RPC-клиента (Remote Procedure Call). Используется для отладки взаимодействия между клиентом и сервером в контексте RPC-вызовов, которые используются для выполнения различных операций в Samba, таких как управление доменными службами, доступ к общим ресурсам и другие действия, связанные с протоколами SMB/CIFS
passdb	Предназначен для регистрации доступа к хранилищу данных паролей
sam	Предназначен для регистрации событий, связанных с управлением учетными записями пользователей и групп в AD (SAM — Security Accounts Manager)
auth	Предназначен для регистрации событий аутентификации пользователей. Включает процессы проверки учетных данных (логин/пароль), использование Kerberos, NTLM и других механизмов аутентификации
winbind	Предназначен для регистрации сообщений при присоединении клиентов к Samba для проведения различных операций. Позволяет анализировать работу сервиса Winbind
vfs	Предназначен для журналирования проблем с правами доступа и некорректным поведением бэкенда, абстрагируемого VFS
idmap	Предназначен для регистрации событий установки соответствия между SID и группами в Linux (Identity Mapping)
quota	Предназначен для регистрации информации, связанной с управлением квотами (quotas) на файловых системах. Квоты используются для ограничения объема дискового пространства, которое может использовать пользователь или группа
acls	Предназначен для регистрации событий проверки и изменения прав доступа на основе списков управления доступом (Access Control Lists)
locking	Предназначен для регистрации событий блокировок файлов базы данных каталога и конкретных записей при одновременном доступе к ним разных клиентов
msdfs	Предназначен для регистрации событий, связанных с поддержкой DFS (Distributed File System) в Samba. DFS позволяет объединять несколько общих ресурсов в одну виртуальную иерархию
dmapi	Предназначен для регистрации событий, связанных с использованием DMAPI (Data Management API) в Samba
registry	Предназначен для регистрации взаимодействия с данными реестра Windows, которые используются в службе каталогов
scavenger	Предназначен для регистрации событий «сборки мусора» (garbage collection) в Samba. Этот процесс используется для очистки устаревших или неиспользуемых данных, таких как открытые файлы, сессии, аутентификации и другие ресурсы, которые больше не нужны

Класс отладки	Описание
dns	Предназначен для регистрации запросов на поиск и изменение записей DNS
ldb	Предназначен для регистрации подключений к базе данных LDAP
tevent	Предназначен для регистрации сообщений библиотеки управления памятью talloc
auth_audit, auth_json_audit	Предназначены для регистрации событий аутентификации и авторизации учетных записей (успешных и неуспешных попытках входа в систему, изменениях паролей и изменениях статусов учетных записей). Могут использоваться, например, для отслеживания попыток несанкционированного входа
kerberos	Предназначен для регистрации событий взаимодействия по протоколу Kerberos
drs_repl	Предназначен для регистрации событий входящей и исходящей репликации на контроллере домена
smb2	Предназначен для регистрации вызовов по протоколу SMB (SMB2 и SMB3)
smb2_credits	Предназначен для регистрации запросов передачи данных по протоколу SMB. Записи содержат информацию о количестве переданных запросов и количестве запросов, которые осталось выполнить для завершения передачи файлов
dsdb_audit, dsdb_json_audit	Предназначены для регистрации изменений в базе данных контроллера домена Samba (sam.ldb) (изменения пользователей, групп, разрешений, структуры каталога и т. д.)
dsdb_password_audit, dsdb_password_json_audit	Предназначены для регистрации событий изменения и сброса паролей
dsdb_transaction_audit, dsdb_transaction_json_audit	Предназначены для регистрации транзакций (фиксация, откат) в базе данных каталога. Могут использоваться для контроля целостности данных
dsdb_group_audit, dsdb_group_json_audit	Предназначены для регистрации изменений в составе групп

Некоторые модули при первом использовании регистрируют динамические классы отладки, например:

- catia
- dfs_samba4
- extd_audit
- fileid
- fruit
- full_audit
- media_harmony
- preopen

- recycle
- shadow_copy
- unityed_media
- virusfilter

Чтобы настроить ведение журналов для определенных классов так, чтобы они писались в другой файл, а не в общий файл журнала, можно добавить ***@PATH*** к классу.

Получить дополнительную информацию и список классов отладки можно на справочной странице smb.conf(5) (**`man smb.conf`**).

53.3.1. Установка уровня журналирования в файле `smb.conf`

Примеры использования параметра ***`log level`*** для настройки уровня журналирования:

- установить уровень журнала 3 для всех классов отладки:

```
log level = 3
```

- установить общий уровень журнала 3, а для классов passdb и auth — 5:

```
log level = 3 passdb:5 auth:5
```

- установить общий уровень журнала 3, а для класса winbind — 1 и писать логи в файл **`/var/log/winbind.log`**:

```
log level = 3 winbind:1@/var/log/winbind.log
```

53.3.2. Установка уровня журналирования при выполнении команд

Команды Samba используют уровень журналирования, установленный в параметре ***`log level`*** в файле **`/etc/samba/smb.conf`**. Для всех команд Samba это значение можно переопределить, используя следующую опцию:

```
-d DEBUGLEVEL, --debuglevel=DEBUGLEVEL
```

Например:

```
$ net usershare add Share2 /tmp/share2 -d 5
# samba-tool group add testgroup12 -d dsdb_audit:3
```

53.4. Настройка ведения журнала аудита

Samba поддерживает ведение журнала событий аутентификации и авторизации, а также ведение журнала изменений базы данных контроллера домена. Это позволяет регистрировать, например, неудачные запросы аутентификации или сбросы пароля.

Ведение журнала аудита является локальной настройкой, эту функцию необходимо включить на каждом сервере Samba. События регистрируются только на том сервере Samba, на котором произошло событие. Чтобы хранить все журналы на централизованном сервере, следует настроить централизованный сервер системных журналов, настроить Samba для регистрации в syslog и настроить syslog для отправки журналов на централизованный сервер.

Для мониторинга файлов журналов и выполнения определенных действий на основе результатов их анализа могут использоваться дополнительные утилиты.

Примечание

Samba генерирует некоторые журналы на узле в конфигурации файлового сервера и члена домена, но полная поддержка доступна только на контроллере домена.

Журнал аудита Samba поддерживает стандартный формат и формат JSON. Можно включить каждый формат по отдельности или оба вместе, используя разные классы отладки журнала (например, ***`auth_audit`*** для ведения записи в стандартном формате и ***`auth_json_audit`*** для ведения записи в формате JSON).

В зависимости от уровня журналирования Samba регистрирует разные события. Чтобы ограничить количество записей в журнале, можно увеличить уровень журналирования только для классов отладки, связанных с аудитом.

53.4.1. Регистрация событий аутентификации и авторизации

Samba поддерживает протоколирование успешных и неуспешных событий аутентификации, а также успешных событий авторизации.

Примечание

Аутентификация

Аутентификация происходит, когда Samba проверяет комбинацию имени пользователя и пароля.

Авторизация

Авторизация происходит при запуске сеанса.

Следующие примеры показывают, в каких случаях Samba регистрирует события аутентификации и авторизации:

1. При входе пользователя в домен центр распространения ключей Kerberos (KDC), работающий на DC, фиксирует событие аутентификации. Если в домене работают несколько контроллеров, запрос аутентификации регистрируется только на контроллере, который обслуживает данный запрос.

2. При подключении к общему ресурсу на участнике домена:

   - участник домена регистрирует событие авторизации;

- при использовании аутентификации Kerberos центр распространения ключей (KDC) на контроллере домена Samba фиксирует событие аутентификации. В случае использования аутентификации Kerberos за нее отвечает KDC. Поэтому Samba на участнике домена не может регистрировать такое событие аутентификации;

  при использовании аутентификации через NT LAN Manager (NTLM) участник домена регистрирует событие аутентификации.

Примечание

При использовании NTLM всегда регистрируется пара событий — событие аутентификации и событие авторизации. Однако при использовании Kerberos регистрируется только одно событие на контроллере домена в момент выдачи билета TGT (Ticket Granting Ticket). После этого каждый раз при получении доступа к какой-либо службе регистрируется событие авторизации.

Для регистрации событий аутентификации и авторизации используются следующие классы отладки:

- **auth_audit** — регистрация в стандартном формате;
- **auth_json_audit** — регистрация в формате JSON.

Для классов **auth_audit** и **auth_json_audit** доступны следующие уровни журналирования (каждый последующий уровень включает все предшествующие ему):

- 2 — неуспешные события аутентификации;
- 3 — успешные события аутентификации;
- 4 — успешные события авторизации;
- 5 — успешные анонимные события аутентификации и авторизации.

Пример включения ведения журнала аудита аутентификации (установить уровень журнала по умолчанию — 1, включить регистрацию неудачных и успешных запросов аутентификации — 3):

1. Установить в секции ***[global]*** файла **/etc/samba/smb.conf**:

   ```
   log level = 1 auth_audit:3 auth_json_audit:3
   ```

2. Перезапустить службу Samba.

Пример записей о неуспешной и успешной попытках аутентификации пользователя с использованием стандартного формата журнала:

```
[2024/05/29 14:32:52.509247,  2] ../../auth/
auth_log.c:858(log_authentication_event_human_readable)
Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[ivanov\
\@TEST@TEST.ALT] at [Wed, 29 May 2024 14:32:52.509236 EET] with [aes256-cts-hmac-
sha1-96] status [NT_STATUS_WRONG_PASSWORD] workstation [(null)] remote host
[ipv4:192.168.0.135:51947] mapped to [TEST]\[ivanov]. local host [NULL]

[2024/05/29 14:39:06.426556,  3] ../../auth/
auth_log.c:858(log_authentication_event_human_readable)
```

```
Auth: [Kerberos KDC,ENC-TS Pre-authentication] user [(null)]\[ivanov\
\@TEST@TEST.ALT] at [Wed, 29 May 2024 14:39:06.426540 EET] with [aes256-cts-hmac-
sha1-96] status [NT_STATUS_OK] workstation [(null)] remote host
[ipv4:192.168.0.135:55134] became [TEST]\[ivanov]
[S-1-5-21-578923263-1107570656-1287136478-1103]. local host [NULL]
```

Пример записей о неуспешной и успешной попытках аутентификации пользователя с использованием формата JSON:

```
{"timestamp": "2024-05-29T14:32:52.509393+0200", "type": "Authentication",
"Authentication": {"version": {"major": 1, "minor": 3}, "eventId": 4625,
"logonId": "5bd240f7cc4de1b5", "logonType": 3, "status":
"NT_STATUS_WRONG_PASSWORD", "localAddress": null, "remoteAddress":
"ipv4:192.168.0.135:51947", "serviceDescription": "Kerberos KDC",
"authDescription": "ENC-TS Pre-authentication", "clientDomain": null,
"clientAccount": "ivanov\\@TEST@TEST.ALT", "workstation": null, "becameAccount":
"ivanov", "becameDomain": "TEST", "becameSid":
"S-1-5-21-578923263-1107570656-1287136478-1103", "mappedAccount": "ivanov",
"mappedDomain": "TEST", "netlogonComputer": null, "netlogonTrustAccount": null,
"netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0,
"netlogonTrustAccountSid": null, "passwordType": "aes256-cts-hmac-sha1-96",
"clientPolicyAccessCheck": null, "serverPolicyAccessCheck": null, "duration":
3129}}

{"timestamp": "2024-05-29T14:39:06.426725+0200", "type": "Authentication",
"Authentication": {"version": {"major": 1, "minor": 3}, "eventId": 4624,
"logonId": "11424f6685e647f9", "logonType": 3, "status": "NT_STATUS_OK",
"localAddress": null, "remoteAddress": "ipv4:192.168.0.135:55134",
"serviceDescription": "Kerberos KDC", "authDescription": "ENC-TS Pre-
authentication", "clientDomain": null, "clientAccount": "ivanov\\@TEST@TEST.ALT",
"workstation": null, "becameAccount": "ivanov", "becameDomain": "TEST",
"becameSid": "S-1-5-21-578923263-1107570656-1287136478-1103", "mappedAccount":
"ivanov", "mappedDomain": "TEST", "netlogonComputer": null,
"netlogonTrustAccount": null, "netlogonNegotiateFlags": "0x00000000",
"netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "passwordType":
"aes256-cts-hmac-sha1-96", "clientPolicyAccessCheck": null,
"serverPolicyAccessCheck": null, "duration": 5421}}
```

53.4.2. Регистрация изменений в базе данных

Для регистрации изменений в базе данных контроллера домена Samba (sam.ldb) используются следующие классы отладки:

- **dsdb_audit** — регистрация в стандартном формате;
- **dsdb_json_audit** — регистрация в формате JSON.

Для регистрации изменений в составе групп используются следующие классы отладки:

- **dsdb_group_audit** — регистрация в стандартном формате;
- **dsdb_group_json_audit** — регистрация в формате JSON.

Для классов **dsdb_audit**, **dsdb_json_audit**, **dsdb_group_audit** и **dsdb_group_json_audit** доступны следующие уровни журналирования:

- 5 — внесение изменений в базу данных;

- 5 — регистрация изменений, полученных через механизм репликации с другого контроллера домена.

События изменения и сброса паролей регистрируются в рамках следующих классов отладки:

- **dsdb_password_audit** — регистрация в стандартном формате;
- **dsdb_password_json_audit** — регистрация в формате JSON.

Примечание

Каждое изменение пароля также регистрируется как событие аутентификации через классы отладки **auth_audit** и **auth_audit_json**.

Для классов **dsdb_password_audit** и **dsdb_password_json_audit** доступны следующие уровни журналирования:

- 5 — успешные события изменения и сброса пароля.

Для регистрации неуспешных транзакций, завершающихся откатом, и событий подготовки фиксации данных (prepare commit) используются следующие классы отладки:

- **dsdb_transaction_audit** — регистрация в стандартном формате;
- **dsdb_transaction_json_audit** — регистрация в формате JSON.

Для классов **dsdb_transaction_audit** и **dsdb_transaction_json_audit** доступны следующие уровни журналирования:

- 5 — неуспешная транзакция (откат);
- 10 — успешная транзакция (фиксация).

В Samba возможны откаты транзакций. Они редко отражают что-либо помимо неуспешного завершения отдельной операции (например, в результате попытки создания записи, которая конфликтует с существующими). Записи о транзакции формируются и фиксируются в системных журналах до ее завершения. Такое журналирование информации о транзакциях позволяет выявлять операции с паролями и операции по внесению изменении в sam.ldb, которые закончились откатом и фактически не были выполнены.

Пример включения ведения журнала аудита базы данных DC (установить уровень журнала по умолчанию — 1, включить ведение журнала изменений базы данных в формате JSON):

1. Установить в секции ***[global]*** файла **/etc/samba/smb.conf**:

```
log level = 1 dsdb_json_audit:5 dsdb_password_json_audit:5
dsdb_group_json_audit:5 dsdb_transaction_json_audit:5
```

2. Перезапустить службу Samba.

53.5. Интерпретация журналов аудита JSON

Если включено ведение журнала аудита в формате JSON, сведения о различных событиях регистрируются в формате JSON. Каждое событие описывается определенным набором атрибутов, соответствующим его типу. Внешний слой атрибутов состоит из трёх элементов: метки времени, типа события и объекта данных (в примере добавлены переносы на новую строку и отступы; реальные записи всегда форматируются в виде одной строки):

```
{
"timestamp": 2024-05-29T14:32:52.509393+0200,
"type": одно из значений "Authentication", "Authorization", "dsdbChange",
        "dsdbTransaction", "passwordChange", "replicatedUpdate",
        "groupChange",
type: { data }
}
```

Примечание

Некоторые атрибуты могут присутствовать в записях, даже если они неприменимы. Например, если NETLOGON не используется (согласно ***serviceDescription***), для параметра ***netlogonComputer*** будет установлено значение «null», для параметра ***netlogonNegotiateFlags*** будет установлено значение «0x00000000», другие параметры, оносящиеся к NETLOGON, будут иметь аналогичные пустые значения.

53.5.1. Общие атрибуты

В таблице Общие атрибуты приведен набор атрибутов, которые присутсвуют при регистрации любого события.

Таблица 53.2. Общие атрибуты

Атрибут	Значение
version	Номер версии формата JSON. Состоит из двух частей: ▪ «major» — увеличивается, если поля меняют значение; ▪ «minor» — увеличивается, если добавляется новое поле. Изменения в перечне возможных значений обычно не приводят к изменению версии. Это распространяется на все данные, предоставляемые клиентами. Также это относится, например, к атрибуту ***passwordType***, набор поддерживаемых форматов которого может меняться с течением времени без изменения версии в JSON

53.5.2. Атрибуты событий аутентификации (Authentication)

В таблице Атрибуты событий аутентификации приведен набор атрибутов, который используется для регистрации событий аутентификации.

Таблица 53.3. Атрибуты событий аутентификации

Атрибут	Значение
authDescription	Тип аутентификации: - «simple bind/TLS», «simple bind» — простая привязка LDAP с каналом TLS или без него; - «guest» — анонимный запрос SMB1; - «bare-NTLM» — запрос SMB, использующий протокол NT1; - «plaintext» — запрос SMB, в виде обычного текста; - «interactive» — аналог физического входа на конкретной рабочей станции; - «network» — проверка подлинности запроса/ответа по сети; - «Unknown Auth Description», «Unknown Pre-authentication» — события KDC; - «ServerAuthenticate» — запрос/ответ компьютера при входе в систему с использованием NETLOGON; - «LDAP Modify» — смена пароля (не событие аутентификации, но регистрируется здесь, чтобы администратор не пропустил его)
becameAccount	Имя учетной записи, под которой выполнен вход (может не совпадать со значением, предоставленным клиентом)
becameDomain	Имя домена, в который произведён вход
becameSid	Идентификатор безопасности (SID) аутентифицированной учетной записи
clientAccount	Имя учётной записи, предоставленное клиентом
clientDomain	Имя домена, предоставленное клиентом
duration	Время (в микросекундах), в течение которого выполнялась аутентификация
eventId	Идентификатор события Windows, указывающий в общих чертах, что произошло: - 4624 соответствует успешной попытке аутентификации; - 4625 соответствует неуспешной попытке аутентификации;
localAddress	Адрес сервера и используемый порт
logonId	Случайный 64-битный идентификатор, помогающий отслеживать события входа в систему на разных этапах
logonType	Тип входа в Windows. Для Samba один из: - 2 — интерактивный, то есть вход выполняется на текущем компьютере; - 3 — сетевой, то есть вход выполняется по сети; - 8 — сетевой с использованием нехешированных паролей, то есть вход выполняется по сети, при этом пароль передается в пакет подтверждения подлинности в нехешированной форме (NetworkCleartext)

Атрибут	Значение
mappedAccount	Имя учетной записи клиента, преобразованное в имя учетной записи Альт Домен
mappedDomain	Имя домена клиента, преобразованное в доменное имя Альт Домен
netlogonComputer	Имя компьютера, заявленное при аутентификации через NETLOGON RPC
netlogonNegotiateFlags	Флаги NETLOGON, согласуемые в процессе взаимодействия клиента и сервера
netlogonSecureChannelType	Тип безопасного канала, используемого для входа по протоколу NETLOGON
netlogonTrustAccount	Учетная запись, используемая для аутентификации по протоколу NETLOGON
netlogonTrustAccountSid	Идентификатор безопасности (SID) учётной записи, используемый для аутентификации по протоколу NETLOGON
passwordType	Алгоритм/протокол пароля (например, «HMAC-SHA256», «NTLMv2», «arcfour-hmac-md5»)
remoteAddress	Заявленный адрес (и порт) удаленного клиента
serviceDescription	Тип службы (например, «LDAP», «SMB2», «NETLOGON», «Kerberos KDC»)
status	Сообщение NT STATUS. Для успешной аутентификации это будет «NT_STATUS_OK». Неудачная аутентификация может иметь значение «NT_STATUS_OK», если аутентификация не удалась после регистрации этого сообщения, но обычно имеет код ошибки. Некоторые типы сообщений при неудачной аутентификации: » NT_STATUS_ACCESS_DENIED — доступ запрещен по неустановленным причинам (наиболее вероятная причина — неправильные учетные данные); » NT_STATUS_WRONG_PASSWORD — неверный пароль; » NT_STATUS_NO_SUCH_USER — пользователь не существует; » NT_STATUS_NO_SUCH_DOMAIN — домен не существует; » NT_STATUS_ACCOUNT_RESTRICTION — учетная запись защищена или иным образом ограничена; » NT_STATUS_DOWNGRADE_DETECTED — клиент, возможно, предпринимает какие-либо действия для использования некорректных способов аутентификации; » NT_STATUS_INVALID_SERVER_STATE — сервер, возможно, используется не по назначению; » NT_STATUS_INVALID_INFO_CLASS — сервер, возможно, используется не по назначению; » NT_STATUS_INVALID_PARAMETER — клиент получил некорректные данные; » NT_STATUS_NETWORK_CREDENTIAL_CONFLICT — в процессе входа произошли изменения (возможно, имеет место гонка в рамках изменения учетных данных, либо при согласовании данных шифрования возникла ошибка);

Атрибут	Значение
	NT_STATUS_NOT_IMPLEMENTED — тип аутентификации не реализован в Samba; NT_STATUS_NOT_SUPPORTED — тип аутентификации, либо способ его использования со стороны клиента не поддерживается Samba; NT_STATUS_INVALID_SYSTEM_SERVICE — выбранная служба аутентификации недоступна; NT_STATUS_INTERNAL_ERROR — сервер не может завершить выполнение аутентификации по причине внутренней ошибки; NT_STATUS_NO_MEMORY — сервер не может завершить аутентификацию по причине нехватки памяти
version	См. описание в таблице Общие атрибуты. Текущая версия: `{"major": 1, "minor": 3}`
workstation	Заявленное имя клиентской рабочей станции

Пример записи об успешной попытке аутентификации:

```
{"timestamp": "2024-05-29T14:39:06.426725+0200", "type": "Authentication",
"Authentication": {"version": {"major": 1, "minor": 3}, "eventId": 4624,
"logonId": "11424f6685e647f9",
"logonType": 3, "status": "NT_STATUS_OK", "localAddress": null, "remoteAddress":
"ipv4:192.168.0.135:55134",
"serviceDescription": "Kerberos KDC", "authDescription": "ENC-TS Pre-
authentication",
"clientDomain": null, "clientAccount": "ivanov\\@TEST@TEST.ALT", "workstation":
null,
"becameAccount": "ivanov", "becameDomain": "TEST", "becameSid":
"S-1-5-21-578923263-1107570656-1287136478-1103",
"mappedAccount": "ivanov", "mappedDomain": "TEST", "netlogonComputer": null,
"netlogonTrustAccount": null,
"netlogonNegotiateFlags": "0x00000000", "netlogonSecureChannelType": 0,
"netlogonTrustAccountSid": null,
"passwordType": "aes256-cts-hmac-sha1-96", "clientPolicyAccessCheck": null,
"serverPolicyAccessCheck": null, "duration": 5421}}
```

53.5.3. Атрибуты событий авторизации (Authorization)

В таблице Успешные события авторизации приведен набор атрибутов, который используется для регистрации успешных событий авторизации.

Таблица 53.4. Успешные события авторизации

Атрибут	Значение
account	Имя авторизуемой учетной записи
accountFlags	Битовое поле атрибутов учетной записи
authType	

Атрибут	Значение
	Строка, описывающая тип авторизации (например, «krb5», «NTLMSSP», «simple bind»)
domain	Имя домена
localAddress	Адрес сервера и используемый порт
logonServer	Сервер, на котором выполнена аутентификация
remoteAddress	Видимый адрес клиента
serviceDescription	Тип службы (например, «LDAP», «SMB2», «DCE/RPC»)
sessionId	Уникальный идентификатор сессии (GUID)
sid	Идентификатор безопасности (SID) авторизуемой учетной записи
transportProtection	Тип защиты, используемой в канале (например, «SMB», «TLS», «SEAL», «NONE»)
version	См. описание в таблице Общие атрибуты. Текущая версия: `{"major": 1, "minor": 2}`

Пример записи об успешной попытке авторизации:

```
{"timestamp": "2024-05-29T15:32:39.282334+0200", "type": "Authorization",
"Authorization": {"version": {"major": 1, "minor": 2}, "localAddress":
"ipv4:127.0.0.1:389",
"remoteAddress": "ipv4:127.0.0.1:43350", "serviceDescription": "LDAP",
"authType": "simple bind", "domain": "NT AUTHORITY", "account": "ANONYMOUS
LOGON",
"sid": "S-1-5-7", "sessionId": "5accdd86-4c6e-4bd2-8ab1-7e95f641ecf2",
"logonServer": "DC1", "transportProtection": "NONE", "accountFlags":
"0x00000010",
"clientPolicyAccessCheck": null, "serverPolicyAccessCheck": null}}
```

53.5.4. Атрибуты событий, связанных с изменениями в базе данных (dsdbChange)

События dsdbChange регистрируются, когда клиент вызывает существенные изменения в базе данных домена (известной как DSDB внутри Samba). Некоторые конкретные изменения, а именно изменения пароля, группы и изменения репликации, регистрируются отдельно как события «passwordChange», «groupChange» и «replicationUpdate».

