

УТВЕРЖДЕН

ЛКНВ.11102-01 89 01-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ 8 СП
(ОС Альт 8 СП)

Руководство администратора

Альт домен

ЛКНВ.11102-01 89 01

Листов 671

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ содержит сведения о построении доменной инфраструктуры на базе Альт домен программного изделия (ПИ) «Операционная система Альт 8 СП» ЛКНВ.11102-01, сокращенное наименование – ОС Альт 8 СП, для процессоров VLIW архитектуры **Эльбрус**.

Далее в документе будет использоваться альтернативное наименование ПИ: ОС Альт СП.

Версия документа: 1.0.

Документ предназначен для администратора ОС Альт СП и содержит общие сведения о структуре, настройке и работе Альт домена ОС Альт СП, компонентах доменной инфраструктуры.

СОДЕРЖАНИЕ

1. Основные сведения о логической модели «Альт Домен»	10
2. Разворачивание домена.....	12
2.1. Подготовка системы к установке сервера «Альт Домен».....	12
2.1.1. Системные требования к серверу (контроллеру домена)	12
2.1.2. Синхронизация времени.....	14
2.1.3. Требования к портам.....	15
2.1.4. Создание первого контроллера домена	16
2.2. Присоединение к домену в роли контроллера домена.....	36
2.2.1. Заведение дополнительного DC с бэкендом SAMBA_INTERNAL.....	38
2.2.2. Заведение дополнительного DC с бэкендом BIND9_DLZ.....	40
2.2.3. Проверка результатов присоединения	42
2.2.4. Настройка NTP-сервера.....	43
2.3. Контроллер домена на чтение (RODC).....	43
2.3.1. Установка и настройка RODC	44
2.3.2. Политики репликации и кеширования паролей на RODC.....	46
2.3.3. Проверка репликации пароля пользователя на сервере RODC.....	48
2.4. Редактирование существующего домена.....	49
2.4.1. Повышение уровня схемы, функционального уровня домена.....	49
2.4.2. Включение RFC2307 после разворачивания домена.....	51
2.4.3. Изменение DNS бэкенда контроллера домена Active Directory.....	52
2.5. Отладочная информация	54
2.5.1. Настройка уровня журналирования Samba	54
2.5.2. Управление процессами	54
2.5.3. DNS	55
2.6. Удаление контроллера домена.....	56
2.6.1. Понижение роли онлайн-контроллера домена.....	56
2.6.2. Понижение автономного контроллера домена	58
2.6.3. Проверка.....	60

3. Клиенты «Альт Домена»	63
3.1. SSSD vs Winbind.....	63
3.2. Подготовка системы к вводу в домен	67
3.2.1. Установка пакетов.....	67
3.2.2. Синхронизация времени.....	68
3.2.3. Настройка DNS	68
3.3. Присоединение к домену в роли участника	71
3.3.1. Параметры команды system-auth	71
3.3.2. Подключение к домену с помощью SSSD.....	72
3.3.3. Подключение к домену с использованием Winbind.....	75
3.3.4. Вход пользователя.....	78
3.4. Отладочная информация	80
3.4.1. Настройка уровня журналирования Samba	80
3.4.2. Ошибка при подключении к IP-адресу 127.0.0.1	80
3.4.3. getent не показывает доменных пользователей и группы.....	80
3.5. Удаление клиента домена.....	81
3.6. Повторная регистрация клиента	82
3.7. Настройка аутентификации доменных пользователей на DC	83
3.7.1. Winbind.....	84
3.7.2. SSSD	86
3.7.3. Генерация keytab-файла.....	89
3.7.4. Службы.....	89
3.7.5. Настройка ролей	89
3.7.6. Групповые политики.....	90
3.7.7. Настройка SSH.....	90
3.8. Настройка обновления паролей аккаунтов машин	90
3.8.1. Локальная политика смены пароля	91
3.8.2. Включение обновления пароля.....	92
3.8.3. Отключение обновления пароля.....	93
3.8.4. Диагностика	94

3.8.5. Восстановление работоспособности	95
4. Инструменты управления объектами домена и групповыми политиками	97
4.1. Групповые политики.....	97
4.2. Установка административных шаблонов и административных инструментов	100
4.2.1. Установка административных шаблонов	100
4.2.2. Административные инструменты	101
4.2.3. Установка RSAT	103
4.2.4. Windows 10 (1809 и более поздние версии)	106
4.2.5. Windows Vista и 7	107
4.3. Включение механизма применения конфигурации на клиентских машинах.....	109
4.4. Модуль клиентской машины для применения конфигурации	112
4.4.1. Утилиты модуля	114
4.4.2. Локальная политика	119
4.4.3. Ключи реестра	121
4.4.4. Модули клиентской стороны (Applier)	125
4.4.5. Периодичность запуска групповых политик.....	127
4.5. Модуль удаленного управления базой данных конфигурации (ADMC) ...	129
4.5.1. Запуск ADCMC	130
4.5.2. Интерфейс ADCMC	130
4.5.3. Свойства объектов.....	137
4.5.4. Выбор контейнера	147
4.5.5. Управление пользователями	148
4.5.6. Управление контактами.....	155
4.5.7. Управление группами	157
4.5.8. Управление компьютерами	162
4.5.9. Управление подразделениями	163
4.5.10. Управление объектами парольных настроек	166
4.5.11. Управление общими папками	170

4.5.12. Управление объектами групповых политик.....	171
4.5.13. Добавление/Удаление UPN суффиксов	188
4.5.14. Роли FSMO.....	190
4.5.15. Выбор объектов	193
4.5.16. Поиск объектов.....	195
4.5.17. Использование сохраненных результатов поиска	200
4.6. Модуль редактирования настроек клиентской конфигурации (GPUI)	204
4.6.1. Запуск GPUI для редактирования доменных политик	205
4.6.2. Выбор набора шаблонов групповых политик	207
4.6.3. Интерфейс	208
4.6.4. Редактирование групповых политик.....	224
4.6.5. Редактирование предпочтений	342
4.6.6. Управление logon-скриптами.....	387
4.7. Расширение возможностей ГП	394
4.7.1. Схема административных шаблонов ADMX	394
4.7.2. Связывание информации из ADMX и ADML-файлов.....	412
4.7.3. Рекомендации для создания ADMX-файлов.....	414
4.7.4. Разработка новой политики	416
4.8. Решение проблем.....	435
4.8.1. Область действия и статус групповой политики	435
4.8.2. Наследование групповых политик	437
4.8.3. Порядок применения групповых политик.....	439
4.8.4. Замыкание групповой политики.....	441
4.8.5. Диагностика применения ГП на стороне клиента	443
4.8.6. Коды ошибок	444
4.8.7. Диагностика проблем при работе с политикой скриптов	447
5. Доверительные отношения (Трасты)	449
5.1. Настройка доверия	449
5.1.1. Общие сведения.....	449
5.1.2. Особенности доверительных отношений в Samba	450

5.2. Настройка DNS	452
5.2.1. Два домена Samba	452
5.2.2. Samba DC и Windows Server с AD	455
5.3. Создание двухстороннего транзитивного подключения	458
5.3.1. Два домена Samba	458
5.3.2. Samba DC и Windows Server с AD	461
5.4. Управление пользователями и группами.....	472
5.4.1. Список пользователей и групп	472
5.4.2. Тестирование аутентификации	474
5.4.3. Просмотр доверия в Windows	475
5.5. Использование трастов на LINUX-клиентах.....	477
5.5.1. Настройка winbind.....	477
5.5.2. Настройка SSSD	478
5.6. Удаление доверия.....	479
5.6.1. На стороне Samba.....	479
5.6.2. На стороне Windows Server с AD	479
6. Администрирование домена	482
6.1. Управление пользователями и группами.....	482
6.1.1. В ADMC	482
6.1.2. Подкоманда user и group утилиты samba-tool	482
6.2. Администрирование DNS.....	501
6.2.1. DNS-записи при вводе машины в домен	501
6.2.2. Подкоманда dns утилиты samba-tool.....	502
6.2.3. Утилита nsupdate	508
6.2.4. Оснастка DNS в RSAT	513
6.2.5. Динамическое обновление DNS-записей	521
6.2.6. Обновление IP-адресов вручную.....	529
6.3. Администрирование сайтов и подсетей.....	530
6.4. Управление парольными политиками.....	533
6.4.1. Глобальные парольные политики.....	533

6.4.2. Объекты настроек паролей (PSO).....	536
6.5. Резервное копирование и восстановление домена	539
6.5.1. Резервное копирование и восстановление из резервной копии	539
6.5.2. Восстановление произвольного контроллера домена после фатального сбоя.....	555
6.6. Роли FSMO.....	557
6.6.1. Семь ролей FSMO	558
6.6.2. Просмотр и передача ролей FSMO.....	562
6.7. Репликация.....	565
6.7.1. Настройка репликации.....	565
6.7.2. Проверка статуса репликации.....	566
6.7.3. Двухнаправленная репликация SysVol	571
6.8. Настройка Samba для привязки к определенным интерфейсам.....	578
6.9. Создание keytab-файла.....	578
6.9.1. Назначение и формат SPN.....	578
6.9.2. Создание SPN и генерация keytab с помощью samba-tool.....	580
6.10. Аутентификация других сервисов в домене	582
6.10.1. Настройка аутентификации Kerberos для веб-сервера Apache	582
6.10.2. Настройка аутентификации Kerberos для веб-сервера Nginx.....	585
6.10.3. Настройка веб-браузеров для SSO	588
6.11. Distributed File System.....	591
6.11.1. Пространство DFS-имен.....	591
6.11.2. Настройка DFS на сервере Samba.....	593
6.12. Настройка SSSD	595
6.12.1. Журналирование SSSD.....	595
6.12.2. Настройки SSSD в ЦУС.....	599
6.12.3. Включение автономной аутентификации.....	603
6.13. Монтирование общих ресурсов samba.....	604
6.13.1. Подключение с использованием gio	604
6.13.2. Подключение с использованием pam_mount	605

6.13.3. Подключение с использованием Autofs.....	606
6.14. Журналирование в Samba.....	609
6.14.1. Настройка бэкендов	609
6.14.2. Настройка файлов журнала.....	610
6.14.3. Уровни журналирования	611
6.14.4. Настройка ведения журнала аудита	614
6.14.5. Интерпретация журналов аудита JSON	619
6.15. Усиление безопасности DC	629
6.15.1. Возможность анонимного получения списка пользователей, групп	629
6.15.2. Отключение Netbios	630
6.15.3. Отключение роли сервера печати.....	630
6.15.4. Отключение NTLMv1	630
6.15.5. Генерация дополнительных хешей паролей	631
6.15.6. Защита DNS-записей wpad и isatap	631
6.15.7. Ограничение диапазона динамических портов.....	631
6.15.8. Аудит запросов к каталогам SYSVOL и NetLogon.....	632
6.15.9. Отправка логов аудита в rsyslog	632
6.16. Инструменты командной строки	633
6.16.1. Команда samba-tool	634
6.16.2. Команда wbinfo.....	636
6.16.3. Команда net	645
6.16.4. Команда adcli	646
6.16.5. Утилита ldapsearch	648
6.16.6. Команда sssctl	657
6.16.7. Команда testparm	659
6.17. Конфигурационные файлы.....	660
6.17.1. Файл sssd.conf.....	660
6.17.2. Файл resolv.conf.....	661
Перечень сокращений	670

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 определенные 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: 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.

Группы – 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 СП 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.

2. РАЗВОРАЧИВАНИЕ ДОМЕНА

Параметры домена:

- имя домена – test.alt;
- контроллер домена (ОС Альт СП Сервер) – dc1.test.alt (192.168.0.132);
- дополнительный контроллер (ОС Альт СП Сервер) – dc2.test.alt (192.168.0.133);
- контроллер только для чтения (ОС Альт СП Сервер) – rodc.test.alt (192.168.0.134);
- рабочая станция 1 (ОС Альт СП) – host-01.test.alt (192.168.0.135);
- рабочая станция 2 (ОС Альт СП) – host-02.test.alt (192.168.0.125);
- рабочая станция 3 (ОС Windows) – PK1.test.alt (192.168.0.109);
- имя пользователя-администратора – Administrator;
- пароль администратора – Pa\$\$word.

2.1. Подготовка системы к установке сервера «Альт Домен»

В этом подразделе перечислены требования для установки сервера (контроллера домена). Перед установкой необходимо убедиться, что система соответствует этим требованиям.

Примечание. Для установки сервера «Альт Домен» нужны привилегии суперпользователя.

Примечание. В условиях реальной эксплуатации рекомендуется использовать два или более DC для обеспечения отказоустойчивости.

2.1.1. Системные требования к серверу (контроллеру домена)

2.1.1.1. RAM

Для демонстрационной/тестовой системы рекомендуется 2 Гбайт ОЗУ.

Для производственной установки рекомендуется не менее 4 Гбайт ОЗУ, а затем 2 Гбайт на каждую дополнительную 1000 пользователей.

Примечание. Параметр, который оказывает наибольшее влияние на требования к памяти, – это количество одновременных открытых сеансов.

2.1.1.2. Размеры хранилища

10 Гбайт 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.

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

2.1.1.4. 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 DC должно состоять минимум из двух компонентов, разделенных 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 параметром sAMAccountName в Active Directory).

2.1.2. 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 рис. 1 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.

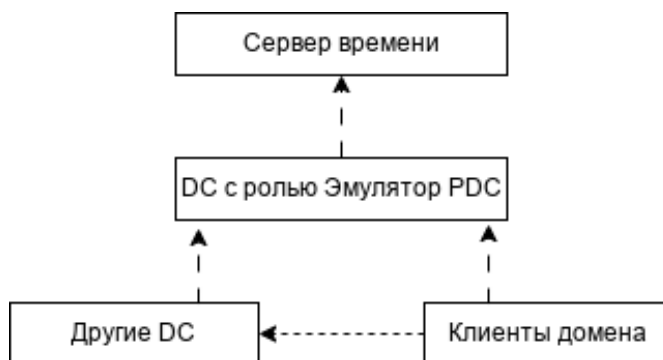


Рис. 1 – Схема синхронизации времени в домене

2.1.3. Требования к портам

Для корректной работы службы Samba на контроллере домена должны быть открыты порты, указанные в таблице 1.

Т а б л и ц а 1 – Порты, используемые контроллером домена AD

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
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 и контроллеров домена с операциями контроллера 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 <code>kadmin</code> для установки и смены пароля Kerberos
LDAPS	636	TCP	Если в файле <code>smb.conf</code> установлен параметр <code>tls enabled = yes</code> (по умолчанию)
Global Catalog	3268	TCP	Для глобального каталога от клиента к контроллеру домена
Global Catalog SSL	3269	TCP	Если в файле <code>smb.conf</code> установлен параметр <code>tls enabled = yes</code> (по умолчанию)

Окончание таблицы 1

Служба	Порт	Протокол	Примечание
Dynamic RPC Ports	49152-65535	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 <code>rpc server port</code> в файле <code>smb.conf</code> . Подробности смотрите в описании параметра на справочной странице <code>man smb.conf</code>

2.1.4. Создание первого контроллера домена

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

1) SAMBA_INTERNAL – встроенный сервер имен:

- используется по умолчанию при подготовке нового домена, присоединении к существующему домену или переносе домена NT4 в AD;
- прост в настройке и не требует дополнительного ПО или знаний о DNS;
- следует использовать для простых настроек DNS.

2) 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 Bind_DLZ использует кеш Bind для рекурсивных запросов. Запросы на сам домен каждый раз передаются модулю DLZ, кеша на этом уровне у него нет.

ВАЖНО

Бэкенд DNS BIND9_FLATFILE не поддерживается.

2.1.4.1. Параметры команды разворачивания домена

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

Ниже описаны некоторые опции (таблица 2). Для получения более подробной информации следует обратиться к man странице `samba-tool(8)`.

Т а б л и ц а 2 – Основные опции для `samba-tool domain provision`

Опция	Описание
<code>-d DEBUGLEVEL,</code> <code>--debuglevel=DEBUGLEVEL</code>	Включить отладку
<code>--interactive</code>	Запрашивать ввод данных у пользователя (интерактивное создание домена)
<code>--domain=DOMAIN</code>	Имя домена NetBIOS (имя рабочей группы)
<code>--domain-guid=GUID</code>	Установить <code>domainguid</code> (иначе используется случайное значение)
<code>--domain-sid=SID</code>	Установить <code>domainsid</code> (иначе используется случайное значение)
<code>--ntds-guid=GUID</code>	Установить GUID объекта NTDS (иначе используется случайное значение)
<code>--host-name=HOSTNAME</code>	Установить имя хоста
<code>--host-ip=IPADDRESS</code>	Установить IPv4 IP-адрес
<code>--host-ip6=IP6ADDRESS</code>	Установить IPv6 IP-адрес
<code>--adminpass=PASSWORD</code>	Пароль основного администратора домена (иначе используется случайное значение)
<code>--krbtgtpass=PASSWORD</code>	Пароль <code>krbtgt</code> (иначе используется случайное значение)
<code>--dns-backend=NAME_SERVER_BACKEND</code>	Бэкенд DNS-сервера: <code>SAMBA_INTERNAL</code> – встроенный сервер имен (по умолчанию), <code>BIND9_FLATFILE</code> – использует текстовую базу данных <code>bind9</code> для хранения информации о зоне, <code>BIND9_DLZ</code> – использует Samba AD для хранения информации о зоне, <code>NONE</code> – полностью пропускает настройку DNS (не рекомендуется)
<code>--dnspass=PASSWORD</code>	Пароль <code>dns</code> (иначе используется случайное значение)
<code>--server-role=ROLE</code>	Позволяет указать тип серверной роли: <code>domain controller</code> , <code>dc</code> (по умолчанию), <code>member server</code> , <code>member</code> или <code>standalone</code>
<code>--function-level=FOR_FUNCTION_LEVEL</code>	Позволяет указать уровень домена и леса: 2000, 2003, 2008, 2008_R2 (по умолчанию) или 2016
<code>--base-schema=BASE_SCHEMA</code>	Версия базовой схемы домена (по умолчанию 2019)
<code>--use-rfc2307</code>	Позволяет поддерживать расширенные атрибуты типа UID и GID в схеме LDAP и ACL на файловой системе Linux
<code>--machinepass=PASSWORD</code>	Пароль для машины (иначе используется случайное значение)
<code>--plaintext-secrets</code>	Сохранять конфиденциальные данные в виде обычного текста на диске (по умолчанию конфиденциальные данные шифруются)
<code>--realm=REALM</code>	Задаёт область Kerberos (LDAP), и DNS имя домена
<code>--option=OPTION</code>	Позволяет установить параметры <code>smb.conf</code> из командной строки
<code>-s FILE, --configfile=FILE</code>	Позволяет указать файл конфигурации

2.1.4.2. Установка пакетов

Установить пакет task-samba-dc для Samba DC на базе Heimdal Kerberos:

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

Примечание. Этот шаг можно пропустить, если при установке ОС на этапе «Установка системы» был выбран профиль «Альт Домен (контроллер домена)» (рис. 2).

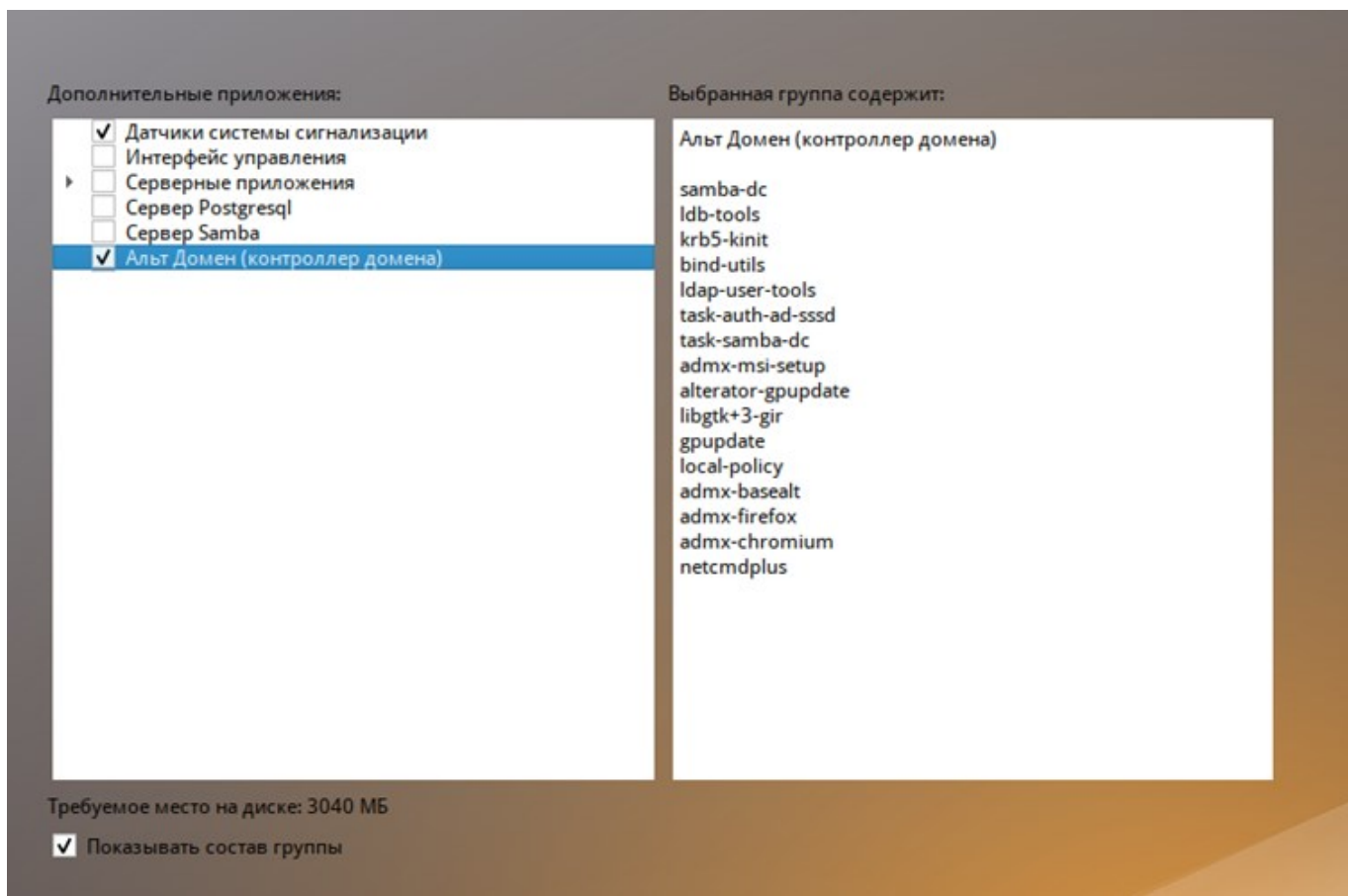


Рис. 2 – Выбор профиля «Альт Домен (контроллер домена)» при установке ОС

Так как Samba в режиме контроллера домена 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
```

Выключить автозагрузку служб и отключить службы можно также в ЦУС в разделе «Система» → «Системные службы» (см. документ «Руководство администратора. ЛКНВ.11102-01 90 01»).

2.1.4.3. Внутренний DNS-сервер Samba (SAMBA_INTERNAL)

Контроллер домена предоставляет внутренний DNS-сервер, который поддерживает основные функции, необходимые для домена. 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-сервер 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);
- нет зоны-заглушки (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` в файле `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 произойдет 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.

2.1.4.3.1. Установка имени контроллера домена

Для сервера должно быть 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 dcl.test.alt
# domainname test.alt
```

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

2.1.4.3.2. 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
```

Иначе в конец этого файла следует добавить строку:

```
name_servers=127.0.0.1
```

и перезапустить сервис resolvconf:

```
# resolvconf -u
```

2.1.4.3.3. Восстановление к начальному состоянию Samba

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

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

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

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

2.1.4.3.4. Разворачивание домена

2.1.4.3.4.1. 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 клавишу <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 трех групп из четырех 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 с 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

```

Запустить службу samba и добавить ее в автозагрузку:

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

Примечание. Если служба samba 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

```

Далее следует перейти к подразделу п. 2.1.4.5 «Настройка Kerberos».

2.1.4.3.4.2. В пакетном режиме

Для пакетной установки необходимо как минимум указать следующие параметры домена:

- 1) `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;
- 2) `--domain=DOMAIN` – имя домена (имя рабочей группы);
- 3) `--adminpass=PASSWORD` – пароль основного администратора домена;
- 4) `--option="dns forwarder=forwarder_ip_address"` – внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;
- 5) `--server-role=ROLE` – тип серверной роли;
- 6) `--dns-backend=NAME_SERVER_BACKEND` – тип серверной роли;
- 7) `--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 трех групп из четырех 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 с ошибкой.

Примечание. В таблице 2 описаны некоторые опции команды `samba-tool domain provision`. Полный список параметров можно увидеть, запустив команду:

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

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

```
# mkdir -p /var/lib/samba/sysvol
```

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. п. 2.4.1).

Далее следует запустить службу samba и добавить ее в автозагрузку:

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

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

Далее следует перейти к разделу «Настройка Kerberos».

2.1.4.3.4.3. Создание домена в ЦУС

При инициализации домена в веб-интерфейсе ЦУС следует в модуле «Домен» указать «Имя домена», отметить пункт «Active Directory», указать IP-адреса внешних DNS-серверов, задать пароль администратора домена и нажать кнопку «Применить» (рис. 3).

Имя домена:

Примечание: имя домена должно соответствовать [RFC 1035](#):

- Имя домена должно состоять из одного или нескольких компонентов, разделённых точками.
- Компоненты имени домена должны начинаться со строчной или прописной латинской буквы, заканчиваться на латинскую букву или цифру, содержать латинские буквы, цифры и символ «-».
- Компонент имени домена не должен превышать 63 символов.
- Имя домена не должно содержать компоненты «localhost», «localdomain» и «local», которые зарезервированы для служебных целей.
- Рекомендуется указывать домен как минимум из двух компонентов, разделённых точками.

Примеры: domain.loc, school-33.domain, department.company

Тип домена: ☐ ALT-домен
(домен, основанный на OpenLDAP и MIT Kerberos. Рекомендуется для аутентификации рабочих станций под управлением ALT Linux)
Этот тип невозможно использовать, поскольку не установлен пакет **alt-domain-server**.

☒ Active Directory
(домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением Windows и Linux)

Дополнительные параметры:

DNS-серверы: (адреса IP внешних серверов DNS)

Пароль администратора: (пароль администратора домена)

Повторите пароль: (повторите фразу)

Текущее состояние:

Служба: %(_ NOT OK (samba service is stopped))

Имя домена: --

Realm: --

Имя DC: --

Сервер LDAP: --

Сервер KDC: --

☐ FreeIPA
(домен для контроллера домена FreeIPA. Рекомендуется для аутентификации рабочих станций под управлением Linux)
Этот тип невозможно использовать, поскольку не установлен пакет **freeipa-server, freeipa-server-dns**.

☐ Только DNS
(обслуживание только запросов DNS)

Внимание: изменение имени домена вступит в силу только после перезагрузки компьютера

☐ Восстановить файл конфигурации по умолчанию (krb5.conf).

Рис. 3 – Окно модуля «Домен»

Примечание. Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских

букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов, не полностью соответствующий требованиям, – это одна из причин завершения развертывания домена с ошибкой.

После успешного создания домена, будет выведена информация о домене (рис. 4).

Перезагрузить сервер для применения изменений.

Active Directory
(домен для контроллера домена Samba AD. Рекомендуется для аутентификации рабочих станций под управлением Windows и Linux)

Дополнительные параметры:

DNS-серверы: 8.8.8.8 (адреса IP внешних серверов DNS)

Пароль администратора: (пароль администратора домена)

Повторите пароль: (повторите фразу)

Текущее состояние:

Служба: OK
Имя домена: test.alt
Realm: TESTALT
Имя DC: dc1.test.alt
Сервер LDAP: dc1.test.alt (192.168.0.132)
Сервер KDC: 192.168.0.132

Рис. 4 – Информационное окно «Текущее состояние»

2.1.4.4. 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 больше одного сервера форвардинга (параметр `dns forwarder` на бэкенде INTERNAL работает только с одним адресом).

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

2.1.4.4.1. Настройка DNS-сервера BIND

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

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

Примечание. Во избежание появления ошибки при запуске bind:

```
мая 03 14:25:13 dc1 named[3825]: samba_dlz: Failed to configure
zone 'test.alt'
мая 03 14:25:13 dc1 named[3825]: loading configuration: already
exists
мая 03 14:25:13 dc1 named[3825]: exiting (due to fatal error)
мая 03 14:39:44 dc1 named[4309]: Loading 'AD DNS Zone' using
driver dlopen
```

не следует, при установке системы, задавать полное имя для DC (dc1.test.alt).

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, связанные с DNS:

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

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.

В таблице 3 описаны некоторые параметры конфигурационного файла /etc/bind/options.conf. Для получения более подробной информации следует обратиться к map странице named.conf(5).

Т а б л и ц а 3 – Основные параметры конфигурационного файла
/etc/bind/options.conf

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)
max-cache-ttl	Указывает максимальное время (в секундах), в течение которого сервер кеширует обычные (положительные) ответы. Максимальный срок кеша по умолчанию – 04800 (одна неделя)
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
recursion	Определяет нужно ли выполнять рекурсивные запросы, если просит клиент, NO – не выполнять. Если ответ найден в кеше, то возвращается из кеша
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; - master – указывает работать в качестве мастер сервера для текущей зоны; - slave – указывает работать в качестве подчиненного сервера для текущей зоны

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 нем подсети, из которых разрешено подавать запросы;

- раскомментировать параметр allow-recursion и указать в нем 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; 192.168.0.152; };
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
```

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

2.1.4.4.2. Восстановление к начальному состоянию Samba

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

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

 **Перед созданием домена необходимо обязательно удалить**
`/etc/samba/smb.conf:`
`# rm -f /etc/samba/smb.conf`

2.1.4.4.3. Разворачивание домена

2.1.4.4.3.1. 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 трех групп из четырех 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 с 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
 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

2.1.4.4.3.2. В пакетном режиме

Для пакетной установки необходимо указать следующие параметры:

- 1) --realm REALM_NAME – имя области Kerberos (LDAP), и DNS имя домена;
- 2) --domain=DOMAIN – имя домена (имя рабочей группы);
- 3) --adminpass=PASSWORD – пароль основного администратора домена;
- 4) --server-role=ROLE – тип серверной роли;
- 5) --dns-backend=NAME_SERVER_BACKEND – бэкенд DNS-сервера;
- 6) --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 трех групп из четырех 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.