В таблице События dsdbChange приведен набор атрибутов, который используется для регистрации событий, связанных с внесением значимых изменений в базу данных службы каталогов.

Таблица 53.5. События dsdbChange

Атрибут	Значение
attributes	Список изменяемых атрибутов
dn	Уникальное составное имя (DN) изменяемого объекта
operation	

Атрибут	Значение
	Операция LDAP, соответствующая выполняемому действию по изменению данных: ▪«Modify» ▪«Add» ▪«Delete»
performedAsSystem	Признак системного или пользовательского действия: ▪«true» — действие выполняется Samba с использованием системной учетной записи; ▪«false» — действие выполняется от имени пользователя
remoteAddress	Удаленный адрес пользователя, инициировавшего операцию
sessionId	Уникальный идентификатор (GUID) сессии аутентификации
status	Строка, указывающая на успешное завершение действия или невозможность его выполнения по той или иной причине; выводимая информация соответствует кодам ответа LDAP, которые фиксируются в атрибуте ***statusCode***. Примеры значений: ▪«Success» ▪«Operations error» ▪«Protocol error» ▪«Time limit exceeded» ▪«Size limit exceeded» ▪«Unsupported critical extension» ▪«No such attribute» ▪«Undefined attribute type» ▪«Constraint violation» ▪«Attribute or value exists» ▪«Invalid attribute syntax» ▪«No such object» ▪«Alias problem» ▪«Invalid DN syntax» ▪«Insufficient access rights» ▪«Unwilling to perform» ▪«Naming violation» ▪«Object class violation» ▪«Not allowed on non-leaf» ▪«Not allowed on RDN» ▪«Entry already exists»
Числовой код, соответствующий статусу в атрибуте ***status***	В общем случае в качестве значения атрибута приводится код ответа LDAP в соответствии с RFC 4511
transactionId	Уникальный идентификатор (GUID) транзакции, в рамках которой выполняется операция (если операция является частью транзакции)

Атрибут	Значение
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице Общие атрибуты. Текущая версия: `{"major": 1, "minor": 2}`

Значение поля ***attributes*** может рассматриваться в качестве аналога описания изменения в формате LDIF.

Например, следующий JSON:

```
"dsdbChange": {
"operation": "Modify",
"dn": "@SAMBA_DSDB",
"attributes": {
"backupDate": {"actions": [
{"action": "add",
    "values": [
    {"value": "2024-05-29T15:32:39.282334+0200"}
    ]
  }
 ]
}}}
```

описывает изменение, выполненное этим LDIF:

```
dn: @SAMBA_DSDB
changetype: modify
add: backupDate
backupDate:  2024-05-29T15:32:39.282334+0200
```

Для секретных атрибутов вместо каких-либо значений указывается тег ***redacted: true***.

Если значение очень длинное (> 1024 байт), оно будет усечено с добавлением «…» и флагом ***truncated: true***, например:

```
"values": [
    {truncated: true,
                "value": "It was the best of times, it was the worst of times, it
was the age…"
    }
]
```

Пример записи о внесении изменений в базу данных:

```
{"timestamp": "2024-05-29T09:52:14.813697+0200", "type": "dsdbChange",
"dsdbChange": {"version": {"major": 1, "minor": 0}, "statusCode": 0,
"status": "Success", "operation": "Modify",
"remoteAddress": "ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:38500",
"performedAsSystem": false,
"userSid": "S-1-5-21-578923263-1107570656-1287136478-500",
"dn": "CN=Марков Кирилл,CN=Users,DC=test,DC=alt", "transactionId":
```

```
"ce759566-8bf9-46ce-95a1-0d632232a220",
"sessionId": "48c760f6-6cdc-4fba-b16d-1689f2cfad33",
"attributes": {"unicodePwd": {"actions": [{"action": "replace", "redacted":
true}]}}}}
```

53.5.5. Атрибуты событий, связанных с транзакциями (dsdbTransaction)

Транзакция связывает вместе несколько операций базы данных; либо все они происходят атомарно, либо ни одна из них не происходит. Если все операции в транзакции завершаются успешно, она фиксируется, а изменения остаются постоянными, но если одна из операций завершается неудачей, все предыдущие операции откатываются, даже если они завершились успешно и были зарегистрированы как события dsdbChange.

Каждая транзакция имеет идентифицирующий GUID; другие операции DSDB, являющиеся частью транзакции, будут включать этот GUID в атрибут ***transactionId***.

В таблице Атрибуты событий, связанных с транзакциями приведен набор атрибутов, связанных с транзакциями (dsdbTransaction).

Таблица 53.6. Атрибуты событий, связанных с транзакциями

Атрибут	Значение
action	Текущий этап транзакции: ▪«begin» ▪«commit» ▪«rollback»
duration	Продолжительность транзакции в микросекундах (до момента записи этого поля)
transactionId	Уникальный идентификатор (GUID) транзакции
version	См. описание в таблице Общие атрибуты. Текущая версия: `{"major": 1, "minor": 0}`

Пример регистрации событий, связанных с транзакциями:

```
{"timestamp": "2024-05-29T20:41:36.895027+0200", "type": "dsdbTransaction",
"dsdbTransaction": {"version": {"major": 1, "minor": 0}, "action": "commit",
"transactionId": "a89149be-5c19-42c2-bf08-94ddc5b0eb78", "duration": 8819}}

{"timestamp": "2024-05-29T20:41:37.691707+0200", "type": "dsdbTransaction",
"dsdbTransaction": {"version": {"major": 1, "minor": 0}, "action": "commit",
"transactionId": "92a8db3a-94d4-4ac5-b929-b1e4344b12e3", "duration": 5697}}
```

53.5.6. Атрибуты событий, связанных с изменением пароля (passwordChange)

PasswordChange — это особый вид dsdbChange.

В таблице Атрибуты событий, связанных с изменением пароля приведен набор атрибутов, который используется для регистрации событий, связанных с изменением пароля (passwordChange).

Таблица 53.7. Атрибуты событий, связанных с изменением пароля

Атрибут	Значение
action	Тип операции: ▸«Change» — смена пароля; ▸«Reset» — сброс пароля
dn	Уникальное составное имя (DN) пользователя, пароль которого изменяется или сбрасывается
eventId	Идентификатор события Windows: ▸4723 соответствует событию смены пароля (Change); ▸4724 соответствует событию сброса пароля (Reset)
remoteAddress	Удаленный адрес пользователя, выполняющего операцию
sessionId	Идентификатор сессии DSDB
status	Текст ошибки
statusCode	Код ошибки
transactionId	Уникальный идентификатор (GUID) транзакции, в рамках которой выполняется операция (если операция является частью транзакции)
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице Общие атрибуты. Текущая версия: `{"major": 1, "minor": 1}`

Пример регистрации события сброса пароля пользователя:

```
{"timestamp": "2024-05-29T15:28:18.876663+0200", "type": "passwordChange",
"passwordChange": {"version": {"major": 1, "minor": 1}, "eventId": 4724,
"statusCode": 0, "status": "Success", "remoteAddress":
"ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:35534",
"userSid": "S-1-5-21-578923263-1107570656-1287136478-500",
"dn": "CN=Орлов Игорь,CN=Users,DC=test,DC=alt", "action": "Reset",
"transactionId": "d7456cd1-6f32-4575-b530-dc22a34bdc6a", "sessionId":
"ce6866f6-43ea-4665-a896-0d10bd3194e1"}}
```

53.5.7. Атрибуты событий, связанных с изменением группы (groupChange)

Событие groupChange указывает на изменение DSDB, которое добавляет или удаляет пользователя из группы.

В таблице Атрибуты событий, связанных с изменением группы приведен набор атрибутов, который используется для регистрации событий, связанных с изменением группы (groupChange).

Таблица 53.8. Атрибуты событий, связанных с изменением группы

Атрибут	Значение
action	Тип операции: - «Removed» — удаление пользователя из группы; - «Added» — добавление пользователя в группу; - «PrimaryGroup» — смена основной группы
eventId	Идентификатор события Windows: - 4728 пользователь добавлен в глобальную группу безопасности; - 4729 пользователь удален из глобальной группы безопасности; - 4732 пользователь добавлен в локальную группу безопасности; - 4733 пользователь удален из локальной группы безопасности; - 4746 пользователь добавлен в локальную группу; - 4747 пользователь удален из локальной группы; - 4751 пользователь добавлен в глобальную группу; - 4752 пользователь удален из глобальной группы; - 4756 пользователь добавлен в универсальную группу безопасности; - 4757 пользователь удален из универсальной группы безопасности; - 4761 пользователь добавлен в универсальную группу; - 4762 пользователь удален из универсальной группы
group	Уникальное составное имя (DN) группы
remoteAddress	Удаленный адрес пользователя, выполняющего операцию
sessionId	Идентификатор сессии DSDB
status	Текст ошибки
Числовой код, соответствующий статусу в атрибуте ***status***	В общем случае в качестве значения атрибута приводится код ответа LDAP в соответствии с RFC 4511
transactionId	Уникальный идентификатор (GUID) транзакции, в рамках которой выполняется операция (если операция является частью транзакции)
user	Уникальное составное имя (DN) пользователя, членство в группе которого изменяется в рамках операции
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице Общие атрибуты. Текущая версия:

Атрибут	Значение
	`{"major": 1, "minor": 1}`

Пример регистрации события добавления пользователя в группу:

```
{"timestamp": "2024-05-29T15:20:19.634972+0200", "type": "groupChange",
"groupChange": {"version": {"major": 1, "minor": 1}, "eventId": 4728,
"statusCode": 0, "status": "Success", "action": "Added",
"remoteAddress": "ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:59778",
"userSid": "S-1-5-21-578923263-1107570656-1287136478-500",
"group": "CN=testgroup,CN=Users,DC=test,DC=alt", "transactionId":
"28372270-093c-4bca-af45-ae3e93b71eda",
"sessionId": "9518687d-8ad1-4c2c-810c-8cc18c2943f7", "user": "CN=Марков
Кирилл,CN=Users,DC=test,DC=alt"}}
```

Глава 54. Усиление безопасности DC

54.1. Возможность анонимного получения списка пользователей, групп

54.2. Отключение Netbios

54.3. Отключение роли сервера печати

54.4. Отключение NTLMv1

54.5. Генерация дополнительных хешей паролей

54.6. Защита DNS-записей wpad и isatap

54.7. Ограничение диапазона динамических портов

54.8. Аудит запросов к каталогам SYSVOL и NetLogon

54.9. Отправка логов аудита в rsyslog

54.1. Возможность анонимного получения списка пользователей, групп

Samba наследует поведение домена NT4, которое больше не требуется в режиме Альт Домен. Например, следующая команда возвращает всех пользователей домена:

```
# rpcclient -U "" -c enumdomusers dc1.test.alt
```

Для отключения такого поведения следует внести изменения в файл **/etc/samba/smb.conf**:

```
[global]
restrict anonymous = 2
```

Может также потребоваться работа с полем ***dSHeuristics***:

```
# samba-tool forest directory_service dsheuristics 0000000
```

54.2. Отключение Netbios

Если конфигурация DNS выполнена правильно, старые протоколы NetBIOS, которые больше не нужны, могут быть отключены. Для этого следует внести изменения в секцию ***global*** файла **/etc/samba/smb.conf**:

```
[global]
disable netbios = yes
smb ports = 445
```

54.3. Отключение роли сервера печати

Контроллер домена не следует настраивать с ролью сервера печати. Сервер Samba, настроенный как файловый сервер, лучше подходит для этой функции.

Для отключения роли сервера печати следует внести изменения в секцию ***global*** файла **/etc/samba/smb.conf**:

```
[global]
printcap name = /dev/null
load printers = no
disable spoolss = yes
printing = bsd
```

54.4. Отключение NTLMv1

Протокол аутентификации NTLMv1 появился в начале 1990-х годов и был быстро заменен на NTLMv2 из-за недостатков безопасности. Он больше не полезен в современных сетях, за исключением случаев использования MS-CHAP-v2, который является протоколом по умолчанию для аутентификации 802.1x на рабочих станциях Windows (например, аутентификация Radius для подключений Wi-Fi). В случае MS-CHAP-v2 использование NTLMv1 можно до некоторой степени допустить, поскольку он инкапсулирован в другой, более надежный протокол.

В Samba есть возможность глобально отключить NTLMv1, если он не используется для аутентификации MS-CHAP-v2. Рекомендуется добавить следующий параметр в секцию ***global*** файла **/etc/samba/smb.conf**:

```
[global]
ntlm auth = mschapv2-and-ntlmv2-only
```

54.5. Генерация дополнительных хешей паролей

Чтобы разрешить передачу хешей в другую базу аутентификации, можно указать Samba генерировать дополнительные хеши, когда пользователь меняет свой пароль. Для этого следует добавить в секцию ***global*** файла **/etc/samba/smb.conf** строку:

```
[global]
password hash userPassword schemes = CryptSHA256 CryptSHA512
```

54.6. Защита DNS-записей wpad и isatap

Серверы Windows AD имеют глобальный черный список запросов DNS с двумя записями:

- wpad
- isatap

В разделе реестра ***GlobalQueryBlockList*** перечислены эти две записи DNS, для предотвращения создания таких записей и перенаправления сетевого трафика неавторизованным объектом, действующим в локальной сети. Протокол автоматического обнаружения веб-прокси (WPAD) по умолчанию настроен в браузерах WPAD, в частности в браузерах Internet Explorer.

Даже если конфигурации wpad и isatap не используются, всё равно важно создать эти две записи, чтобы предотвратить их использование обходным путем, поскольку в Альт Домен нет способа заблокировать создание записей, так как это можно сделать в Microsoft AD.

Создание записей wpad и isatap в Альт Домен:

```
# samba-tool dns add `hostname -s` `hostname -d` wpad A 127.0.0.1 -P
# samba-tool dns add `hostname -s` `hostname -d` isatap A 127.0.0.1 -P
```

54.7. Ограничение диапазона динамических портов

По умолчанию Альт Домен использует очень широкий динамический диапазон для вызовов MS-RPC. Рекомендуется ограничить этот диапазон. Для этого следует добавить в секцию ***global*** файла **/etc/samba/smb.conf** строку:

```
[global]
rpc server dynamic port range = 50000-55000
```

Примечание

Если используется фаервол, то его нужно будет перенастроить.

54.8. Аудит запросов к каталогам SYSVOL и NetLogon

Для возможности аудита запросов к каталогам SYSVOL и NetLogon следует добавить в файл **/etc/samba/smb.conf** строки:

```
[global]
...
full_audit:failure = none
full_audit:success = pwrite write renameat
full_audit:prefix = IP=%I|USER=%u|MACHINE=%m|VOLUME=%S
full_audit:facility = local7
```

```
full_audit:priority = NOTICE
...
[sysvol]
...
vfs objects = dfs_samba4, acl_xattr, full_audit
...
[netlogon]
...
vfs objects = dfs_samba4, acl_xattr, full_audit
```

54.9. Отправка логов аудита в rsyslog

54.9.1. Настройка rsyslog

На стороне приёмника сообщений (сервера):

1. Установить пакет *rsyslog-classic*:

```
# apt-get install rsyslog-classic
```

2. В файле **/etc/rsyslog.d/00_common.conf** раскомментировать строки:

```
# Для UDP
module(load="imudp")
input(type="imudp" port="514")
# Для TCP
module(load="imtcp")
input(type="imtcp" port="514")
```

3. Создать шаблон для логов **/etc/rsyslog.d/myrules.conf**:

```
$template remote-incoming-logs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* action(type="omfile" dynaFile="remote-incoming-logs"
dirCreateMode="0755" fileCreateMode="0644")
```

Примечание

Согласно данному шаблону все сообщения от любых источников (facility) с любым уровнем важности (priority) будут сохраняться на сервере в файлы **/var/log/<имя_узла-отправителя_лога>/<приложение-отправитель_лога>.log**.

4. Перезапустить службу rsyslog:

```
# systemctl restart rsyslog
```

На стороне отправителя сообщений (клиента):

1. Установить пакет *rsyslog-classic*:

```
# apt-get install rsyslog-classic
```

2. Создать файл **/etc/rsyslog.d/all.conf**, в котором прописать протокол (@@ — TCP, @ — UDP) и адрес доставки сообщений:

```
*.* @@192.168.0.111:514 # Отправка логов на сервер (TCP)
```

3. Перезапустить службу rsyslog:

```
# systemctl restart rsyslog
```

При корректной настройке на сервере в каталоге **/var/log/** должен появиться каталог с именем узла, который отправляет лог-файлы:

```
# ls -l /var/log/node02/
итого 12
-rw------- 1 root adm  810 апр  3 12:30 crond.log
-rw------- 1 root adm 1194 апр  3 12:19 login.log
-rw------- 1 root adm 2509 апр  3 12:19 rsyslogd.log
```

54.9.2. rsyslog на том же узле

В секцию ***global*** файла **/etc/samba/smb.conf** добавить строку:

```
[global]
log level = 1 auth_json_audit:3@/var/log/samba/samba_audit.log
```

Создать файл **/etc/rsyslog.d/send_samba.conf**:

```
module(load="imfile" PollingInterval="10") #needs to be done just once
input(type="imfile"
     File="/var/log/samba/samba_audit.log"
     Tag="samba_auth"
     Severity="info"
     Facility="auth")
if ($syslogtag == "samba_auth") then {
   action(type="omfwd" target="dc1.test.alt" port="514" protocol="tcp"
          action.resumeRetryCount="100"
          queue.type="linkedList" queue.size="10000")
}
```

54.9.3. rsyslog на вышестоящем узле

В секцию ***global*** файла **/etc/samba/smb.conf** добавить строку:

```
[global]
log level = 1 auth_json_audit:3@/var/log/samba/samba_audit.log
```

Создать файл **/etc/rsyslog.d/recv_samba.conf**:

```
$ModLoad imtcp
$InputTCPServerRun 514
if ($syslogtag == "samba_auth")  then /var/log/samba/audit_auth.log
```

Глава 55. Планирование и настройка диапазонов идентификаторов UID и GID (Winbind/IDMapping)

55.1. Планирование диапазонов идентификаторов

55.2. Домен * по умолчанию

55.3. Использование tdb

55.4. Использование ad

55.5. Использование rid

55.6. Использование autorid

Домены Windows различают пользователей и группы по уникальным идентификаторам безопасности (SID). Однако в Linux для каждого пользователя и группы требуются уникальные идентификаторы UID и GID. Служба winbindd отвечает за предоставление информации о пользователях и группах домена.

Чтобы служба winbindd могла предоставлять уникальные идентификаторы для пользователей и групп в Linux, необходимо на клиенте домена настроить сопоставление идентификаторов в файле **`smb.conf`** для:

- локальной база данных (домен * по умолчанию);
- домена AD;
- каждого доверенного домена, пользователи которого должны иметь доступ к ресурсам.

Samba предоставляет различные модули сопоставления идентификаторов для конкретных конфигураций. Наиболее часто используемыми модулями являются:

- tdb — в доменах * по умолчанию;
- ad — в AD доменах;
- rid — в AD доменах;
- autorid — в AD доменах и доменах * по умолчанию.

55.1. Планирование диапазонов идентификаторов

Независимо от того, хранятся ли UID и GID Linux в AD (если в AD включены расширения схемы RFC2307) или настроена их автоматическая генерация, для каждой конфигурации домена требуется уникальный диапазон идентификаторов. Этот диапазон не должен пересекаться с диапазонами других доменов.

Примечание

При пересечении диапазонов идентификаторов работа системы не будет корректной.

Пример непересекающихся диапазонов сопоставления идентификаторов для доменов по умолчанию (*), AD-DOM и TRUST-DOM:

```
[global]
...
idmap config * : backend = tdb
idmap config * : range = 10000-999999

idmap config AD-DOM:backend = rid
idmap config AD-DOM:range = 2000000-2999999

idmap config TRUST-DOM:backend = rid
idmap config TRUST-DOM:range = 4000000-4999999
```

Примечание

Можно назначить только один диапазон для каждого домена. Поэтому необходимо оставить достаточно места между диапазонами доменов, чтобы была возможность расширить диапазон позже, если домен вырастет. Если позже назначить домену другой диапазон, права на файлы и каталоги, ранее созданные пользователями и группами, будут утрачены.

Важно

Максимальное значение uid/gid:

```
2^31 - 1 = 2147483647
```

При планировании диапазонов необходимо также учитывать, что в Linux есть специальные UID, которые нельзя использовать:

- 0 — root (суперпользователь);
- 65534 — nobody UID (UID «переполнения» или аналогичный) используется в системах Linux для обозначения пользователя, который не имеет прав доступа к системным ресурсам;
- 65535, он же «16-разрядный (uid_t) -1uid_t». До того, как ядро Linux 2.4 было 16-разрядным, и программы скомпилированные для этого, следовательно, предполагали, что (uid_t)-1 равно 65535. Таким образом, этот UID непригоден для использования.

55.2. Домен * по умолчанию

В доменной среде должна быть добавлена одна конфигурация сопоставления идентификаторов для каждого из следующих параметров:

- домен, членом которого является клиент, на котором производится настройка;
- каждый доверенный домен.

Для всех остальных объектов присваиваются идентификаторы из домена по умолчанию. Сюда входят:

- локальные пользователи и группы;
- встроенные учетные записи и группы, такие как BUILTIN\Administrators.

Бэкенд домена по умолчанию должен быть доступен для записи, чтобы назначенные идентификаторы постоянно сохранялись.

Для домена по умолчанию можно использовать один из следующих бэкендов:

tdb

В данном случае необходимо задать достаточно большой диапазон идентификаторов, чтобы включать объекты, которые будут созданы в будущем и которые не являются частью определенной конфигурации сопоставления идентификаторов домена.

Например, в разделе **`[global]`** в файле **`smb.conf`** можно задать:

```
idmap config * : backend = tdb
idmap config * : range = 10000-999999
```

Для получения более подробной информации см. Использование tdb

autorid

При использовании бэкенда autorid при настройке домена * по умолчанию необязательно добавлять дополнительные конфигурации сопоставления идентификаторов для доменов.

Например, в разделе **`[global]`** в файле **`smb.conf`** можно задать:

```
idmap config * : backend = autorid
idmap config * : range = 10000-999999
```

Для получения более подробной информации см. Использование autorid

55.3. Использование tdb

Служба winbindd по умолчанию использует доступный для записи бэкенд tdb для хранения таблиц сопоставления идентификаторов безопасности (SID), UID и GID. Это относится к локальным и встроенным пользователям и группам.

Этот бэкенд следует использовать только для домена * по умолчанию.

55.4. Использование ad

Можно настроить пользователя Samba AD на использование бэкенда ad.

Бэкенд ad реализует API, доступный только для чтения, для чтения информации об учетной записи и группе из AD. Это обеспечивает следующие преимущества:

- все настройки пользователей и групп хранятся централизованно в AD;
- идентификаторы пользователей и групп совпадают на всех клиентах;

- идентификаторы не хранятся в локальной базе данных, которая может быть повреждена, и, следовательно, права на файлы не могут быть потеряны.

Примечание

Бэкенд ad не поддерживает домены AD с односторонними доверительными отношениями. Если настраивается участник домена в AD с односторонними доверительными отношениями, следует вместо этого использовать одну из следующих серверных частей сопоставления идентификаторов: tdb, rid или autorid.

Таблица 55.1. Атрибуты из AD, которые считывает бэкенд ad

Имя атрибута AD	Тип объекта	Сопоставление
sAMAccountName	Пользователь и группа	Имя пользователя или группы в зависимости от объекта
uidNumber	Пользователь	Идентификатор пользователя (UID)
gidNumber	Группа	Идентификатор группы (GID)
loginShell	Пользователь	Путь к командной строке пользователя

Предварительные требования:

- и пользователи, и группы должны иметь уникальные идентификаторы, заданные в AD. Идентификаторы должны находиться в диапазоне, настроенном в файле **smb.conf**. Объекты, идентификаторы которых находятся за пределами диапазона, не будут доступны на клиенте;
- у пользователей и групп должны быть заданы все необходимые атрибуты в AD;
- настроено сопоставление идентификаторов в файле **smb.conf**.

Пример:

```
idmap config * : backend = tdb
idmap config * : range = 3000-7999

idmap config TEST : backend = ad
idmap config TEST : range = 10000-999999
idmap config TEST : schema_mode = rfc2307
```

Чтобы разрешить клиенту домена считывать командную строку входа в систему и путь к домашнему каталогу пользователей из соответствующего атрибута AD, необходимо установить:

```
idmap config DOMAIN : unix_nss_info = yes
```

В качестве альтернативы можно установить единый путь к домашнему каталогу для всего домена и командную строку входа, которые будут применяться ко всем пользователям. Например:

```
template shell = /bin/bash
template homedir = /home/%U
```

55.5. Использование rid

Можно настроить клиента домена для использования бэкенда rid.

В AD SID состоит из нескольких частей, где каждая часть кодирует информацию, связанную с доменом или самой учетной записью. SID выглядит примерно так:

```
S-1-5-21-XXXXXXXXXX-YYYYYYYYYY-ZZZZZZZZZZ-RID
```

Где:

- S-1-5-21 — префикс SID, общая часть для идентификаторов безопасности Windows;
- XXXXXXXXXX-YYYYYYYYYY-ZZZZZZZZZZ — уникальная часть домена;
- RID — число, уникальное для каждой учетной записи в домене (например, пользователя или группы).

Для настройки idmap rid в Samba, RID берётся из последней части SID и используется для определения UID/GID на основе заранее заданного диапазона.

Если задаётся конфигурацию idmap rid, например:

```
idmap config DOMAIN : backend = rid
idmap config DOMAIN : range = 10000-999999
```

Samba берёт RID из SID и добавляет его к началу диапазона range. Например, для пользователя с SID S-1-5-21-XXXXXXXXXX-YYYYYYYYYY-ZZZZZZZZZZ-1000, UID будет вычислен как 10000 + 1000 = 11000.

Бэкенд rid реализует доступный только для чтения API для вычисления информации об учетной записи и группе на основе алгоритмической схемы сопоставления для доменов. При настройке необходимо задать наименьшее и наибольшее значения идентификаторов в параметре **`idmap config DOMAIN : range`**. Samba не будет сопоставлять пользователей или группы с более низким или более высоким RID, чем указано в этом параметре.

Примечание

Для бэкенда rid нельзя назначать новые идентификаторы, например, для BUILTIN групп. Поэтому не следует использовать этот бэкенд для домена * по умолчанию.

Важно

Необходимо планировать интервал с запасом, в соответствии с прогнозированием увеличения количества объектов, так как максимальное значение RID равно 2147483647.

Пример:

```
idmap config * : backend = tdb
idmap config * : range = 10000-999999

idmap config DOMAIN : backend = rid
idmap config DOMAIN : range = 2000000-2999999
```

Примечание

Пользователи и группы, чьи идентификаторы не входят в диапазон, игнорируются.

55.6. Использование autorid

Бэкенд autorid работает аналогично бэкенду для сопоставления идентификаторов rid, но может автоматически назначать идентификаторы для разных доменов. Это позволяет использовать autorid в следующих ситуациях:

- только для домена * по умолчанию;
- для домена * по умолчанию и дополнительных доменов, без необходимости создавать конфигурации сопоставления идентификаторов для каждого из дополнительных доменов (любые домены, кроме основного). Они могут быть доверенными доменами в инфраструктуре AD. Для таких доменов можно не указывать подробную конфигурацию в **`smb.conf`**.
- только для определенных доменов (те домены, для которых вручную заданы конкретные параметры сопоставления идентификаторов).

Пример:

```
idmap config * : backend = autorid
idmap config * : range = 100000-9999999
```

Примечание

По умолчанию значение rangesize равно 100000.

При необходимости можно задать другой размер диапазона:

```
idmap config * : rangesize = 200000
```

Примечание

После того как был задан диапазон и клиент домена начал его использовать, можно будет увеличить только верхний предел диапазона. Любое другое изменение диапазона (range) или размера диапазона (rangesize) может привести к нарушению сопоставления идентификаторов.

Клиент присваивает это количество непрерывных идентификаторов каждому объекту домена до тех пор, пока не будут взяты все идентификаторы из диапазона, заданного в параметре **`idmap config * : range`**.

Примечание

Диапазон (range) должен быть кратен размеру диапазона (rangesize).

Глава 56. Инструменты командной строки

56.1. samba-tool

56.2. wbinfo

56.3. net

56.4. adcli

56.5. ldapsearch

56.6. sssctl

56.7. testparm

Таблица 56.1. Основные инструменты командной строки

Утилита	Описание
samba-tool	Основная утилита управления Samba
wbinfo	Позволяет получить информацию от демона winbindd
net	Инструмент администрирования Samba и удаленных серверов CIFS
adcli	Инструмент для выполнения действий в домене Active Directory
ldapsearch	Утилита для поиска информации в LDAP
testparm	Проверка корректности содержимого основного файла конфигурации Samba — **`/etc/samba/smb.conf`**

56.1. samba-tool

Для управления Samba AD DC в состав пакета Samba входит инструмент командной строки **`samba-tool`**.

Таблица 56.2. Основные команды samba-tool

Команда	Описание
computer	Управление учетными записями компьютеров
contact	Управление контактами
dbcheck	Проверка локальной базы данных домена на наличие ошибок
delegation	Управление делегированием
dns	Управление параметрами доменной службы DNS

Команда	Описание
domain	Управление параметрами домена
drs	Управление службой репликации каталогов (Directory Replication Services, DRS)
dsacl	Управление списками контроля доступа DS
forest	Управление конфигурацией леса
fsmo	Управление ролями (Flexible Single Master Operations, FSMO)
gpo	Управление групповыми политиками
group	Управление группами
ldapcmp	Сравнение двух баз данных ldap
ntacl	Управление списками контроля доступа ACL
processes	Вывод списка процессов
ou	Управление организационными подразделениями (OU)
rodc	Управление контроллером домена (Read-Only Domain Controller, RODC)
schema	Управление и запрос схемы
sites	Управление сайтами
spn	Управление службой принципалов (Service Principal Name, SPN)
testparm	Проверка конфигурационного файла на корректность синтаксиса
time	Получение показаний текущего времени сервера
user	Управление пользователями
visualize	Графическое представление состояния сети Samba

Получить дополнительную информацию можно на справочной странице samba-tool(8) (**`man samba-tool`**).

Пример получения дополнительной информации о подкоманде:

```
$ samba-tool fsmo --help
```

Примеры:

- вывести список групповых политик:

```
# samba-tool gpo listall
GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
path         : \
\test.alt\sysvol\test.alt\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
dn           :
CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=alt
version      : 0
flags        : NONE

GPO          : {FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
display name : scripts
path         : \\test.alt\sysvol\test.alt\Policies\{FE6268E4-FDEB-4DCA-94E8-
BB1170C66F45}
dn           : CN={FE6268E4-FDEB-4DCA-94E8-
BB1170C66F45},CN=Policies,CN=System,DC=test,DC=alt
version      : 65536
```

```
flags        : NONE

GPO          : {6AC1786C-016F-11D2-945F-00C04FB984F9}
display name : Default Domain Controllers Policy
path         : \
\test.alt\sysvol\test.alt\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}
dn           :
CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=alt
version      : 0
flags        : NONE

GPO          : {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
display name : Общие каталоги
path         : \\test.alt\sysvol\test.alt\Policies\{44F1A3E9-BD0D-44D7-AC1D-
CEEF2817C573}
dn           : CN={44F1A3E9-BD0D-44D7-AC1D-
CEEF2817C573},CN=Policies,CN=System,DC=test,DC=alt
version      : 0
flags        : NONE
```

- вывести все связанные контейнеры для объекта групповой политики:

```
# samba-tool gpo listcontainers {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
Container(s) using GPO {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
    DN: OU=OU,DC=test,DC=alt
    DN: OU=KDE,DC=test,DC=alt
```

- вывести список групповых политик, связанных с контейнером:

```
# samba-tool gpo getlink OU=OU,DC=test,DC=alt
GPO(s) linked to DN OU=OU,DC=test,DC=alt
    GPO     : {96D5897A-CEFB-4A1B-90AF-5D83707130C4}
    Name    : Файлы
    Options : NONE

    GPO     : {A12547D7-2FFA-4E37-9382-D6767489E3DF}
    Name    : kde
    Options : NONE

    GPO     : {75E65DF7-56A7-48E1-A393-F5FFAA1010FD}
    Name    : Control_ping
    Options : NONE

    GPO     : {FE6268E4-FDEB-4DCA-94E8-BB1170C66F45}
    Name    : scripts
    Options : NONE

    GPO     : {44F1A3E9-BD0D-44D7-AC1D-CEEF2817C573}
    Name    : Общие каталоги
    Options : NONE

    GPO     : {0CCFA74C-57F5-42B5-98E2-007D4A59C4C4}
    Name    : firefox
    Options : NONE

    GPO     : {2CF4EB19-343E-448A-BBBC-A9EC2F7C22E9}
    Name    : Установка пакетов
    Options : NONE
```

56.2. wbinfo

Команда **`wbinfo`** создает запросы и возвращает информацию к (от) демона winbindd(8).

Таблица 56.3. Параметры команды wbinfo

Параметр	Описание	Пример

-a|--authenticate username%password	Попытаться аутентифицировать пользователя через winbindd(8).
	
	Проверяет два метода аутентификации: plaintext password (применяется при входе пользователя в систему локально), challenge/response password (использует NTLM или Kerberos)
		`$ wbinfo -a TEST\\ivanov`
		`Enter TEST\ivanov's password:`
		`plaintext password authentication succeeded`
		`Enter TEST\ivanov's password:`
		`challenge/response password authentication succeeded`

--allocate-gid	Получить новый GID из idmap	
--allocate-uid	Получить новый UID из idmap	

--all-domains	Вывести список всех доменов (доверенных и собственный)	`$ wbinfo --all-domains`
		`BUILTIN`
		`TEST`
		`EXAMPLE`

-c|--change-secret	Изменить пароль доверительной учетной записи. Может использоваться вместе с доменом для изменения паролей учетных записей междоменного доверия	
--ccache-save <имя_пользователя>%<пароль>	Сохранить имя пользователя и пароль для ccache	
--change-user-password <имя_пользователя>	Изменить пароль пользователя (будет запрошен старый и новый пароль)	`# wbinfo --change-user-password ivanov` `Enter ivanov's old password:`

Параметр	Описание	Пример
		Enter ivanov's new password: Password change for user ivanov succeeded
--dc-info <домен>	Вывести текущий контроллер домена для домена	$ **wbinfo --dc-info TEST** dc1.test.alt (192.168.0.132)
--domain <домен>	Определяет домен, в котором будут выполняться любые указанные операции	
-D|--domain-info <домен>	Показать информацию об указанном домене	$ **wbinfo -D TEST** Name : TEST Alt_Name : test.alt SID : S-1-5-21-578923263-1107570656-1287136478 Active Directory : Yes Native : Yes Primary : Yes
--dsgetdcname <домен>	Найти DC для домена	$ **wbinfo --dsgetdcname TEST** \\dc1.test.alt \\192.168.0.132 1 d75c7b83-9472-4646-adb2-52b3d6968eb6 test.alt test.alt 0xe00013fd Default-First-Site-Name Default-First-Site-Name
--gid-info <gid>	Получить информацию о группе по gid	

Параметр	Описание	Пример
		`$ wbinfo --gid-info 10000` `domain admins:*:10000:`
--group-info <группа>	Получить информацию о группе по имени группы	`$ wbinfo --group-info "TEST\\domain admins"` `domain admins:*:10000:`

-g|--domain-groups	Вывести список доменных групп	`$ wbinfo -g`
		`…`
		`TEST\domain admins`
		`TEST\domain users`
		`TEST\domain guests`
		`TEST\domain computers`
		`…`

--get-auth-user	Эта функция была перенесена в утилиту **net** (см. **net help getauthuser**)	
--getdcname <домен>	Вывести имя контроллера домена для указанного домена	`$ wbinfo --getdcname TEST` `DC1`
-G|--gid-to-sid <gid>	Преобразовать идентификатор группы UNIX в SID Windows NT. Если указанный gid не относится к диапазону gid idmap, операция завершится ошибкой	`$ wbinfo -G 10000` `S-1-5-21-578923263-1107570656-1287136478-512`
-i|--user-info <имя_пользователя>	Вывести информацию о пользователе	

Параметр	Описание	Пример
		`$ wbinfo -i TEST\\ivanov` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`
-I|--WINS-by-ip ip	Вывести NetBIOS-имя, связанное с IP-адресом	`$ wbinfo -I 192.168.0.135` `192.168.0.135 WORK135`

-K|--krb5auth <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя через Kerberos	`$ wbinfo -K TEST\\ivanov`
		`Enter TEST\ivanov's password:`
		`plaintext kerberos password authentication for [TEST\ivanov] succeeded (requesting cctype: FILE)`

--krb5ccname KRB5CCNAME	Запросить определенный тип кеша учетных данных Kerberos, используемый для аутентификации	
--lanman	Использовать криптографию Lanman для аутентификации пользователей	
--logoff	Выйти из системы	
--logoff-uid UID	Определяет идентификатор пользователя, используемый во время запроса на выход из системы	
--logoff-user <имя_пользователя>	Определяет имя пользователя, используемое во время запроса на выход из системы	
--lookup-sids SID1,SID2...	Поиск SID	

Параметр	Описание	Пример
		`$ wbinfo --lookup-sids S-1-5-21-578923263-1107570656-1287136478-512` `S-1-5-21-578923263-1107570656-1287136478-512 -> <none>\Domain Admins 2`

-m|--trusted-domains	Вывести список доверенных доменов	`$ wbinfo --trusted-domains`
		`BUILTIN`
		`TEST`
		`EXAMPLE`

-n|--name-to-sid <имя>	Вывести SID, связанный с указанным именем. Если домен не указан, используется домен, указанный в параметре ***workgroup*** **smb.conf**	`$ wbinfo -n TEST\\ivanov` `S-1-5-21-578923263-1107570656-1287136478-1103 SID_USER (1)`

-N|--WINS-by-name <name>	Вывести IP-адрес, связанный с именем NetBIOS, указанным в параметре name	`$ wbinfo -N WORK135`
		`192.168.0.135`
		`WORK135`

--ntlmv1	Использовать криптографию NTLMv1 для аутентификации пользователей	
--ntlmv2	Использовать криптографию NTLMv2 для аутентификации пользователей	
--online-status <домен>	Показать, поддерживает ли winbind в настоящее время активное соединение или нет. Если домен не указан, будет выведен статус текущего домена	

Параметр	Описание	Пример

		`$ wbinfo --online-status`
		`BUILTIN : active connection`
		`TEST : active connection`

--own-domain	Вывести собственный домен	`$ wbinfo --own-domain` `TEST`

--pam-logon <имя_пользователя>%<пароль>	Попытаться аутентифицировать пользователя так же, как это сделал бы pam_winbind	`$ wbinfo --pam-logon ivanov`
		`Enter ivanov's password:`
		`plaintext password authentication succeeded`

-p|--ping	Проверяет запущен ли winbindd(8)	`$ wbinfo -p` `Ping to winbindd succeeded`
-P|--ping-dc	Проверить безопасное соединение с контроллером домена	`$ wbinfo -P` `checking the NETLOGON for domain[TEST] dc connection to "dc1.test.alt" succeeded`
-r|--user-groups <имя_пользователя>		

Параметр	Описание	Пример

	Получить список идентификаторов групп, к которым принадлежит пользователь. Доступно только при наличии пользователя на контроллере домена	`$ wbinfo -r ivanov`
		`10001`
		`10003`

-R|--lookup-rids rid1, rid2, rid3..	Преобразовать RID в имена	
--remove-gid-mapping GID,SID	Удалить существующее сопоставление GID и SID из базы данных	
--remove-uid-mapping UID,SID	Удалить существующее сопоставление UID и SID из базы данных	
-s|--sid-to-name sid	Преобразовать SID в имя	`$ wbinfo -s S-1-5-21-578923263-1107570656-1287136478-1103` `TEST\ivanov 1`
--separator	Вывести активный разделитель winbind	`$ wbinfo --separator` `\`
--sequence	Команда устарела, вместо неё следует использовать параметр ***--online-status***	
--set-auth-user <имя_пользователя>%<пароль>	Эта функция была перенесена в утилиту **net** (см. **net help setauthuser**)	
--set-gid-mapping GID,SID	Создать сопоставление GID и SID в базе данных	
--set-uid-mapping UID,SID	Создать сопоставление UID и SID в базе данных	
-S|--sid-to-uid sid	Преобразовать SID в идентификатор пользователя	`$ wbinfo -S S-1-5-21-578923263-1107570656-1287136478-1103` `10000`

Параметр	Описание	Пример
--sid-aliases sid	Получить псевдонимы SID для заданного SID	
--sid-to-fullname sid	Преобразовать SID в полное имя пользователя (ДОМЕН\имя пользователя)	`$ wbinfo --sid-to-fullname S-1-5-21-578923263-1107570656-1287136478-1103` `TEST\Иван Иванов 1`
--sids-to-unix-ids sid1,sid2,sid3...	Преобразовать SID в Unix ID	`$ wbinfo --sids-to-unix-ids S-1-5-21-578923263-1107570656-1287136478-1103` `S-1-5-21-578923263-1107570656-1287136478-1103 -> uid 10000`
-t|--check-secret	Проверить, что доверительная учетная запись рабочей станции, созданная при добавлении сервера Samba в домен Windows NT, работает. Может использоваться вместе с доменом для проверки учетных записей междоменного доверия	

-u|--domain-users	Вывести список доменных пользователей	`$ wbinfo -u`
		`administrator`
		`krbtgt`
		`ivanov`
		`guest`

--uid-info uid	Получить информацию о пользователе по идентификатору	`$ wbinfo --uid-info 10000` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`

Параметр	Описание	Пример
--usage	Вывести краткую справку о программе	

--user-domgroups sid	Вывести группы пользователей домена	`$ wbinfo --user-domgroups S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-513`

--user-sidinfo sid	Получить информацию о пользователе по sid	`$ wbinfo --user-sidinfo S-1-5-21-578923263-1107570656-1287136478-1103` `ivanov:*:10000:10001:Иван Иванов:/home/TEST.ALT/ivanov:/bin/bash`

--user-sids sid	Получить SID групп пользователя	`$ wbinfo --user-sids S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-1103`
		`S-1-5-21-578923263-1107570656-1287136478-513`
		`S-1-5-32-545`

-U|--uid-to-sid uid	Преобразовать идентификатор пользователя UNIX в SID	`$ wbinfo -U 10000` `S-1-5-21-578923263-1107570656-1287136478-1103`
-Y|--sid-to-gid sid	Преобразовать SID в идентификатор группы UNIX	

Параметр	Описание	Пример
		`$ wbinfo -Y S-1-5-21-578923263-1107570656-1287136478-513 10001`

56.3. net

net — инструмент администрирования Samba и удаленных серверов CIFS. Синтаксис:

```
net <протокол> <функция> <дополнительные_параметры> <параметры_цели>
```

где <протокол> — протокол, используемый при выполнении команды. Возможные значения: ads (Active Directory), rap (Win9x/NT3) или rpc (WindowsNT4/2000/2003/2008/2012). Если протокол не указан, **net** пытается определить его автоматически.

Таблица 56.4. Основные команды net ads

Команда	Описание
info	Вывод информации о домене
join	Присоединение машины к домену
testjoin	Проверка, действителен ли пароль учетной записи компьютера
leave	Удалить локальную машину из домена AD
status	Вывод информации об учетной записи компьютера
user	Список/изменение пользователей
group	Список/изменение групп
dns	Выполнить динамическое обновление DNS
password	Изменить пароль пользователей
changetrustpw	Изменить пароль доверительной учетной записи
printer	Список/изменение записей принтера
search	Выполнить поиск LDAP с использованием фильтра
dn	Выполнить поиск LDAP по DN
sid	Выполнить поиск LDAP по SID
workgroup	Показать имя рабочей группы
lookup	Найти контроллер домена AD с помощью поиска CLDAP
keytab	Управление локальным файлом keytab
spnset	Управление именами участников-служб (SPN)
gpo	Управление объектами групповой политики
kerberos	Управление keytab Kerberos
enctypes	Список/изменение enctypes

Получить дополнительную информацию можно на справочной странице net(8) (**man net**).

Пример получения дополнительной информации о подкоманде:

```
# net time --help
```

Получение информации о домене:

```
# net ads info
LDAP server: 192.168.0.132
LDAP server name: dc1.test.alt
Realm: TEST.ALT
Bind Path: dc=TEST,dc=ALT
LDAP port: 389
Server time: Ср, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Ср, 20 мар 2024 11:13:27 EET
```

Получение информации об учетной записи компьютера:

```
# net ads status -U administrator
```

56.4. adcli

adcli — инструмент для выполнения действий в домене Active Directory.

Таблица 56.5. Основные команды adcli

Команда	Описание
info домен	Вывести информацию о домене
join домен	Присоединить данную машину к домену (создает учетную запись компьютера в домене и настраивает keytab для этой машины. Не настраивает службу аутентификации, например, sssd)
update	Обновляет пароль учетной записи компьютера на контроллере домена для локальной машины, записывает новые ключи в keytab и удаляет старые ключи
testjoin	Проверить, действителен ли пароль учетной записи компьютера
create-user [--domain=домен] пользователь	Создать учетную запись пользователя
delete-user [--domain=домен] пользователь	Удалить учетную запись пользователя
passwd-user [--domain=домен] пользователь	Установить (повторно) пароль пользователя
create-group [--domain=домен] группа	Создать группу
delete-group [--domain=домен] группа	Удалить группу
add-member [--domain=домен] группа пользователь или компьютер…	Добавить пользователей в группу
remove-member [--domain=домен] группа пользователь…	Удалить пользователей из группы
preset-computer [--domain=домен] компьютер…	

Команда	Описание
	Предустановить учетные записи компьютеров (предварительно создает одну или несколько учетных записей компьютеров в домене, чтобы позже компьютеры могли использовать их при присоединении к домену. При этом, машины могут присоединяться с помощью одноразового пароля или автоматически без пароля)
reset-computer [--domain=домен] компьютер	Сбросить учетную запись компьютера (если соответствующая машина присоединена к домену, её членство будет нарушено)
delete-computer [--domain=домен] компьютер	Удалить учетную запись компьютера
show-computer [--domain=домен] компьютер	Показать атрибуты учетной записи компьютера, хранящиеся в AD
create-msa [--domain=домен]	Создать управляемую учетную запись службы (MSA) в заданном домене AD (это бывает нужно, если компьютер не должен присоединяться к домену Active Directory, но к нему необходим LDAP доступ)

Получить дополнительную информацию можно на справочной странице adcli(8) (**`man adcli`**).

Пример получения дополнительной информации о подкоманде:

```
# adcli testjoin --help
```

Получение информации о домене:

```
# adcli info test.alt
[domain]
domain-name = test.alt
domain-short = TEST
domain-forest = test.alt
domain-controller = dc1.test.alt
domain-controller-site = Default-First-Site-Name
domain-controller-flags = pdc gc ldap ds kdc timeserv closest writable good-
timeserv full-secret
domain-controller-usable = yes
domain-controllers = dc1.test.alt dc2.test.alt
[computer]
computer-site = Default-First-Site-Name
```

Показать атрибуты учетной записи компьютера:

```
# adcli show-computer -D test.alt win2012
Password for Administrator@TEST.ALT:
sAMAccountName:
 WIN2012$
userPrincipalName:
 - not set -
msDS-KeyVersionNumber:
 1
msDS-supportedEncryptionTypes:
```

```
 28
dNSHostName:
 win2012.test.alt
servicePrincipalName:
 HOST/win2012.test.alt
 RestrictedKrbHost/win2012.test.alt
 HOST/WIN2012
 RestrictedKrbHost/WIN2012
 Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/win2012.test.alt
operatingSystem:
 Windows Server 2012 R2 Standard
operatingSystemVersion:
 6.3 (9600)
operatingSystemServicePack:
 - not set -
pwdLastSet:
 133294743593838200
userAccountControl:
 4096
description:
 - not set -
```

Создать группу testldap в подразделении OU:

```
# adcli create-group -D test.alt -O OU=OU,dc=test,dc=alt testldap
Password for Administrator@TEST.ALT:
```

56.5. ldapsearch

ldapsearch — утилита для поиска информации в LDAP. Синтаксис:

```
ldapsearch <параметры> <фильтр> <атрибуты>
```

ldapsearch открывает соединение с сервером LDAP, подключается к нему и выполняет поиск с помощью фильтра.