Примечание. В таблице 2 описаны некоторые опции команды `samba-tool domain provision`. Полный список параметров можно увидеть, запустив команду:

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

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. п. 2.4.1).

2.1.4.4.4. 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
```

2.1.4.4.5. 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.
```

2.1.4.5. Настройка Kerberos

Внести изменения в файл `/etc/krb5.conf`. Следует раскомментировать строку `default_realm` и содержимое разделов `realms` и `domain_realm`, и указать название домена (обратите 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
```

2.1.4.6. Настройка NTP-сервера

Настройка сервера времени `chrony` в качестве NTP-сервера:

- установить пакет `chrony`:

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

- включить доступ к серверу `chrony`:

```
# control chrony server
```

- 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
```

- включить и запустить службу по умолчанию:

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

- убедиться в нормальной работе NTP-сервера:

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

Примечание. Параметр `iburst` используется для ускорения начальной синхронизации.

2.1.4.7. 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 4.19.7)
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:

1) проверка наличия `nameserver 127.0.0.1` в `/etc/resolv.conf`
(для `SAMBA_INTERNAL`):

```
# 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
```

2) проверка имен 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 41 days on Ср 03 июл 2024  
11:18:36
```

Просмотр полученного билета:

```
# klist  
  
Ticket cache: FILE:/tmp/krb5cc_0  
Default principal: administrator@TEST.ALT  
  
Valid starting      Expires            Service principal  
22.05.2024 11:28:23 22.05.2024 21:28:23 krbtgt/TEST.ALT@TEST.ALT  
renew until 29.05.2024 11:28:20
```

2.2. Присоединение к домену в роли контроллера домена

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

Системные требования к дополнительному DC такие же, как и для первого контроллера домена (см. п. 2.1.1).

Примечание. В терминологии контроллеров домена нет понятия PDC/BDC, т. е. все контроллеры равны, но один из них выступает владельцем ролей FSMO.

Заведение дополнительного контроллера домена выполняется путем 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`:

- 1) `--realm REALM_NAME` – имя области Kerberos (LDAP), и DNS имя домена;
- 2) `--dns-backend=NAME_SERVER_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"
```

- 3) `--option='idmap_ldb:use rfc2307 = yes'` – если первый контроллер домена создавался с ключом `--rfc2307`, то и для текущего необходимо это учесть, указав данный параметр;
- 4) `--site=SITE` – привязка контроллера домена к определенному сайту AD;
- 5) `--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;
- 6) `--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.

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.

2.2.1. Заведение дополнительного DC с бэкендом SAMBA_INTERNAL

Все действия 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 SAMBA_INTERNAL:

1) установить пакет `task-samba-dc`, который установит все необходимое:

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

2) обязательно добавить в `/etc/resolv.conf` 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 удален):

```
# 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 дополнительного DC (команда выполняется на узле dc1.test.alt):

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

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

- 6) на добавляемом DC 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) для проверки настройки запросить билет Kerberos для администратора домена:

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

⚠ 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
22.05.2024        13:35:08        22.05.2024      23:35:08
krbtgt/TEST.ALT@TEST.ALT
renew until 29.05.2024 13:35:05
```

- 9) ввести дополнительный DC в домен test.alt в качестве контроллера домена:

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

При успешном завершении будет выведена информация о присоединении к домену:

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

10) сделать службу samba запускаемой по умолчанию и запустить ее:

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

2.2.2. Заведение дополнительного DC с бэкендом BIND9_DLZ

Все действия 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» п. 2.1.4.4.1);

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 удален):

```
# 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 дополнительного DC (команда выполняется на узле dc1.test.alt):

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

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

- 7) на добавляемом DC 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) для проверки настройки запросить билет Kerberos для администратора домена:

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

⚠ Имя домена должно быть указано в верхнем регистре.

- 9) убедиться, что билет получен:

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

Valid starting      Expires            Service principal
22.05.2024 13:35:08 22.05.2024 23:35:08 krbtgt/TEST.ALT@TEST.ALT
renew until 29.05.2024 13:35:05
```

- 10) ввести дополнительный DC в домен test.alt в качестве контроллера домена:

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

При успешном завершении будет выведена информация о присоединении к домену:

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

11) сделать службы samba и bind запускаемыми по умолчанию и запустить их:

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

2.2.3. 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 (в списке адресов должен отображаться IP-адрес добавленного контроллера домена):

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

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

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

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. п. 6.7.

3) на добавляемом 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
```

2.2.4. Настройка NTP-сервера

Настроить NTP для работы в режиме сервер (см. п. 2.1.4.6).

2.3. Контроллер домена на чтение (RODC)

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

Основная цель контроллера домена, доступного только на чтение (RODC – read-only domain controller) – 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 леса и домена должен соответствовать 2008R2. Это можно проверить, выполнив следующую команду на контроллере домена:

```
# 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.

2.3.1. Установка и настройка RODC

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

Все дальнейшие действия выполняются на узле rodс.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 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 удален):

```
# 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:

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

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

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:
```

⚠ 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
22.05.2024          14:06:04          23.05.2024          00:06:04
krbtgt/TEST.ALT@TEST.ALT
renew until 23.05.2024 14:06:01
```

8) 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
```

Если все 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.

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

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

9) сделать службу samba запускаемой по умолчанию и запустить ее:

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

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

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

2.3.2. 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:

- 1) «Allowed RODC Password Replication Group»;
- 2) «Denied RODC Password Replication Group».

Первая группа по умолчанию пуста, а во второй содержатся административные группы безопасности, пароли пользователей которых нельзя реплицировать и кэшировать на RODC. В группу «Denied RODC Password Replication Group» по умолчанию входят группы (рис. 5):

- «Cert Publishers»;
- «Domain Admins»;
- «Domain Controllers»;
- «Enterprise Admins»;

- «Group Policy Creator Owners»;
- «Read-only Domain Controllers»;
- «Schema Admins»;
- учетная запись «krbtgt».

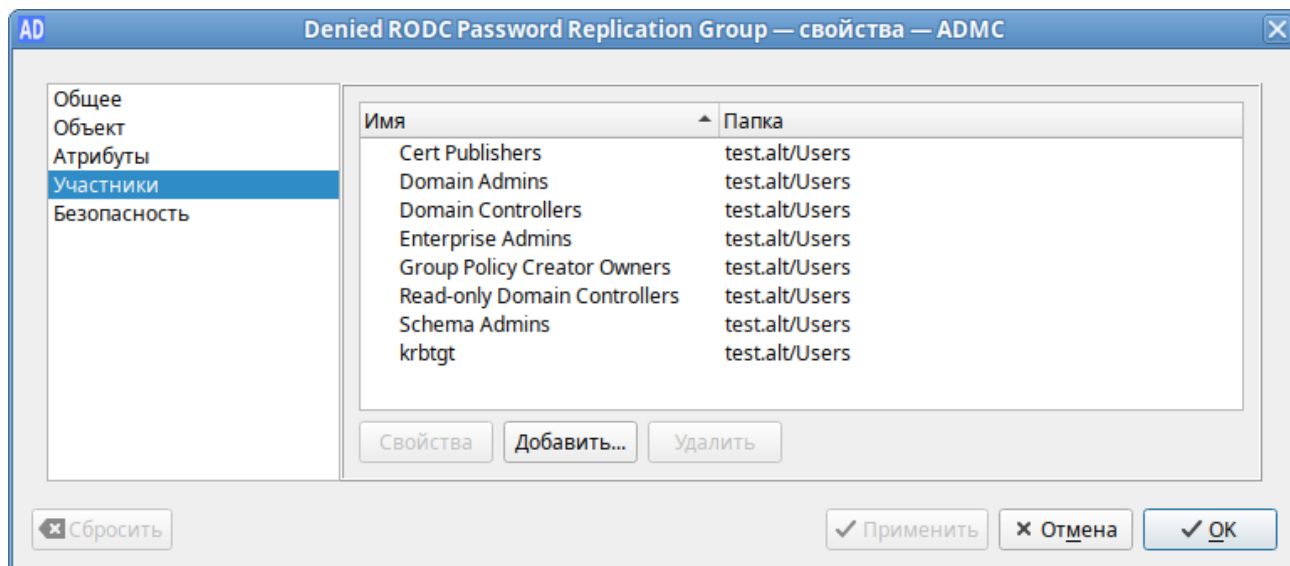


Рис. 5 – Список участников «Denied RODC Password Replication Group» в ADCM

Список участников группы «Denied RODC Password Replication Group» можно получить, выполнив команду:

```
# 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
```

Список участников группы «Allowed RODC Password Replication Group» можно получить, выполнив команду:

```
# 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).

2.3.3. 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 create ivanov --given-name='Иван' \
--surname='Иванов' --mail-address='ivanov@test.alt'
```

```
New Password:
```

```
Retype Password:
```

```
User 'ivanov' added successfully
```

```
# samba-tool user setexpiry ivanov --noexpiry
# 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
```

2.4. Редактирование существующего домена

2.4.1. 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 домена, 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 каталогов:

```
# 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
```

2.4.2. Включение RFC2307 после разворачивания домена

Примечание. До запуска этой процедуры следует убедиться, что она необходима.

Проверка того, что расширения NIS установлены в домене:

```
# 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.



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 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 действия 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
```

Samba реплицирует обновленную схему на все контроллеры домена в лесу.

2.4.3. Изменение DNS бэкенда контроллера домена Active Directory

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

2.4.3.1. 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.п. 2.1.4.4.1);

2) остановить службу samba:

```
# systemctl stop samba
```

3) выполнить миграцию:

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

4) отключить модуль SAMBA_INTERNAL в файле 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 ее запускаемой по умолчанию:

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

6) запустить службу samba:

```
# systemctl start samba
```

2.4.3.2. 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 ее 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 `INTERNAL DNS` – это одна из настроек по умолчанию для параметра `server services`, удаление параметра `server services` включает все серверы по умолчанию, включая `DNS-сервер`.

2.5. Отладочная информация

2.5.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в п. 6.14.3.

2.5.2. 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. п. 6.14.3);
- можно запустить Samba в интерактивном режиме и посмотреть на результат:

```
# samba -i
```

2.5.3. DNS

2.5.3.1. Устранение неполадок, связанных с серверной частью DNS

2.5.3.1.1. 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 ее автоматический запуск во время загрузки;
- перезапустить Samba.

2.5.3.1.2. Samba с BIND9_DLZ

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

- при создании контроллера домена использовался параметр `--dns-backend=BIND9_DLZ`;

- при подключении к домену использовался параметр `--dns-backend=BIND9_DLZ`;
- домен был обновлен до Bind9 с помощью команды `samba_upgradedns` и опции `--dns-backend=BIND9_DLZ`.

2.6. Удаление контроллера домена

В некоторых ситуациях необходимо навсегда удалить контроллер домена из домена. Если для обычного участника домена достаточно просто удалить соответствующую учетную 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 таймаутов и неудачных попыток репликации;
- вход в систему доменных пользователей может завершиться ошибкой или занять больше времени.

2.6.1. Понижение роли онлайн-контроллера домена

Если удаляемый контроллер домена все еще 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;

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 samba:

```
# 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 DNS.

2.6.2. 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 домену, и его нельзя понизить так, как описано в п. 2.6.1. Это гарантирует, что все изменения, такие как изменения пароля, 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:
Settings,CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=alt
```

```
CN=NTDS
```

```

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;

3) убедиться, что понижаемый контроллер домена отключен;

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 удаленного 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 DNS.

ВАЖНО

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

2.6.3. Проверка

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

На машине, введенной в домен, запустить модуль удаленного управления базой данных конфигурации (ADMC) (подробнее см. п. 4.5). Выбрать запись Domain Controllers и убедиться, что пониженный контроллер домена был удален (рис. 6).

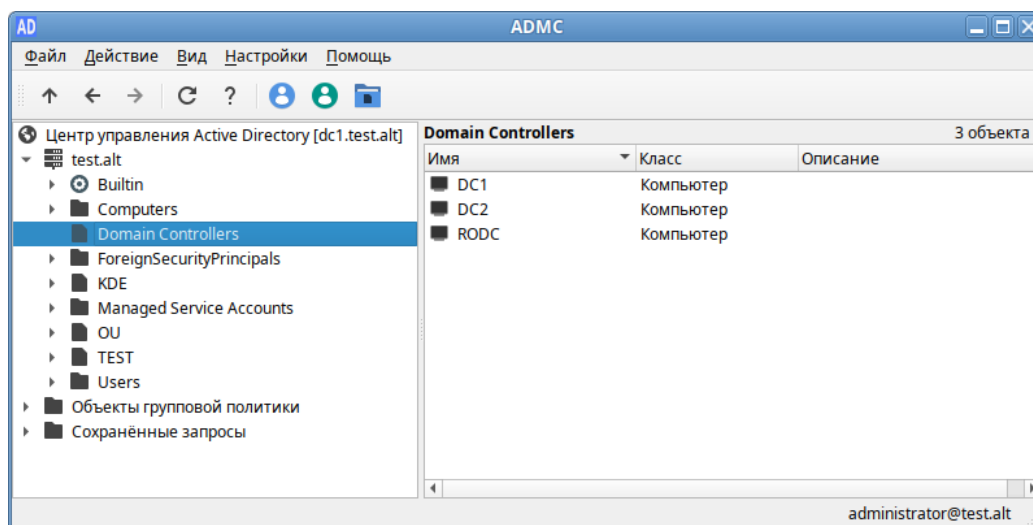


Рис. 6 –ADMC. Просмотр списка контроллеров домена

Проверить, что контроллер домена был понижен, можно также в RSAT (см. п. 4.2.3). Для этого на машине Windows введенной в домен:

- 1) открыть приложение «Active Directory – пользователи и компьютеры», перейти к записи «Контроллеры домена» и убедиться, что пониженный контроллер домена был удален (рис. 7).

Если запись все еще присутствует в списке, ее можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить»;

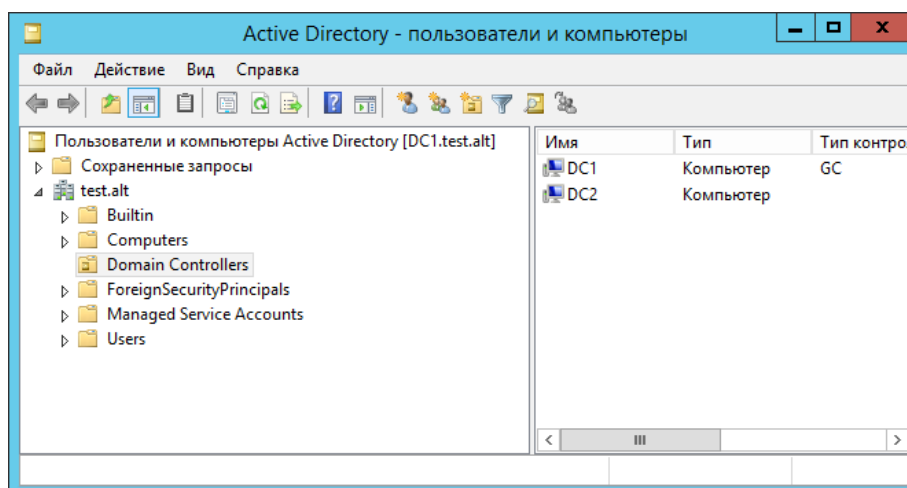


Рис. 7 – Окно приложения «Active Directory – пользователи и компьютеры»

- 2) открыть приложение «Active Directory – сайты и службы», и убедиться, что контроллер домена с пониженным статусом больше не указан ни в одной записи сайта Active Directory (рис. 8).

Если запись все еще присутствует в списке, ее можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить»;

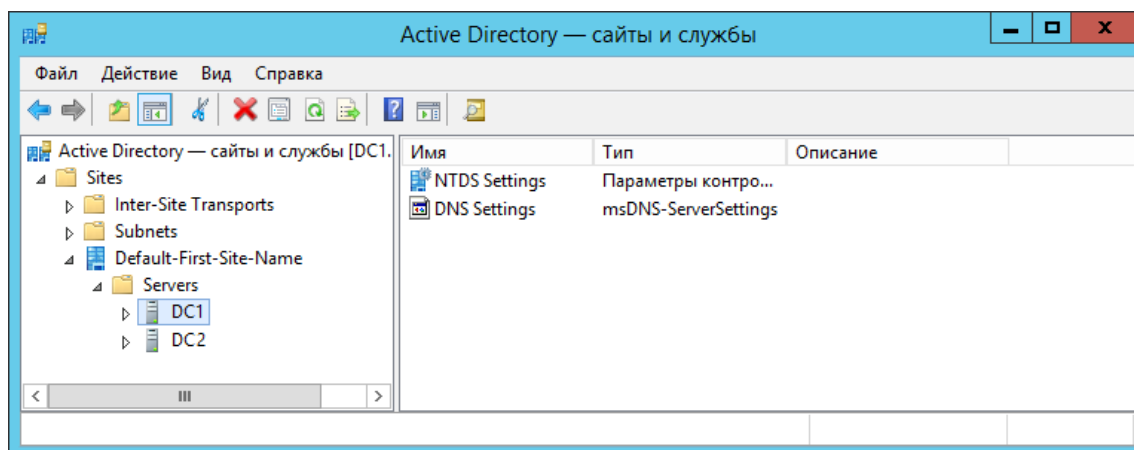


Рис. 8 – Окно приложения «Active Directory – сайты и службы»

- 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 (рис. 9).

Если записи все еще присутствуют в списке, их можно удалить вручную, выбрав в контекстном меню записи пункт «Удалить».

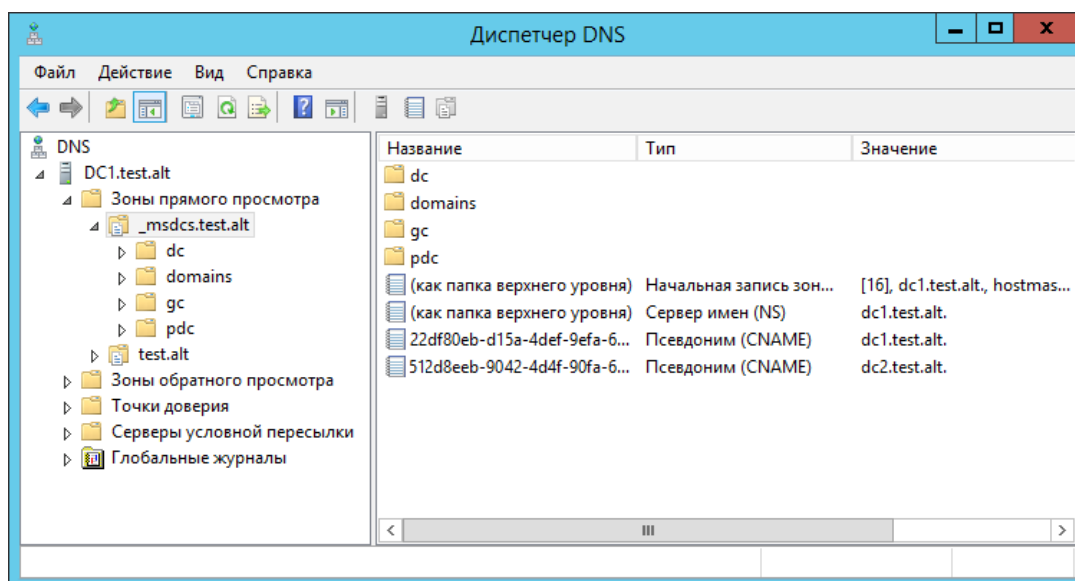


Рис. 9 – Окно «Диспетчер DNS»

3. КЛИЕНТЫ «АЛЬТ ДОМЕНА»

Клиентами «Альт Домена» 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

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

3.1. SSSD vs Winbind

Существует несколько способов включения операционных систем на базе ядра Linux в «Альт Домен». В этом разделе описаны функции и возможности двух вариантов интеграции: решение на основе Samba Winbind и решение на базе SSSD.

Машины под управлением ОС «Альт» рекомендуется вводить в «Альт Домен» с помощью SSSD, но есть несколько исключений:

- 1) если в сети уже развернуты системы Linux, которые уже используют Samba Winbind для целей интеграции;
- 2) если используется AD с включенным протоколом NTLM (так как SSSD не поддерживает протокол NTLM);
- 3) если SSSD не поддерживает определенную функцию, которую поддерживает Winbind (например, SSSD не поддерживает доверительные отношения между лесами при прямом подключении к «Альт Домен»).

Ниже рассмотрены преимущества и недостатки интеграции на основе Samba Winbind (рис. 10) и на базе SSSD (рис. 11).

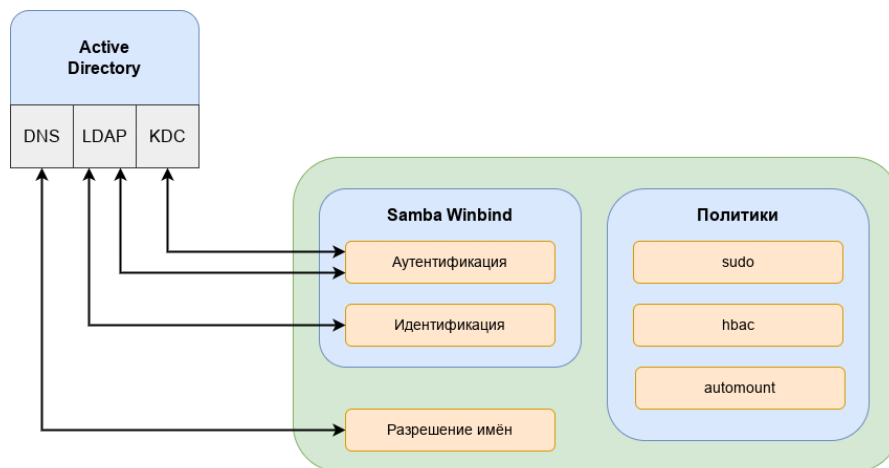


Рис. 10 – Схема интеграции на основе Samba Winbind

Преимущества варианта интеграции с использованием Samba Winbind:

- Samba Winbind эмулирует клиент Windows в системе Linux и использует преимущества собственных протоколов Windows и расширений протокола LDAP;
- Winbind понимает концепцию доменов и лесов, а также работает с доверием между доменами и лесами;
- Winbind может обнаруживать серверы, используя DNS;
- Winbind может переключиться на другой сервер, если контроллер домена AD становится недоступным;
- Winbind может динамически выполнять сопоставление идентификаторов на основе идентификаторов объектов «Альт Домен» (SID) или использовать атрибуты POSIX, хранящиеся в «Альт Домен» (если эти расширения были загружены);
- Winbind хорошо интегрируется с клиентом Samba FS и CIFS;
- безопасность соединения основана на идентификации клиентской системы и ключах Kerberos, выданных этой системе.

Ограничения Samba Winbind:

- политики не управляются централизованно и должны распространяться вне группы;
- может подключаться только к «Альт Домен».

SSSD – это группа служб, которые являются частью ядра операционной системы Linux и работают вместе для обеспечения аутентификации, поиска удостоверений и возможностей управления доступом для системы Linux. SSSD может взаимодействовать с «Альт Домен», FreeIPA, MS AD или любыми другими стандартными реализациями сервера LDAP и/или Kerberos (рис. 11, рис. 12).

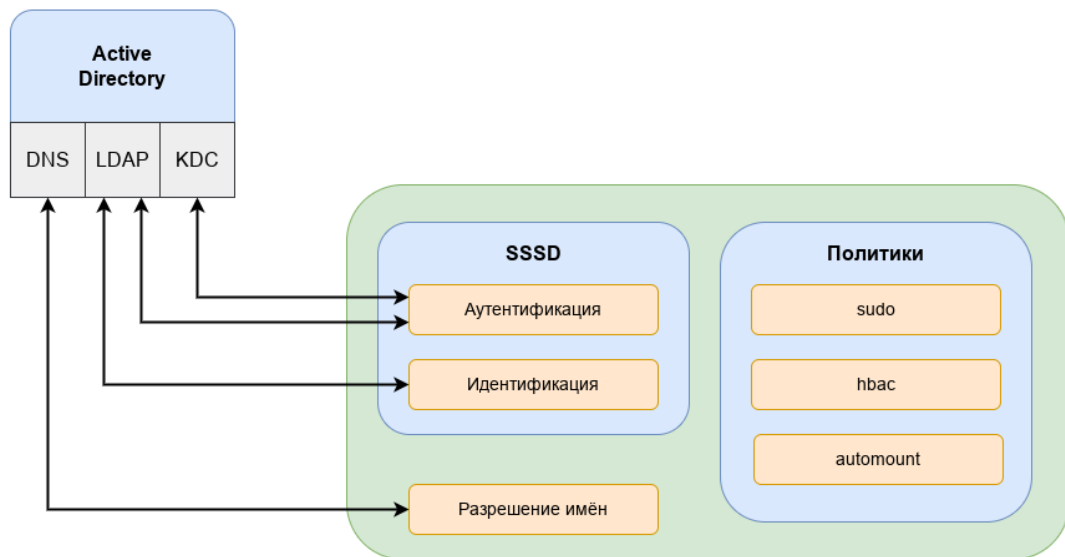


Рис. 11 – Схема интеграции на базе SSSD

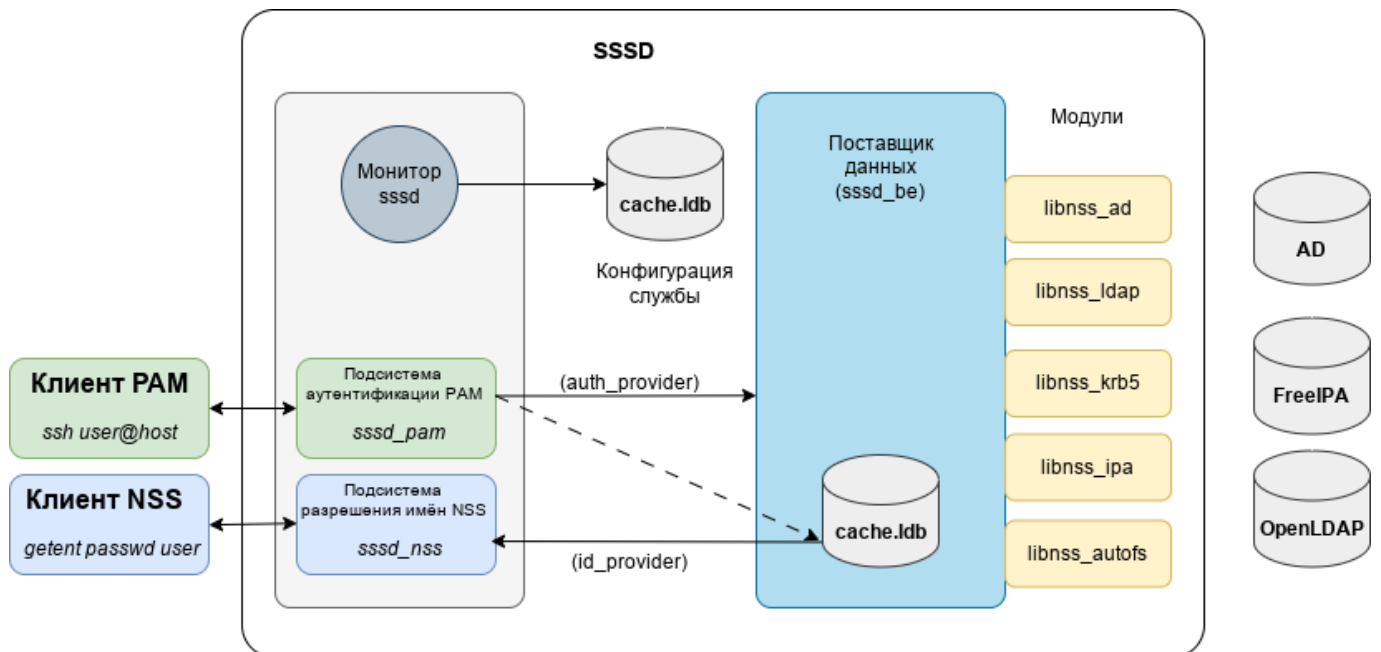


Рис. 12 – Схема интеграции конфигураций на базе SSSD

Единственным серьезным ограничением для интеграции с использованием SSSD является поддержка (старого) протокола NTLM. SSSD не реализует этот протокол, потому что по современным стандартам NTLM больше не является безопасным для развертывания. Наилучшей практикой является отказ от использования NTLM.

Преимущества SSSD (рис. 12):

- возможность загрузки и применения политик управления доступом на основе хоста с использованием объектов групповой политики, управляемых в «Альт Домен»;
- может взаимодействовать с разными источниками идентификации, а не только с «Альт Домен»;
- поддерживает очистку DNS (т. е. обнаруживает, были ли удалены или обновлены записи DNS для серверов);
- предоставляет расширенные интерфейсы идентификации на локальной шине сообщений (D-Bus). Этот интерфейс можно использовать для лучшей интеграции приложений, работающих в ОС Linux, с корпоративными источниками идентификации, такими как AD и FreeIPA.

Сравнение Winbind и SSSD представлено в таблице 4.

Т а б л и ц а 4 – Сравнение Winbind и SSSD

Категория	Описание	Winbind	SSSD
Аутентификация	Проверка подлинности с использованием Kerberos	Да	Да
	Проверка подлинности LDAP	Да	Да
	Поддержка нескольких доменов AD	Да	Да
	Поддержка лесов AD	Да	Да
	Поддержка гетерогенных сетей AD/FreeIPA	Нет	Да
Безопасность	Простота настройки безопасной конфигурации	Нет	Да
	Система имеет идентификатор и ее ключ используется для защиты доступа к центральному серверу	Да	Да
	Поддержка NTLM	Да	Нет
Поиск и сопоставление идентификаторов	Динамическое сопоставление идентификаторов AD SID	Да	Да
	Использование преимуществ конкретных расширений и протоколов AD	Да	Да

Окончание таблицы 4

Категория	Описание	Winbind	SSSD
DNS	Обновление и очистка DNS AD	Нет	Да
	Поддержка сайтов AD DNS	Да	Да
Обмен файлами	Интеграция с Samba FS	Да	Да
	Интеграция с клиентом CIFS	Да	Да
Служба печати	Сервер печати CUPS с использованием Kerberos	Да	Да
Политики	Централизованное управление контролем доступа на основе хоста через GPO	Нет	Да
Интеграция с другими сервисами и приложениями	Интеграция с основными утилитами, такими как SSH, sudo, automount	Нет	Да
	Расширенные интерфейсы идентификации по локальной шине сообщений D-Bus	Нет	Да
	Специальные функции для приложений (Docker, Cockpit, GSS Proxy и др.)	Нет	Да

3.2. Подготовка системы к вводу в домен

3.2.1. Установка пакетов

Установить пакет task-auth-ad-sssd:

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

Примечание. Этот шаг можно пропустить, если при установке ОС на этапе «Установка системы» был выбран профиль «Клиент Альт Домен» (рис. 13).

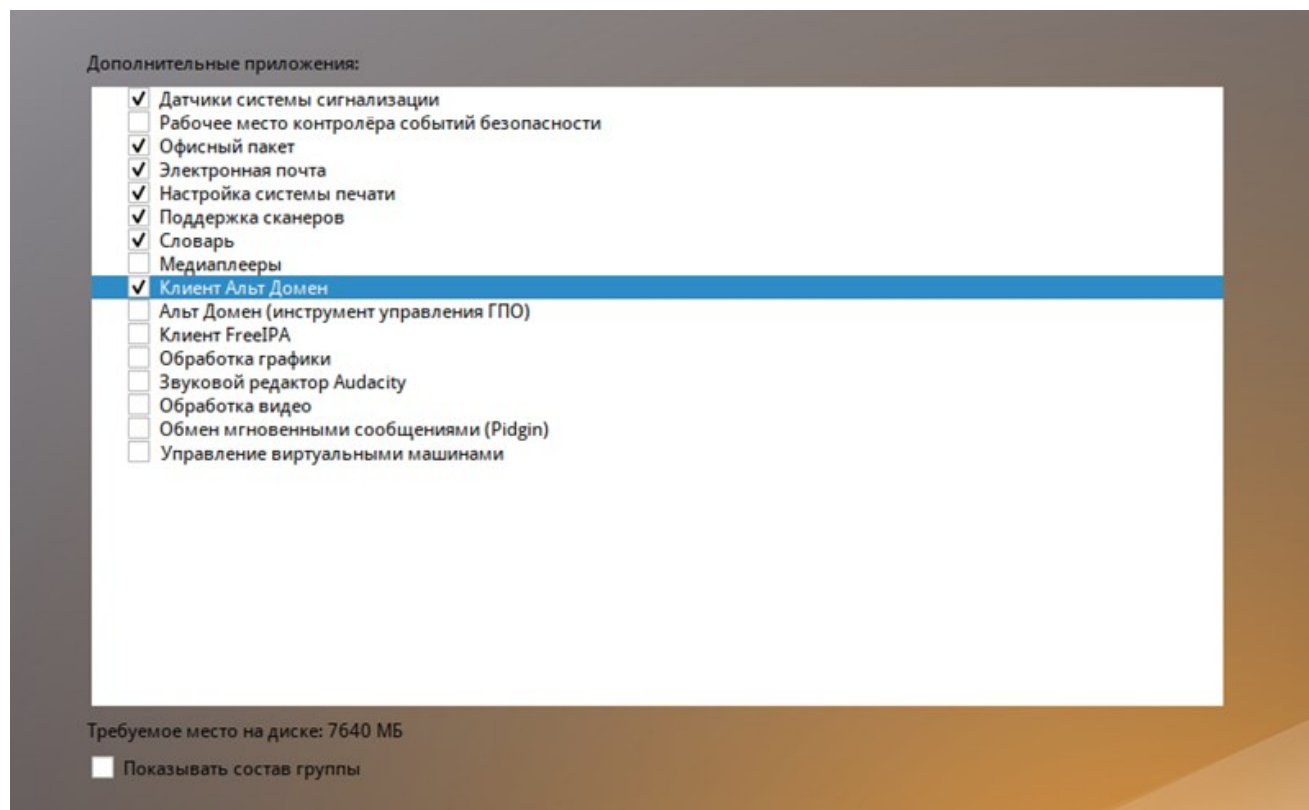


Рис. 13 – Выбор профиля «Клиент Альт Домен» при установке ОС

3.2.2. Синхронизация времени

Синхронизация времени с контроллером домена производится автоматически.

3.2.3. Настройка DNS

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

Для ввода компьютера в домен, на нем 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.

3.2.3.1. Настройка клиентов для использования DNS-серверов вручную

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

В ЦУС в разделе «Сеть» → «Ethernet интерфейсы» задать имя компьютера, указать в поле «DNS-серверы» DNS-сервер домена и в поле «Домены поиска» – домен для поиска (рис. 14).

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

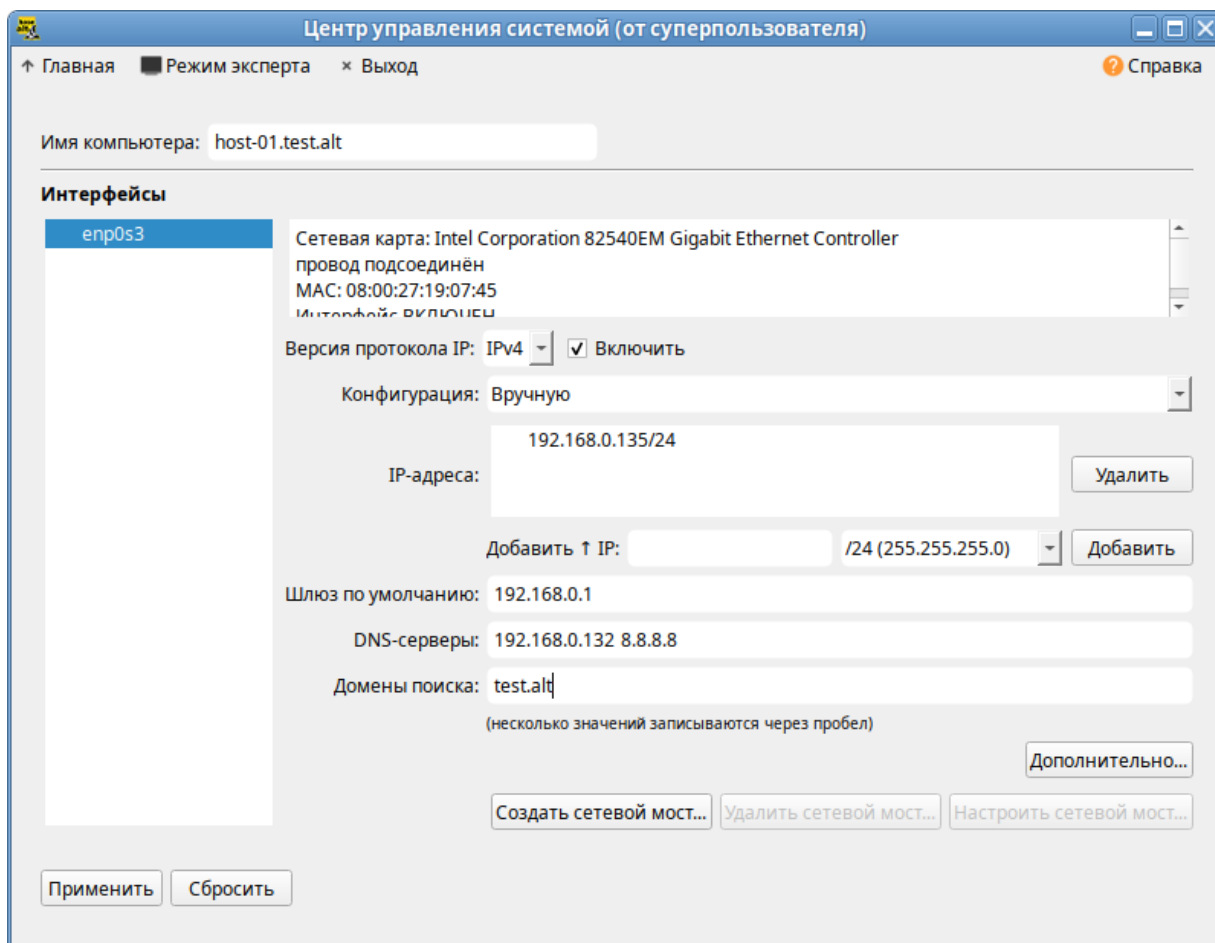


Рис. 14 – Окно «Центр управления системой»

В консоли:

- 1) задать имя компьютера:

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

- 2) 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;

- 3) 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;

4) 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
```

3.2.3.2. 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 «Альт Домен» обратная зона не настраивается автоматически.

«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.
```

3.3. Присоединение к домену в роли участника

3.3.1. Параметры команды system-auth

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

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

В таблице 5 приведено описание опций этой команды.

Т а б л и ц а 5 – Опции 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
--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:

- 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] [--gro]
```

3.3.2. Подключение к домену с помощью 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 кэшированием 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.

3.3.2.1. 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.

3.3.2.2. Ввод в домен в ЦУС

Для ввода компьютера в домен в ЦУС необходимо выбрать пункт «Пользователи» → «Аутентификация» (пакет alterator-auth).

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» (рис. 15).

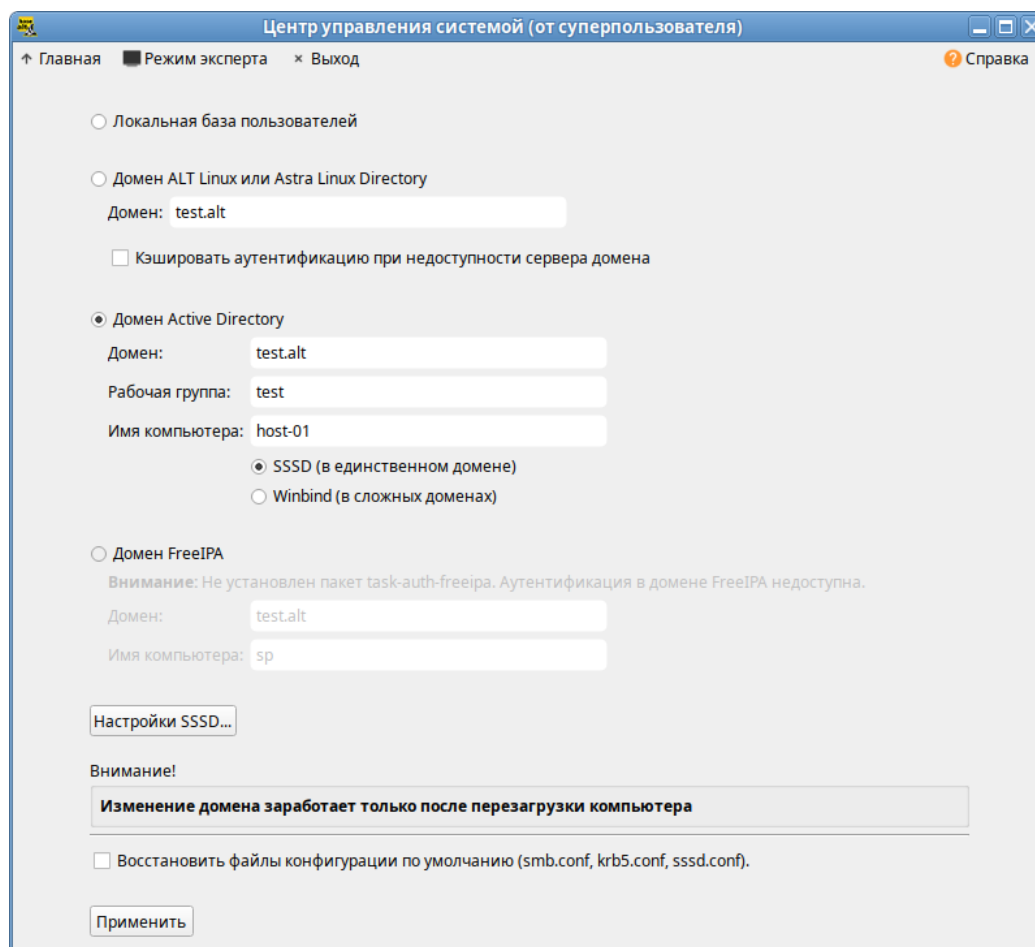


Рис. 15 – Окно модуля «Аутентификация»

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК» (рис. 16).

При успешном подключении к домену, отобразится соответствующая информация (рис. 17).

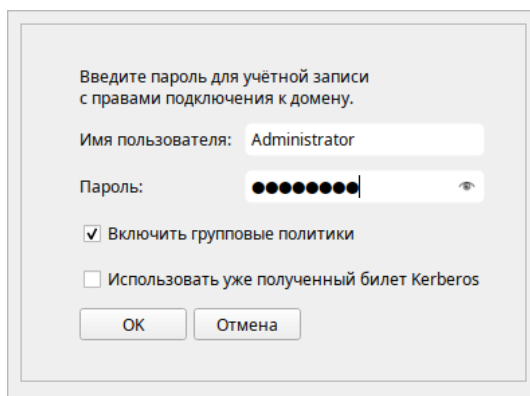


Рис. 16 – Окно ввода имени пользователя и пароля

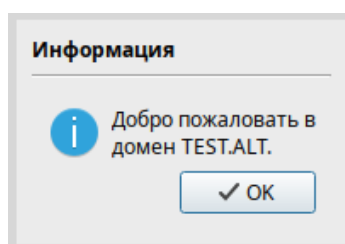


Рис. 17 – Информационное окно

Примечание. Если на машине установлен пакет `alterator-grupdate`, при подключении машины к домену можно включить групповые политики. Для включения групповых политик необходимо в окне ввода учетных записей пользователя с правами подключения к домену отметить пункт «Включить групповые политики» (рис. 16).

Перезагрузить рабочую станцию для применения всех настроек.

3.3.2.3. Проверка результатов присоединения

Проверка корректности подключения:

- 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. п. 6.14 и п. 5.5.2.

3.3.3. 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.

3.3.3.1. 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.

3.3.3.2. Ввод в домен в ЦУС

Для ввода компьютера в домен в ЦУС необходимо выбрать пункт «Пользователи» → «Аутентификация» (пакет alterator-auth).

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» (рис. 18).

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку «ОК» (рис. 19).

При успешном подключении к домену отобразится соответствующая информация (рис. 20).

Перезагрузить рабочую станцию для применения всех настроек.

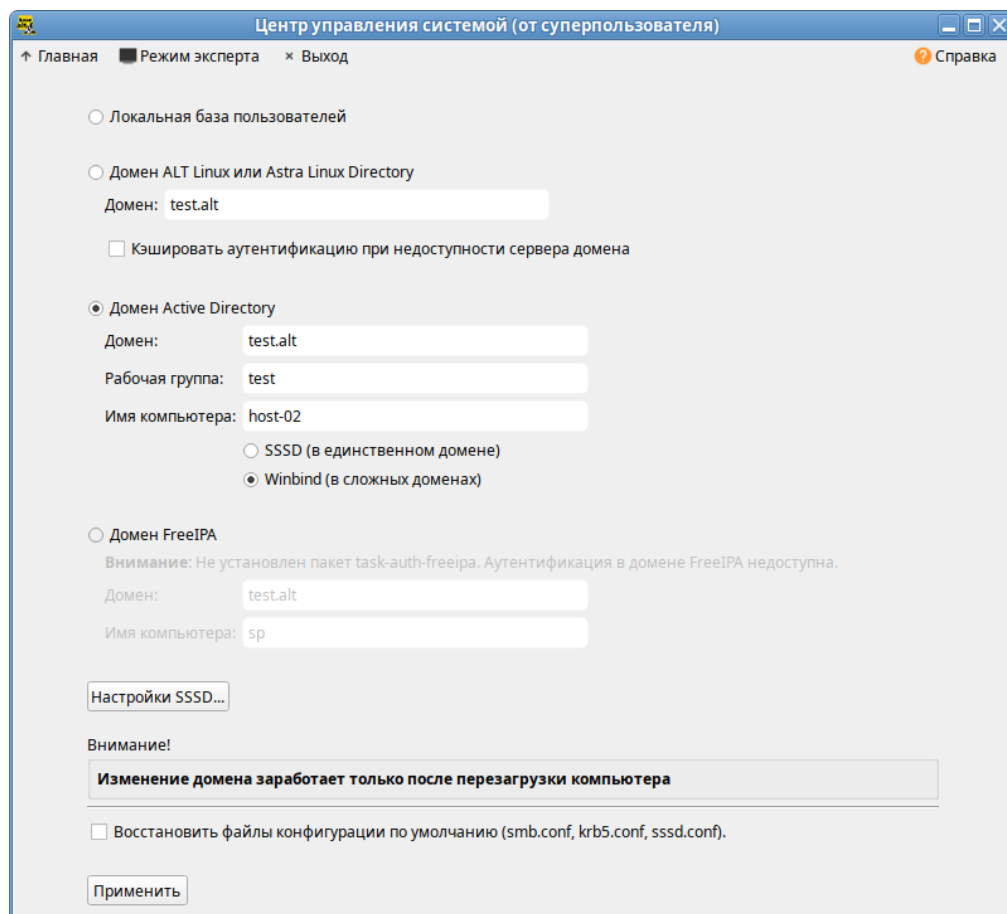


Рис. 18 – Ввод в домен в «Центр управления системой»

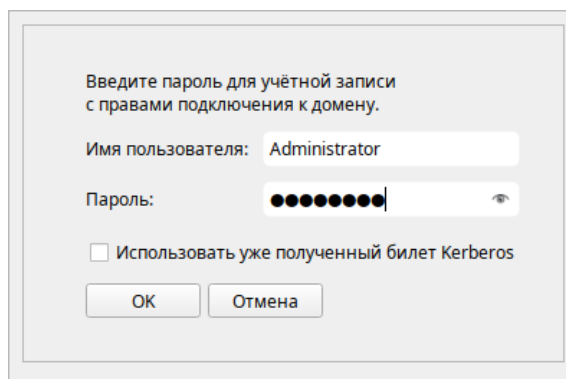


Рис. 19 – Окно ввода имени пользователя и пароля

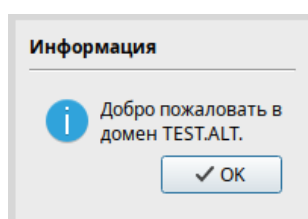


Рис. 20 – Информационное окно

3.3.3.3. Проверка результатов присоединения

Проверка корректности подключения:

- 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: Cp, 27 мар 2024 10:36:51 EET
KDC server: 192.168.0.132
Server time offset: 2
Last machine account password change: Cp, 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
```

3.3.4. Вход пользователя

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

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 клавишу <Enter> или кнопку «Войти» (рис. 21). В открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти» (рис. 22).

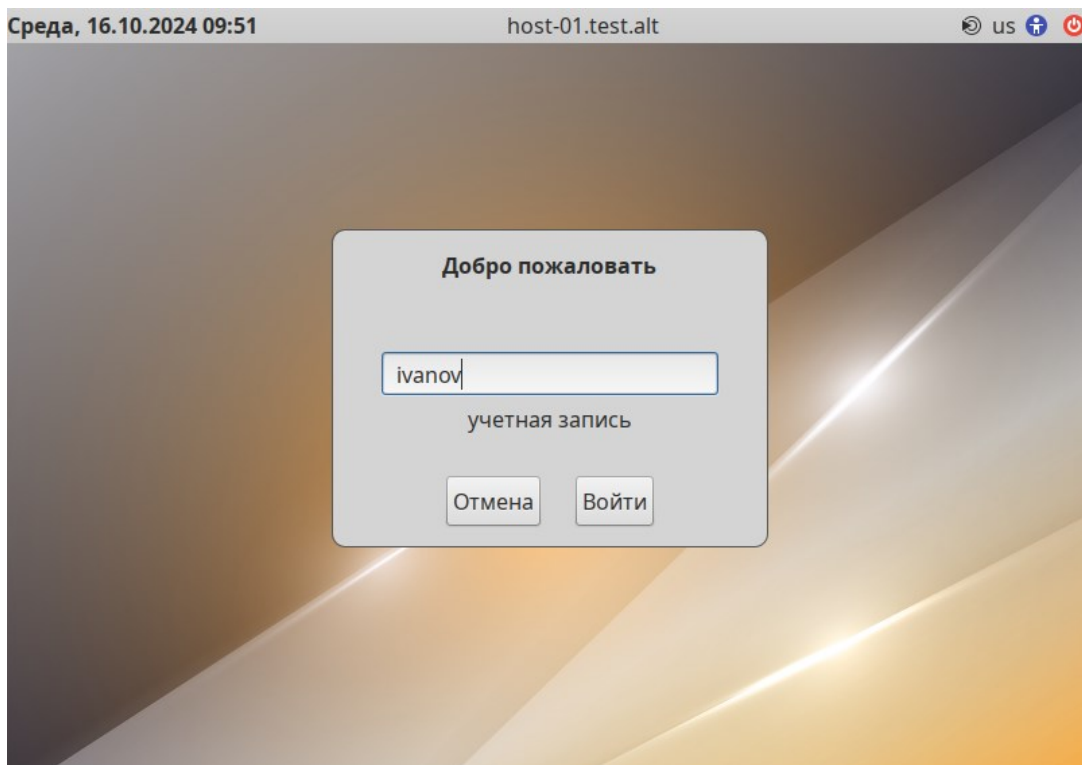


Рис. 21 – Ввод логина учетной записи пользователя домена

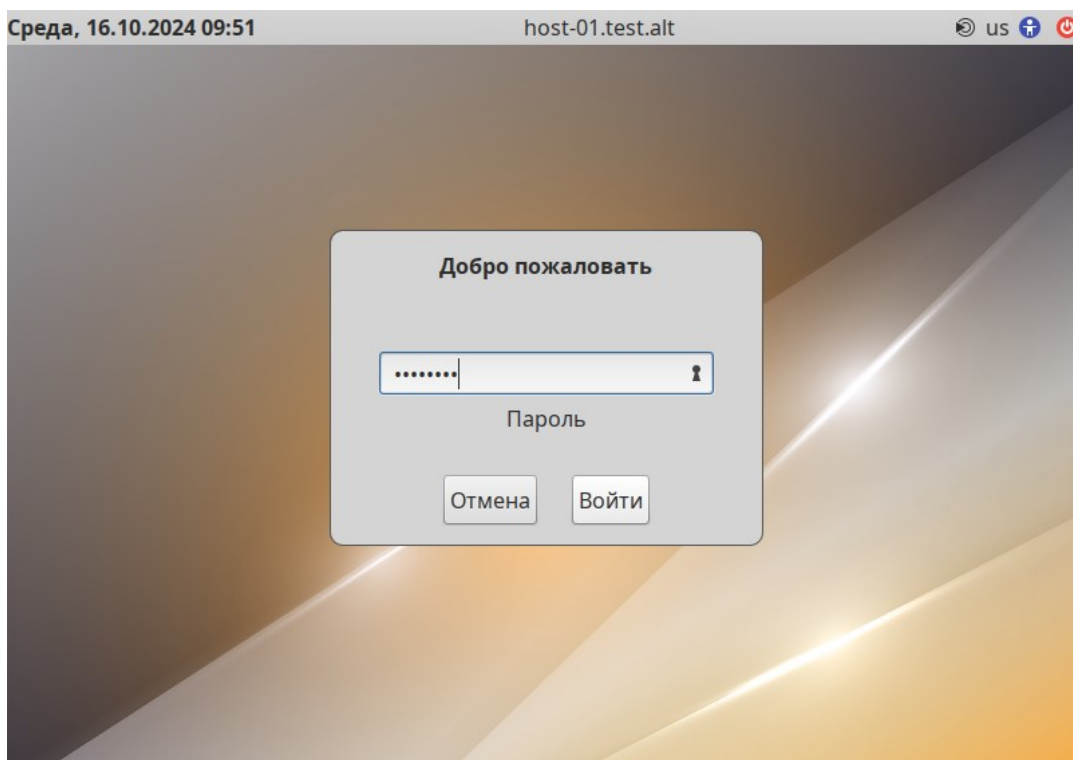


Рис. 22 – Ввод пароля

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 используемых для стандартного имяобразования в Linux) может наблюдаться некорректное поведение системы (например, не выставляются переменные окружения `XDG_RUNTIME_DIR` и `DBUS_SESSION_BUS_ADDRESS`). Для возможности использовать для входа привычные способы написания (с доменным суффиксом, точками, символами верхнего регистра) необходимо выполнить команду:

```
# 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.