Если утилита **ldapsearch** найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если в этом списке указан знак *, возвращаются все пользовательские атрибуты. Если в этом списке указан знак +, возвращаются все операционные атрибуты. Если атрибуты не указаны, то возвращаются все пользовательские атрибуты.

Результаты поиска отображаются в виде расширенной версии LDIF. Формат вывода контролируется с помощью параметра ***-L***.

Таблица 56.6. Параметры команды ldapsearch

Параметр	Описание
Параметры поиска	
-a {never|always|search|find}	

Параметр	Описание
	Задает способ преобразования псевдонимов. Может принимать значения: never (по умолчанию), always, search или find, указывающие, соответственно, что псевдонимы не преобразуются, преобразуются всегда, преобразуются при поиске, либо преобразуются только при определении базового объекта для поиска
-A	Получить только атрибуты (без значений)
-b basedn	Позволяет переопределить заданную по умолчанию начальную точку поиска
-c	Режим продолжения операции (не останавливать поиск при ошибках)
-E [!]ext[=extparam]	Указывает расширения поиска. Знак '!' обозначает критичность расширения. Общие расширения: - [!]domainScope (диапазон домена) - !dontUseCopy - [!]mv=<filter> (RFC 3876 фильтр совпавших значений) - [!]pr=<size>[/prompt|noprompt] (RFC 2696 постраничный вывод результатов/запрос вывода) - [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...] (RFC 2891 сортировка на стороне сервера) - [!]subentries[=true|false] (RFC 3672 подзаписи) - [!]sync=ro[/<cookie>] (RFC 4533 LDAP Sync refreshOnly) [!]sync=rp[/<cookie>][/<slimit>] (LDAP Sync refreshAndPersist) - [!]vlv=<before>/<after>(/<offset>/<count>|:<value>) (ldapv3-vlv-09 вид виртуального списка) - [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]] - [!]<oid>[=:<b64value>] (общий контроль; нет обработки ответа)
-f file	Считать серию строк из файла ***file*** и выполнить по одному поиску LDAP для каждой строки. В этом случае заданный в командной строке фильтр ***filter*** интерпретируется как шаблон, в котором первое и только первое вхождение ***%s*** заменяется строкой из файла ***file***. Любые другие вхождения символа % в шаблоне будут рассматриваться как ошибка. Если требуется, чтобы в поисковом фильтре присутствовал символ %, он должен быть закодирован как \25 (смотрите RFC 4515). Если в качестве значения ***file*** указан символ «-», то строки считываются со стандартного ввода
-F prefix	URL-префикс для временных файлов (по умолчанию: file://path, где **path** либо **/tmp/.private/<user>**, либо значение, указанное в параметре ***-T***)
-l limit	Ограничение на время поиска (в секундах). Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число)
-L[LL]	

Параметр	Описание
	Управление выводом результатов поиска в формате обмена данными LDAP (LDAP Data Interchange Format): ***-L*** — вывести ответы в формате LDIFv1, ***-LL*** — отключить вывод комментариев, ***-LLL*** — отключить вывод версии LDIF
-M[M]	Включить элемент управления Manage DSA IT. ***-MM*** делает этот элемент управления критичным
-P {2|3}	Версия протокола LDAP (по умолчанию 3)
-s {base|one|sub|children}	Задает область поиска. Может принимать одно из следующих значений: base, one, sub (по умолчанию) или children, что означает поиск только по базовому объекту, на одном уровне, по всему поддереву и по дочерним записям соответственно
-S attr	Отсортировать возвращаемые записи по атрибуту ***attr***. По умолчанию возвращаемые записи не сортируются. Если в качестве ***attr*** задана строка нулевой длины (""), записи сортируются по компонентам их уникального имени Distinguished Name. По умолчанию **ldapsearch** выводит записи по мере их получения. При использовании параметра ***-S*** все данные сначала получаются, потом сортируются, потом выводятся
-t[t]	При указании одного ***-t*** полученные непечатаемые значения записываются в набор временных файлов (полезно при работе со значениями, содержащими несимвольные данные, такими как jpegPhoto или audio). При указании второго ***-t*** все полученные значения записываются в файлы
-T path	Временные файлы записываются в указанный в ***path*** каталог (по умолчанию **/tmp/.private/<user>**)
-u	Включить в вывод форму удобного для пользователя имени (User Friendly Name, UFN) уникального имени (Distinguished Name, DN)
-z limit	Ограничить количество возвращаемых в результате поиска записей значением **limit**. Значение 0 (ноль) или none означает, что ограничений нет. Значение max означает максимальное допустимое протоколом значение (целое число)
Общие параметры	
-d debuglevel	Установить уровень отладки LDAP
-D binddn	Использовать указанное в ***binddn*** уникальное имя Distinguished Name при подсоединении к каталогу LDAP. При SASL-подсоединениях сервер будет игнорировать это значение
-e [!]ext[=extparam]	Указывает общие расширения. Знак '!' обозначает критичность расширения. Общие расширения: - [!]assert=<filter> (RFC 4528; фильтр RFC 4515) - [!]authzid=<authzid> (RFC 4370; "dn:<dn>" или "u:<user>") - [!]chaining[=<resolveBehavior>[/<continuationBehavior>]] - [!]manageDSAit (RFC 3296) - [!]noop - ppolicy - [!]postread[=<attrs>] (RFC 4527; разделённый запятыми список атрибутов)

Параметр	Описание
	▫[!]preread[=<attrs>] (RFC 4527; разделённый запятыми список атрибутов) ▫[!]relax ▫[!]sessiontracking ▫abandon, cancel, ignore (сигнал SIGINT посылает abandon/cancel, либо в ответ на него посылается ignore; если расширение помечено как критичное, сигнал SIGINT не принимается; ненастоящие элементы управления
-h host	Сервер LDAP
-H URI	Указывает URI (возможно, несколько), ссылающийся на LDAP-сервер (серверы). В URI допускаются поля: протокол/хост/порт
-I	Использовать интерактивный режим SASL
-n	Демонстрируется, что будет сделано, но реальный поиск не выполняется. Используется для отладки совместно с параметром ***-v***
-N	Не использовать обратное разрешение DNS для получения канонического имени хоста SASL
-O props	Параметры безопасности SASL
-o opt[=optparam]	Указывает опции общего назначения. Возможные опции: ▫nettimeout=<timeout> (в секундах, либо «none» или «max») ▫ldif-wrap=<width> (в символах, либо «no» для предотвращения переноса строк)
-p порт	Порт, на котором сервер LDAP принимает запросы. Номер порта по умолчанию — 389. Если номер порта не задан, и указан параметр ***-Z***, то применяется номер порта LDAP SSL по умолчанию, равный 636
-Q	Использовать тихий режим SASL. Запросы не выводятся никогда
-R realm	Задаёт realm аутентификационного идентификатора для SASL. Форма realm зависит от того, какой механизм аутентификации в действительности используется
-U authcid	Идентификатор аутентификации SASL. Форма идентификатора зависит от того, какой механизм аутентификации в действительности используется
-v	Запустить в подробном режиме (диагностические сообщения посылаются в стандартный вывод)
-V[V]	Вывести информацию о версии. При указании ***-VV***, после вывода информации о версии осуществляется выход. При указании ***-V***, после вывода информации о версии выполняется поиск согласно заданным критериям
-w passwd	Использовать указанное значение ***passwd*** в качестве пароля для простой аутентификации
-W	Запрашивать ввод пароля для простой аутентификации (используется для того, чтобы не указывать пароль в командной строке)
-x	Использовать простую аутентификацию

Параметр	Описание
-X authzid	Идентификатор авторизации SASL ("dn:<dn>" или "u:<user>")
-y file	Считать пароль из файла ***file***. В качестве пароля используется всё содержимое файла. Поэтому файл не должен содержать символа переноса строки
-Y mech	Задаёт механизм SASL, который будет использоваться для аутентификации. Если параметр не указан, программа выберет лучший из известных серверу механизмов
-Z[Z]	Запустить запрос TLS (***-ZZ*** для запроса успешного ответа)

56.5.1. Фильтр

Фильтр должен быть указан в строковом формате фильтров LDAP (см. RFC 4515). Если фильтр не указан, используется фильтр по умолчанию (objectClass=*)

Синтаксис LDAP-фильтра имеет вид:

```
<Атрибут><оператор сравнения><значение>
```

Вместо имени атрибута можно использовать его идентификатор (Attribute-Id). Тело фильтра должно быть заключено в скобки

Таблица 56.7. Примеры LDAP-фильтров

Запрос	LDAP фильтр
Все пользователи:	(sAMAccountType=805306368)
Отключенные (Disabled) пользователи:	(&(sAMAccountType=805306368) (useraccountcontrol:1.2.840.113556.1.4.803:=2))
Заблокированные (Locked) пользователи:	(&(sAMAccountType=805306368)(badPwdCount>=4))
Пользователи, у которых в настройках указано «Пароль никогда не истекает»	(&(objectCategory=person)(objectClass=user) (userAccountControl:1.2.840.113556.1.4.803:=65536))
Пользователи которые не меняли пароль с 5 мая 2023 года (см. https://www.epochconverter.com/ldap для преобразования даты во временную метку Windows)	(&(objectCategory=person)(pwdLastSet<=133278047990000000))
Пользователи с незаполненным полем mail	(&(objectCategory=group)(!(mail=*)))
Пользователи, которые должны сменить пароль при следующем входе в систему	(&(sAMAccountType=805306368)(pwdLastSet=0))
Пользователи с ограниченным сроком действия учетной записи	(&(sAMAccountType=805306368)(accountExpires>=1) (accountExpires<=9223372036854775806))

Запрос	LDAP фильтр
Пользователи, созданные за определенный период (формат даты: YYYY MM DD HH mm ss.s Z)	(&(sAMAccountType=805306368) (whenCreated>=20230401000000.0Z<=20230701000000.0Z))
Все компьютеры	(objectCategory=computer)
Все контроллеры домена	(&(objectCategory=computer) (userAccountControl:1.2.840.113556.1.4.803:=8192))
Контроллеры домена, доступные только для чтения	(&(objectCategory=computer) (userAccountControl:1.2.840.113556.1.4.803:=67108864))
Группы, в которых нет пользователей	(&(objectCategory=group)(!(member=*)))
Группы, с ключевым словом admin в имени	(&(objectCategory=group)(samaccountname=*admin*))
Все группы безопасности (Security)	(&(objectCategory=group) (groupType:1.2.840.113556.1.4.803:=2147483648))
Все члены группы Sales (без учёта вложенности)	(memberOf=CN=Sales,CN=Users,DC=test,DC=alt)
Все члены группы Sales (с учётом вложенности)	(memberOf:1.2.840.113556.1.4.1941:=CN=Sales,CN=Users,DC=test,DC=alt)
Все группы, в которые входит пользователь testldap	(&(objectCategory=group) (member=CN=testldap,CN=Users,DC=test,DC=alt)))
Все подразделения (OU)	(objectCategory=organizationalUnit)
Все объекты групповой политики	(objectCategory=groupPolicyContainer)
Все отношения доверия	(objectClass=trustedDomain)
Объекты связанные с ролями FSMO	(fsMORoleOwner=*)
PDC Emulator	(&(objectClass=domainDNS)(fSMORoleOwner=*))
RID Master	(&(objectClass=rIDManager)(fSMORoleOwner=*))
Объект AD с определенным SID	(objectSID=S-1-5-21-1723588197-2340999690-1379671080-1105)

56.5.2. Формат вывода

Если найдена одна или несколько записей, то каждая запись передается в поток вывода в следующем формате:

```
Отличительное имя (DN)
имя_атрибута: значение
имя_атрибута: значение
имя_атрибута: значение
…
```

Записи разделяются пустыми строками.

Если задан параметр ***-t*** вместо реальных значений атрибутов будут выводиться URI временных файлов, в которые эти значения помещаются. Если задан параметр ***-A*** будут выводиться только имена атрибутов.

Примечание

Значение атрибута записывается в 7-битной кодировке ASCII и отделяется от его имени символом «:». Значения, не подходящие под эту кодировку, записываются в кодировке base64 и отделяются от имени атрибута символами «::»:

```
имя_атрибута:: base64_значение_атрибута
```

Например:

```
dn::
Q0490JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsCxDTj1Vc2VycyxEQz10ZXN0LERDPWFsdA==
cn:: 0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==

…
$  echo "0JfQsNC50YbQtdCy0LAg0J7Qu9GM0LPQsA==" | base64 -d
Зайцева Ольга
```

Чтобы отобразить строки в кодировке base64 можно использовать следующую команду:

```
$ ldapsearch -LLL -D testldap@test.alt -x -W | perl -MMIME::Base64
-MEncode=decode -n -00 -e 's/\n
+//g;s/(?<=:: )(\S+)/decode("UTF-8",decode_base64($1))/eg;print'
```

56.5.3. Примеры

Вывести всех пользователей, фамилия которых начинается с буквы «К»:

```
$ ldapsearch -LLL -H ldap://192.168.0.132:389 \
-D testldap@test.alt -b "dc=test,dc=alt" \
-x -W "(&(sAMAccountName=*)(sn=K*))" cn sn
```

где:

- ***-H ldap://192.168.0.132:389*** — сервер LDAP;
- ***-D testldap@test.alt*** — пользователь с правом чтения в каталоге LDAP;
- ***-b "dc=test,dc=alt"*** — контейнер AD, в котором будет выполняться поиск;
- ***-x*** — использовать простую аутентификацию;
- ***-W*** — спросить пароль;
- ***"(&(sAMAccountName=*)(sn=K*))"*** — выражение, по которому будут отфильтрованы результаты;
- ***cn sn*** — поля, которые необходимо вывести.

Параметры по умолчанию можно задать в файле **/etc/openldap/ldap.conf**, например:

```
BASE    dc=test,dc=alt
URI     ldap://dc1.test.alt
```

Команда с использованием базы поиска и URI по умолчанию:

```
$ ldapsearch -LLL -D testldap@test.alt \
-x -W "(&(sAMAccountName=*)(sn=K*))" cn sn
```

Вывести фамилию и электронную почту всех пользователей, из подразделения OU, у которых непустое поле mail:

```
$ ldapsearch -LLL -H ldap://192.168.0.132:389 \
-D testldap@test.alt -b "ou=OU,dc=test,dc=alt" -s one \
-x -W "(&(sAMAccountName=*)(mail=K*))" sn mail
```

В данном примере не будут выведены записи только из подразделения OU, но не из его дочерних подразделений.

Считать последовательность строк из файла **new.filter** и выполнить функцию поиска LDAP для каждой строки:

```
$ ldapsearch -H ldap://192.168.0.132:389 \ -D testldap@test.alt -b
"dc=test,dc=alt" -x -W -f new.filter "(samaccountname=%s)" cn
```

Содержимое файла **new.filter**:

```
z*
ivanov
k*
*k
```

Команда выполняет поиск по поддереву для каждого фильтра, начиная с samaccountname=z*. Когда этот поиск завершается, начинается поиск для фильтра cn=ivanov и т.д. Пример вывода вышеуказанной команды с параметром ***-n***:

```
 LDAPv3
# base <dc=test,dc=alt> with scope subtree
# filter pattern: (samaccountname=%s)
# requesting: dn
#

#
# filter: (samaccountname=z*)
#

#
# filter: (samaccountname=ivanov)
#

#
# filter: (samaccountname=k*)
#
```

```
#
# filter: (samaccountname=*k)
#
```

56.6. sssctl

sssctl — это инструмент командной строки, который предоставляет унифицированный способ получения информации о состоянии Security System Services Daemon (SSSD).

Утилиту **sssctl** можно использовать для сбора следующей информации:

- состоянии домена;
- аутентификации пользователя;
- доступа пользователей к клиентам определенного домена;
- кешированном содержимом.

С помощью утилиты **sssctl** можно:

- управлять кешем SSSD;
- управлять журналами;
- проверить конфигурационные файлы.

Таблица 56.8. Основные команды sssctl

Команда	Описание
Статус SSSD	
domain-list	Вывести список доступных доменов
domain-status домен	Вывести информацию о домене
user-checks пользователь	Вывести информацию о пользователе и проверить аутентификацию
access-report домен	Создать отчёт о правилах управления доступом, которые применяются к клиентскому компьютеру (работает только для домена FreeIPA)
Информация о кешированном содержимом	
user-show пользователь	Информация о кеше пользователя
group-show группа	Информация о кеше группы
netgroup-show группа	Информация о кеше сетевой группы
Инструменты для работы с локальными данными	
client-data-backup	Резервное копирование локальных данных
client-data-restore	Восстановление локальных данных из резервной копии
cache-remove	Резервное копирование локальных данных и удаление кешированного содержимого
cache-upgrade	Выполнить обновление кеша

Команда	Описание
cache-expire	Сделать недействительными кешированные объекты
cache-index действие	Управление индексами кеша
Инструменты для управления журналированием	
logs-remove	Удалить существующие файлы журналов SSSD
logs-fetch файл	Архивировать файлы журналов SSSD в tarball
debug-level [уровень]	Изменить или вывести уровень журналирования SSSD
analyze	Анализ зарегистрированных данных
Инструменты для проверки файлов конфигурации	
config-check	Выполнить статический анализ конфигурации SSSD
Инструменты, связанные с сертификатом	
cert-show сертификат	Вывести информацию о сертификате
cert-map сертификат	Показать пользователей, привязанных к сертификату

Получить дополнительную информацию можно на справочной странице sssctl(8) (**`man sssctl`**).

Пример получения дополнительной информации о подкоманде:

```
# sssctl user-show --usage
```

или:

```
# sssctl user-show --help
```

Получение информации о домене:

```
# sssctl domain-status TEST.ALT
Online status: Online

Active servers:
AD Global Catalog: dc1.test.alt
AD Domain Controller: dc1.test.alt

Discovered AD Global Catalog servers:
- dc1.test.alt

Discovered AD Domain Controller servers:
- dc1.test.alt
```

Показать информацию о кеше пользователя:

```
# sssctl user-show kim
Name: kim
Cache entry creation date: 03/27/24 20:57:31
Cache entry last update time: 06/03/24 16:49:12
Cache entry expiration time: 06/03/24 18:19:12
Initgroups expiration time: 06/03/24 18:19:12
Cached in InfoPipe: N
```

Показать данные авторизации пользователя:

```
# sssctl user-checks kim
user: kim
action: acct
service: system-auth

SSSD nss user lookup result:
 - user name: kim
 - user id: 1939201105
 - group id: 1939200513
 - gecos: Олег Ким
 - home directory: /home/TEST.ALT/kim
 - shell: /bin/bash

SSSD InfoPipe user lookup result:
 - name: kim
 - uidNumber: 1939201105
 - gidNumber: 1939200513
 - gecos: Олег Ким
 - homeDirectory: not set
 - loginShell: not set

testing pam_acct_mgmt

pam_acct_mgmt: Success

PAM Environment:
 - no env -
```

56.7. testparm

С помощью команды **testparm** можно проверить содержимое файла конфигурации **/etc/samba/smb.conf**.

Пример проверки настройки Samba:

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions

# Global parameters
[global]
```

```
    dns forwarder = 8.8.8.8
    ldap server require strong auth = No
    passdb backend = samba_dsdb
    realm = TEST.ALT
    server role = active directory domain controller
    workgroup = TEST
    rpc_server:tcpip = no
    rpc_daemon:spoolssd = embedded
    rpc_server:spoolss = embedded
    rpc_server:winreg = embedded
    rpc_server:ntsvcs = embedded
    rpc_server:eventlog = embedded
    rpc_server:srvsvc = embedded
    rpc_server:svcctl = embedded
    rpc_server:default = external
    winbindd:use external pipes = true
    idmap_ldb:use rfc2307 = yes
    idmap config * : backend = tdb
    map archive = No
    vfs objects = dfs_samba4 acl_xattr

[dfs]
    msdfs root = Yes
    path = /media/dfsroot

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/test.alt/scripts
    read only = No

[free]
    guest ok = Yes
    path = /mnt/win/free
    read only = N
```

Глава 57. Конфигурационные файлы

57.1. smb.conf

57.2. krb5.conf

57.3. sssd.conf

57.4. resolv.conf

57.5. Bind

57.1. smb.conf

`/etc/samba/smb.conf` — файл конфигурации Samba.

57.2. krb5.conf

`/etc/krb5.conf` — файл конфигурации Kerberos.

57.3. sssd.conf

`/etc/sssd/sssd.conf` — файл конфигурации SSSD.

Для работы с Active Directory в SSSD имеется специальный AD-провайдер *sssd-ad*.

Минимальный конфигурационный файл (**`/etc/sssd/sssd.conf`**) для sssd-ad:

```
[sssd]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sssd-drop-privileges unprivileged|privileged|default
user = _sssd

# SSSD will not start if you do not configure any domains.

domains = TEST.ALT
[nss]

[pam]
[domain/TEST.ALT]
id_provider = ad
auth_provider = ad
chpass_provider = ad
access_provider = ad
default_shell = /bin/bash
fallback_homedir = /home/%d/%u
debug_level = 0
;cache_credentials = true
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
```

Получить подробную информацию можно на справочной странице sssd.conf(5) (**`man sssd.conf`**).

57.4. resolv.conf

`/etc/resolv.conf` — файл конфигурации ресолвера (механизма преобразования имен хостов в адреса IP).

Файл конфигурации ресолвера (resolver) содержит информацию, которая считывается функциями разрешения имён при первом их вызове процессом. Файл разработан в удобочитаемом формате, и содержит список ключевых слов со значениями, которые предоставляют различного рода информацию для функций разрешения имён. Файл настройки считается надёжным источником информации DNS (например, информация об AD-бите DNSSEC будет возвращаться в неизменном виде из этого источника).

Если этот файл не существует, то будет опрашиваться только служба имён на локальной машине; доменное имя определяется из имени узла, а список поиска будет содержать это доменное имя.

Обычно в файле **/etc/resolv.conf** указан как минимум 1 сервер имен, на который будут перенаправляться все DNS запросы:

```
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
nameserver 192.168.197.241
```

Важно

Файл **/etc/resolv.conf** не должен редактироваться. Его автоматически генерирует **resolvconf**. Редактировать можно файл **/etc/net/ifaces/<interface>/resolv.conf**

Поддерживаются следующие параметры настройки:

nameserver IP-адрес сервера имён

Интернет-адрес сервера имён, на который надо переправлять все запросы, либо адрес IPv4 (в точечной нотации), либо адрес IPv6 в нотации с двоеточием (и, возможно, с точками) в соответствии с RFC 2373. Может быть указано до **MAXNS** (в настоящее время 3) серверов имён, ключевое слово должно быть указано для каждого сервера. Если указано несколько серверов, библиотека распознавателя запрашивает их в указанном порядке. Если в файле нет строк ***nameserver***, по умолчанию используется сервер имён на локальном компьютере. Используемый алгоритм заключается в том, чтобы попробовать обратиться к первому указанному серверу имён, и, если время ожидания запроса истекло, попробовать обратиться к следующему серверу, и т.д. пока не будет исчерпан список серверов, а затем повторять попытки, пока не будет сделано максимальное количество повторных попыток.

options

Позволяют изменять некоторые внутренние переменные функций определения имён. Синтаксис:

```
options параметр …
```

где **параметр** может иметь следующие значения:

attempts:n

Задаёт количество попыток, которое преобразователь предпримет, отправляя запрос на свои серверы имён, прежде чем закончить работу и вернуть ошибку. По умолчанию используется RES_DFLRETRY (в настоящее время равно 2). Значение этого параметра скрыто ограничено числом 5.

debug

Устанавливает RES_DEBUG в _res.options (эффективно, только если glibc был собран с поддержкой отладки; см. **resolver(3)**).

edns0 (начиная с *glibc 2.6*)

Задаёт значение RES_USE_EDNSO в _res.options. Включает поддержку расширений DNS, описанных в RFC 2671.

inet6

Задаёт значение RES_USE_INET6 в _res.options. Это приводит к выполнению запроса AAAA перед запросом A внутри функции **gethostbyname(3)**, и отображению ответов IPv4 в «туннелированной форме» IPv6, если записи AAAA не были найдены, но существует набор записей A. Начиная с *glibc 2.25*, эта опция устарела; приложения должны использовать **getaddrinfo(3)**, а не **gethostbyname(3)**.

ip6-bytestring (с *glibc 2.3.4* до *glibc 2.24*)

Задаёт значение RES_USE_BSTRING в _res.options. Это приводит к поиску обратной записи IPv6, с использованием формата значимых битов, описанного в RFC 2673; если этот параметр не установлен (по умолчанию), то используется формат полубайта. Эта опция была удалена в *glibc 2.25*, так как она полагалась на несовместимое с предыдущими версиями расширение DNS.

ip6-dotint/no-ip6-dotint (с *glibc 2.3.4* до *glibc 2.24*)

Устанавливает/сбрасывает значение RES_NOIP6DOTINT в _res.options. Если указан сброс (ip6-dotint), то выполняется поиск обратной записи IPv6 в зоне ip6.int; если задана установка (no-ip6-dotint), то по умолчанию выполняется поиск обратной записи IPv6 в зоне ip6.arpa. Эти параметры доступны в версиях *glibc* до 2.24, где по умолчанию используется no-ip6-dotint. Поскольку ip6-dotint перестала поддерживаться, эти опции были удалены в *glibc 2.25*.

ndots:n

Задаёт минимальное количество точек, которые должны обязательно присутствовать в имени, переданном функции res_query(3) (см. **resolver(3)**), прежде чем будет сделан первоначальный абсолютный запрос. По умолчанию **n** равно 1, поэтому если в имени есть точки, сначала имя пытаются разрешить как абсолютное, прежде чем добавлять к нему элементы из списка поиска. Значение этой опции скрыто ограничено числом 15.

no-check-names

Задаёт значение RES_NOCHECKNAME в _res.options, что приводит к отключению в современном BIND проверки в поступающих именах узлов и почтовых именах недопустимых символов, таких как символы подчёркивания (_), не-ASCII или управляющие символы.

no-reload (начиная с *glibc 2.16*)

Задаёт значение RES_NORELOAD в _res.options. Эта опция отключает автоматическую перезагрузку измененного файла конфигурации.

no-tld-query (начиная с *glibc 2.14*)

Задаёт значение RES_NOTLDQUERY в _res.options. Этот параметр указывает res_nsearch() не пытаться разрешить неполное имя, как если бы оно было доменом верхнего уровня. Данный параметр может привести к проблемам, если в качестве TLD указано «localhost», а не localhost в одном или более элементах списка поиска. Данный параметр не действует, если не установлен RES_DEFNAMES или RES_DNSRCH.

rotate

Задаёт значение RES_ROTATE в _res.options, что приводит к циклическому выбору указанных серверов имён. Без этой опции распознаватель всегда будет запрашивать первый сервер имён в списке и использовать последующий сервер имён только в случае сбоя первого. Эта опция позволяет распределить нагрузку между разными серверами имён.

single-request-reopen (начиная с *glibc 2.9*)

Задаёт RES_SNGLKUPREOP в _res.options. Для разрешения имён используется единый сокет для запросов A и AAAA. Некоторое оборудование ошибочно возвращает только один ответ. Когда это происходит, клиент продолжает ждать второго ответа.

Указание этого параметра изменяет это поведение так, что если два запроса с одного порта не обрабатываются правильно, то сокет будет закрыт и открыт новый перед посылкой второго запроса.

single-request (начиная с *glibc 2.10*)

Задаёт значение RES_SNGLKUP в _res.options. По умолчанию, *glibc* начиная с версии 2.9 выполняет поиск по IPv4 и IPv6 параллельно.

Некоторые приложения DNS-серверов не могут обработать такие запросы должным образом и делают паузу между ответами на запрос. Этот параметр отключает данное поведение, что заставляет *glibc* делать запросы IPv6 и IPv4 последовательно (за счет некоторого замедления процесса разрешения имени).

timeout:n

Задаёт промежуток времени, который функции определения имён будут ждать ответа от удалённого сервера имён перед тем как повторить запрос другому серверу имён. Это время может не совпадать с общим временем, затраченным на любой вызов API-интерфейса преобразователя, и нет гарантии, что один вызов API-интерфейса преобразователя соответствует одному тайм-ауту. Измеряется в секундах, значение по умолчанию — RES_TIMEOUT (в настоящее время равно 5). Значение этой опции скрыто ограничено числом 30.

trust-ad (начиная с *glibc 2.31*)

Задаёт значение RES_TRUSTAD в _res.options. Этот параметр управляет поведением бита AD распознавателя-заглушки. Если проверяющий преобразователь устанавливает в ответе бит AD, это означает, что данные в ответе были проверены в соответствии с протоколом DNSSEC. Чтобы полагаться на бит AD, локальная система должна доверять как распознавателю, проверяющему DNSSEC, так и сетевому пути к нему, поэтому требуется явное согласие. Если активна опция ***`trust-ad`***, тупиковый распознаватель устанавливает бит AD в исходящих DNS-запросах (чтобы включить поддержку

бита AD) и сохраняет бит AD в ответах. Без этой опции бит AD в запросах не устанавливается и всегда удаляется из ответов, прежде чем они будут возвращены приложению. Это означает, что приложения могут доверять биту AD в ответах, если параметр ***trust-ad*** установлен правильно.

В *glibc* версии 2.30 и более ранних AD не устанавливается автоматически в запросах и без изменений передается приложениям в ответах.

use-vc (начиная с *glibc 2.14*)

Задаёт значение RES_USEVC в _res.options. Данный параметр включает принудительное использование TCP для запросов DNS.

search список поиска

По умолчанию список поиска содержит одну запись — имя локального домена. Он определяется по локальному имени хоста, возвращаемому функцией **gethostname(2)**; локальным доменным именем считается всё, что следует после первого знака «.». Если имя хоста не содержит «.», предполагается, что корневой домен является именем локального домена.

Это поведение можно изменить, перечислив имена доменов, в которых нужно вести поиск, после ключевого слова ***search*** через пробел или символ табуляции. При разрешении запросов имён, в которых меньше точек чем указано в **ndots** (по умолчанию 1), будет использован каждый компонент пути поиска пока не будет найдено соответствующее имя. Для сред с несколькими субдоменами см. параметры **ndots:n**, чтобы избежать атак типа «человек посередине» и ненужного трафика для корневых DNS-серверов. Обратите внимание, что этот процесс может быть медленным и будет генерировать много сетевого трафика, если серверы для перечисленных доменов не являются локальными, и что время ожидания запросов истечет, если сервер для одного из доменов недоступен.

При наличии нескольких директив ***search*** используется только список поиска из последнего экземпляра.

Список поиска может содержать не более шести доменов и не может быть длиннее 256 символов. В *glibc 2.25*и более ранних версиях список поиска мог содержать не более шести доменов и не мог быть длиннее 256 символов. Начиная с *glibc 2.26* список поиска не ограничен.

Директива ***domain*** — это устаревшее название директивы ***search***, которая обрабатывает только одну запись в списке поиска.

sortlist

Позволяет сортировать адреса, возвращаемых функцией **gethostbyname(3)**. Список сортировки задается в виде пар IP-адрес/сетевая маска. Маску сети указывать не обязательно, по умолчанию используется естественная маска сети. IP-адрес и маска сети разделяются косой чертой. В списке можно указывать до 10 пар. Пример:

```
sortlist 130.155.160.0/255.255.240.0 130.155.0.0
```

Ключевое слово ***search*** системного файла **resolv.conf** можно переопределить для каждого процесса, задав для переменной среды LOCALDOMAIN список доменов поиска, разделенных пробелами.

Ключевое слово ***options*** системного файла **resolv.conf** можно переопределить для каждого процесса, задав для переменной среды RES_OPTIONS список параметров преобразователя, разделенных пробелами.

Любые изменения, внесенные вручную в файл конфигурации **/etc/resolv.conf**, обязательно будут перезаписаны при изменениях в сети или перезагрузке системы.

Ключевое слово и значение должны находиться в одной строке, и кроме того, строка должна начинаться с ключевого слова (например, ***nameserver***). Значение следует за ключевым словом, разделенным пробелом.

Строки, начинающиеся с точки с запятой (;) или решетки (#), считаются комментариями.

Resolvconf – это платформа для обновления системной информации о серверах DNS. Он настраивается как посредник между программами, которые предоставляют эту информацию и программами, которые используют эту информацию.

Обновить файл **/etc/resolv.conf**, чтобы внести изменения в DNS:

```
# resolvconf -u
```

Пример файла **/etc/resolv.conf**:

```
search test.alt example.test
nameserver 192.168.0.132
nameserver 8.8.8.8
```

Запись search позволяет использовать в качестве адреса только хост-имя для компьютеров в домене test.alt. Например, чтобы обратиться системе work.test.alt, пользователь должен ввести в качестве адреса только хост-имя, work. Когда преобразователь пытается разрешить доменное имя, например, work, он сначала формирует полное доменное имя, используя имя домена test.alt, в work.test.alt и выполняет DNS-запрос, используя это полное доменное имя. Если это не удается, то преобразователь пробует следующий в очереди домен и запрашивает IP-адрес work.example.test.

При этом, когда преобразователь пытается разрешить доменное имя work.ru, он сначала запросит work.ru как абсолютное доменное имя. Если DNS не сможет разрешить его, то только тогда преобразователь объединит его с поисковым доменом, чтобы сформировать work.ru.test.alt, и повторит запрос.

Решение о том, выполняется ли первый запрос как абсолютное доменное имя или нет, полностью зависит от количества точек, присутствующих в доменном имени. По умолчанию доменное имя, содержащее по крайней мере 1 точку, заставит преобразователь запрашивать его дословно, не объединяя его с какими-либо поисковыми доменами. Количество точек для первого запроса абсолютного доменного имени настраивается в значении параметра ***ndots*** (см. описание параметров выше).

57.5. Bind

Основные файлы настройки DNS:

- **/etc/named.conf** — основной файл конфигурации, содержит в себе ссылки на остальные конфигурационные файлы;

- **/etc/bind/options.conf** — файл для глобальных настроек службы;
- **/etc/bind/rndc.conf** — получить информацию DNS об удаленном сервере;
- **/etc/bind/local.conf** — файл для настроек зоны DNS;
- **/var/lib/samba/bind-dns/named.conf** — инструмент для динамического обновления записей DNS.

Конфигурационный файл BIND 9 состоит из разделов, операторов и комментариев. Правила синтаксиса файла named.conf:

- список IP должен быть разделен символом «;», можно указывать подсеть в формате 192.168.0.1/24 или 192.168.0.1/255.255.255.0, (для исключения IP-адреса перед ним нужно поставить знак !);
- строки начинающиеся с символа «#», «//» и заключенные в «/*» и «*/» считаются комментариями;
- в файлах описания зон символ @ является переменной, хранящей имя зоны, указанной в конфигурационном файле **named.conf** или в директиве @ $ORIGIN текущего описания зоны;
- каждая завершенная строка параметров должна завершаться символом «;».

В таблице Разделы конфигурационного файла bind приведены некоторые разделы файла конфигурации.

Таблица 57.1. Разделы конфигурационного файла bind

Раздел	Описание
acl	Позволяет задать именованный список сетей. Формат раздела: acl имя_сети {ip; ip; ip; };
controls	Объявляет каналы управления, которые будут использоваться утилитой rndc
dnssec-policy	Описывает ключ DNSSEC и политику подписи для зон
key	Указывает ключевую информацию для использования при аутентификации и авторизации с использованием TSIG
:any:key-store	Описывает хранилище ключей DNSSEC
logging	Указывает, какую информацию регистрирует сервер и куда отправляются сообщения журнала
options	Задает глобальные параметры конфигурационного файла, управляющие всеми зонами
parental-agents	Определяет именованный список серверов для включения в списки родительских агентов основной и дополнительной зон
primaries	Определяет именованный список серверов для включения в основные и дополнительные зоны или списки уведомлений
server	Устанавливает определенные параметры конфигурации для каждого сервера
tls	Указывает информацию о конфигурации для соединения TLS
http	Указывает информацию о конфигурации для HTTP-соединения
trust-anchors	

Раздел	Описание
	Определяет якоря доверия DNSSEC: при использовании с ключевым словом Initial-key или Initial-ds якоря доверия поддерживаются в актуальном состоянии с помощью обслуживания якоря доверия RFC 5011; при использовании со static-key или static-ds ключи являются постоянными.
zone	Определяет описание зон(ы)

В таблице Основные параметры конфигурационного файла bind описаны некоторые параметры файла **/etc/bind/options.conf**. Для получения более подробной информации следует обратиться к man странице **named.conf(5)**.

Таблица 57.2. Основные параметры конфигурационного файла bind

Опция	Описание
directory	Указывает каталог расположения таблиц зон
listen-on	Определяет адреса IPv4, на которых сервер прослушивает DNS-запросы
listen-on-v6	Определяет адреса IPv6, на которых сервер прослушивает DNS-запросы
allow-query	IP-адреса и подсети, от которых будут обрабатываться запросы. Если параметр не задан, сервер отвечает на все запросы
allow-transfer	Устанавливает возможность передачи зон для slave-серверов
allow-query-cache	IP-адреса и подсети, которые могут получить доступ к кешу этого сервера
allow-recursion	IP-адреса и подсети, от которых будут обрабатываться рекурсивные запросы (для остальных будут выполняться итеративные запросы). Если параметр не задан, сервер выполняет рекурсивные запросы для всех сетей
pid-file	Указывает путь к файлу, в который сервер записывает идентификатор процесса
tkey-gssapi-keytab	Устанавливает файл таблицы ключей KRB5, который будет использоваться для обновлений GSS-TSIG. Это файл таблицы ключей KRB5, который можно использовать для обновлений GSS-TSIG. Если этот параметр установлен, а **tkey-gssapi-credential** не установлен, обновления разрешены с любым ключом, соответствующим участнику в указанной вкладке ключей
minimal-responses	Контролирует, добавляет ли сервер записи в разделы полномочий и дополнительных данных. При значении yes сервер добавляет записи в авторитетные и дополнительные разделы только тогда, когда такие записи требуются протоколом DNS (например, при возврате делегирования или отрицательных ответах). Это обеспечивает лучшую производительность сервера, но может привести к увеличению количества клиентских запросов
max-cache-ttl	Указывает максимальное время (в секундах), в течение которого сервер кеширует обычные (положительные) ответы. Максимальный срок кеша по умолчанию — 04800 (одна неделя)

Опция	Описание
forward	Позволяет указать каким образом сервер обрабатывает запрос клиента. При значении *first* DNS-сервер будет пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders. Если разрешить имя с помощью данных серверов не удалось, то попытаться разрешить имя самостоятельно. Если указать значение *none*, сервер не будет пытаться разрешить имя самостоятельно
forwarders	DNS-сервер, на который будут перенаправляться запросы клиентов
dnssec-validation	Включает проверку DNSSEC в именованных файлах. Если установлены значения auto (по умолчанию) и yes, проверка DNSSEC включена. Если установлено значение no, проверка DNSSEC отключена
type	Указывает тип зоны, описываемой в текущем разделе. Тип зоны может принимать следующие значения: ▸forward — указывает зону переадресации, которая переадресовывает запросы, пришедшие в эту зону; ▸hint — указывает вспомогательную зону (данный тип содержит информацию о корневых серверах, к которым сервер будет обращаться в случае невозможности найти ответ в кеше); ▸master — указывает работать в качестве мастер сервера для текущей зоны; ▸slave — указывает работать в качестве подчиненного сервера для текущей зоны.

Часть VIII. Решение проблем

Содержание

58. Диагностика

Глава 58. Диагностика

58.1. Инструмент диагностики состояния контроллера домена

58.2. Инструмент диагностики клиента домена

58.3. ALT Diagnostic Tool

58.1. Инструмент диагностики состояния контроллера домена

diag-domain-controller — инструмент диагностики состояния контроллера домена.

diag-domain-controller содержит набор проверок и тестов, по результатам которых можно определить корректность настроек компьютера для работы в качестве контроллера домена. **diag-domain-controller** имеет модульную структуру. Модули можно вызывать общим списком или отдельно.

Установка:

```
# apt-get install diag-domain-controller
```

Синтаксис:

```
diag-domain-controller [options] [<diagnostic-task>]
```

где diagnostic-task — название функции из списка тестов. Если не указывать название функции, будут запущены все тесты.

Возможные опции:

- **-l**, **--list** — вывести список тестов;
- **-V**, **--version** — вывести версию и выйти;
- **-v**, **--verbose** — подробный вывод на терминал;
- **r[FILE]**, **--report=[FILE]** — записать подробный вывод в файл отчета (**report_<текущая дата>.txt**) и создать архив, содержащий файл отчета и файлы **smb.conf**, **krb5.conf**. Необязательный параметр — имя архива. Если файл не указан, будет создан архив **$TMP/report_<текущая дата>.tar.gz**;
- **-a**, **-alterator** — вывод для использования в приложениях alterator;
- **-h**, **--help** — показать справку и выйти.

Возможные состояния тестов:

- DONE — успешное выполнение модуля;
- WARN — предупреждение для некритических тестов в модуле;
- FAIL — неудачное выполнение теста.

В таблице Тесты diag-domain-controller приведены тесты, доступные в **diag-domain-controller** в настоящее время.

Таблица 58.1. Тесты diag-domain-controller

Тест	Описание
is_domain_info_available	Проверка доступности просмотра общей информации о домене
is_hostname_correct	Проверка правильного написания доменного имени узла
is_hostname_static_and_transient	Проверка совпадения статического и временного имени хоста
is_not_empty_sysvol	Проверяет, содержит ли файлы каталог sysvol. Если каталог sysvol не пустой, также выводит неполный список файлов каталога.

Тест	Описание
	Для возможности просмотра списка вложенных каталогов требуется запуск от root
is_samba_package_installed	Проверяет, установлен ли в системе пакет Samba (*samba-dc* или *samba-dc-mitkrb5*). Выводит информацию о данных пакетах
is_samba_service_running	Проверяет, запущена ли служба Samba
is_resolve_local	Проверяет, разрешает ли контроллер домена DNS-запросы локально (файл **/etc/resolv.conf** содержит строку nameserver 127.0.0.1)
is_krb5_conf_file_exists	Проверяет наличие файла конфигурации **/etc/krb5.conf** и отображает содержимое этого файла
is_smb_conf_file_exists	Проверяет наличие файла конфигурации **/etc/samba/smb.conf** и отображает содержимое этого файла
is_there_way_to_cache_kerberos_tickets	Проверяет метод кеширования билетов Kerberos (**control krb5-conf-ccache**)
is_dns_lookup_kdc_enabled	Проверяет, включен ли поиск доменного имени Kerberos через DNS (значение параметра ***dns_lookup_kdc*** в файле **/etc/krb5.conf**)
is_resolv_conf_file_exists	Проверяет наличие файла конфигурации **/etc/resolv.conf** и отображает содержимое этого файла
does_resolv_conf_and_default_realm_it_match	Проверяет соответствие записи области (realm) в файле конфигурации **/etc/krb5.conf** одному из доменных имен в файле **/etc/resolv.conf**
does_smb_realm_and_krb5_default_realm_it_match	Проверяет соответствие записи домена в файле конфигурации **/etc/krb5.conf** записи realm в файле конфигурации **smb.conf**
are_there_errors_in_samba_databases	Проверяет наличие ошибок в базах Samba. Требуется запуск от root
is_ntp_service_running	Проверяет, включена ли служба NTP
is_time_synchronization_enabled	Проверяет, включена ли синхронизация времени

Примеры (команды запускаются на контроллере домена):

- вывести список тестов:

```
$ diag-domain-controller -l
is_domain_info_available
is_hostname_correct
is_hostname_static_and_transient
is_not_empty_sysvol
is_samba_package_installed
is_samba_service_running
is_resolve_local
is_krb5_conf_file_exists
is_smb_conf_file_exists
is_there_way_to_cache_kerberos_tickets
is_dns_lookup_kdc_enabled
is_resolv_conf_file_exists
does_resolv_conf_and_default_realm_it_match
```

```
does_smb_realm_and_krb5_default_realm_it_match
are_there_errors_in_samba_databases
is_ntp_service_running
is_time_synchronization_enabled
```

- запустить тест is_domain_info_available:

```
$ diag-domain-controller is_domain_info_available
================================================
General information about the domain controller:
Forest           : test.alt
Domain           : test.alt
Netbios domain   : TEST
DC name          : dc1.test.alt
DC netbios name  : DC1
Server site      : Default-First-Site-Name
Client site      : newSite

================================================
[DONE]: is_domain_info_available
```

- запустить все тесты:

```
$ diag-domain-controller
[DONE]: is_domain_info_available
[DONE]: is_hostname_correct
[DONE]: is_hostname_static_and_transient
[DONE]: is_not_empty_sysvol
[DONE]: is_samba_package_installed
[DONE]: is_samba_service_running
[FAIL]: is_resolve_local
[DONE]: is_krb5_conf_file_exists
[DONE]: is_smb_conf_file_exists
[WARN]: is_there_way_to_cache_kerberos_tickets
[DONE]: is_dns_lookup_kdc_enabled
[DONE]: is_resolv_conf_file_exists
[DONE]: does_resolv_conf_and_default_realm_it_match
[DONE]: does_smb_realm_and_krb5_default_realm_it_match
[WARN]: are_there_errors_in_samba_databases
[WARN]: is_ntp_service_running
[DONE]: is_time_synchronization_enabled
```

58.2. Инструмент диагностики клиента домена

diag-domain-client — инструмент диагностики состояния клиента домена.

diag-domain-client содержит набор проверок и тестов, по результатам которых можно определить корректность настроек компьютера для работы в домене, а также убедиться, что доступны все необходимые ресурсы домена. **diag-domain-client** имеет модульную структуру. Модули можно вызывать общим списком или отдельно.

Утилита позволяет записать результат в log-файл. Процесс диагностики зависит от того, находится ли компьютер в домене или нет. Выполнение некоторых проверок требует полномочий суперпользователя. Для корректной работы необходимо получить Kerberos-билет доменного пользователя.

Установка:

```
# apt-get install diag-domain-client
```

Синтаксис:

```
diag-domain-client [options] [<test-function-name>]
```

где test-function-name — название функции из списка тестов. Если не указывать название функции, будут запущены все тесты.

Возможные опции:

- **-h**, **--help** — показать справку и выйти;
- **-V**, **--version** — вывести версию и выйти;
- **-v**, **--verbose** — подробный вывод;
- **-w[FILE]**, **--logfile[=FILE]** — записать подробный вывод в файл по указанному пути. Если файл не указан, вывод будет записан в файл **./diag-domain-client.log**. В случае если файл уже существует, то запись производится в файл с постфиксом (например, **diag-domain-client.log.1**, **diag-domain-client.log.2** и т.д.);
- **-f**, **--force** — принудительная запись в существующий файл;
- **-l**, **--list** — вывести список тестов.

Возможные состояния тестов:

- DONE — успешное выполнение модуля;
- SKIP — пропуск проверки, если проверка выполняется без полномочий суперпользователя;
- WARN — предупреждение для некритических тестов в модуле;
- FAIL — неудачное выполнение теста.

Если компьютер введен в домен, утилита **diag-domain-client** выдаёт FAIL для тех проверок, когда несоответствие проверяемого элемента приводит к неработоспособности машины в домене. При выполнении программы не суперпользователем некоторые проверки могут быть пропущены (SKIP) или находиться в состоянии WARN. В случае успешного выполнения отображается статус DONE.

В таблице Тесты и проверки diag-domain-client приведены тесты и проверки, доступные в **diag-domain-client** в настоящее время.

Таблица 58.2. Тесты и проверки diag-domain-client

Тест/Проверка	Описание
check_hostnamectl	Отображает полную информацию о узле и соответствующие настройки: имя, значок, система, версия ядра, архитектура, информация о виртуализации (при наличии)
test_hostname	Проверяет, является ли имя компьютера полностью определенным именем домена (FQDN)
check_system_auth	

Тест/Проверка	Описание
	Отображает метод аутентификации пользователей, используемый в подсистеме PAM (sss, winbind — компьютер введен в домен, local — не введен). Выводит содержимое файла **`/etc/pam.d/system-auth`**
is_samba_package_installed	Проверяет, установлен ли в системе пакет Samba (*samba-dc* или *samba-dc-mitkrb5*)
test_domain_system_auth	Проверяет, подходит ли метод аутентификации для работы машины в домене (допустимые значения: sss, winbind)
check_system_policy	Отображает, какие политики применяются в процессе PAM-аутентификации: local — никакие, gpupdate — локальные и доменные
test_gpupdate_system_policy	Проверяет, настроено ли применение групповых политик в системе
check_krb5_conf_exists	Проверяет наличие, отображает права доступа и содержимое файла конфигурации **`krb5.conf`**
check_krb5_conf_ccache	Отображает текущий способ кеширования Kerberos-билетов — keyring, file, dir
test_keyring_krb5_conf_ccache	Проверяет настроенный способ кеширования Kerberos-билетов (для keyring)
check_krb5_conf_kdc_lookup	Проверяет включен ли поиск Kerberos-имени домена через DNS. Допустимыми значениями для «dns_lookup_kdc» в **`/etc/krb5.conf`** являются — true/yes
check_krb5_keytab_exists	Проверяет наличие, права доступа и дату последнего изменения файла **`/etc/krb5.conf`**. В этом файле хранятся принципалы и хеши пароля доменной учётной записи компьютера
check_keytab_credential_list	Отображает содержимое файла **`/etc/krb5.conf`** (файл с учётными данными машинного пользователя). В этом файле хранятся принципалы и хеши пароля доменной учётной записи компьютера. Требуется запуск от root, иначе SKIP
check_resolv_conf	Проверяет наличие и выводит содержимое файла конфигурации разрешения имен **`resolv.conf`**
compare_resolv_conf_with_default_realm	Сравнивает домен для поиска (поле search в **`/etc/resolv.conf`**) с доменом по умолчанию, указанным для Kerberos
check_smb_conf	Проверяет наличие и выводит содержимое файла настроек конфигурации Samba
compare_smb_realm_with_krb5_default_realm	Сравнивает домен, указанный в файле конфигурации Samba, с доменом по умолчанию, указанным для Kerberos
test_smb_realm	Проверяет корректное заполнение информации о домене в конфигурационных файлах Samba и Kerberos
test_domainname	Сверяет доменное имя из **`/etc/hostname`** с именем домена в составе FQDN-имени узла
check_time_synchronization	

Тест/Проверка	Описание
	Отображает настройку синхронизации времени с сервером; выводит подробную информацию — часовой пояс, временную зону и т.д. Необходимо для корректной работы с сертификатами, электронной подписью, билетами Kerberos
test_time_synchronization	Проверяет, включена ли синхронизация времени
check_nameservers	Проверяет доступность всех контроллеров домена по имени (**host <domain FQDN>**) и IP-адресу (работает ли **resolv.conf**)
check_domain_controllers	Проверяет доступность всех контроллеров домена в домене (из srv-записей). Отображает версии контроллеров домена (из LDAP)
check_kerberos_and_ldap_srv_records	Проверяет наличие srv-записей вида _kerberos._udp.<domain FQDN> и _ldap._tcp.<domain FQDN> для домена. Требуется для корректной работы машины в домене. Без записей Kerberos, sssd и winbind не смогут найти контроллеры домена
compare_netbios_name	Сравнивает короткое имя машины из **/etc/hostname** с NetBios-именем машины в **smb.conf**
check_common_packages	Проверяет наличие установленных основных пакетов и их версий (*alterator-auth*, *libnss-role*, *libkrb5* и *libsmbclient*)
check_group_policy_packages	Проверяет наличие установленных основных пакетов и их версий для управления групповыми политиками (*local-policy* и *gpupdate*)
check_sssd_ad_packages	Проверяет наличие установленного мета-пакета и его версии для аутентификации с помощью sssd (*task-auth-ad-sssd*)
check_sssd_winbind_packages	Проверяет наличие установленного мета-пакета и его версии для аутентификации с помощью winbind (*task-auth-ad-winbind*)

Примеры:

- вывести список тестов:

```
$ diag-domain-client -l
check_hostnamectl
test_hostname
check_system_auth
test_domain_system_auth
check_system_policy
test_gpupdate_system_policy
check_krb5_conf_exists
check_krb5_conf_ccache
test_keyring_krb5_conf_ccache
check_krb5_conf_kdc_lookup
check_krb5_keytab_exists
check_keytab_credential_list
check_resolv_conf
compare_resolv_conf_with_default_realm
check_smb_conf
compare_smb_realm_with_krb5_default_realm
test_smb_realm
test_domainname
check_time_synchronization
test_time_synchronization
check_nameservers
```

```
check_domain_controllers
check_kerberos_and_ldap_srv_records
compare_netbios_name
check_common_packages
check_group_policy_packages
check_sssd_ad_packages
check_sssd_winbind_packages
```

- запустить тест check_smb_conf:

```
$ diag-domain-client check_smb_conf
is_domain_info_available
[DONE]: is_domain_info_available
```

- запустить тест check_krb5_conf_kdc_lookup с подробным выводом информации:

```
$ diag-domain-client check_krb5_conf_kdc_lookup -v
================================================================================
=
| Samba environment diagnostic tool |
--------------------------------------------------------------------------------
-
Version: 0.2.8
Date: Ср 09 окт 2024 12:54:51 EET
--------------------------------------------------------------------------------
-
System information
Kernel: 5.10.212-std-def-alt1
Branch: p10
================================================================================
=

================================================================================
=
| check_krb5_conf_kdc_lookup |
--------------------------------------------------------------------------------
-

/etc/krb5.conf: dns_lookup_kdc is enabled

--------------------------------------------------------------------------------
-
Check DNS lookup kerberos KDC status: [DONE]
================================================================================
=
```

- запустить все тесты:

```
$ diag-domain-client
Check hostname persistance: [DONE]
Test hostname is FQDN (not short): [DONE]
System authentication method: [DONE]
Domain system authentication enabled: [DONE]
System policy method: [DONE]
System group policy enabled: [DONE]
Check Kerberos configuration exists: [DONE]
Kerberos credential cache status: [DONE]
Using keyring as kerberos credential cache: [DONE]
```

```
Check DNS lookup kerberos KDC status: [DONE]
Check machine crendetial cache is exists: [DONE]
Check machine credentials list in keytab: [SKIP]
Check nameserver resolver configuration: [DONE]
Compare krb5 realm and first search domain: [DONE]
Check Samba configuration: [DONE]
Compare samba and krb5 realms: [DONE]
Check Samba domain realm: [DONE]
Check hostname FQDN domainname: [DONE]
Check time synchronization: [DONE]
Time synchronization enabled: [WARN]
Check nameservers availability: [WARN]
Check domain controllers list: [FAIL]
Check Kerberos and LDAP SRV-records: [DONE]
Compare NetBIOS name and hostname: [DONE]
Check common packages: [DONE]
Check group policy packages: [DONE]
Check SSSD AD packages: [DONE]
Check SSSD Winbind packages: [WARN]
```

- записать вывод теста check_krb5_conf_kdc_lookup в файл **/tmp/diag-domain-client.log**:

```
$ diag-domain-client check_krb5_conf_kdc_lookup -w/tmp/diag-domain-client.log
Check DNS lookup kerberos KDC status: [DONE]
```

просмотреть содержимое файла **/tmp/diag-domain-client.log**:

```
$ cat /tmp/diag-domain-client.log
================================================================================
=
| Samba environment diagnostic tool |
--------------------------------------------------------------------------------
-
Version: 0.2.8
Date: Ср 09 окт 2024 12:54:24 EET
--------------------------------------------------------------------------------
-
System information
Kernel: 5.10.212-std-def-alt1
Branch: p10
================================================================================
=

================================================================================
=
| check_krb5_conf_kdc_lookup |
--------------------------------------------------------------------------------
-

/etc/krb5.conf: dns_lookup_kdc is enabled

--------------------------------------------------------------------------------
-
Check DNS lookup kerberos KDC status: [DONE]
================================================================================
=
```

58.3. ALT Diagnostic Tool

ALT Diagnostic Tool (ADT) — приложение для диагностики ОС с графическим и терминальным интерфейсом.

Утилита ADT позволяет:

- проводить диагностику системы посредством набора подготовленных утилит;
- выводить на экран результаты диагностики;
- сохранять файл журнала с результатами диагностики;
- выполнять операции, требующие привилегий, от учетной записи непривилигированного пользователя.

Программа ADT предназначена для:

- системных администраторов;
- опытных пользователей;
- службы технической поддержки.

Запуск инструментов диагностики регулируется системным администратором, позволяя создавать отчеты пользователям, не передавая им административные полномочия.

58.3.1. Установка

Для работы с ADT необходимо установить:

- ADT (пакет *adt*);
- диагностические инструменты (например, пакеты *diag-domain-client*, *diag-domain-controller*).

Установка ADT:

```
# apt-get install adt
```

Установка инструментов диагностики состояния клиента домена и состояния контроллера домена:

```
# apt-get install diag-domain-client diag-domain-controller
```

58.3.2. Работа с ADT

Запустить и добавить в автозагрузку службу alterator-manager:

```
# systemctl enable --now alterator-manager.service
```

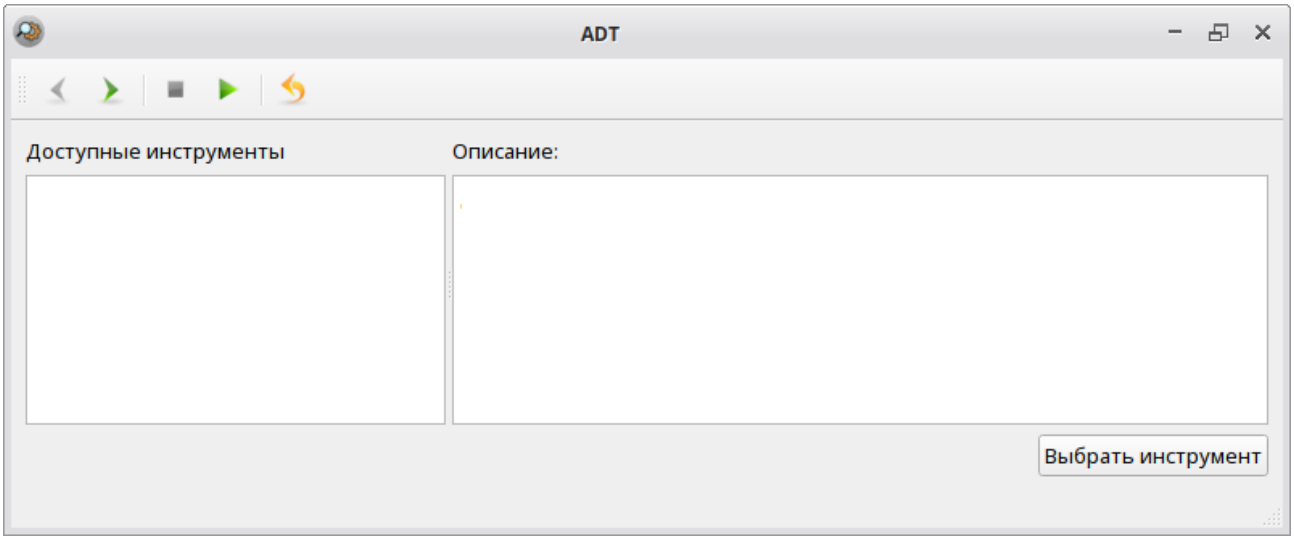
Запустить ADT можно:

- из командной строки:

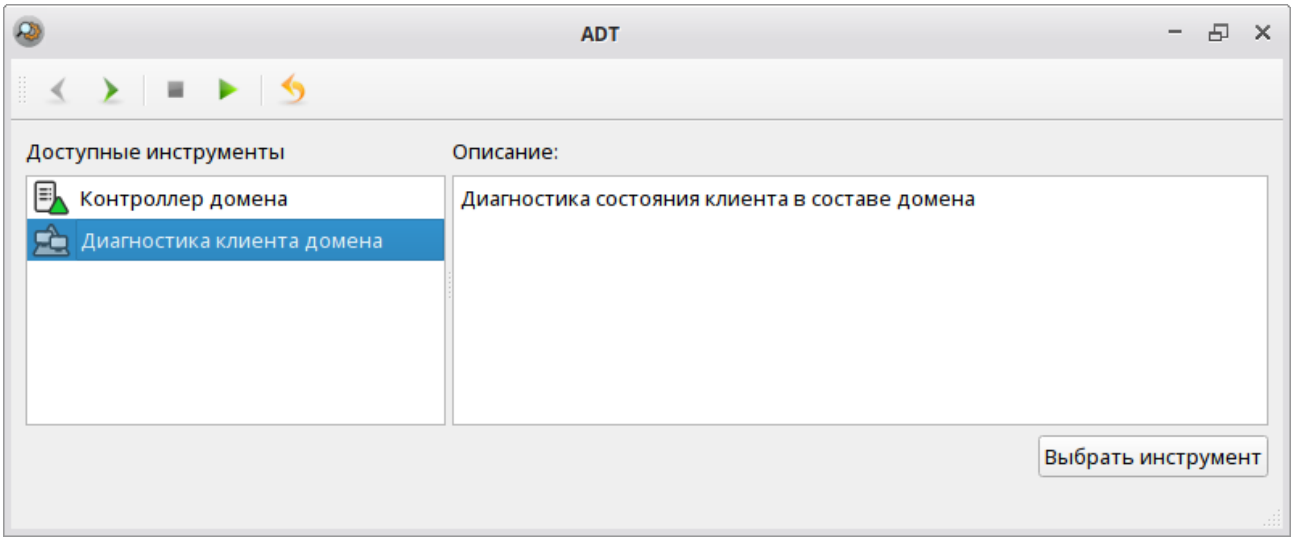
```
$ adt
```

- в рабочей среде Mate: **Меню** → **Системные** → **ADT**;
- в рабочей среде KDE5: **Меню запуска приложений** → **Настройки** → **ADT**.

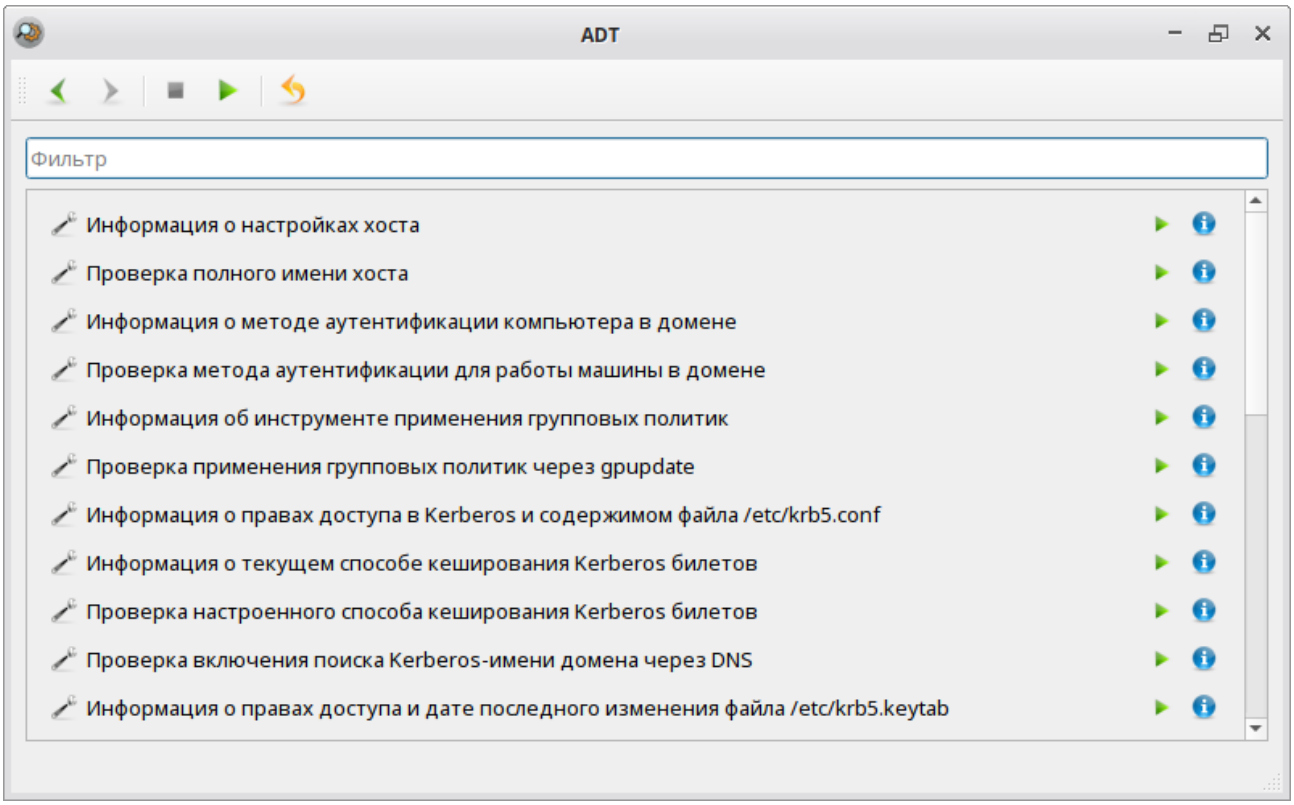
Внешний вид программы ADT без установленных инструментов диагностики:



Внешний вид программы ADT с инструментами диагностики:

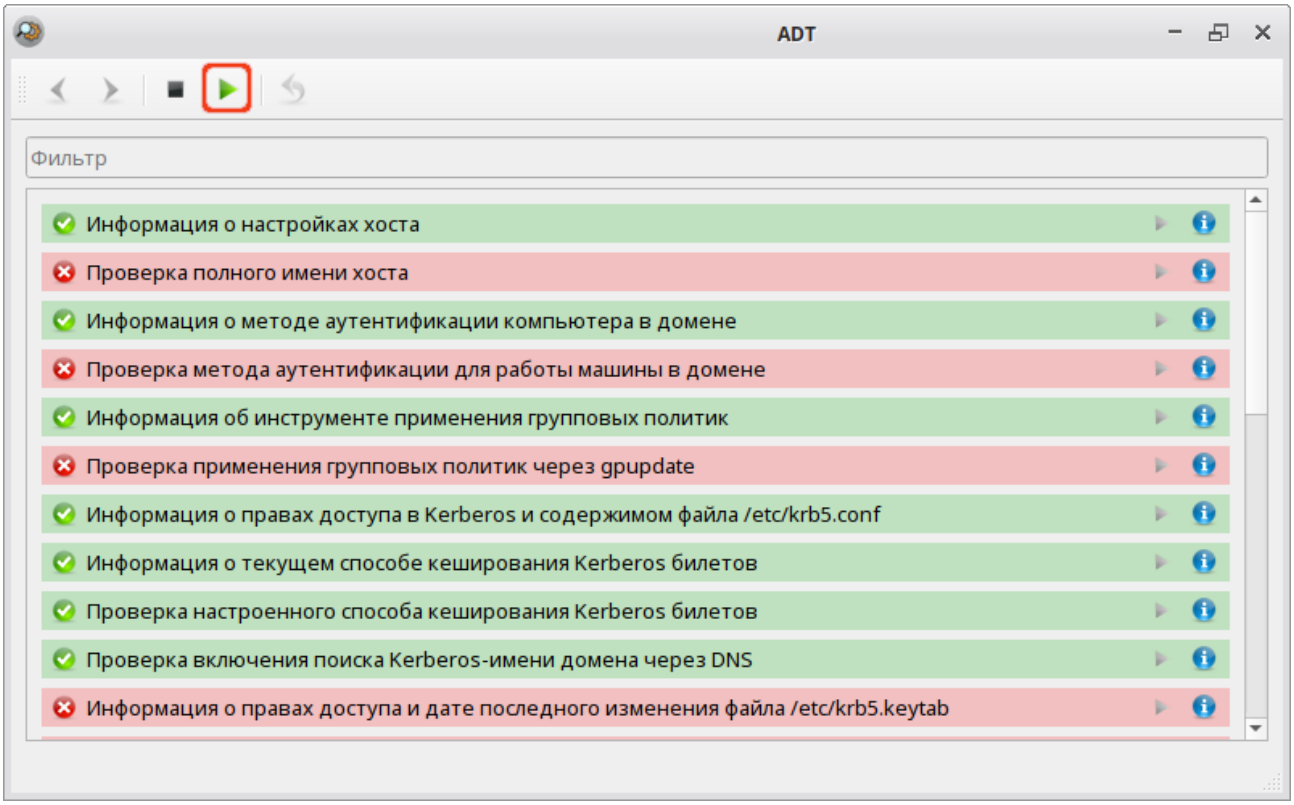


Для выбора набора тестов следует дважды щелкнуть мышью по его названию, либо выделить набор и нажать кнопку **Выбрать инструмент**. Откроется окно с набором тестов инструмента:

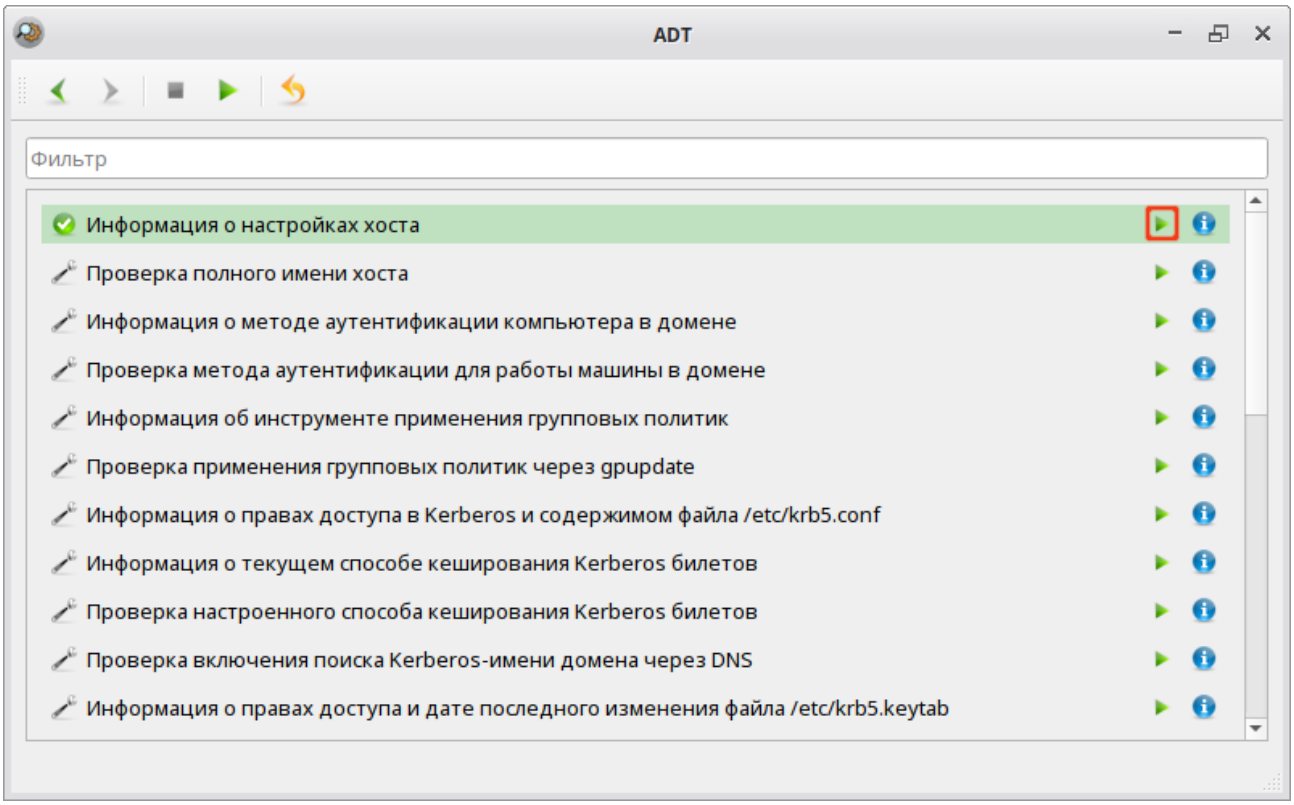


В области управления инструментом диагностики доступны опции: **Отчет**, **Запустить все тесты**, **Назад**. Напротив каждого теста находятся кнопки **Запустить** и **Журнал**.

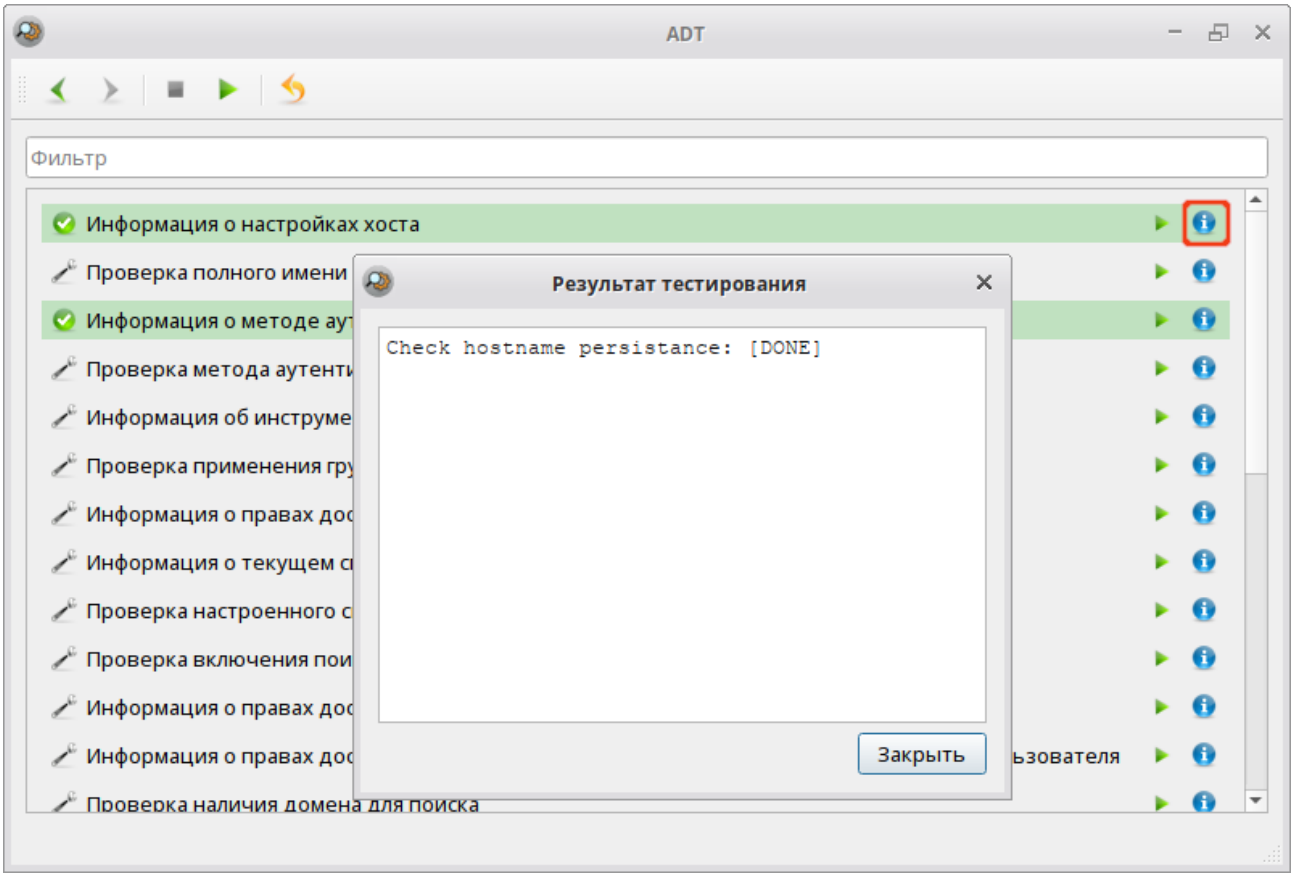
Нажатие на кнопку **Запустить все тесты** запускает весь набор тестов выбранного инструмента:



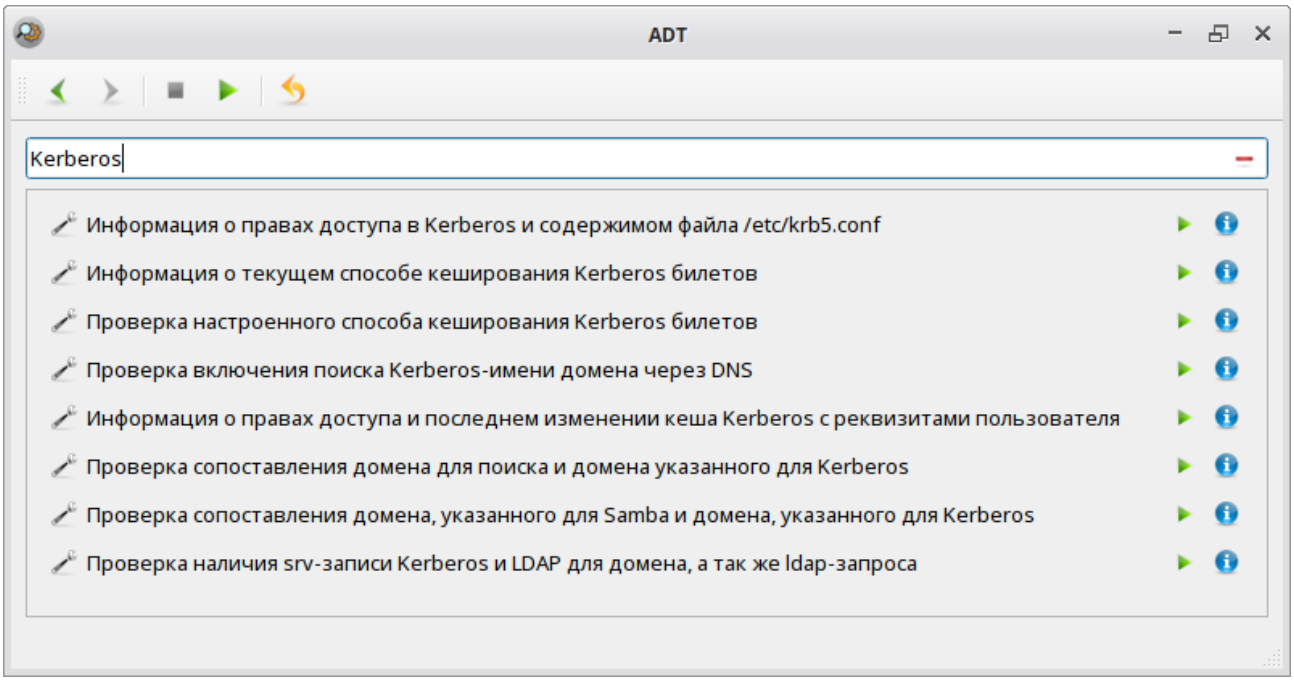
Для того чтобы запустить отдельный тест, необходимо нажать кнопку **Запустить**, расположенную справа от названия теста:



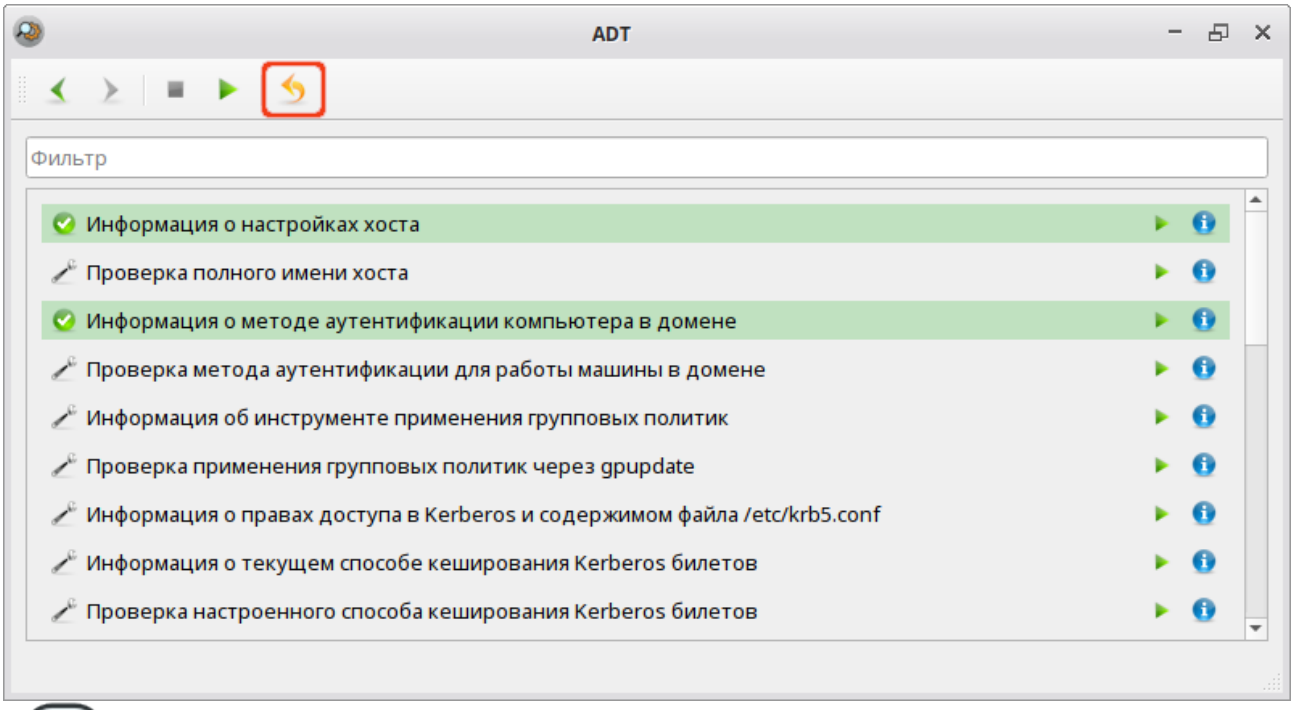
Нажатие на кнопку **Журнал** выводит отчет теста от утилиты инструмента диагностики (если инструмент поддерживает такую возможность):



Для поиска конкретного теста среди доступных можно воспользоваться строкой **Фильтр**:



Для сохранения полного отчёта инструмента в файл (если инструмент поддерживает такую возможность) следует нажать кнопку **Отчет** на панели инструментов:



Примечание

Для возможности генерирования файла с отчетом, инструмент диагностики должен поддерживать опции **-r**, **--report**.

58.3.3. Руководство администратора

58.3.3.1. Компоненты

Alterator-manager — модульный сервис, предназначенный для конфигурации посредством D-Bus. Весь функционал реализуется в виде модулей, а интерфейсы описываются в конфигурационных файлах «alterator entry».

Система межпроцессного взаимодействия D-Bus — механизм для обмена сообщениями между различными программами в ОС. D-Bus позволяет программам отправлять сообщения и вызывать методы других программ, обеспечивая совместную работу и координацию между приложениями. D-Bus представляет из себя совокупность следующих шин:

- Системная шина — создаётся при старте демона D-Bus. Предназначена для взаимодействия между различными системными службами, а также взаимодействие пользовательских приложений с этими службами;
- Сессионная шина — создаётся для каждого пользователя во время авторизации как отдельный экземпляр. Предназначена для взаимодействия между пользовательскими приложениями в рамках одной сессии.

На шинах D-Bus регистрируются службы, предоставляющие определенные функции. Они могут быть как частью операционной системы, так и сторонними приложениями.

Для каждой службы заводятся объекты, представляющие собой абстракции реальных ресурсов или служб.

У каждого объекта есть один или несколько интерфейсов, которые определяют, какие действия можно совершить с объектом. Интерфейсы описывают методы (функции), которые можно вызвать, свойства, которые можно запросить или изменить, и сигналы, которые объект может отправлять.

Объекты, создаваемые службами. Каждая служба может создавать объекты, которые представляют собой абстракции реальных ресурсов или служб. Например, служба сетевого менеджера может предоставлять объекты для каждого сетевого соединения.

Интерфейсы объектов. У каждого объекта есть один или несколько интерфейсов, которые определяют, какие действия можно совершить с объектом. Интерфейсы описывают методы (функции), которые можно вызвать, свойства, которые можно запросить или изменить, и сигналы, которые объект может отправлять.

Каждая служба поддерживающая D-Bus представлена в виде объектов на этих шинах. А взаимодействие между ними осуществляется посредством интерфейсов и методов этих объектов.

На системной шине методы запускаются с правами root и имеют высокие привилегии. На сессионной шине методы запускаются с правами пользователя и не имеют доступа к системным ресурсам, которые требуют высоких привилегий. С точки зрения alterator-manager диагностический инструмент является объектом на D-Bus, описанном в двух файлах «alterator entry»:

- **`.backend`** — описывает интерфейс диагностического инструмента, обеспечивающий взаимодействие с D-Bus. В нем же описываются методы интерфейса: info, run, list, report;

- **`.diagnostictool`** — описывает отображение диагностического инструмента в ADT. Содержит информацию о тестах, доступных в рамках описываемого диагностического инструмента.

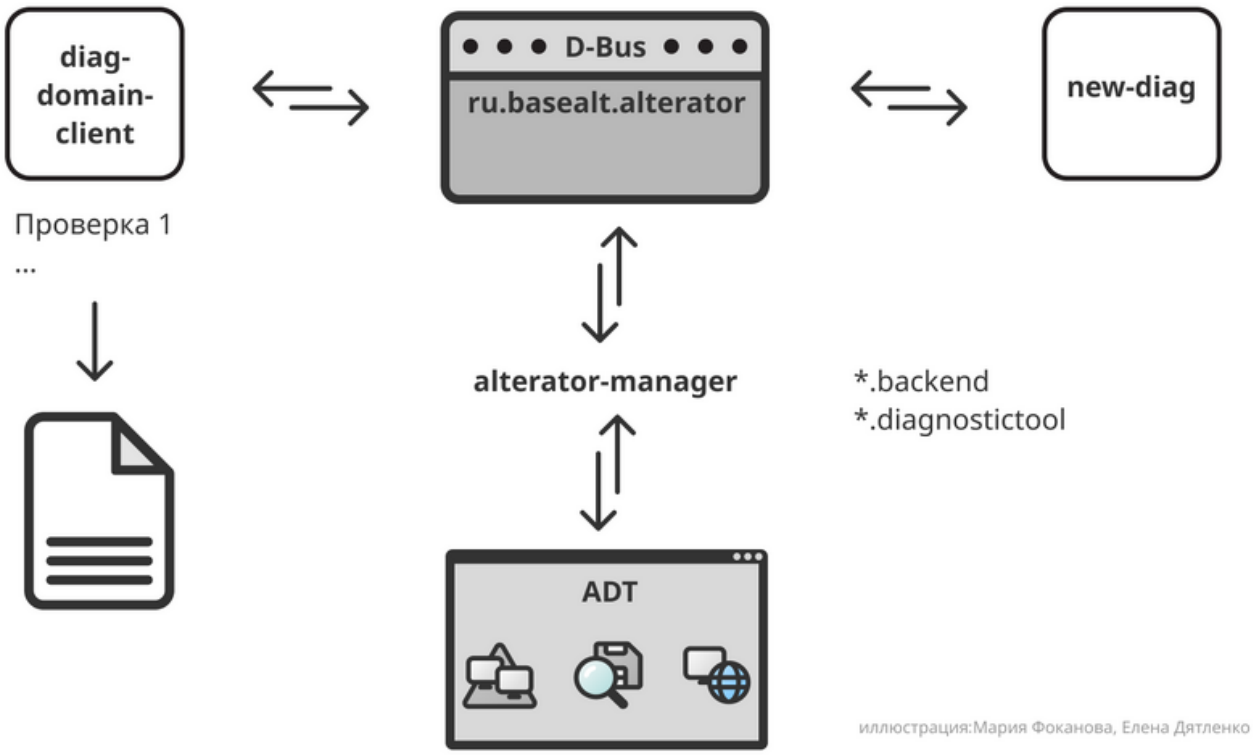
alterator-module-executor — модуль альтератора для обработки файлов **`.backend`** и запуска исполняемых файлов.

58.3.3.2. Алгоритм работы

Алгоритм работы ALT Diagnostic Tool:

1. Systemd служба alterator-manager во время запуска создает на шине D-Bus службу с именем «ru.basealt.alterator».
2. Systemd служба alterator-module-executor собирает информацию из файлов **`.backend`** обо всех установленных диагностических инструментах и создает объекты на системной и сессионных (в зависимости от расположения backend-файлов) шинах D-Bus с именами вида «ru.basealt.alterator.<имя инструмента>».
3. ADT формирует список диагностических инструментов, обращаясь к D-Bus и получая информацию обо всех объектах сервиса «ru.basealt.alterator», имеющих интерфейс «ru.basealt.alterator.diag1».
4. Для каждого диагностического инструмента ADT вызывает на D-Bus метод List, чтобы получить список всех возможных тестов.
5. ADT запускает через D-Bus метод Run, передав ему в качестве параметра имя теста.
6. По коду возврата ADT получает информацию об успешном/неуспешном прохождении теста, а из данных, полученных из stderr и stdout формирует журнал выполнения теста.

Блок-схема взаимодействия компонентов:



58.3.3.3. Разработка инструмента диагностики

58.3.3.3.1. Формат файлов инструмента диагностики

Минимальный набор файлов для инструмента диагностики в ADT:

- исполняемый файл;
- файлы **.backend** и **.diagnostictool** (или **.diag**), описывающие сущности Alterator Entry.

Примечание

Оба варианта **.diagnostictool** и **.diag** считаются верными.

58.3.3.3.2. Требования к исполняемому файлу

Исполняемый файл может быть как бинарным, так и текстовым (написанным на интерпретируемом языке). Файл должен поддерживать запуск в следующем виде:

```
/путь_к_исполняемому_файлу {param}
```

где {param} — означает имя теста, который необходимо выполнить.

При успешном завершении теста исполняемый файл должен завершиться с кодом возврата 0. При неуспешном завершении теста — с кодом возврата отличным от 0.

Лог выполнения нужно выводить в стандартный вывод.

Необходима также поддержка следующих ключей:

- **-l** или **--list** — вывод списка тестов. Список необходимо выводить в стандартный вывод. Имя каждого теста должно быть с новой строки;
- **-r** или **report** — сгенерировать файл с отчетом. Файл с отчетом может представлять собой как текстовые данные, так и бинарные (например, архив). Его содержимое необходимо направить в стандартный вывод. ADT получит этот вывод и сохранит в файл с именем вида «имя_инструмента_дата» и суффиксом, указанным в файле **.diagnostictool**.

Исполняемый файл рекомендуется разместить в каталоге согласно стандарту FHS (Filesystem Hierarchy Standard).

58.3.3.3.3. Рекомендации к файлам .backend и .diagnostictool

Для описания файлов **.backend** и **.diagnostictool** следует воспользоваться спецификацией Alterator Entry

Файлы **.backend** и **.diagnostictool** являются текстовыми и содержат описание в виде секций. Синтаксис файлов:

```
[имя секции1]
Поле1 = значение
Поле2 = значение
ПолеN = значение
[имя секции2]
Поле1 = значение
```

```
Поле2 = значение
ПолеN = значение
[имя секцииN]
Поле1 = значение
Поле2 = значение
ПолеN = значение
```

При этом следует учитывать:

- все поля чувствительны к регистру и должны начинаться с заглавной буквы;
- перед и после знака «=» пробелы;
- значения полей указываются без кавычек;
- значения могут содержать пробелы;
- сли строка начинается с символа «#», то она считается комментарием и при чтении информации из файла игнорируется.

Имя каталога должно соответствовать суффиксу в имени файла:

- **`./backends`** для файла **`.backend`**;
- **`./diagnostictools`** для файла **`.diagnostictool`** (или **`.diag`**).

58.3.3.3.3.1. Файл .diagnostictool

Файл **`.diagnostictool`** имеет имя вида **`<имя диагностического инструмента>.diagnostictool`**.

Если разрабатываемый диагностический инструмент предполагается распространять, то файлы сущностей необходимо разместить в каталоге **`/usr/share/alterator/diagnostictools/`**. В противном случае, рекомендуется использовать каталог **`/etc/alterator/diagnostictools/`**.

Файл **`.diagnostictool`** содержит информацию для GUI Он включает секцию [Alterator Entry] и секции, описывающие варианты тестирования.

Секция [Alterator Entry]:

- [Alterator Entry]
  - Name — идентификатор инструмента (имя без пробелов);
  - Type — всегда Diagnostictool;
  - DisplayName — имя инструмента;
  - DisplayName[локаль] — имя инструмента, выводящееся в GUI, если используется интерфейс с использованием указанной в скобках локали;
  - Comment — описание инструмента;
  - Comment[локаль] — описание, выводящиеся в GUI, если используется интерфейс с использованием указанной в скобках локали;
  - Icon — имя файла с иконкой;

- ReportSuffix — суффикс файла с отчетом. Этот файл будет создаваться при вызове метода Report.

- Секции, описывающие варианты тестирования:

  - [Название секции соответствует названию теста]

  - DisplayName — идентификатор теста (имя без пробелов);

  - DisplayName[локаль] — имя теста, выводящееся в GUI, если используется интерфейс с использованием указанной в скобках локали;

  - Comment — описание теста;

  - Comment[локаль] — описание теста, выводящееся в GUI, если используется интерфейс с использованием указанной в скобках локали.

58.3.3.3.3.2. Файл .backend

Файл **`.backend`** имеет имя вида **`<имя диагностического инструмента>.ru.basealt.alterator.backend`**.

Если разрабатываемый диагностический инструмент предполагается распространять, то файлы сущностей необходимо разместить в каталоге:

- **`/usr/share/alterator/backends/system`** — если объект необходимо создать на системной шине;

- **`/usr/share/alterator/backends/user`** — если объект необходимо создать на сессионной шине;

В противном случае, рекомендуется использовать каталог:

- **`/etc/alterator/backends/system/`** — если объект необходимо создать на системной шине;

- **`/etc/alterator/backends/user/`** — если объект необходимо создать на сессионной шине;

Секция [Alterator Entry] описывает информацию об объекте и содержит следующие поля:

- [Alterator Entry]

  - Type — содержит тип метода. Всегда имеет значение Backend;

  - Module — всегда executor;

  - Name — идентификатор инструмента (имя без пробелов);

  - Interface — идентификатор интерфейса. Имеет значение ru.basealt.alterator.diag1. Можно сократить до diag1;

  - thread_limit — указывает максимальное число потоков при одновременном выполнении нескольких методов.

Секция Info описывает метод Info и содержит следующие поля:

- [Info]
  - execute — в качестве параметра необходимо передать команду, выводящую содержимое файла **.diagnostictool** (**cat <путь к файлу>**);
  - stdout_bytes — всегда enabled;
  - thread_limit — всегда 3;
  - action_id — содержит идентификатор метода. Всегда имеет значение Info.

Секция Run описывает метод Run и содержит следующие поля:

- [Run]
  - execute — содержит строку для запуска тестов вида **<путь к исполняемому файлу> {param}**;
  - stdout_signal_name — всегда diag1_stdout_signal. ADT ожидает сигнал с таким именем;
  - stderr_signal_name — всегда diag1_stderr_signal. ADT ожидает сигнал с таким именем;
  - action_id — содержит идентификатор метода. Всегда имеет значение Run.

Секция List описывает метод List и содержит следующие поля:

- [List]
  - execute — содержит команду для вывода списка всех возможных тестов в виде **<путь к исполняемому файлу> -l**;
  - stdout_strings — всегда enabled;
  - action_id — содержит идентификатор метода. Всегда имеет значение List.

Секция Report содержит следующие поля:

- [Report]
  - execute — содержит команду для создания отчета в виде **<путь к исполняемому файлу> -R**;
  - stdout_bytes — всегда enabled;
  - action_id — содержит идентификатор метода. Всегда имеет значение Report.

58.3.3.4. Пример инструмента диагностики

Ниже представлен пример диагностического инструмента для определения производителя материнской платы.

Пример состоит из трех файлов:

- исполняемый файл: **/usr/bin/diag-example**;
- файл .backend: **/usr/share/alterator/backends/diag-example.backend**;

- файл .diag, описывающий тесты: **/usr/share/alterator/diagnostictools/diag-example.diag**.

58.3.3.4.1. Исполняемый файл

Содержимое исполняемого файла **/usr/bin/diag-example**:

```
#!/bin/bash
#
# Copyright (c) 2024 Evgeny Sinelnikov <sin@altlinux.org>
#
# Example diagnostic tool
#
# SPDX-License-Identifier: GPL-2.0-or-later
#

set -euo pipefail

. shell-getopt

PROG="${0##*/}"
PROG_VERSION='0.0.1'

cmd="run"
global_retval=0

print_version()
{
cat <<EOF
$PROG version $PROG_VERSION
Written by Evgeny Sinelnikov <sin@altlinux.org>

Copyright (C) 2024 Evgeny Sinelnikov <sin@altlinux.org>
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
EOF
exit
}

show_usage()
{
cat <<EOF
$PROG - example diagnostic tool.