3.4. Отладочная информация

3.4.1. Настройка уровня журналирования Samba

Дополнительные сведения см. в п. 6.14.3.

3.4.2. 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`.

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
...
```

3.4.3. `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
```

3.5. 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 учетная 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, учетная запись компьютера не удаляется из каталога; удаляется только конфигурация локального клиента. Если необходимо удалить учетную 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 в файле `/etc/lightdm/lightdm.conf` закомментировать строку в группе `[SeatDefaults]`:

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

3.6. 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 `/etc/samba/smb.conf`, `/etc/sss/sss.conf` и `/etc/krb5.conf` к виду по умолчанию и повторно ввести машину в домен.

Примечание. Привести файлы 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`, `sss.conf`)» и нажать кнопку «Применить» (рис. 23).

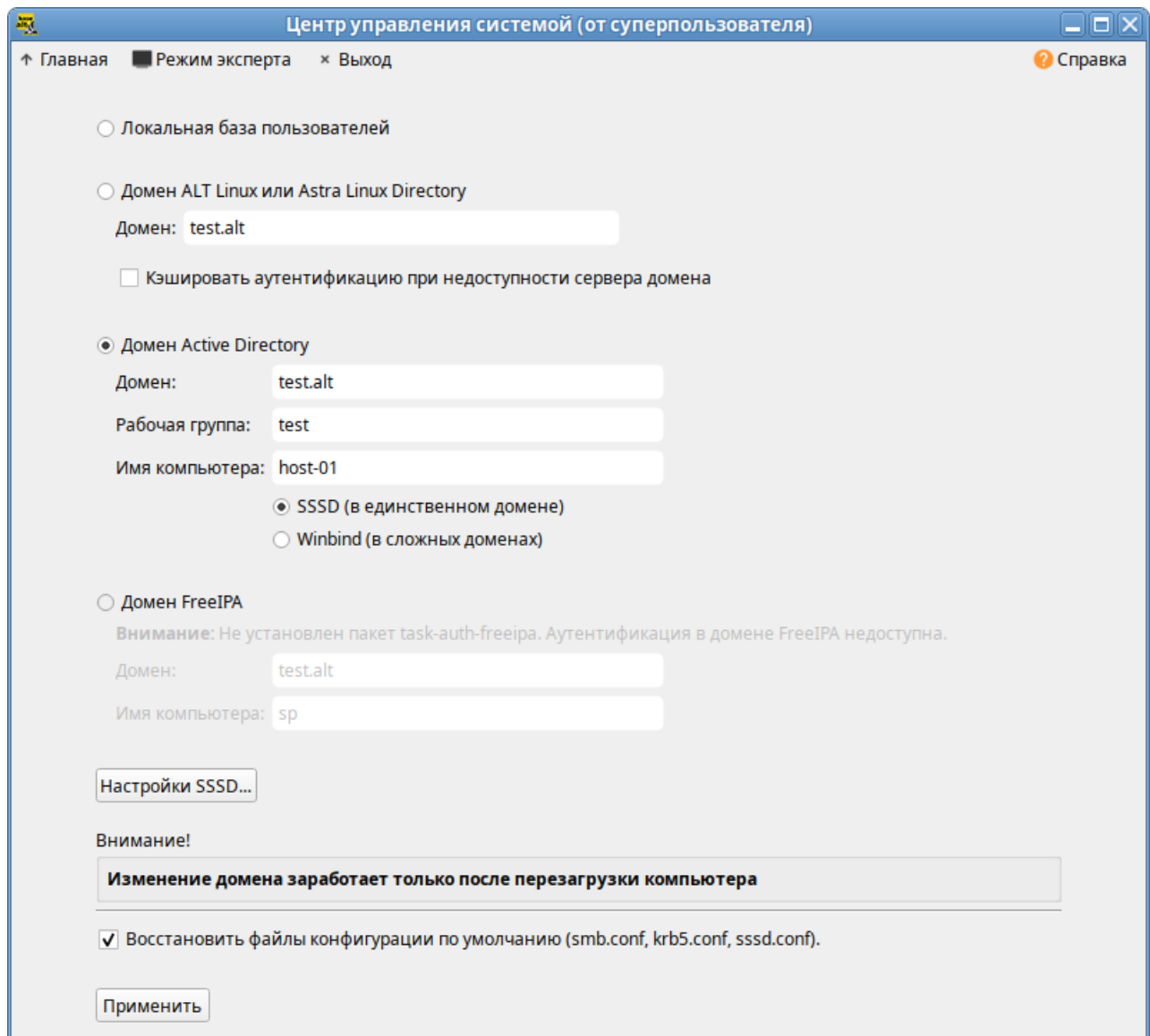


Рис. 23 – Ввод в домен в «Центр управления системой»

3.7. Настройка аутентификации доменных пользователей на DC

ВАЖНО

На текущий момент (samba 4.19.7, groupdate 0.10.6) данный метод не позволяет применять групповые политики на контроллере домена.

ВАЖНО

На текущий момент (samba 4.19.7, sssd 2.9.4) для каталога `/var/lib/samba/sysvol` SID'ы домена некорректно транслируются в UNIX user id и group id.

Контроллер домена в рамках доменной инфраструктуры является, в том числе, еще 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;
- все, что поддерживает обычная клиентская машина (в качестве клиента SSSD или Winbind).

ВАЖНО

В качестве клиента на контроллере домена рекомендуется использовать Winbind. Использование SSSD нежелательно.

3.7.1. Winbind

3.7.1.1. Установка пакетов

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

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

3.7.1.2. Изменение файлов конфигурации

3.7.1.2.1. 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]
```


3.7.1.2.2. 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
```

3.7.1.2.3. 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
```

3.7.1.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации Winbind-модуля:

```
# control system-auth winbind
```

3.7.2. SSSD

3.7.2.1. Установка пакетов

На контроллере домена должны быть установлены пакеты task-auth-ad-sssd и gpupdate:

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

3.7.2.2. Изменение файлов конфигурации

3.7.2.2.1. Настройка Kerberos (krb5.conf)

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

```
includedir /etc/krb5.conf.d/
dns_lookup_realm = false
default_realm = TEST.ALT
```

Пример файла /etc/krb5.conf:

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

3.7.2.2.2. Настройка SSSD (sssd.conf)

В файле `/etc/sss/sss.conf` должны быть заданы следующие параметры:

```
user = root
ad_maximum_machine_account_password_age = 0
```

Значения остальных параметров в файле должны соответствовать аналогичному файлу на обычных клиентах домена.

Пример файла `/etc/sss/sss.conf`:

```
[sss]
config_file_version = 2
services = nss, pam

# Managed by system facility command:
## control sss-drop-privileges unprivileged|privileged|default
user = root

# 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 = false
ad_gpo_ignore_unreadable = true
ad_gpo_access_control = permissive
ad_update_samba_machine_account_password = true
ad_maximum_machine_account_password_age = 0
```

3.7.2.2.3. Настройка Samba (smb.conf)

В файле `/etc/samba/smb.conf` должны быть заданы следующие параметры:

```
idmap config * : range = 200000-2000200000
idmap config * : backend = sss
```

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
```

```

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

```

```

kerberos method = system keytab
wins support = no
winbind use default domain = yes
winbind enum users = no
winbind enum groups = no
winbind refresh tickets = yes
winbind offline logon = yes

```

```

idmap config * : range = 200000-2000200000
idmap config * : backend = sss

```

```

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

```

```

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

```

3.7.2.2.4. Настройка NSS (nsswitch.conf)

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

```

passwd: files sss systemd
shadow: tcb files sss
group: files [SUCCESS=merge] sss role system

```

Пример файла /etc/nsswitch.conf:

```

passwd:    files sss systemd
shadow:    tcb files sss
group:     files [SUCCESS=merge] sss role systemd
gshadow:   files

```

```

hosts:     files myhostname dns

```

```

ethers:    files
netmasks:  files
networks:  files
protocols: files
rpc:       files
services:  files

```

```

automount: files
aliases:   files

```

3.7.2.3. Настройка аутентификации

Необходимо переключить PAM-стек на использование для аутентификации sss-модулей:

```
# control system-auth sss
```

3.7.3. Генерация keytab-файла

Необходимо сгенерировать системный keytab-файл для машинного аккаунта контроллера домена. Для этого следует выполнить следующую команду:

```
# net ads keytab create
```

3.7.4. Службы

Необходимо отключить сервис nscd:

```
# systemctl disable --now nscd
```

Если используется схема с SSSD клиентом, необходимо запустить и включить автоматический запуск для службы sssd:

```
# systemctl enable --now sssd
```

3.7.5. 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».

3.7.6. Групповые политики

Для включения поддержки групповых политик необходимо выполнить команду:

```
# gpupdate-setup enable --local-policy ad-domain-controller
```

ВАЖНО

Работа групповых политик на контроллере домена с SSSD клиентом может быть не стабильной.

3.7.7. Настройка SSH

Разрешить удаленный 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
```

Для применения настроек необходимо перезапустить сервис sshd:

```
# systemctl restart sshd
```

Примечание. Данные настройки можно применить с помощью механизма групповых политик control. Подробнее см. п. 4.6.4.2.

3.8. Настройка обновления паролей аккаунтов машин

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 отличие 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.

3.8.1. Локальная политика смены пароля

Сменой пароля учетной 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 учетной 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) (рис. 24).

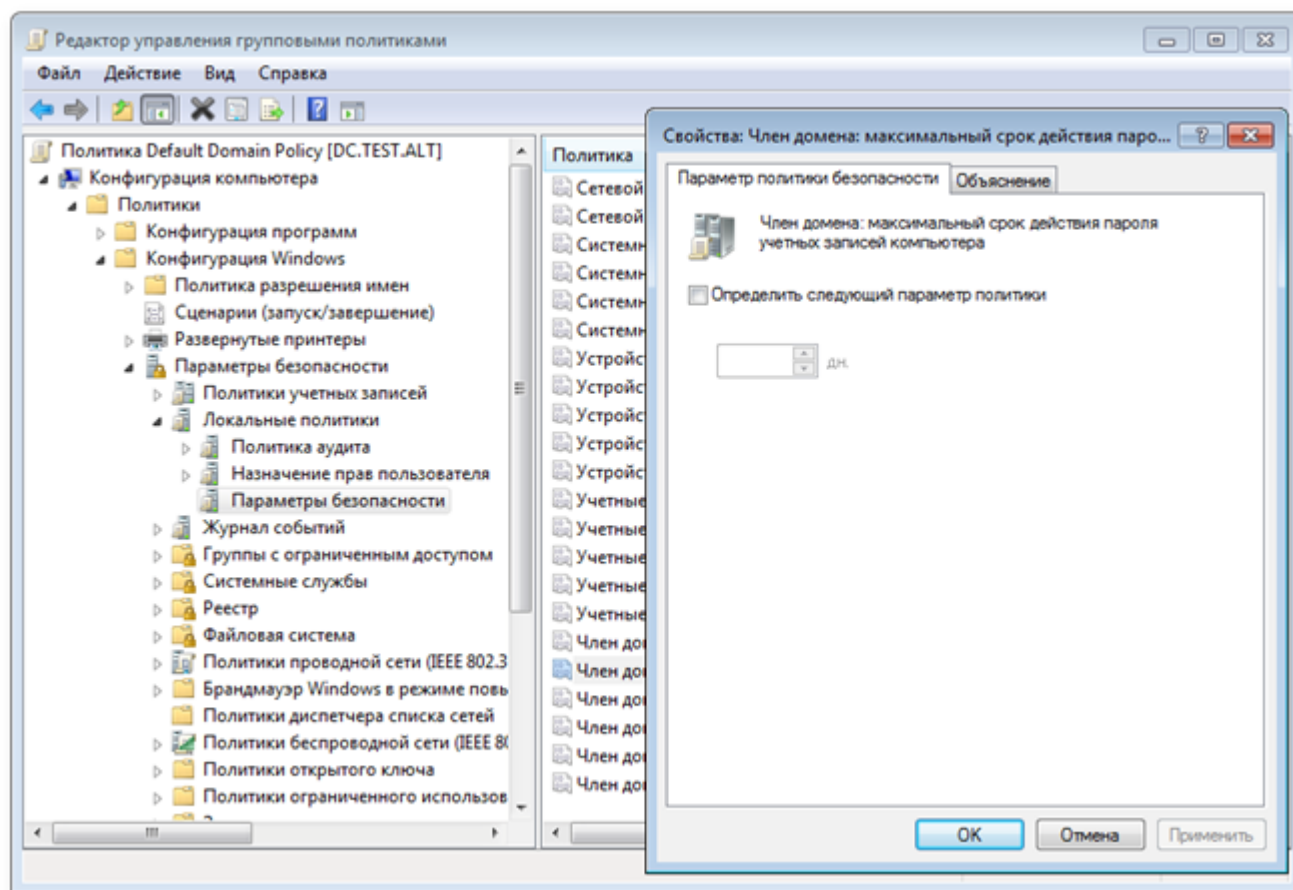


Рис. 24 – Окно параметра «Член домена»

Примечание. На данный момент в ADMS (adms 0.16.4) нет возможности настроить данные параметры групповой политики. Необходимо использовать оснастку RSAT «Управление групповыми политиками» (см. п. 4.2.3).

Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учетной записи компьютера. Значение по умолчанию: 30 дней.

С помощью параметра «Член домена: отключить изменение пароля учетных записей компьютера» можно отключить обновления пароля машинного аккаунта совсем, но делать этого не рекомендуется.

ВАЖНО

Указанные выше параметры корректно работают на машинах с ОС MS Windows 2000 и старше.

ВАЖНО

На машинах с ОС Альт СП (sssd 2.9.4) данные параметры игнорируются.

3.8.2. Включение обновления пароля

3.8.2.1. ОС Windows

Для включения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Windows 2000 и старше дополнительных действий не требуется. Периодичность обновления настраивается с помощью соответствующей групповой политики.

3.8.2.2. ОС Альт СП

За обновление пароля машинного аккаунта на машинах под управлением ОС Альт СП отвечают сервисы `sssd` и `winbind`.

3.8.2.2.1. Winbind

Winbind, на текущий момент (`samba-winbind 4.19.7`), не умеет после смены пароля учетной записи компьютера обновлять системный `keytab`-файл (`/etc/krb5.keytab`). Поэтому, во избежание конфликтов с `sssd`, следует отключить этот функционал.

Для отключения периодического обновления пароля учетной записи компьютера необходимо в файл `smb.conf` в секцию `[global]` добавить параметр `machine password timeout = 0`:

```
[global]
machine password timeout = 0
```


3.8.2.2.2. SSSD

SSSD для обновления пароля учетной записи компьютера использует утилиту `adcli`. Необходимо убедиться, что пакет `adcli` установлен в системе:

```
# apt-get install adcli
```

Периодичностью обновления пароля учетной записи компьютера можно управлять с помощью параметра `ad_maximum_machine_account_password_age` (секция `[domain/<Домен>]`) в `/etc/sss/sss.conf`. Значение по умолчанию: 30 дней.

Для корректного функционирования обновления пароля учетной записи компьютера `sss` необходим доступ на запись в файл `/etc/krb5.keytab`. Для этого недостаточно привилегий пользователя `_sss`, от которого обычно и запускается `sss`. Необходимо запускать `sss` с правами суперпользователя. Для этого следует в файле `/etc/sss/sss.conf` в секции `[sss]` изменить значение параметра `user` на `root`:

```
[sss]
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/sss/sss.conf:
  ad_update_samba_machine_account_password = true
```

3.8.3. Отключение обновления пароля

3.8.3.1. ОС Windows

Для отключения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Windows 2000 и старше достаточно включить параметр групповой политики «Default domain policy» «Член домена: отключить изменение пароля учетных записей компьютера».

3.8.3.2. ОС Альт СП

Для отключения периодического обновления пароля учетной записи компьютера на машинах под управлением ОС Альт СП необходимо:

- в файле `/etc/sss/sss.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
```

3.8.4. Диагностика

3.8.4.1. Дата последней смены пароля

Дата последней смены пароля учетной записи компьютера хранится в базе данных «Альт Домен». Запросить ее можно одним из способов:

- на введенной 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 учетной записи компьютера будет показана в параметре:

```
Last machine account password change.
```

3.8.4.2. Потеря доверия между машиной и доменом

Для проверки того, имеет ли машина возможность аутентифицироваться в домене, можно выполнить следующие действия:

- убедиться, что `keytab`-файла (`/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 учетной записи компьютера (в примере WORK\$), используя файл /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).

3.8.5. 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.

4. ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ОБЪЕКТАМИ ДОМЕНА И ГРУППОВЫМИ ПОЛИТИКАМИ

4.1. Групповые политики

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 (таких как, например, Puppet и Ansible) тремя ключевыми особенностями:

- интеграцией в инфраструктуру AD;
- соответствием декларативной части настроек конфигураций конкретным дистрибутивным решениям;
- наличием не только управления конфигурациями компьютеров, но и конфигурациями пользователей.

В ОС Альт СП для применения групповых политик используется инструмент `groupdate` (см. п. 4.4). Инструмент рассчитан на работу на машине, введенной 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).

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.

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. Некоторые задачи управления конфигурациями можно решить как через пользовательские, так и через машинные параметры.

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 такой механизм, как GConf или dconf, а также определенные 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, является то, что значения конфигурационных настроек при их задании перезаписываются, теряя исходное состояние. В рамках дистрибутивных решений ОС Альт СП 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.

Далее, для терминологического упрощения, политики и предпочтения называются одним термином «Групповая политика» (ГП) с поправками на особенности их применения.

Список групповых политик, которые можно настроить и применять в «Альт Домен» представлен в таблице 6.

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 утверждены технически.

Логическая структура инструментов управления (рис. 25) 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).

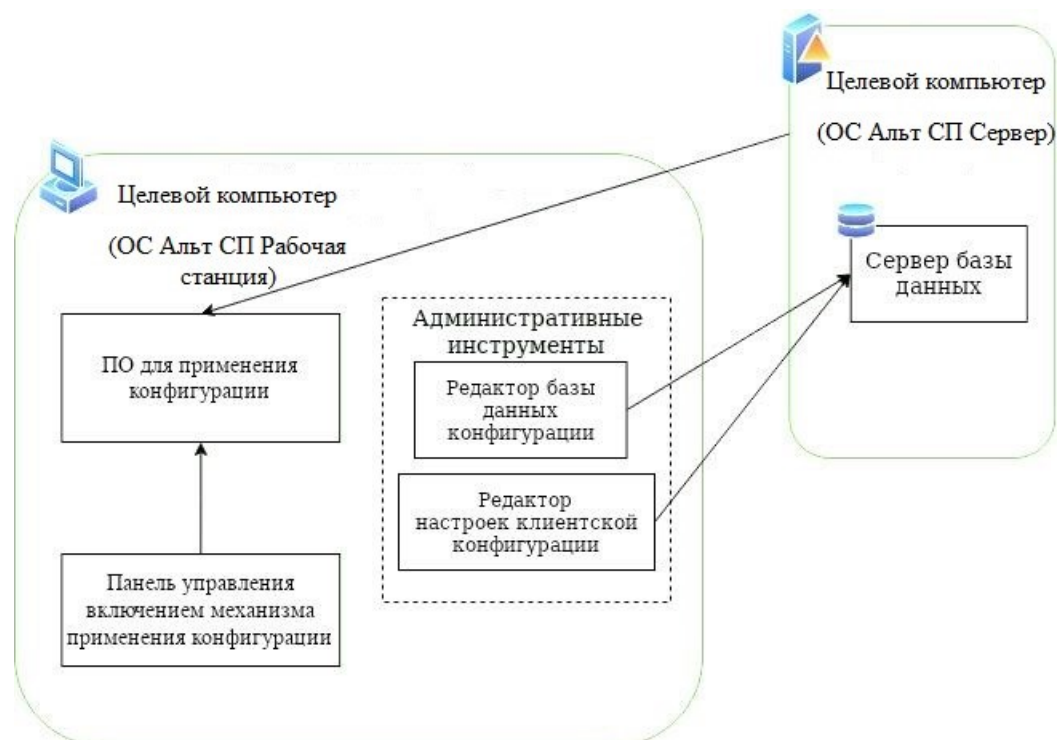


Рис. 25 – Логическая структура

Т а б л и ц а 6 – 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 веб-браузера Firefox	Стабильная	ADMX-файлы Mozilla Firefox (пакет admx-firefox)
Настройка веб-браузера Chromium	Стабильная	ADMX-файлы Google Chrome (пакет admx-chromium)
Настройка «Яндекс.Браузера»	Стабильная	ADMX-файлы Yandex (пакет admx-yandex-browser)
Управление Gsettings (настройки графической среды MATE и удаленного доступа к рабочему столу VNC)	Стабильная	ADMX-файлы ALT (пакет admx-basealt)
Настройки среды рабочего стола KDE	Экспериментальная	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	

4.2. Установка административных шаблонов и административных инструментов

4.2.1. Установка административных шаблонов

Для задания конфигурации необходимо на контроллере домена установить административные шаблоны (ADMX-файлы). Для этого следует:

1) установить пакеты политик:

```
# apt-get install admx-basealt admx-yandex-browser \
    admx-chromium admx-firefox admx-msi-setup
```

доступны следующие пакеты политик:

- admx-basealt – ADMX-файлы, специфичные для BaseALT;

- admx-yandex-browser – ADMX-файлы для управления настройками Яндекс.Браузера;
- admx-firefox – ADMX-файлы для управления настройками веб-браузера Mozilla Firefox;
- admx-chromium – ADMX-файлы для управления настройками веб-браузера Google Chrome.

Примечание. Шаг установки пакетов политик можно пропустить, если при установке ОС на этапе «Установка системы» был выбран профиль «Альт Домен (контроллер домена)» (рис. 2).

- 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/`):

```
# 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 <admx-msi-
source>]
Removing admx-msi-setup temporary files...
```

4.2.2. Административные инструменты

Административные инструменты обычно устанавливаются на рабочей станции, введенной в домен.

Примечание. Шаг установки административных инструментов можно пропустить, если при установке рабочей станции на этапе «Установка системы» был выбран профиль «Альт Домен (инструмент управления ГПО)» (рис. 26).

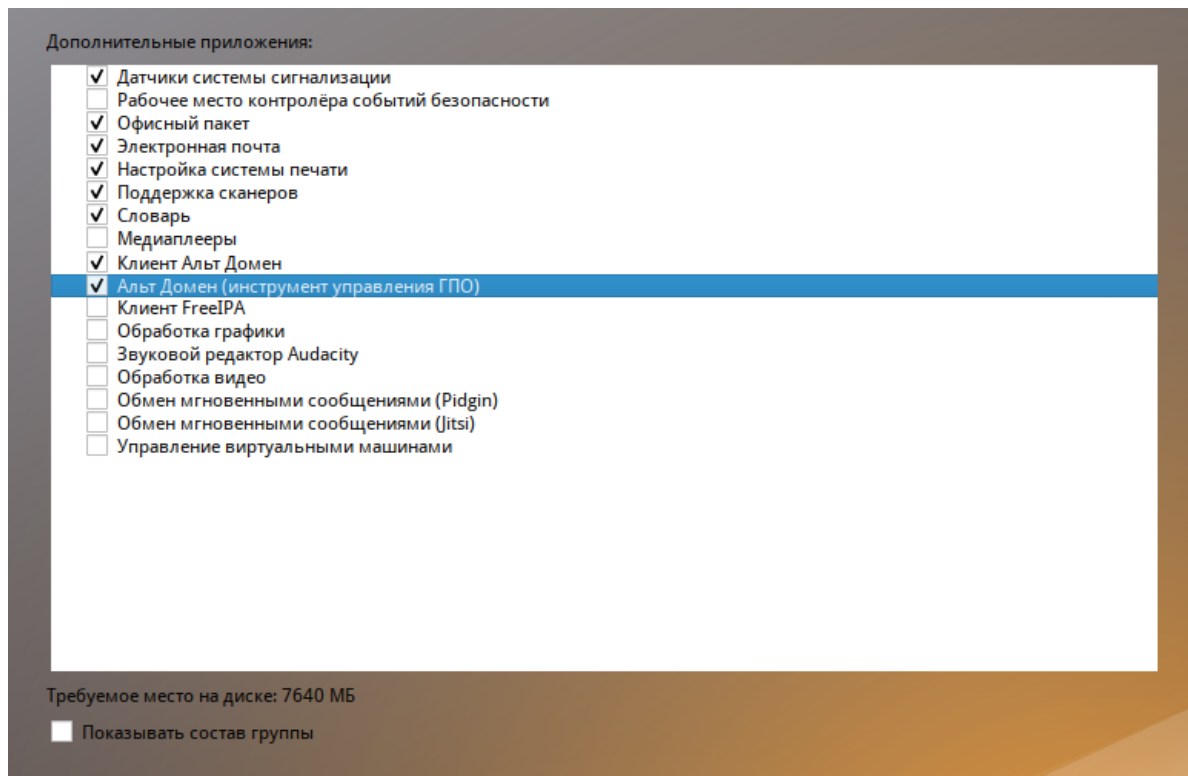


Рис. 26 – Выбор профиля «Клиент Альт Домен» при установке ОС

4.2.2.1. ADMC

Установить пакет `admc` (дистрибутив ОС Альт СП Рабочая станция):

```
# 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. п. 4.5.

4.2.2.2. GPUI

Установить пакет `gpi` (дистрибутив ОС Альт СП Рабочая станция):

```
# apt-get install gpi
```

В настоящее время GPUI не умеет читать файлы ADMX с контроллера домена. Поэтому для корректной работы необходимо также установить пакеты admx и файлы ADMX от Microsoft:

```
# apt-get install admx-basealt admx-yandex-browser \  
admx-chromium admx-firefox admx-msi-setup  
# admx-msi-setup
```

Примечание. Для использования GPUI необходимо предварительно получить ключ Kerberos для администратора домена.

Подробнее о работе с GPUI см. п. 4.6

4.2.3. Установка RSAT

Для администрирования «Альт Домен» из Windows можно использовать средства удаленного администрирования сервера Microsoft (RSAT).

4.2.3.1. Windows Server

В ОС Windows Server средства удаленного администрирования сервера Microsoft (RSAT) включены по умолчанию.

Для установки необходимо выполнить следующие пункты:

- 1) запустить Диспетчер серверов;
- 2) на Windows Server 2012, 2012 R2, и 2016:
 - выбрать «Управление» → «Добавить роли и компоненты» (рис. 27);

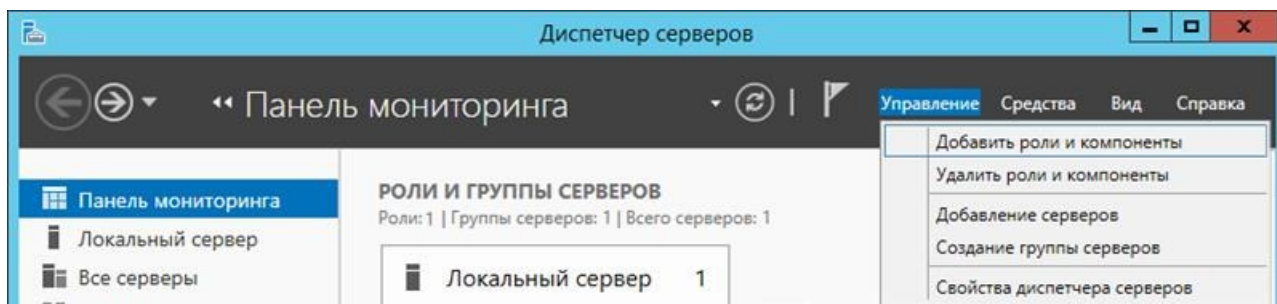


Рис. 27 – Диспетчер сервисов

- в открывшемся окне «Мастер добавления ролей и компонентов» выбрать пункт «Установка ролей или компонентов» (рис. 28);

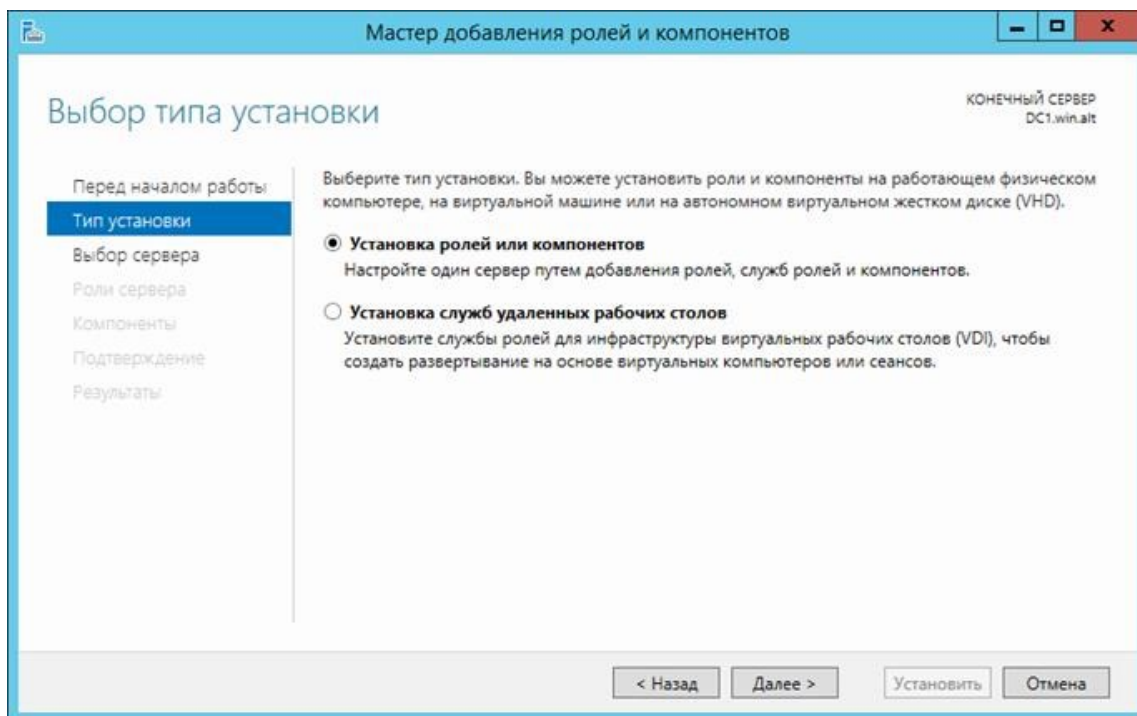


Рис. 28 – Выбор типа установки

- выбрать узел, на котором будут установлены компоненты (рис. 29);
- на шаге «Роли сервера» выбрать роль «Доменные службы Active Directory»;

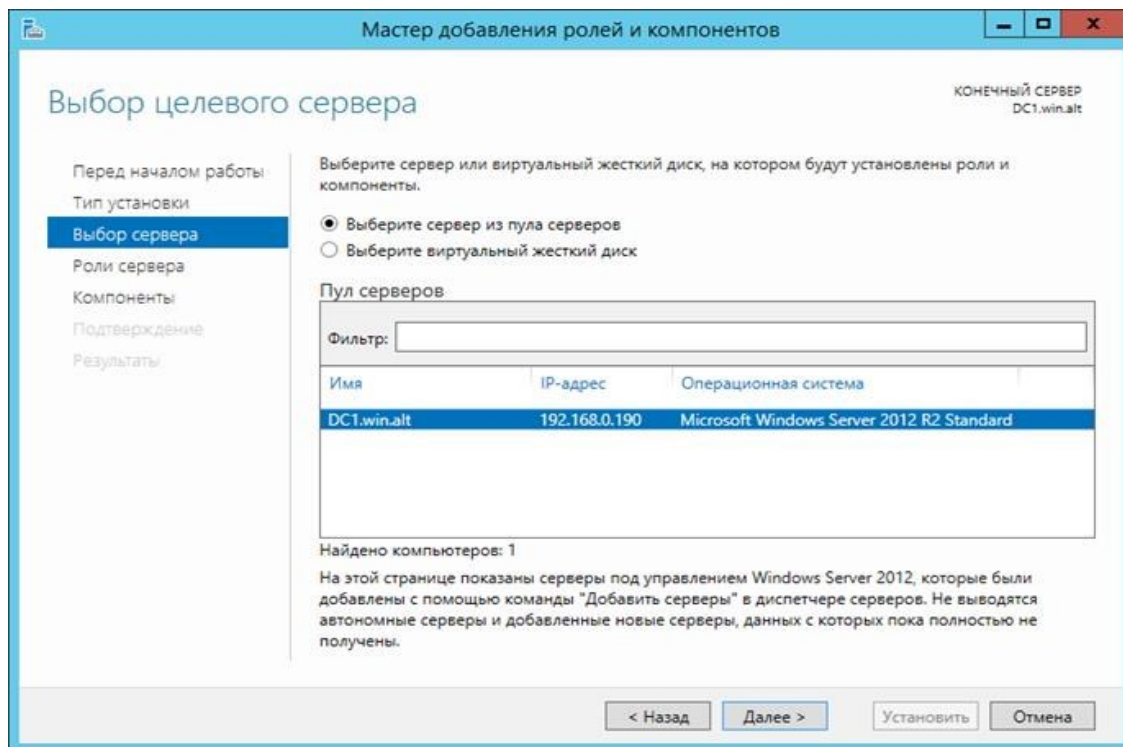


Рис. 29 – Выбор целевого сервера

- 3) на Windows Server 2008 и 2008 R2 в дереве навигации выбрать «Компоненты» и нажать «Добавить компоненты»;
- 4) выбрать компоненты для установки (рис. 30). Рекомендуемые компоненты см. в таблице 7.

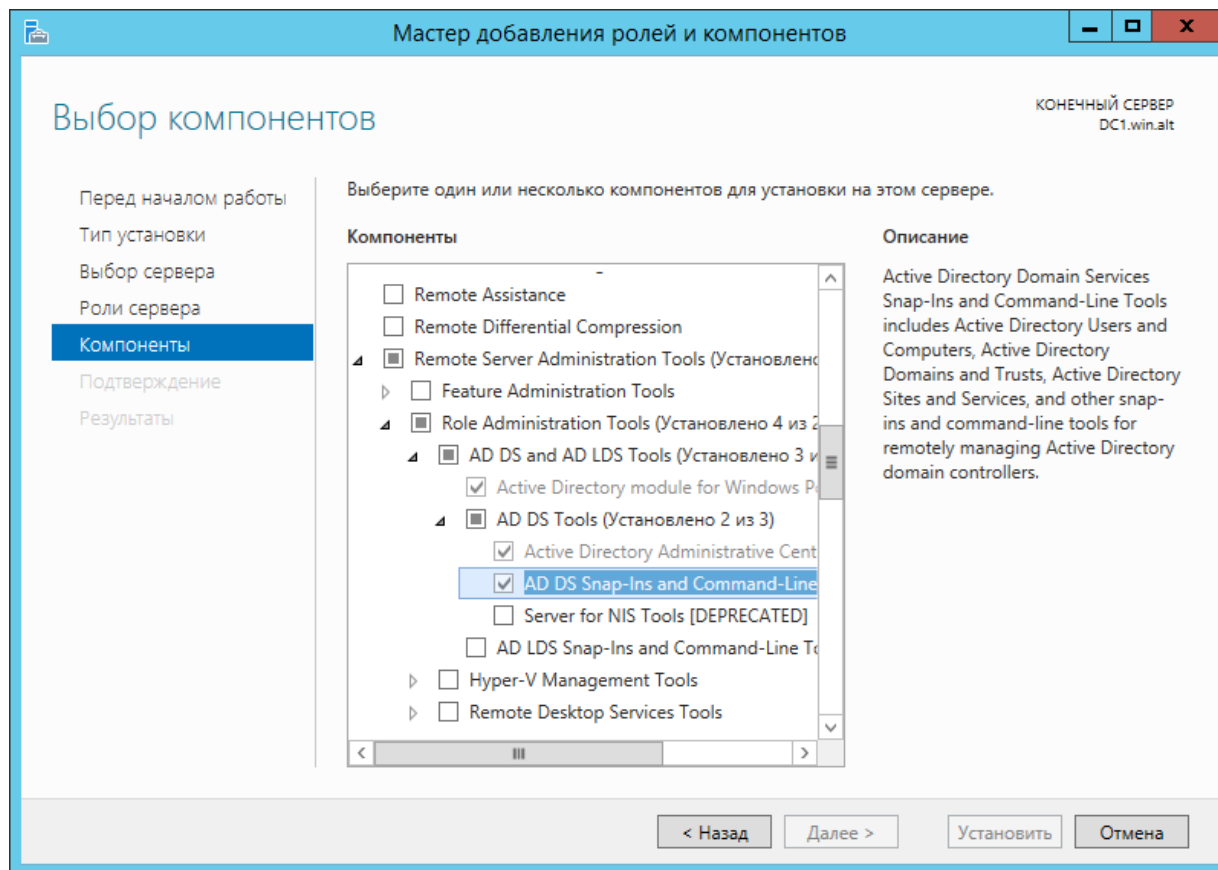


Рис. 30 – Выбор компонентов

Т а б л и ц а 7 – Компоненты Windows для администрирования домена

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 команды Active Directory (AD) PowerShell
DNS Server tools	Оснастка MMC DNS для удаленного управления DNS

4.2.4. Windows 10 (1809 и более поздние версии)

В Windows 10 1809 и более поздних версиях RSAT устанавливается в качестве дополнительной функции. Для установки компьютер должен иметь доступ в Интернет.

Для установки RSAT выполнить следующие действия:

- 1) перейти в раздел «Settings» → «Apps» → «Optional Features» → «View features» («Параметры Windows» → «Приложения» → «Дополнительные возможности» → «Добавить компонент») (рис. 31);

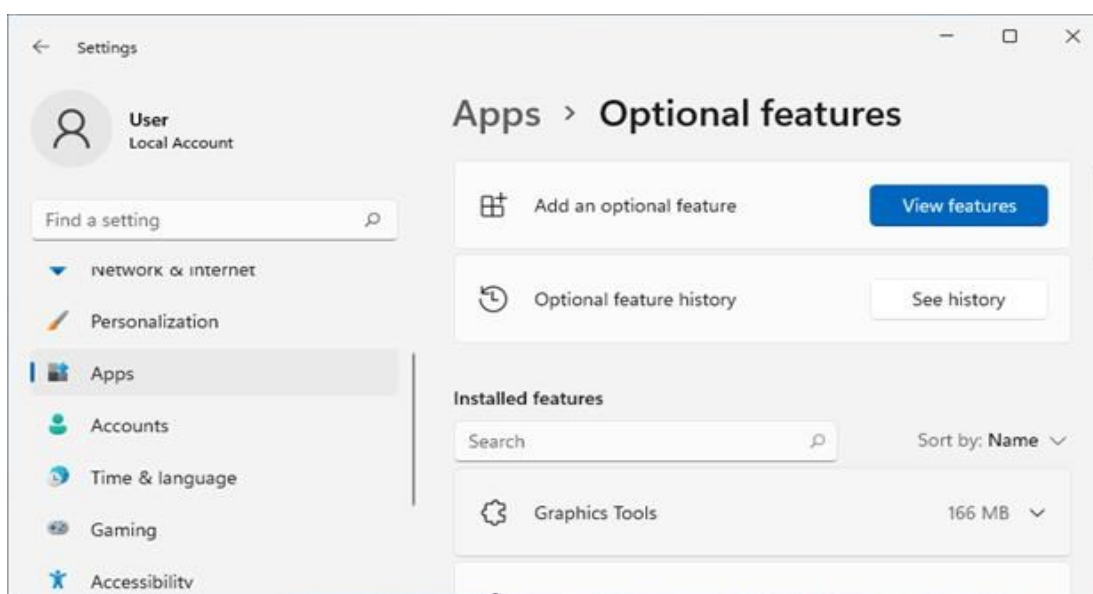


Рис. 31 – Дополнительные возможности

- 2) выбрать нужные компоненты RSAT (рекомендованные компоненты RSAT представлены в таблице 8) и нажать кнопку «Next» (рис. 32);

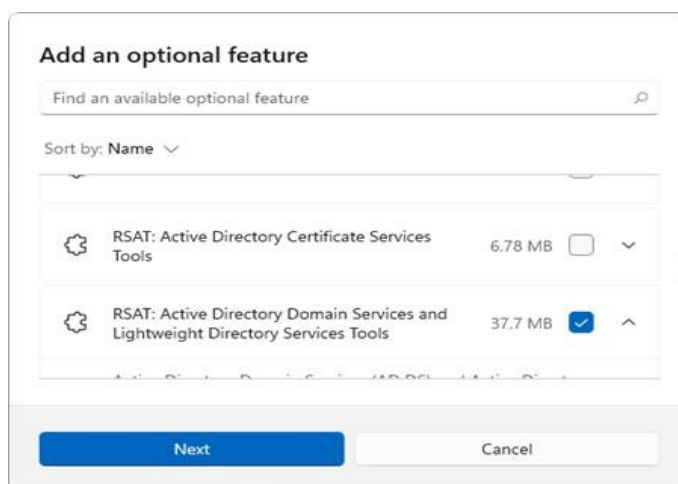


Рис. 32 – Добавление компонентов

3) нажать кнопку «Install».

Т а б л и ц а 8 – Рекомендуемые компоненты RSAT

Компонент	Описание
RSAT: Group Policy Management Tools	Включает консоль управления групповыми политиками (gpmmc.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).

4.2.5. 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.

Для установки RSAT необходимо выполнить следующие действия:

- 1) перейти в «Панель управления» → «Программы» → «Включение или отключение компонентов Windows» (рис. 33);

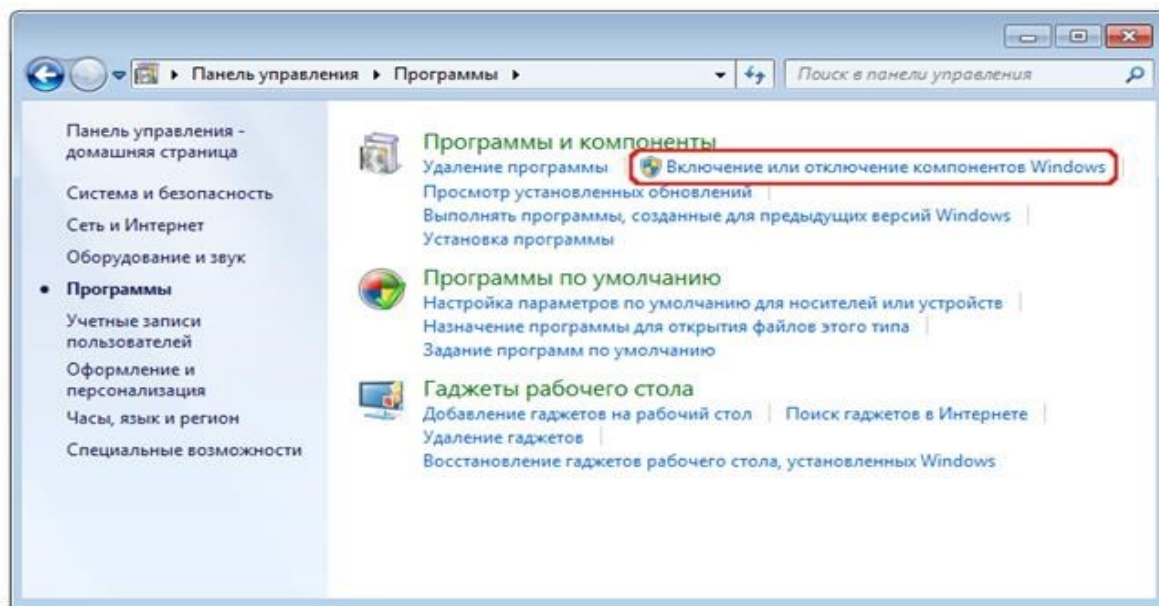


Рис. 33 – «Включение или отключение компонентов Windows»

2) включить компоненты, представленные на рис. 34 и описанные в таблице 9;

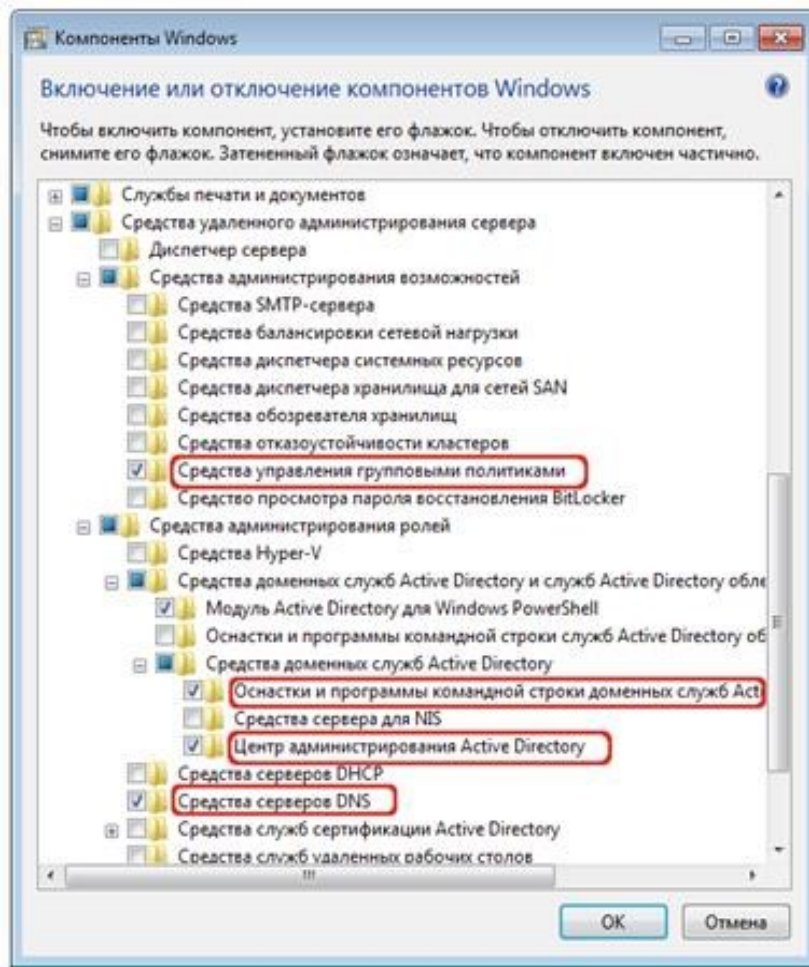


Рис. 34 – Компоненты для включения

Т а б л и ц а 9 – Рекомендуемые компоненты Windows

Компонент	Описание
Group Policy Management Tools (Средства управления групповыми политиками)	Включают консоль управления групповыми политиками (gpms.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)	Средства сервера для сетевых информационных служб добавляет вкладку Атрибуты UNIX (UNIX Attributes) в свойства объектов ADUC. Позволяет настраивать атрибуты RFC2307. Включает программу командной строки upclear.exe

Окончание таблицы 9

Компонент	Описание
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 удаленных 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).

3) нажать кнопку «ОК».

4.3. 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.

Модуль панели управления операционной системы для включения механизма применения конфигурации на клиентских машинах представляет собой следующие модули ЦУС:

- «Аутентификация» (пакет alterator-auth);
- «Групповые политики» (пакет alterator-gpupdate).

Включить групповые политики 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 следует в модуле ЦУС «Аутентификация» (пакет alterator-auth) выбрать пункт «Домен Active Directory», заполнить поля «Домен», «Рабочая группа» и «Имя компьютера», и нажать кнопку «Применить» (рис. 35).

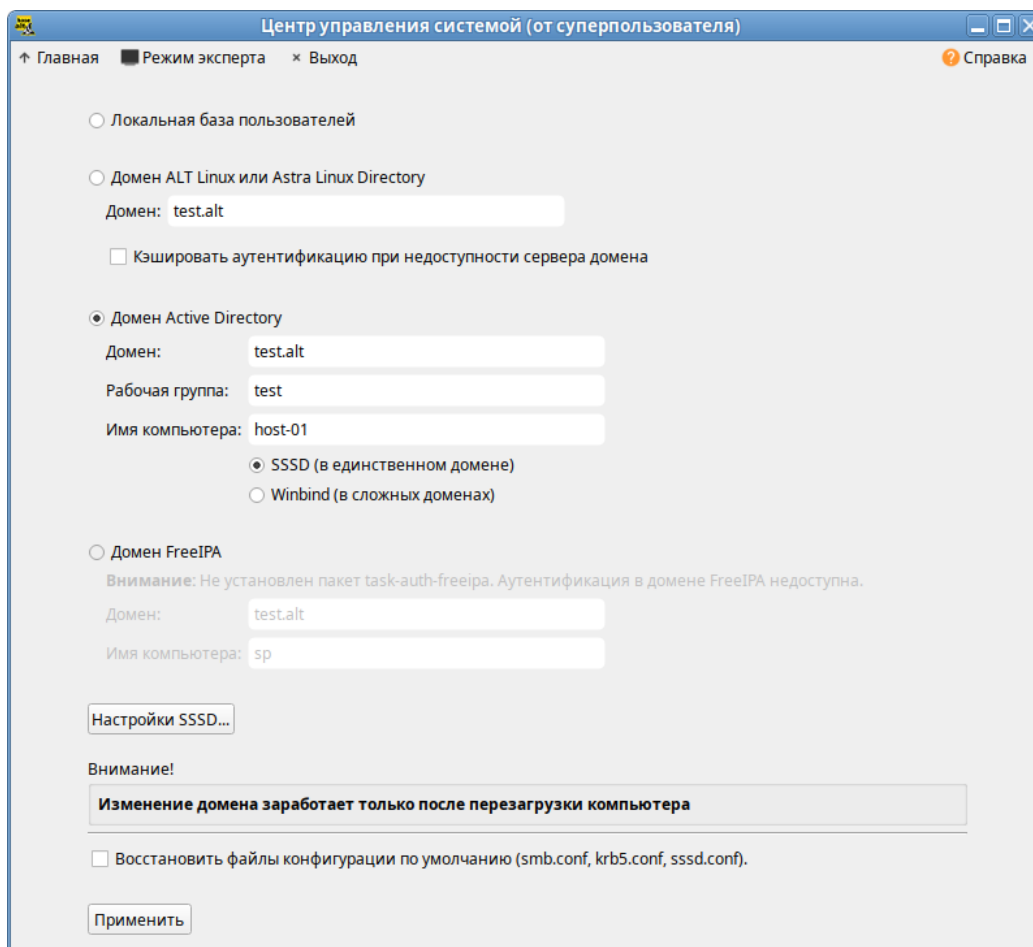


Рис. 35 – Ввод в домен в ЦУС

В открывшемся окне ввести имя пользователя, имеющего право вводить машины в домен, и его пароль, отметить пункт «Включить групповые политики» и нажать кнопку «ОК» (рис. 36).

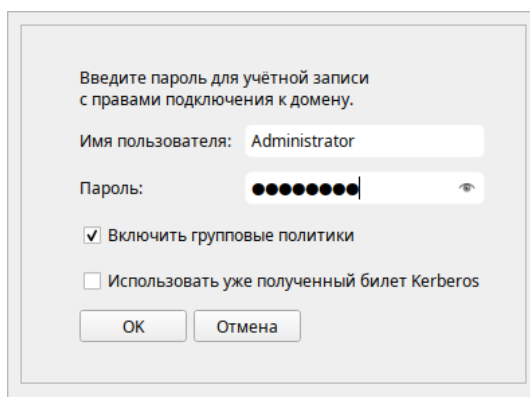


Рис. 36 – Включение групповых политик при вводе в домен

Включить поддержку управления групповыми политиками на машине, уже введенной в домен, можно в модуле ЦУС «Групповые политики» (рис. 37).

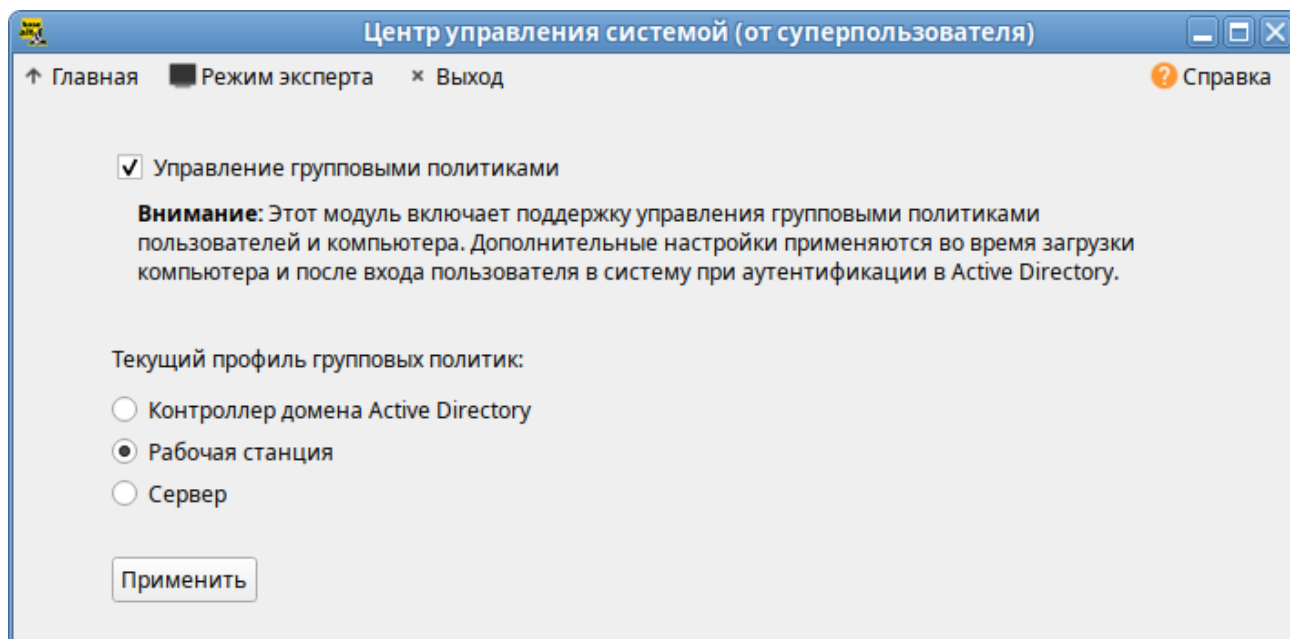


Рис. 37 – Включение поддержки управления групповыми политиками

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»;
- «Рабочая станция».

Для возможности включения групповых политик на машинах под управлением ОС Альт СП, на которых не установлена графическая оболочка, модуль «Групповые политики» доступен также в веб-интерфейсе ЦУС (рис. 38).

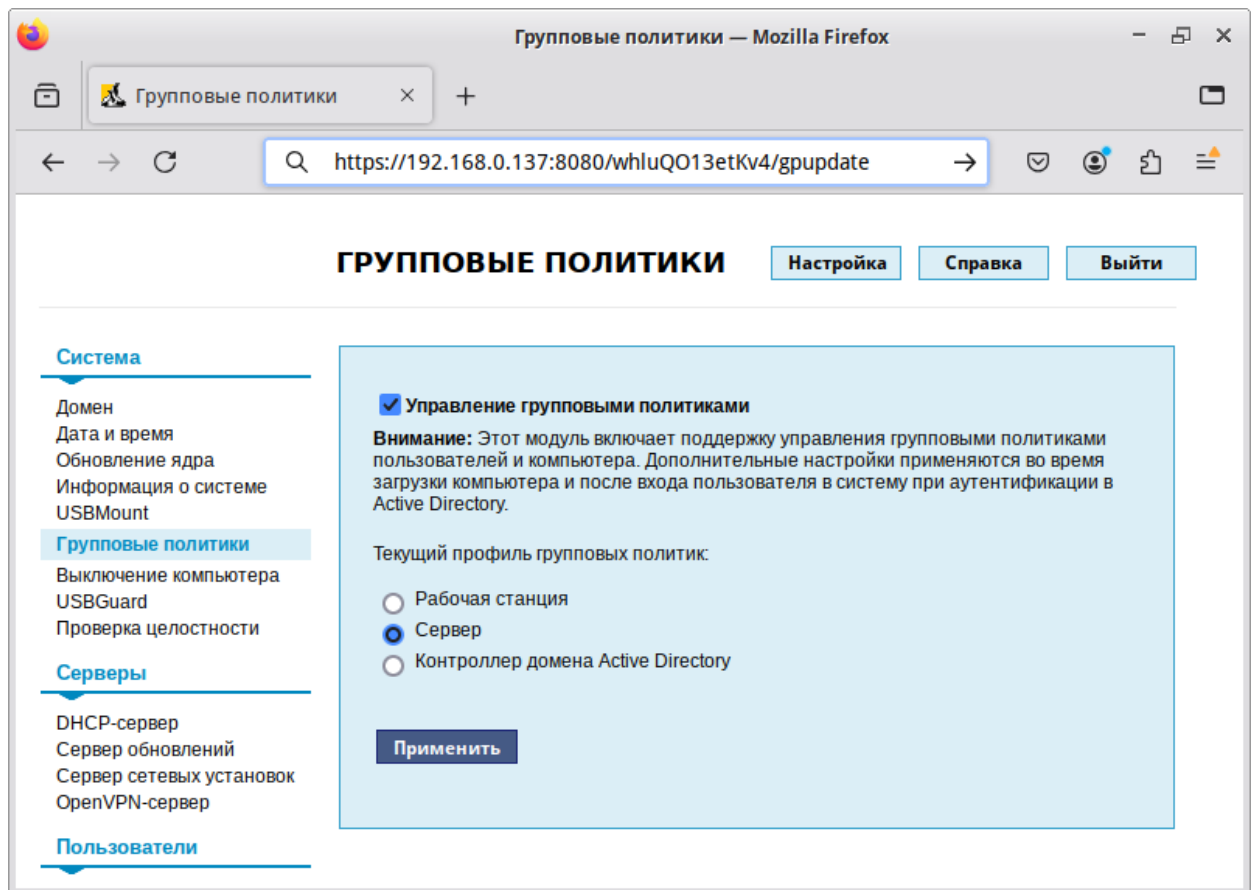


Рис. 38 – Веб-интерфейс модуля «Групповые политики»

4.4. Модуль клиентской машины для применения конфигурации

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 веб-браузера Mozilla Firefox и создание файла политик

для него, а модуль ntp отвечает за чтение настроек, касающихся NTP-сервера, и создание 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, обрабатываются в определенном порядке. Сначала обрабатываются объекты групповой политики, 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 (рис. 39).

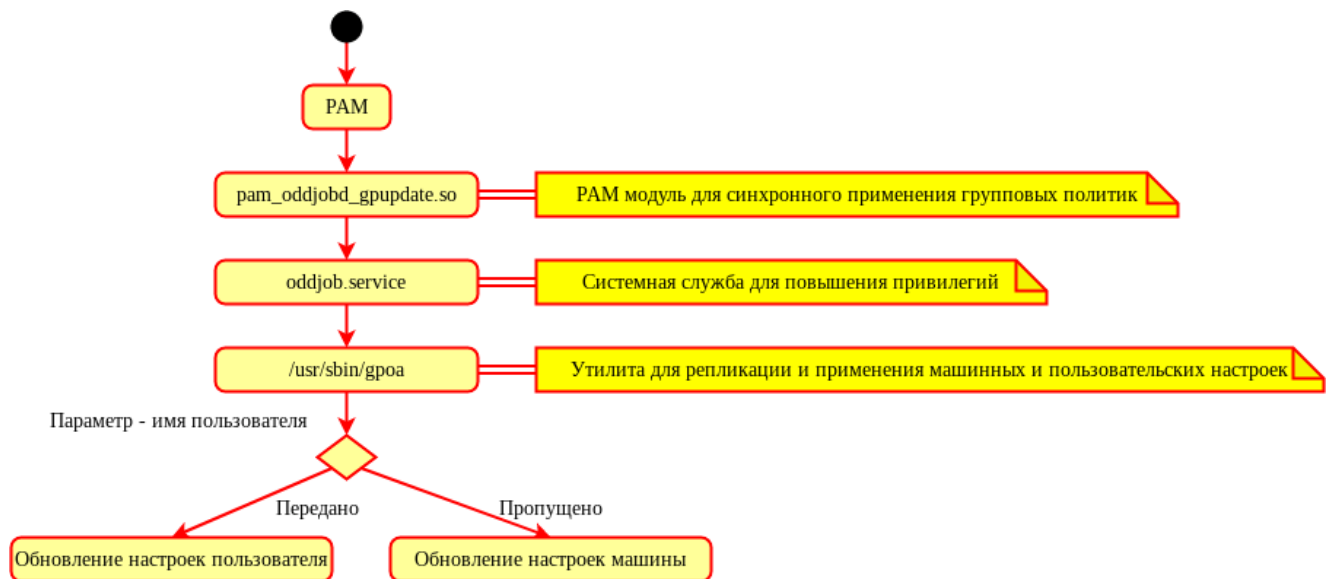


Рис. 39 – Механизм применения групповых политик

Часть проекта, отвечающая за получение и применение групповых политик, внутри использует базу данных («реестр»), для хранения настроек, полученных из различных источников.

4.4.1. Утилиты модуля

Модуль состоит из трех утилит:

- gpoa – системная утилита, осуществляющая применение групповых политик для компьютера или пользователя (gpoa без параметра обрабатывает 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] [--nouupdate] [--noplugins] [--list-backends] [--loglevel LOGLEVEL] [пользователь]
```