Usage: $PROG [options] [<diagnostic-task>]

Options:
-l, --list               list of diagnostic tasks;
-V, --version            print program version and exit;
-h, --help               show this text and exit.

Report bugs to https://bugzilla.altlinux.org/

EOF
exit
}

TEMP=$(getopt -n "$PROG" -o "l,V,h" -l "list,version,help" -- "$@") || show_usage
eval set -- "$TEMP"
```

```
while :; do
case "$1" in
    --) shift; break
        ;;
    -l|--list) cmd="list";
        ;;
    -V|--version) print_version
        ;;
    -h|--help) show_usage
        ;;
    *) fatal "Unrecognized option: $1"
        ;;
esac
shift
done

task_list="$*"

task_show()
{
local func="$1"

echo "$func"
}

task_run()
{
local retval=126
local func="$1"

if test -n "$task_list"; then
    echo "$task_list" | tr ' ' '\n' | grep -q "^$func\$" ||
        return 0
fi

$func && retval=0 || retval="$?"
test $retval = 0 || global_retval=1

return $retval
}

task()
{
local task="$1"

case "$cmd" in
    list) task_show "$task"
        ;;
    run) task_run "$task" && echo "[DONE]: $task" || echo "[FAIL]: $task"
        ;;
    *) fatal "Unrecognized command: $cmd"
        ;;
esac
}

is_gigabyte()
{
/usr/sbin/dmidecode -s baseboard-manufacturer | grep -q "^Gigabyte Technology"
```

```
}

is_std_def_kernel_running()
{
uname -r | grep -q '^[[:digit:]]\+\.[[:digit:]]\+\.[[:digit:]]\+-std-def-'
}

task is_gigabyte
task is_std_def_kernel_running

exit "$global_retval"
```

58.3.3.4.2. Файл .backend

Содержимое файла **/usr/share/alterator/backends/diag-example.backend**:

```
[Alterator Entry]
Type = Backend
Module = executor
Name = diag_example
Interface = diag1

[Info]
execute = cat /usr/share/alterator/diagnostictools/diag-example.diag
stdout_bytes = enabled
stdout_byte_limit = 200000
action_id = Info

[Run]
execute = diag-example {param}
stdout_signal_name = diag_example_stdout_signal
stderr_signal_name = diag_example_stderr_signal
thread_limit = 1
action_id = Run

[List]
execute = diag-example -l
stdout_strings = enabled
stdout_strings_limit = 200000
action_id = List
```

58.3.3.4.3. Файл .diag, описывающий тесты

Содержимое файла **/usr/share/alterator/diagnostictools/diag-example.diag**:

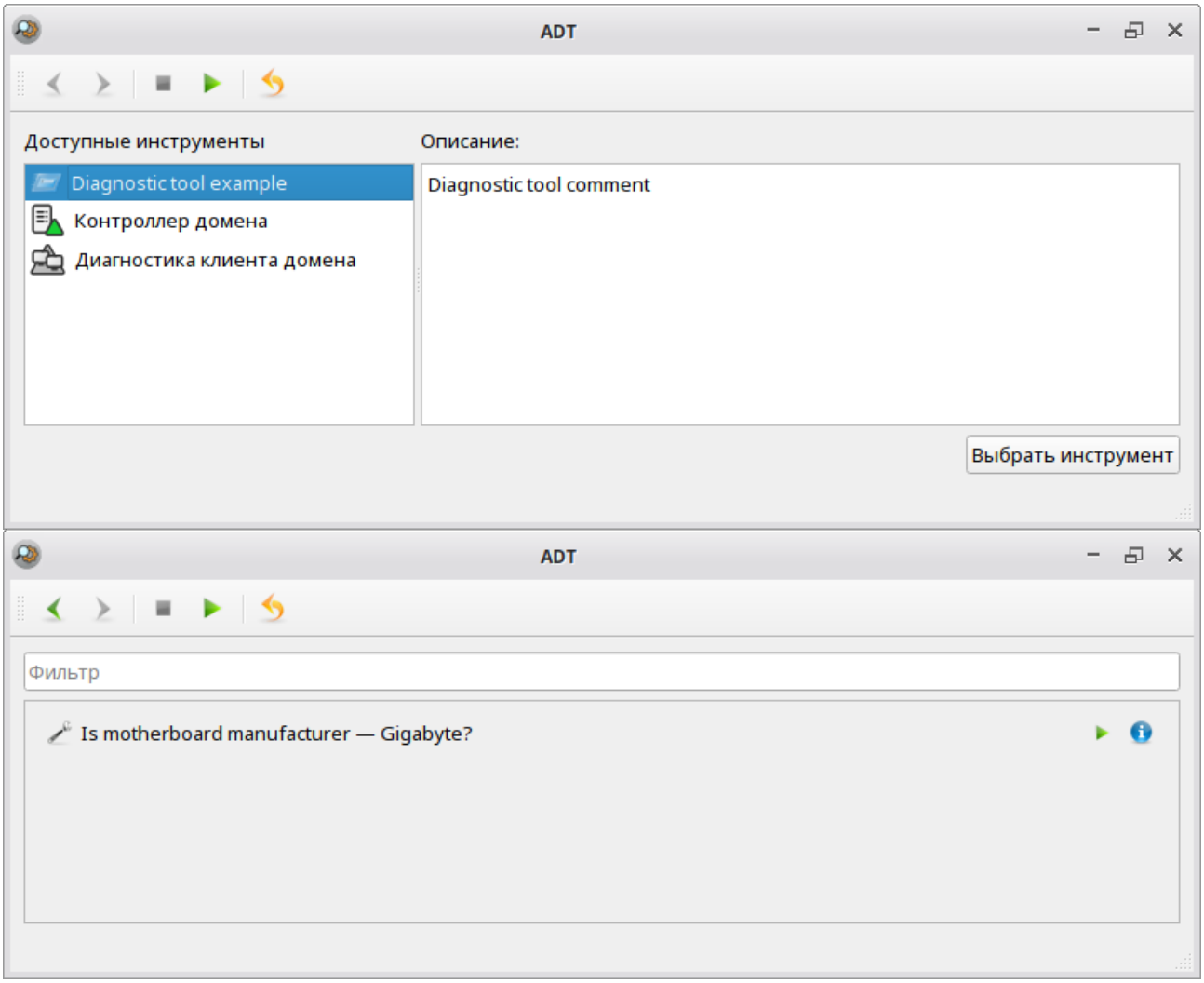
```
[Alterator Entry]
Type = diag
Name = Example
DisplayName = Diagnostic tool example
DisplayName[ru] = Пример инструмента диагностики
Comment = Diagnostic tool comment
Comment[ru] = Комментарий к диагностическому инструменту
Icon = system-run

[is_gigabyte]
DisplayName = Is motherboard manufacturer — Gigabyte?
DisplayName[ru] = Производитель материнской платы — Gigabyte?
```

58.3.3.4.4. Отображение диагностического инструмента в интерфейсе ADT

Примечание

Для того чтобы новый диагностический инструмент отображался интерфейсе ADT, необходимо перезапустить alterator-manager:

```
# systemctl restart alterator-manager.service
```

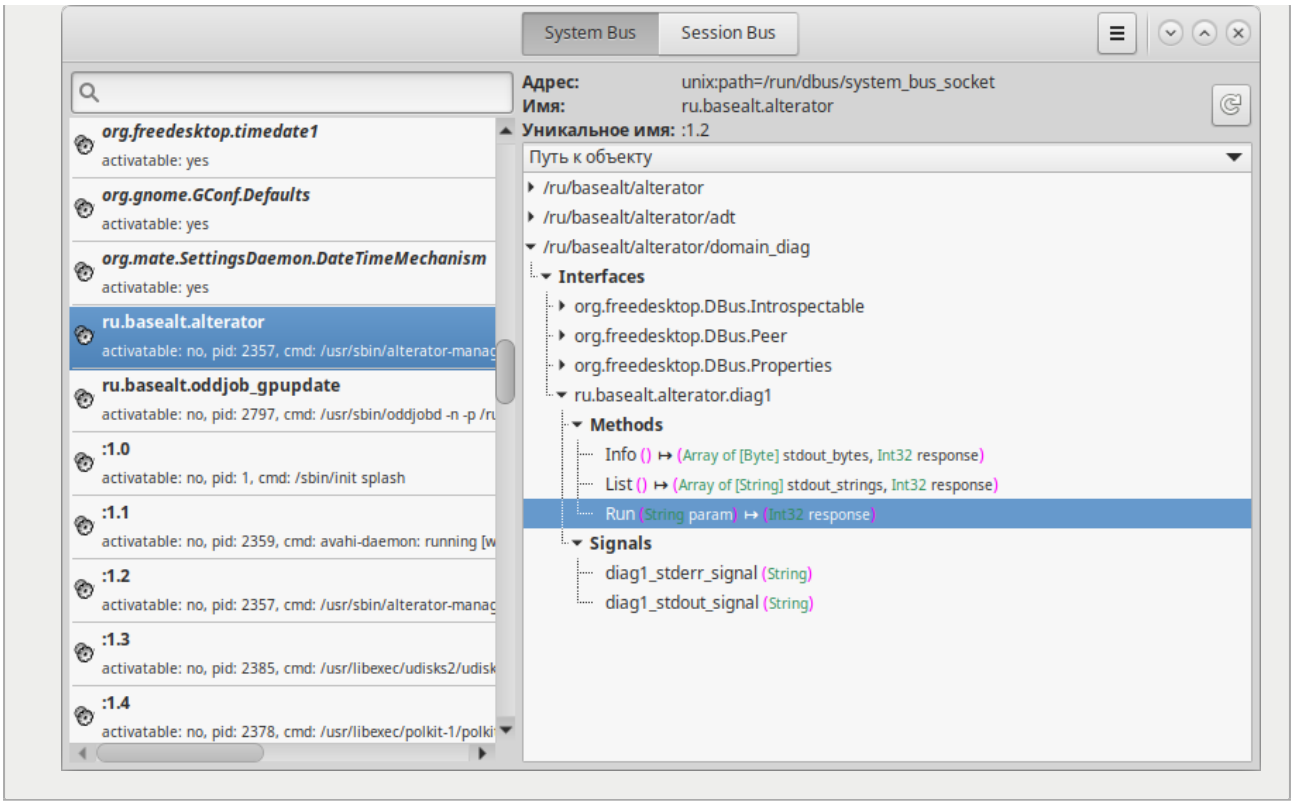


58.3.4. Ошибки и нестандартные случаи

Если диагностический инструмент не отображается, необходимо проверить объект alterator-manager с именем *ru.basealt.alterator* на системной шине D-Bus:

Примечание

Для этого можно использовать утилиту D-Feet (пакет *d-feet*):



Часть IX. Примечания

Содержание

59. Настройка беспарольного доступа по ssh

60. Центр управления системой

Глава 59. Настройка беспарольного доступа по ssh

Генерация SSH-ключа (на DC1):

```
# ssh-keygen -t ed25519
```

На вопрос о файле для сохранения ключа нажать **Enter** (по умолчанию). На вопрос о пароле к ключу также нажать **Enter** (не указывать пароль).

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для пользователя user:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@dc2.test.alt
```

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для администратора. Для этого подключаемся к DC2 и под root копируем публичную часть ключа:

```
# ssh user@dc2.test.alt
[user@dc2 ~]$ su -
Password:
[root@dc2 ~]# cat /home/user/.ssh/authorized_keys >>.ssh/authorized_keys
[root@dc2 ~]# exit
```

```
выход
[user@dc2 ~]$ exit
выход
Connection to dc2 closed.
```

Теперь есть возможность удалённо выполнять команды на DC2 с привилегиями администратора.

Глава 60. Центр управления системой

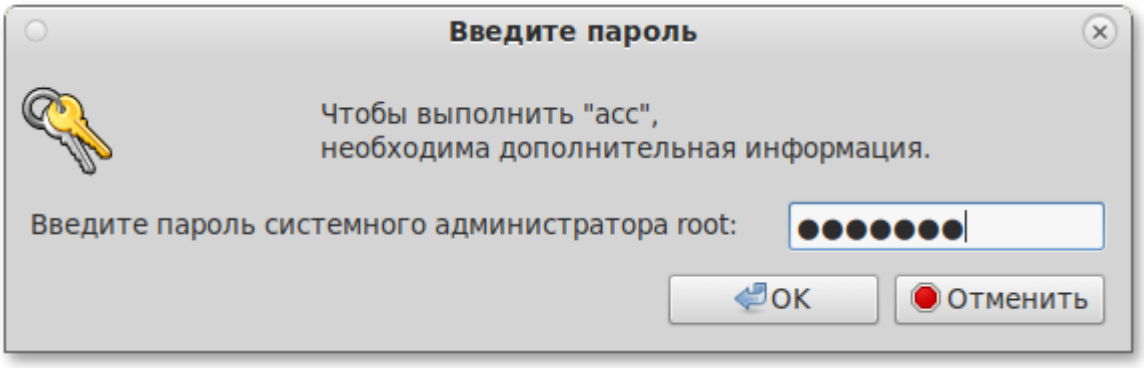
Центр управления системой (ЦУС, альтератор) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

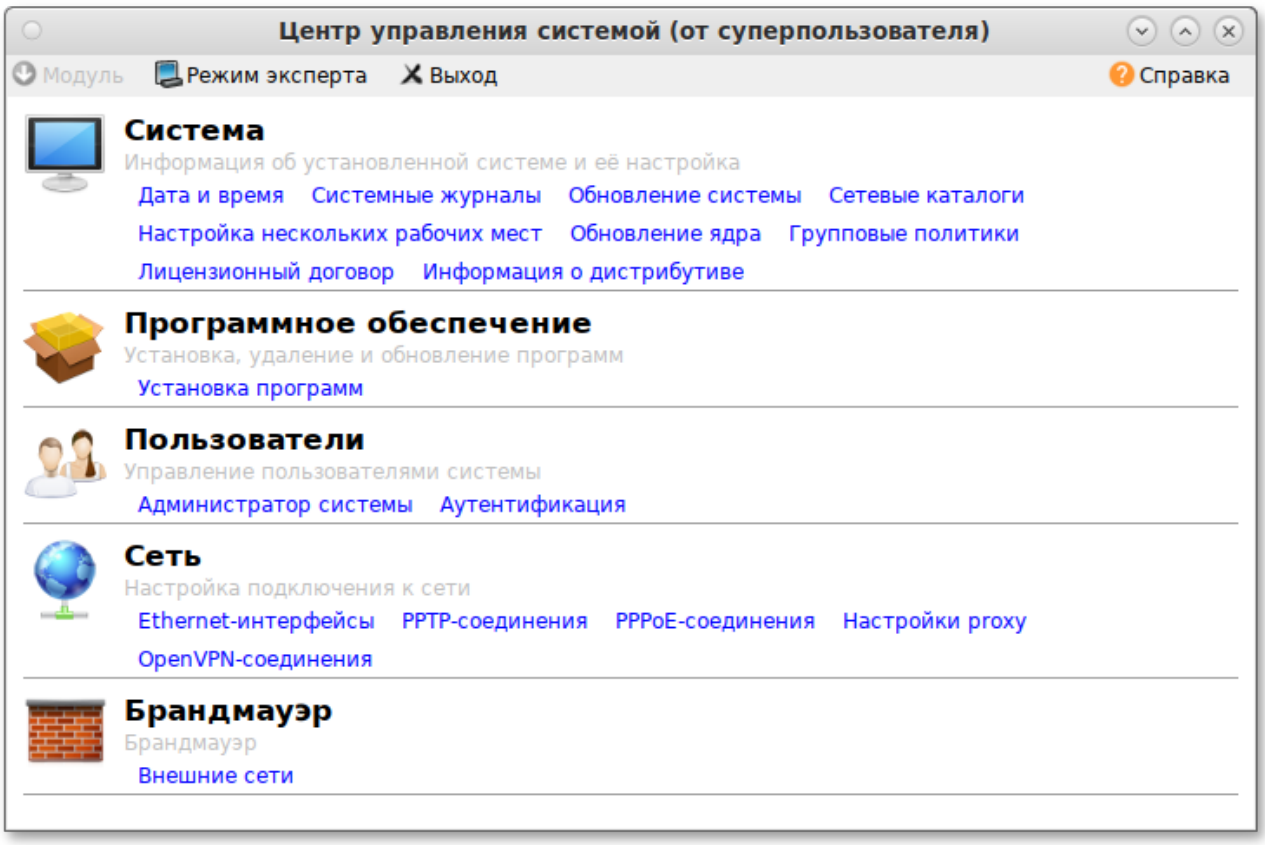
ЦУС состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

Запустить ЦУС в графической среде можно следующими способами:

- в графической среде MATE: **Система** → **Администрирование** → **Центр управления системой**;
- в графической среде XFCE, KDE: **Меню запуска приложений** → **Настройки** → **Центр управления системой**;
- из командной строки: командой **`acc`**.

Запуск ЦУС требует административных прав, и если запустить его от обычного пользователя, он запросит пароль администратора системы (root):





ЦУС имеет также веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет *alterator-fbi*:

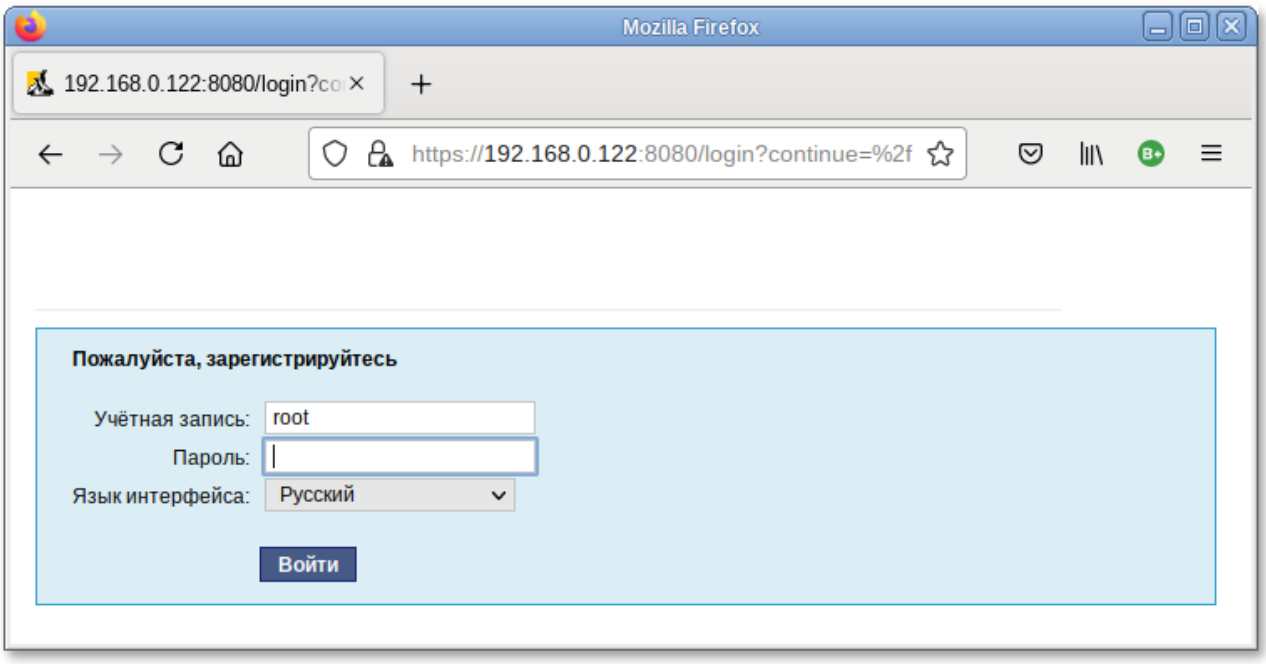
```
# apt-get install alterator-fbi
```

И запущены сервисы **ahttpd** и **alteratord**:

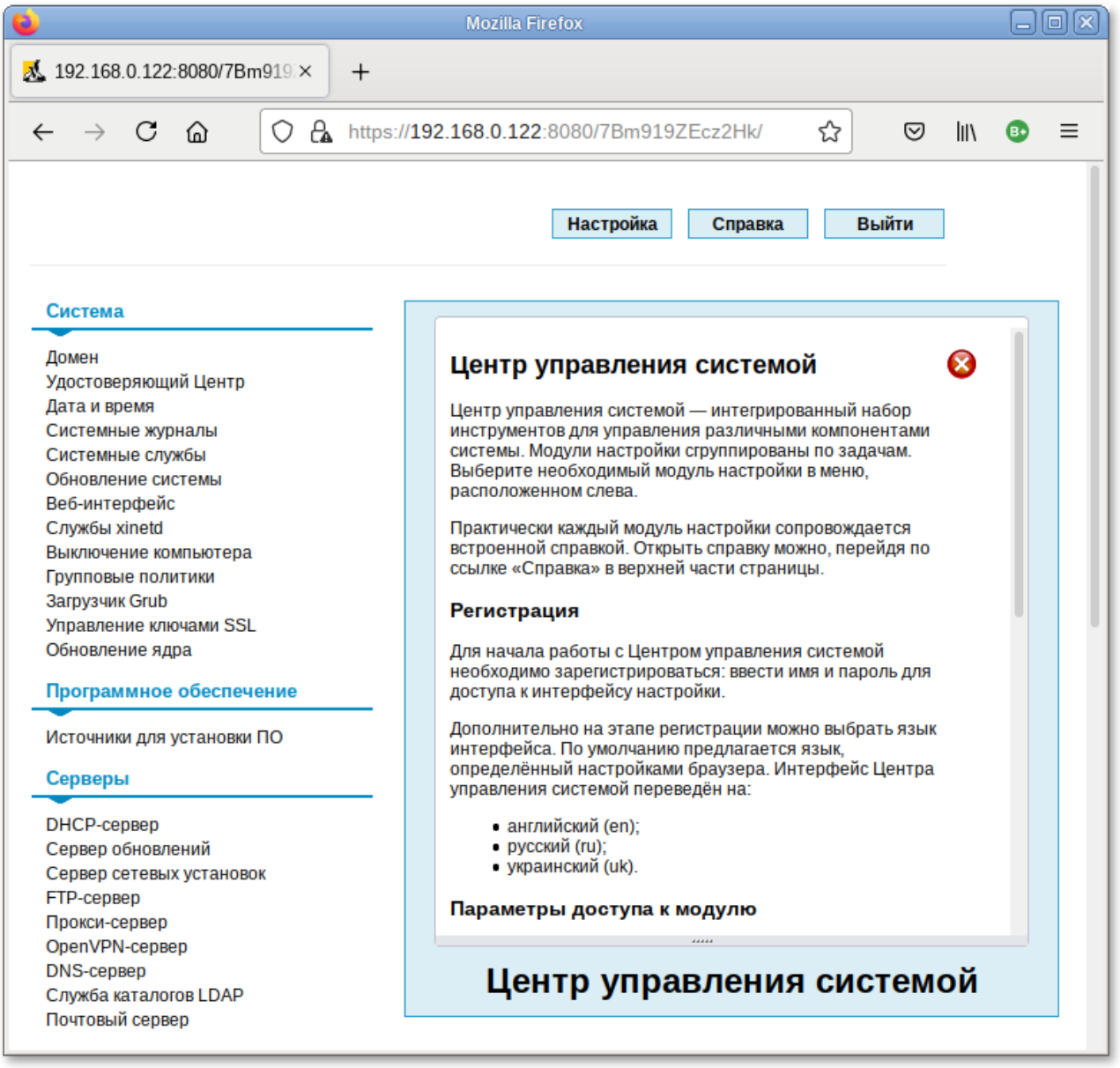
```
# systemctl enable --now ahttpd
# systemctl enable --now alteratord
```

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы необходимо перейти по адресу **https://ip-адрес:8080/**.

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (**root**) и пароль пользователя:



После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс.



Установленные пакеты, которые относятся к ЦУС, можно посмотреть, выполнив команду:

```
$ rpm -qa | grep alterator*
```

Прочие пакеты для ЦУС можно найти, выполнив команду:

```
$ apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
# apt-get remove alterator-net-openvpn
```