Опции команды `gpoa` указаны в таблице 10.

Т а б л и ц а 10 – Опции команды `gpoa`

Ключ	Описание
<code>-h, --help</code>	Вывести справку о команде
<code>--dc DC</code>	Указать полное имя (FQDN) контроллера домена для реплицирования SYSVOL
<code>--nodomain</code>	Работать без домена (применить политику по умолчанию)
<code>--noupdate</code>	Не пытаться обновить хранилище, только запустить <code>appliers</code>
<code>--nopugins</code>	Не запускать плагины
<code>--list-backends</code>	Показать список доступных бэкэндов
<code>--loglevel LOGLEVEL</code>	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] [-s]
```

Опции команды `gpupdate` указаны в таблице 11.

Т а б л и ц а 11 – Опции команды `gpupdate`

Ключ	Описание
<code>-h, --help</code>	Вывести справку о команде
<code>-u USER,</code> <code>--user USER</code>	Имя пользователя для обновления GPO
<code>--target TARGET</code>	Указать политики, которые нужно обновить (пользователя или компьютера). Возможные значения: All (по умолчанию), Computer, User
<code>--loglevel LOGLEVEL</code>	Установить уровень журналирования
<code>-s, --system</code>	Запустить <code>gpupdate</code> в системном режиме

Только root может указать любое имя пользователя для обновления.

Пользователь может выполнять `grpupdate` только для машины или самого себя.

Примеры работы с командой `grpupdate`:

- получить и применить настройки для текущей машины:

```
$ grpupdate --target Computer
Apply group policies for computer.
```

- получить и применить настройки для текущего пользователя:

```
$ grpupdate --target User
Apply group policies for kudrin.
```

- получить и применить настройки для текущего пользователя и машины:

```
$ grpupdate
Apply group policies for kudrin.
```

- попытаться получить настройки для пользователя `ivanov` (с правами пользователя `kim`):

```
$ grpupdate -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 grpupdate для указанного пользователя. Будут
обновлены настройки текущего пользователя.|{'username': 'kim'}
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_grpupdate'}
2024-06-10 17:17:18.119|[D00006]| Запускается GPOA для пользователя
обращением к oddjobd через D-Bus|{'username': 'kim'}
2024-06-10 17:17:37.972|[D00012]| Получен код возврата из
утилиты|{'retcode': dbus.Int32(0)}
Apply group policies for kim.
```

- попытаться получить настройки для пользователя `ivanov` (с правами суперпользователя):

```
# grpupdate -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_grpupdate'}
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.
```


Синтаксис команды `gpupdate-setup`:

`gpupdate-setup [-h]` действие

Опции команды `gpupdate-setup` указаны в таблице 12.

Т а б л и ц а 12 – Опции команды `gpupdate-setup`

Ключ	Описание
<code>list</code>	Показать список доступных типов локальной политики
<code>list-backends</code>	Показать список доступных бэкэндов
<code>status</code>	Показать текущий статус групповой политики (действие по умолчанию)
<code>enable</code>	Включить подсистему групповой политики
<code>disable</code>	Отключить подсистему групповой политики
<code>update</code>	Обновить состояние. Проверяет, в каком состоянии находилась служба <code>gpupdate</code> . В случае, если служба <code>gpupdate</code> запущена, <code>gpupdate-setup</code> также запустит весь перечень служб (например, <code>gpupdate-run-scripts</code>)
<code>write</code>	Операции с групповыми политиками (включить, отключить, указать тип политики по умолчанию)
<code>set-backend</code>	Установить или изменить активную в данный момент серверную часть (бэкэнд)
<code>default-policy</code>	Показать название политики по умолчанию
<code>active-policy</code>	Показать название текущего профиля политики
<code>active-backend</code>	Показать текущий настроенный бэкэнд

Примеры работы с командой `gpupdate-setup`:

- просмотр текущего состояния подсистемы групповых политик:

```
# gpupdate-setup
disabled
```

- включение групповых политик (для включения через ЦУС доступен соответствующий графический модуль управления, а также отметка во время введения машины в домен см. п. 3.3.2.2):

```
# 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
```

- выключение групповых политик:

```
# 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.
```

- вывод списка доступных бэкендов:

```
# gpupdate-setup list-backends
local
samba
```

- включение групповых политик и установка профиля политики по умолчанию server:

```
# gpupdate-setup write enable server
```

По умолчанию, нет необходимости конфигурирования gpupdate. Однако в файле /etc/gpupdate/gpupdate.ini можно указать в явном виде следующие опции:

1) 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);

2) 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 нужно 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
```

4.4.2. 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 ее единообразно на всех клиентах. Формат шаблонов политик, по умолчанию, представляет собой архивный формат политик Samba с дополнительными модификациями. Состав локальной политики может меняться или адаптироваться системным администратором (таблица 13).

Т а б л и ц а 13 – Состав локальной политики

Параметры	Описание	Комментарий
<code>oddjobd.service</code>	Включение <code>oddjobd.service</code> (механизм <code>Systemd</code>)	Нужно для обеспечения возможности запуска <code>gpupdate</code> для пользователя с правами администратора
<code>gpupdate.service</code>	Включение <code>gpupdate.service</code> (механизм <code>Systemd</code>)	Нужно для регулярного обновления настроек машины
<code>sshd.service</code>	Включение <code>sshd.service</code> (механизм <code>Systemd</code>)	Нужно для обеспечения возможности удаленного администрирования
<code>sshd-gssapi-auth</code> , <code>ssh-gssapi-auth</code>	Включение аутентификации с помощью GSSAPI на сервере OpenSSH (механизм <code>Control</code>)	Отвечает за возможность аутентификации в домене при доступе через SSH
<code>sshd-allow-groups</code> , <code>sshd-allow-groups-list</code>	Ограничение аутентификации на сервере OpenSSH по группам <code>wheel</code> и <code>remote</code> (механизм <code>Control</code>)	Нужно для ограничения доступа при доступе через SSH для всех пользователей домена (только при наличии соответствующей привилегии)

Окончание таблицы 13

Параметры	Описание	Комментарий
system-policy	Применяет групповые политики при логине (механизм Control)	
OpenSSH	Открытие порта 22	Нужно для обеспечения возможности подключения по SSH на машинах при старте Firewall applier

Пример локальной политики (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>

```

Локальную политику рекомендуется править только опытным администраторам.

4.4.3. 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 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-iiid='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-iiid='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='#0000000000000'
foreground-color='#F5F5F5F5E4E4'
palette='#2E2E34343636:#CCCC00000000:#4E4E9A9A0606:#C4C4A0A00000:
#34346565A4A4:#757550507B7B:#060698209A9A:#D3D3D7D7CFCF:#55555757
5353:#EFEF29292929:#8A8AE2E23434:#FCFCE9E94F4F:#72729F9FCFCF:#ADA
D7F7FA8A8:#3434E2E2E2E2:#EEEEEEEEEECEC'
use-theme-colors=false
visible-name='По умолчанию'
```

4.4.4. 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 14).

Т а б л и ц а 14 – 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 PolKit	polkit	Управляет генерацией настроек PolicyKit. Работа с правилами PolicyKit ведется методом генерации файлов .rules
Управление настройками 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 веб-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 веб-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.Браузер	yandex_browser	Генерирует файл политики для Яндекс.Браузера (policies.json). Данные настройки устанавливаются из ADMX-файлов для Яндекс.Браузера. Может быть вызван только машинной политикой.

Продолжение таблицы 14

Расширение клиентской стороны	Модуль	Описание
Управление ярлыками запуска программ	shortcuts	Управляет .desktop файлами (создание/удаление/замена)
Управление ярлыками запуска программ	shortcuts_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)
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	inifiles	Управляет INI-файлами (создание/удаление/пересоздание)
Управление INI-файлами	inifiles_user	Управляет INI-файлами в контексте пользователя
Управление переменными среды	envar	Управляет переменными среды
Управление переменными среды	envar_user	Управляет переменными среды в контексте пользователя
Управление общими каталогами	networkshares	Управляет общими каталогами
Управление общими каталогами	networkshares_user	Управляет общими каталогами в контексте пользователя
Управление общими каталогами	networkshares	Управляет общими каталогами
Управление общими каталогами	networkshares_user	Управляет общими каталогами в контексте пользователя

Окончание таблицы 14

Расширение клиентской стороны	Модуль	Описание
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
Управление logon-скриптами	scripts_user	Управление скриптами в контексте пользователя

Модель групповых политик вызывает Applier отвечающие за внесение изменений, согласно параметрам политики. Для выполнения настроек, указанных в параметрах групповой политики, расширения клиентской стороны изменяют конкретные параметры операционной системы. Изменения, внесенные в операционную систему при помощи модуля групповых политик, записываются в журналы событий.

4.4.5. Периодичность запуска групповых политик

Каждый фронтенд срабатывает на определенные ветки настроек. Запуск фронтенда для машины по умолчанию производится раз в час средством `Systemd – gupdate.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 – gupdate-user.timer`.

Для мониторинга и контроля времени выполнения службы `gupdate.service` используются системный таймер `gupdate.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=1
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 в файле /usr/lib/systemd/user/gpupdate-user.timer значение параметра OnUnitActiveSec:

```
[Unit]
Description=Run gpupdate-user every hour

[Timer]
OnStartupSec=1
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, внесенные 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. п. 4.6.5.10).

Просмотреть список запущенных системных таймеров можно, выполнив команду:

```
$ systemctl list-timers
```

Просмотреть список запущенных пользовательских таймеров можно, выполнив команду:

```
$ systemctl --user list-timers
```

4.5. Модуль удаленного управления базой данных конфигурации (ADMC)

Компонент удаленного управления базой данных конфигурации (далее – ADCM) предназначен для управления:

- объектами в домене (пользователями, группами, компьютерами, подразделениями);
- групповыми политиками.

ADMC позволяет:

- создавать и администрировать учетные записи пользователей, компьютеров и групп;
- менять пароли пользователя;
- создавать организационные подразделения, для структурирования и выстраивания иерархической системы распределения учетных записей в домене;
- 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.

4.5.1. Запуск ADMC

Запуск ADMC осуществляется из меню запуска приложений: пункт «Системные» → «ADMC» или из командной строки (команда `admc`).

Примечание. Для использования ADMC нужно предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

```
$ kinit administrator
```

4.5.2. Интерфейс ADMC

Интерфейс ADMC приведен на рис. 40.

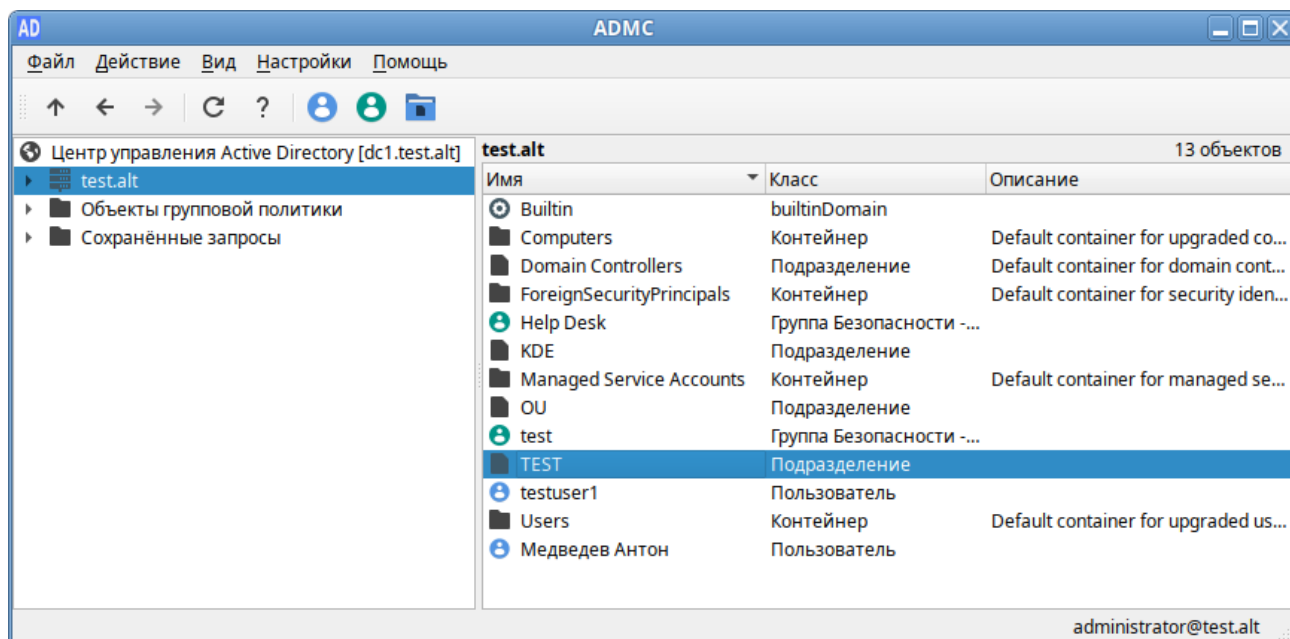


Рис. 40 – Интерфейс ADMC

Включить/выключить отображение панелей можно, отметив соответствующий пункт в меню «Вид» (рис. 41).

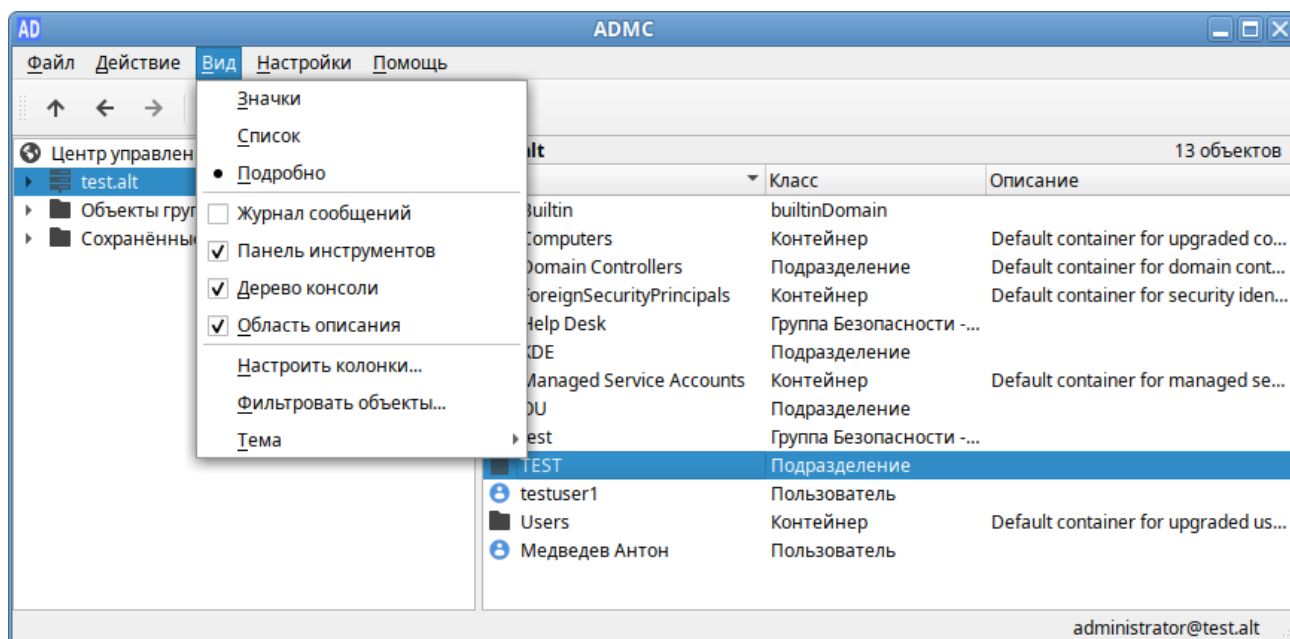


Рис. 41 – Включение/выключение отображения панелей

В панели «Журнала сообщений» отображаются сообщения о статусе приложения. Эти сообщения содержат отчеты обо всех выполненных действиях над объектами (рис. 42).

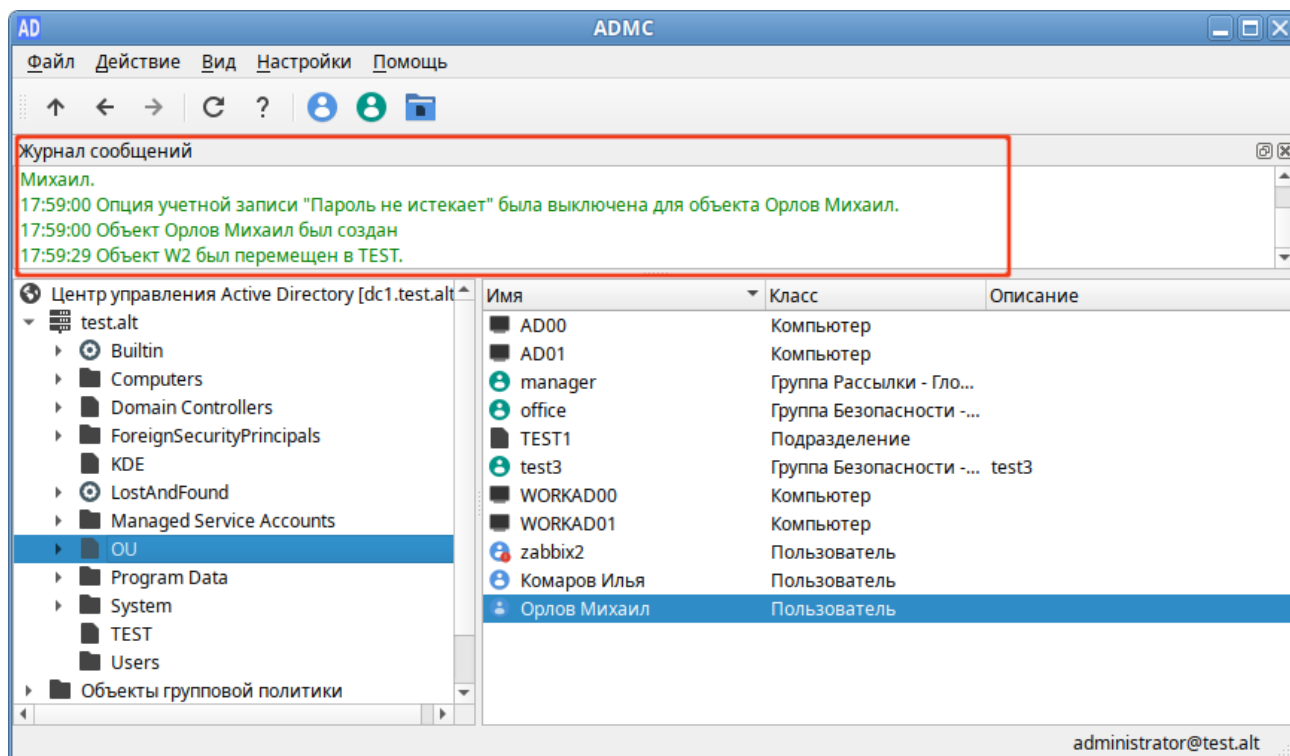


Рис. 42 – Панель «Журнал сообщений»

«Панель инструментов» содержит кнопки для быстрого запуска некоторых действий (рис. 43).

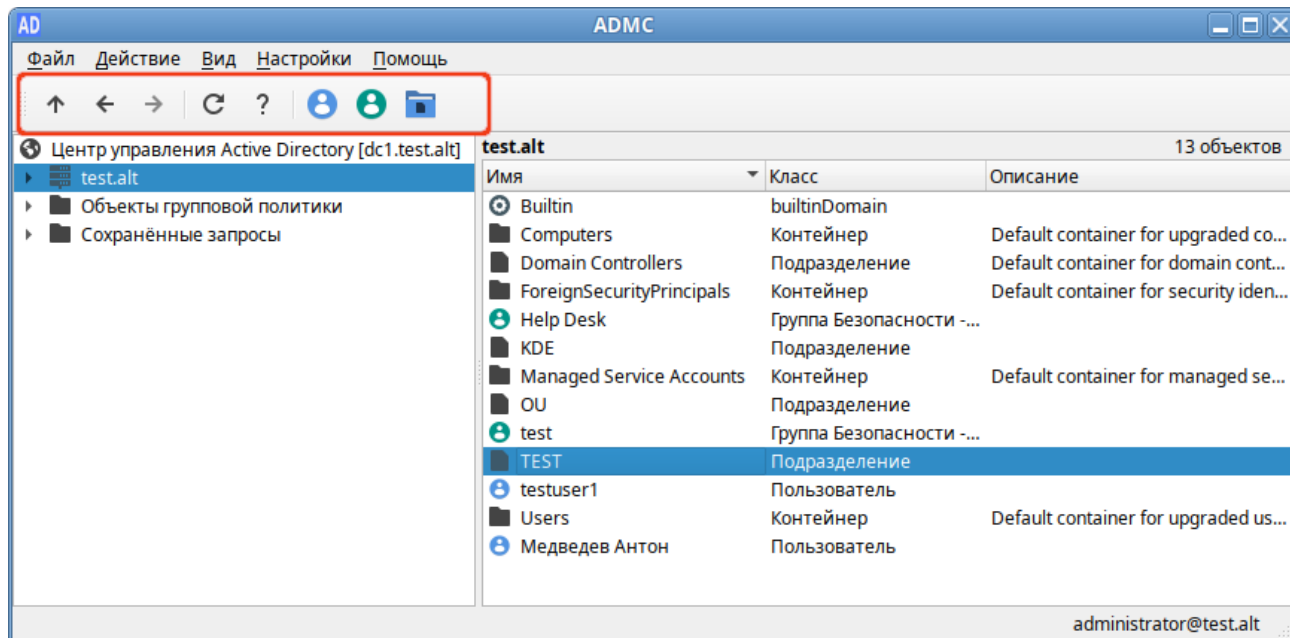


Рис. 43 – «Панель инструментов»

Панель дерева объектов домена («Дерево консоли») отображается слева, в правой панели будут отображаться сведения о выбранном объекте. По умолчанию в дереве отображаются объекты типа «контейнер» (рис. 44).

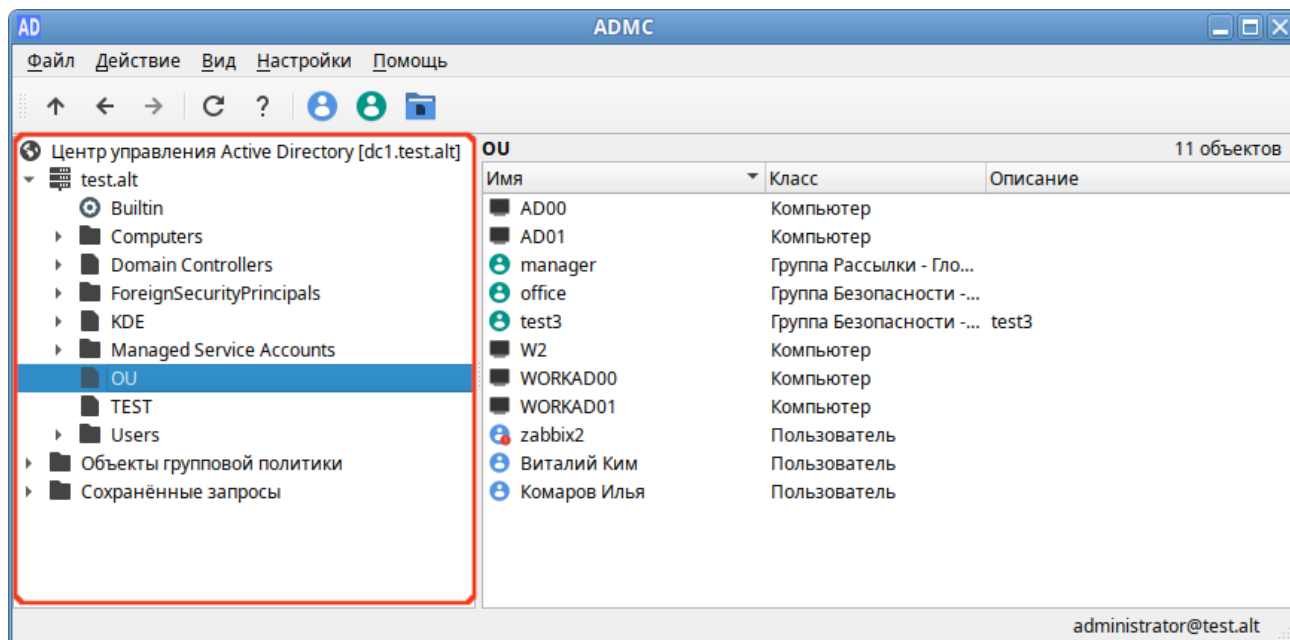


Рис. 44 – Панель «Дерево консоли»

В области описания отображается название контейнера и количество объектов в контейнере (рис. 45).

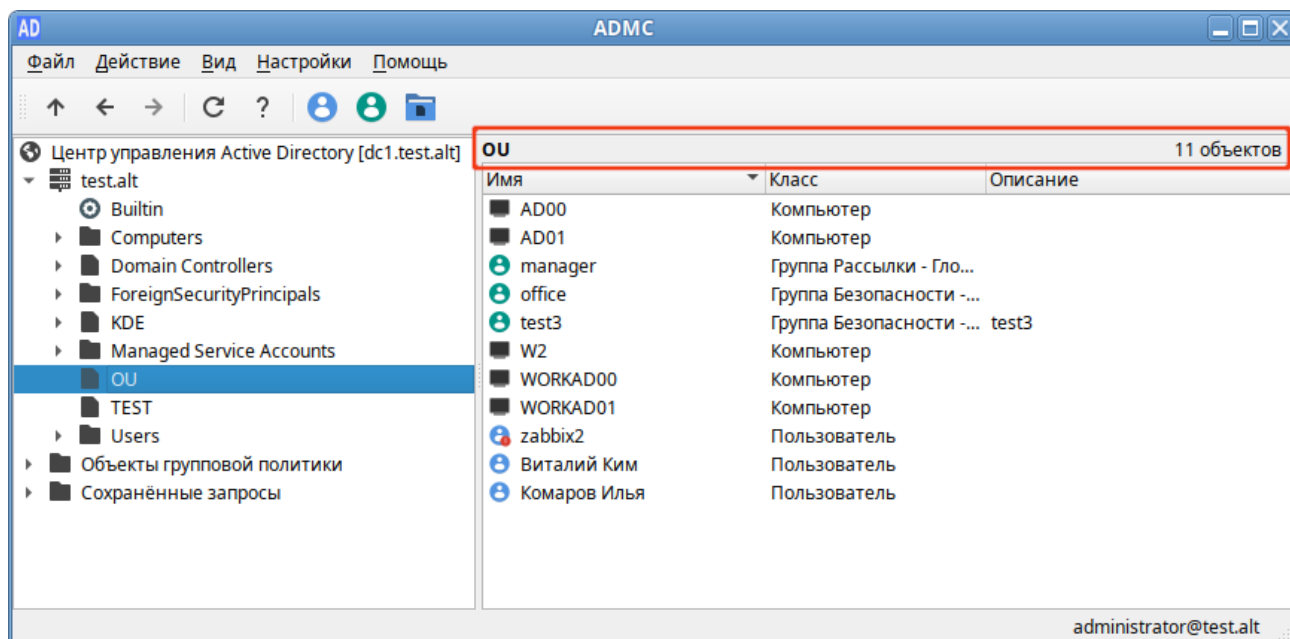


Рис. 45 – Панель «Область описания»

В меню «Вид» → «Тема» можно выбрать тему значков (рис. 46).

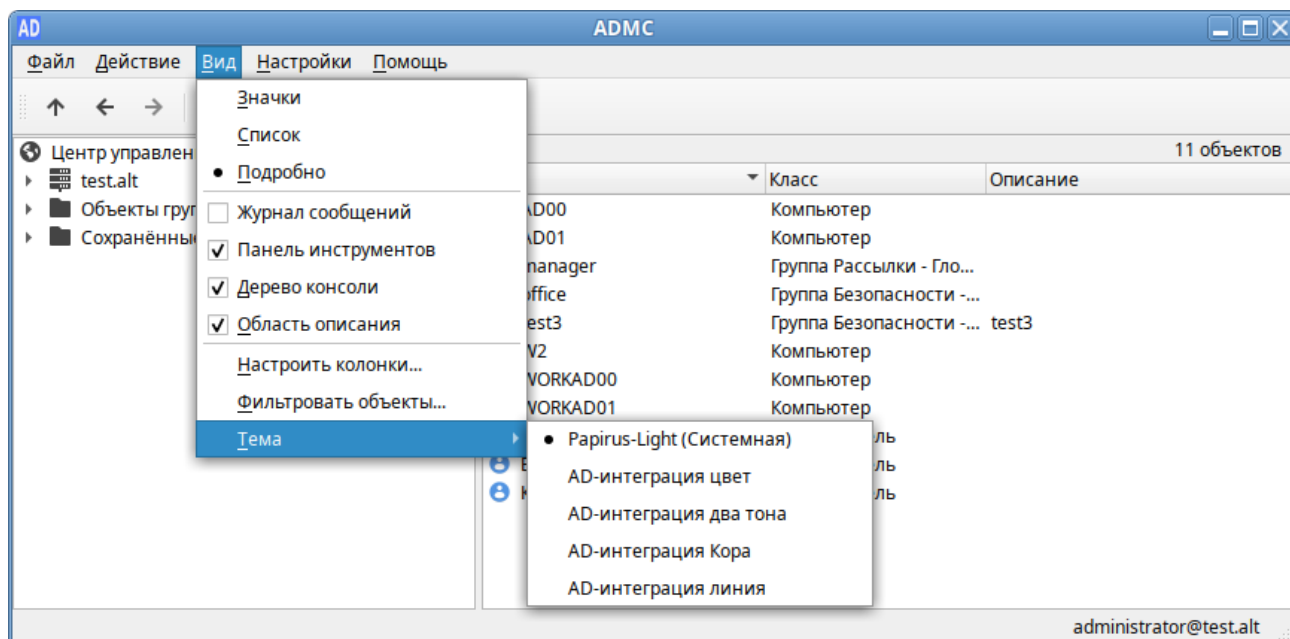


Рис. 46 – Выбор темы

Системная тема берется 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 (рис. 47).

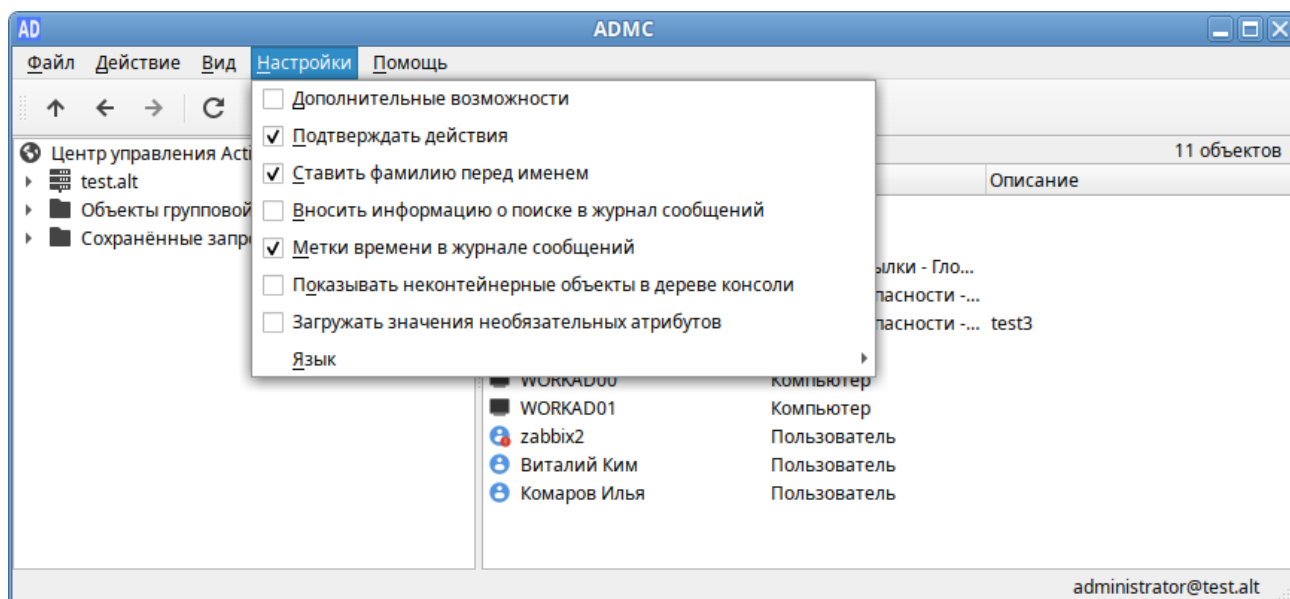


Рис. 47 – Меню «Настройки»

Если отмечен пункт «Дополнительные возможности», будут показаны расширенные объекты и элементы приложения.

Если отмечен пункт «Подтверждать действия», при выполнении потенциально опасных действий будет выводиться окно «Подтвердить действие», например, при удалении объекта (рис. 48).

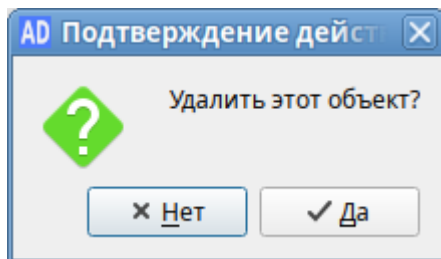


Рис. 48 – Окно «Подтвердить действие»

Другие параметры программы:

- «Ставить фамилию перед именем» – изменить формат полного имени (поле «сн») 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, учетные записи пользователей и компьютерные учетные записи) в панели дерева объектов домена;
- «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 (рис. 49): дерево с сайтами, контроллерами домена и ролями FSMO (рис. 50). Данный виджет также содержит версию контроллера домена, количество сайтов и контроллеров домена, режимы работы домена и леса, версию схемы домена.

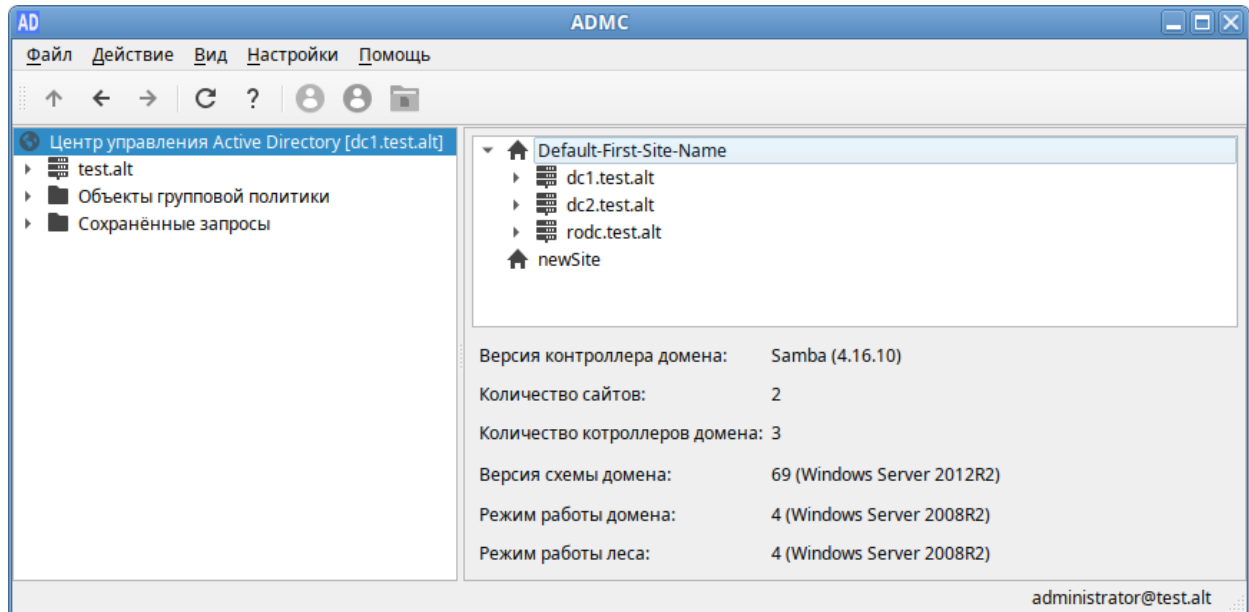


Рис. 49 – Информация о домене

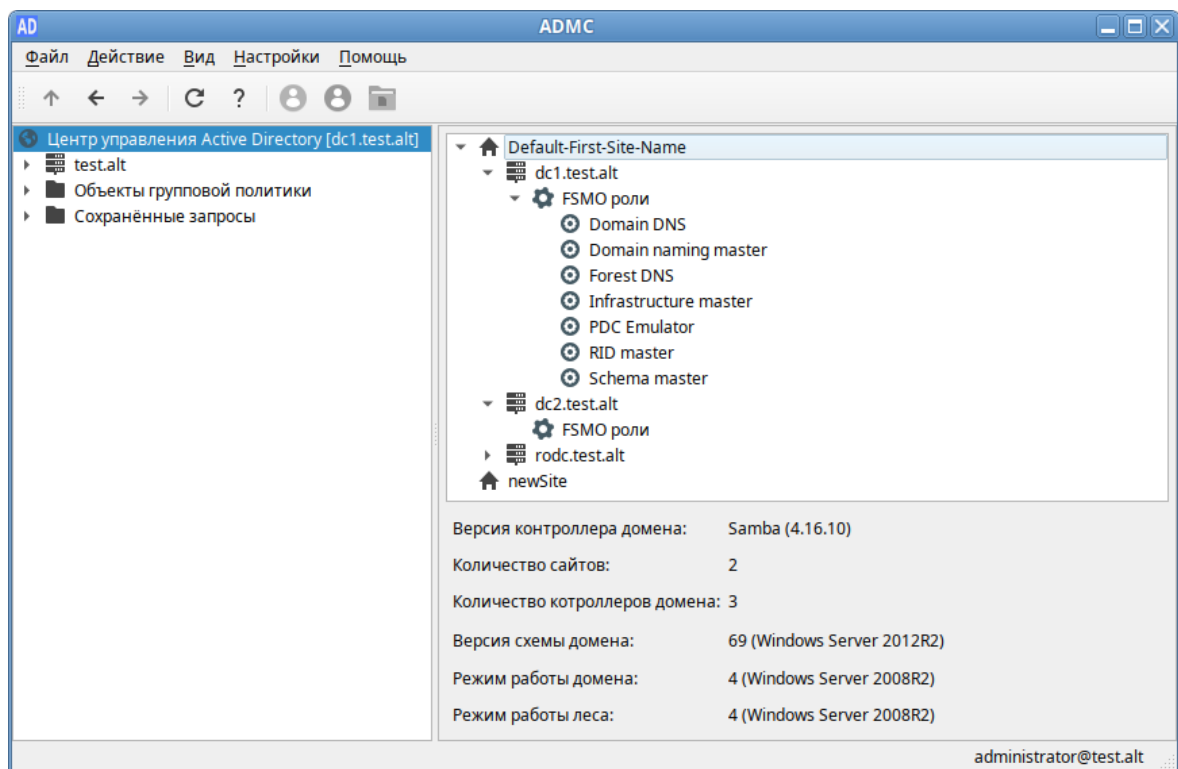


Рис. 50 – Роли FSMO

Меню операций с объектом открывается из строки меню (пункт «Действие») после выбора объекта (рис. 51) или в контекстном меню объекта (рис. 52).

Меню операций содержит действия применимые к выделенному объекту.

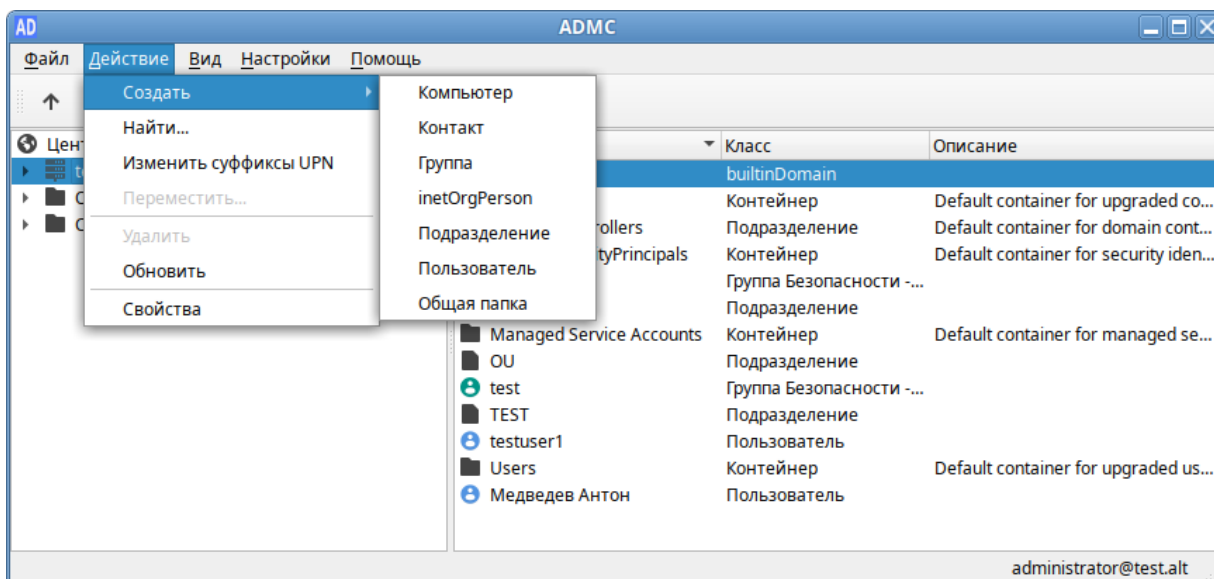


Рис. 51 – Пункт «Действие»

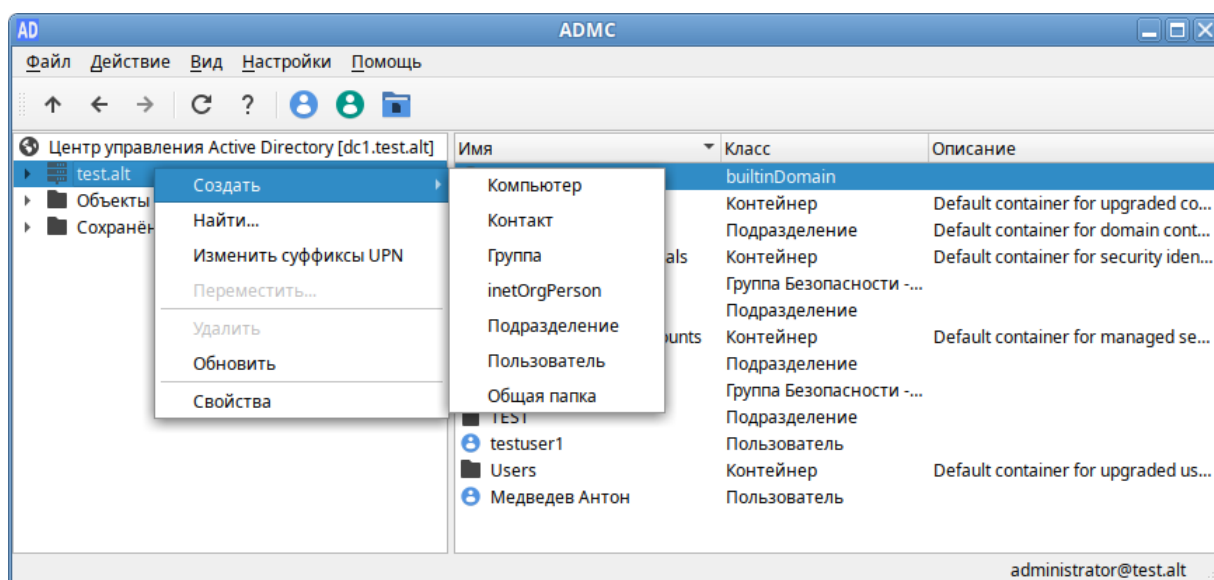


Рис. 52 – Контекстное меню объекта

4.5.3. 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 (рис. 53).

По умолчанию отображается вкладка «Общее». Назначение каждой группы параметров приведено в таблице 15.

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 учетной записи любого объекта домена. В качестве значений параметров указаны названия соответствующих им полей в домене (таблица 16).

Рис. 53 – Окно «Учетная запись пользователя – Свойства»

Т а б л и ц а 15 – Назначение вкладок окна «Свойства учетной записи пользователя»

Вкладка	Описание	Расширенный режим
Общее	Основная вкладка, содержащая информацию, идентифицирующую личность пользователя, которой соответствует данная учетная запись	-
Учетная запись	Характеристики учетной 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	-
Атрибуты	Список атрибутов объекта	+
Объект	Информация об объекте	+
Делегирование		-
Безопасность	Права доступа к объекту	+

Т а б л и ц а 16 – 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 суммы значений трех параметров: First Name, Initials и Last Name	displayName	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 учетной 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
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 (рис. 54).

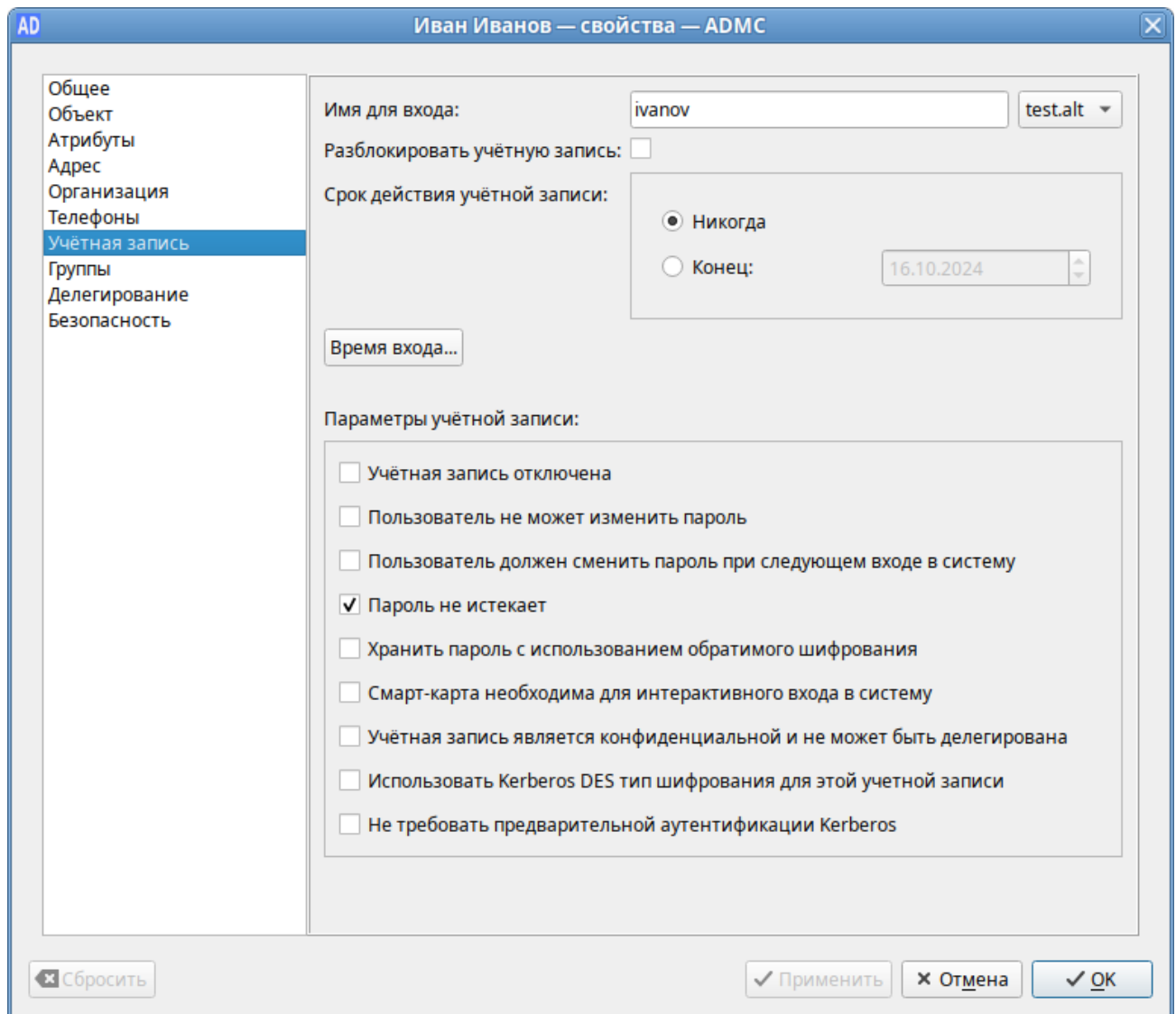


Рис. 54 – Вкладка «Учетная запись»

Соответствие параметров на вкладке «Учетная запись» полям в AD приведено в таблице 17.

Т а б л и ц а 17 – 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 учетную запись	Позволяет разблокировать учетную запись пользователя, если она была заблокирована, например, из-за слишком большого количества неудачных попыток входа	userAccountControl = 16	Целое число
Срок действия учетной записи	Дата отключения учетной записи (по умолчанию «Никогда» – неограниченный срок действия). Если нужно задать дату окончания срока действия учетной 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 учетной записи никогда не истечет	userAccountControl = 0x10000 (65536)	Целое число
Хранить пароль с использованием обратимого шифрования (ENCRYPTED_TEXT_PWD_A LLOWED)	Для шифрования ключей использовать DES-шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности	userAccountControl = 0x0080 (128)	Целое число

Окончание таблицы 17

Поле на вкладке «Учетная запись»	Примечание	Поле в Active Directory	Тип
Смарт-карта нужна 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 учетной 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

Примечание. userAccountControl – атрибут управления учетной 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 (рис. 55).

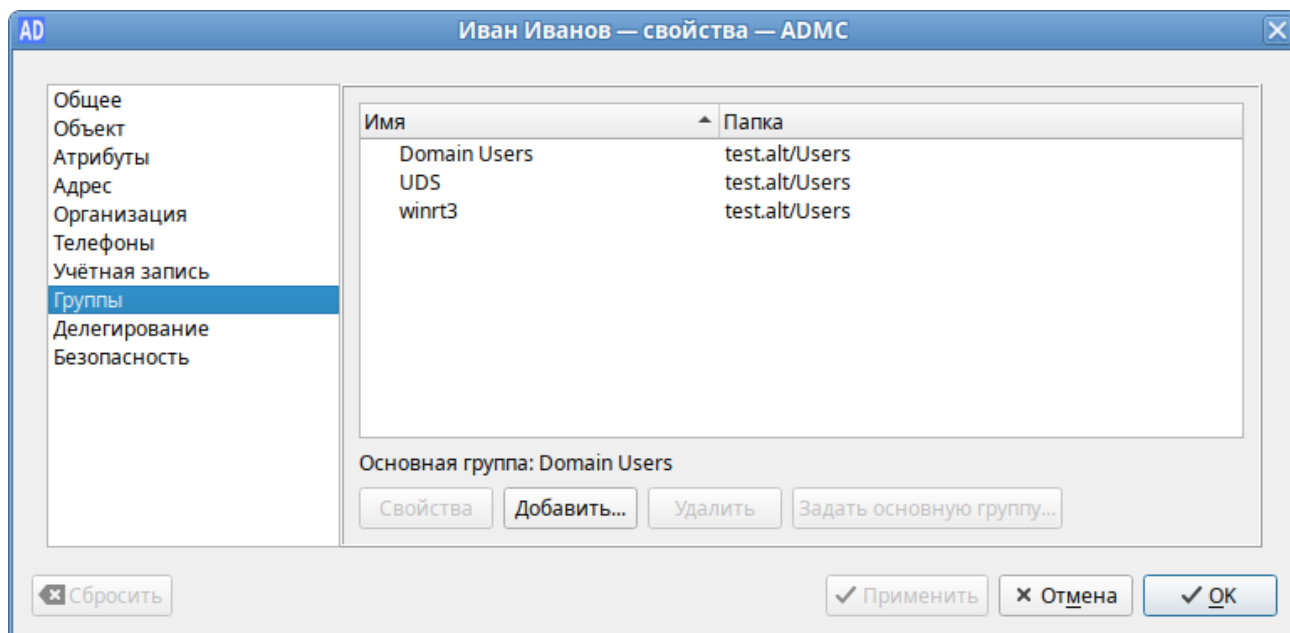


Рис. 55 – Вкладка «Группы»

На вкладке «Делегирование» доступно два параметра (рис. 56):

- «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.

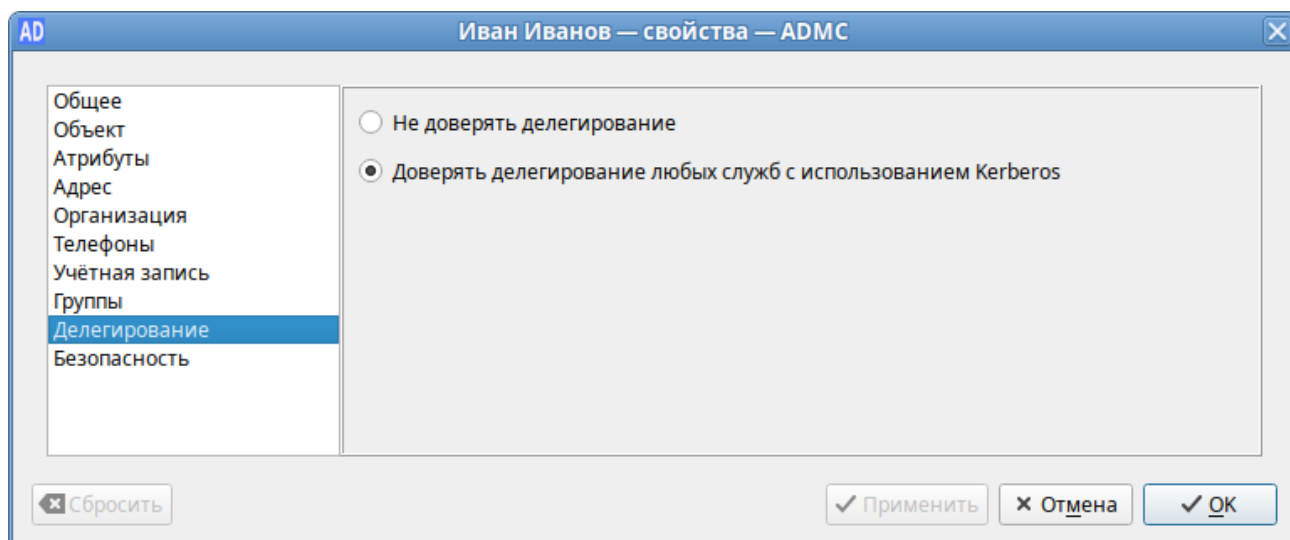


Рис. 56 – Вкладка «Делегирование»

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» (рис. 57).

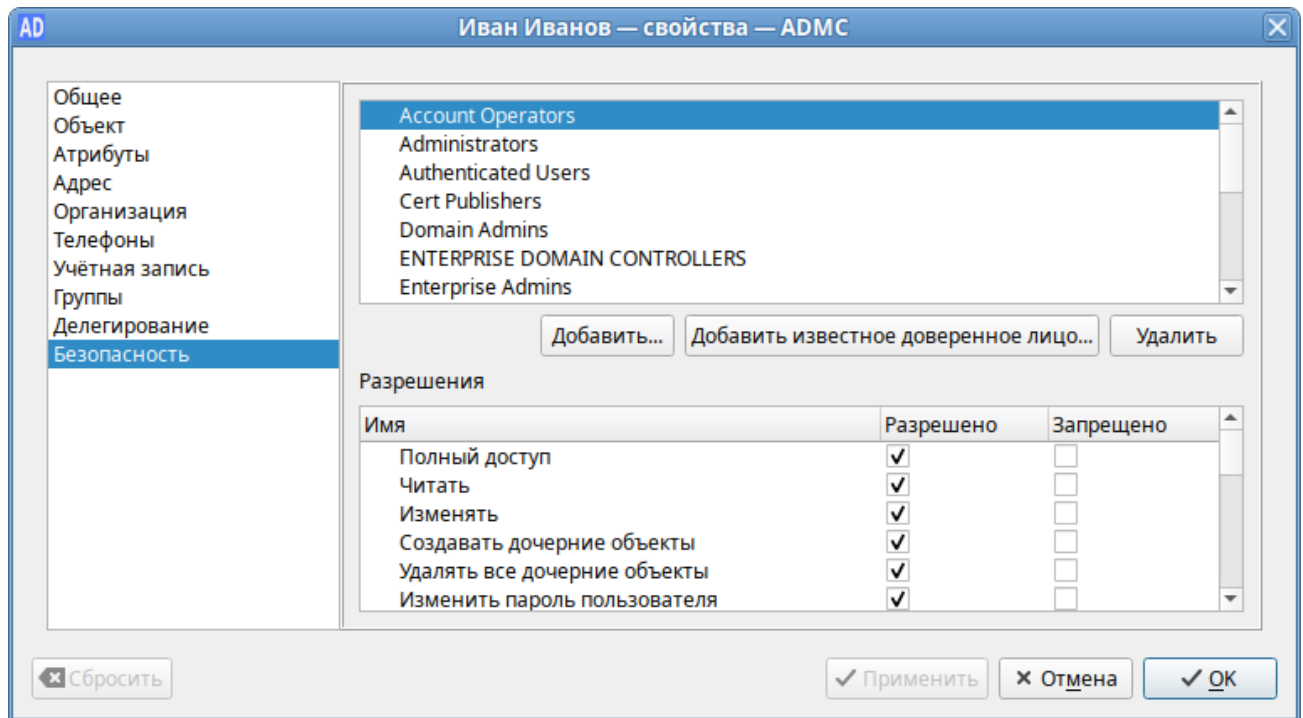


Рис. 57 – Вкладка «Безопасность»

В поле «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» (рис. 58).

Эту вкладку можно использовать для просмотра и редактирования атрибутов, недоступных через другие вкладки окна «Свойства объекта» (например, для просмотра значений неизменяемых атрибутов).

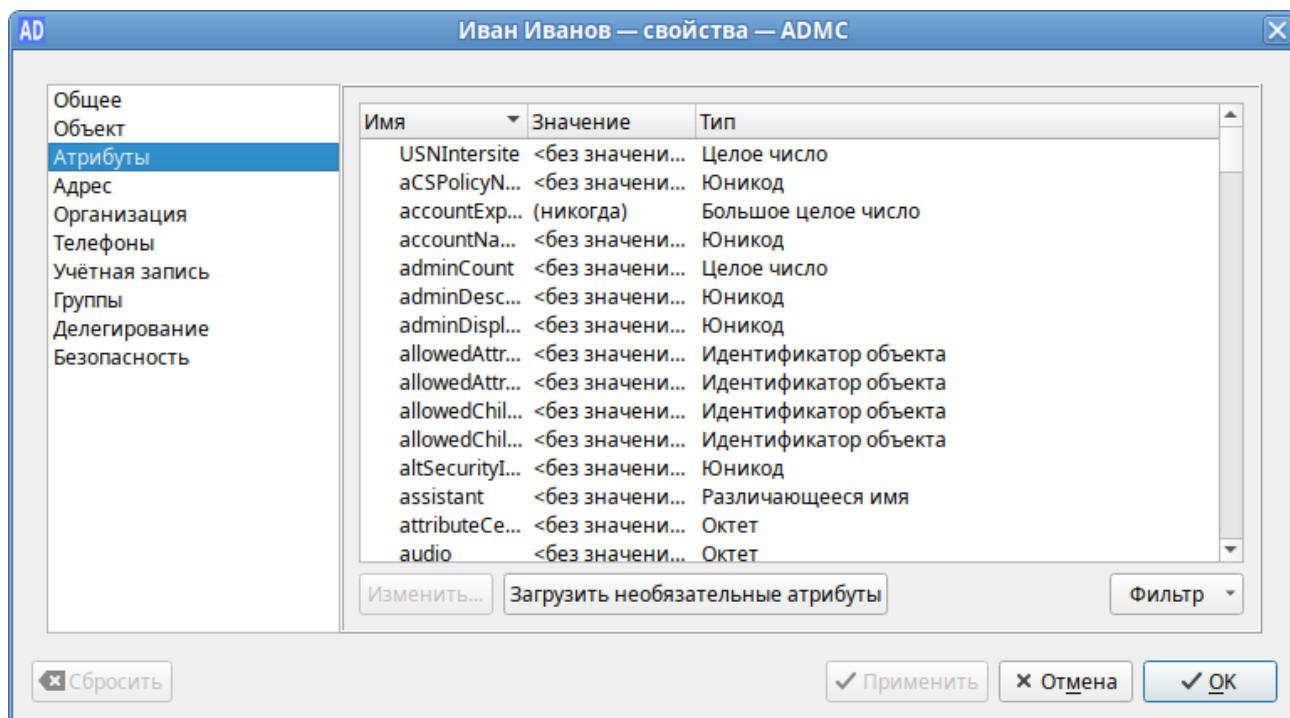


Рис. 58 – Вкладка «Атрибуты»

Содержимое окна редактирования атрибута зависит от типа атрибута (рис. 59, рис. 60).

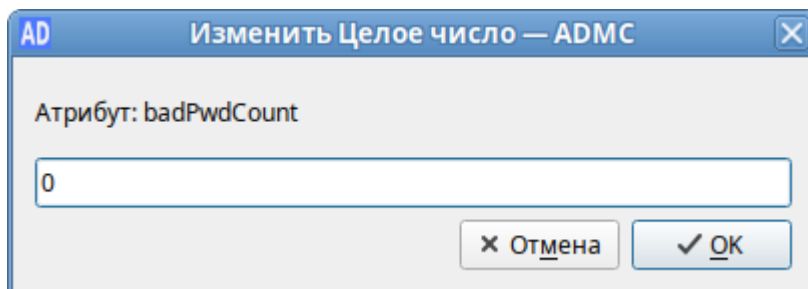


Рис. 59 – Окно редактирования атрибута целого типа

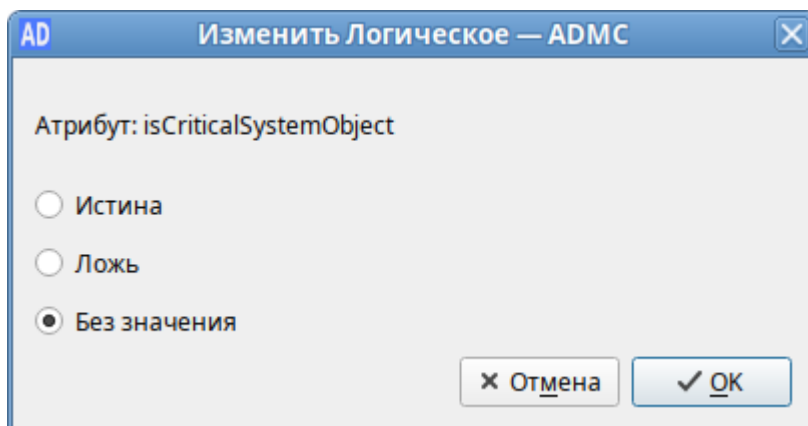


Рис. 60 – Окно редактирования атрибута логического типа

Для большинства атрибутов домена 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) (рис. 61).

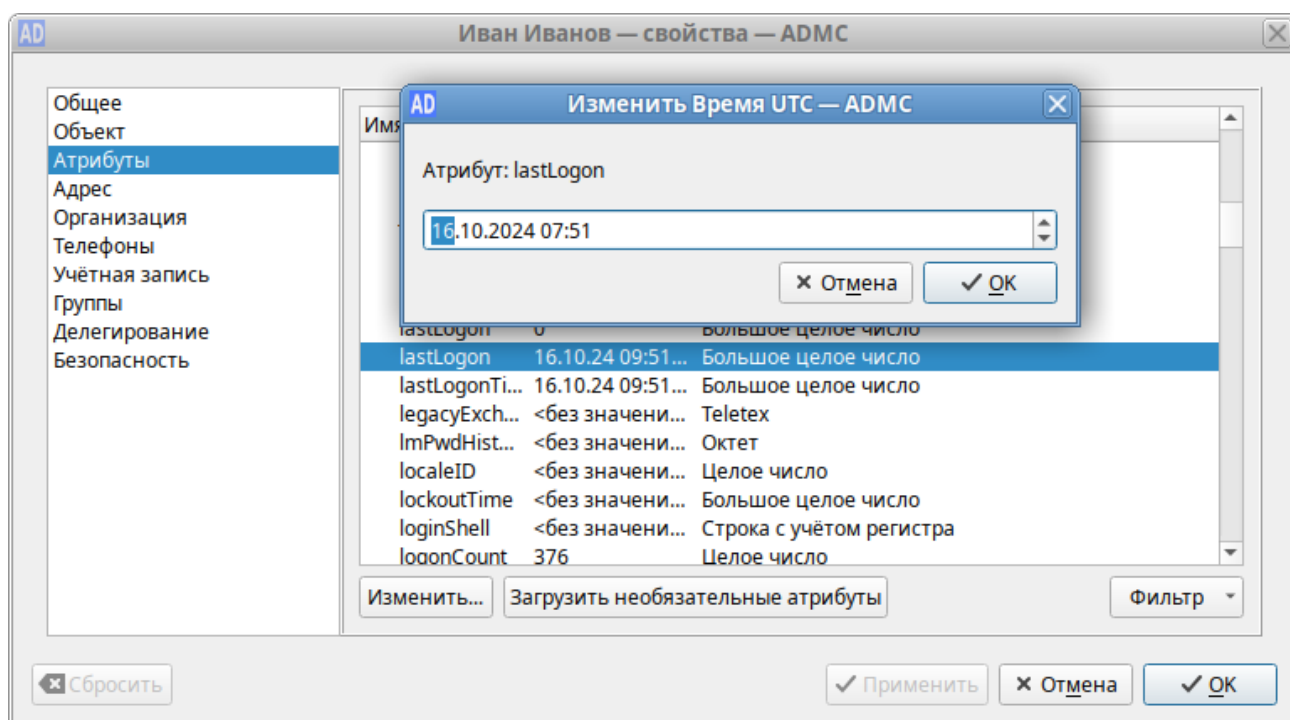


Рис. 61 – Атрибут `lastLogon`

Кнопка «Загрузить необязательные атрибуты» позволяет загрузить значения необязательных атрибутов.

Кнопка «Фильтр» позволяет управлять отображением списка атрибутов (рис. 62):

- «Без значения» – показывать пустые атрибуты;
- «Только для чтения» – показывать все атрибуты, в том числе 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`).

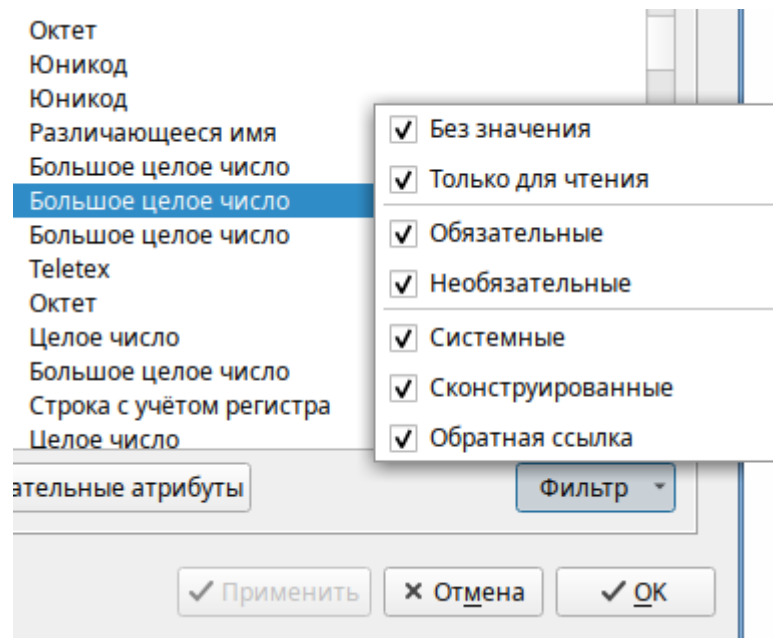


Рис. 62 – Кнопка «Фильтр»

4.5.4. 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 (рис. 63).

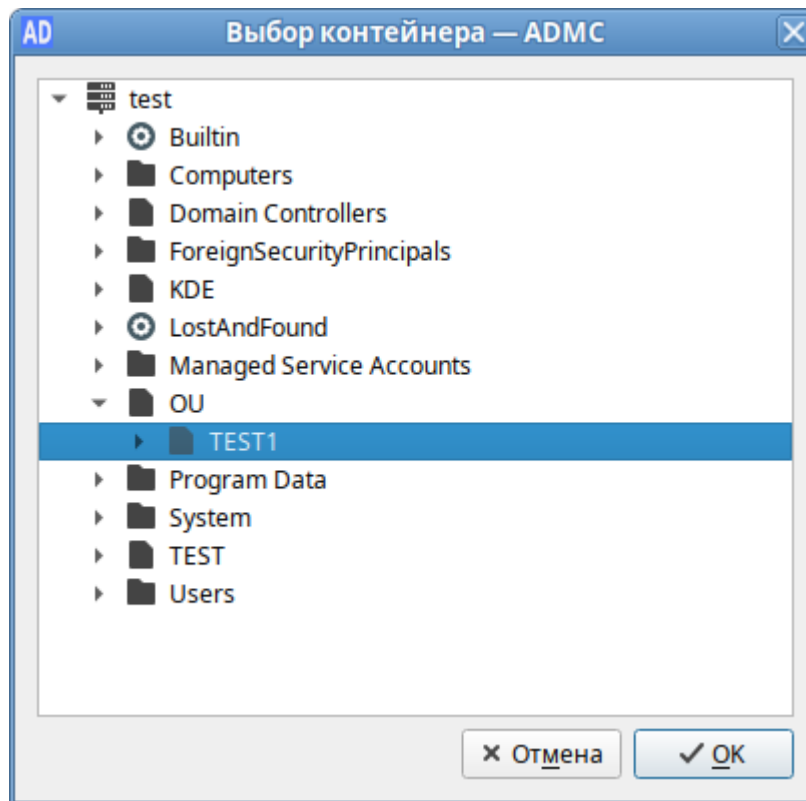


Рис. 63 – Выбор контейнера, в который следует переместить объект

4.5.5. Управление пользователями

Учетная запись пользователя «Альт Домен»:

- удостоверяет личность пользователя;
- разрешает или запрещает доступ к ресурсам домена.

В ADMS предусмотрена возможность создания новых учетных записей пользователей в доменных службах «Альт Домен» и управления существующими учетными записями пользователей.

Примечание. Для доступа к некоторым операциям нужно 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 учетной записи InetOrgPerson в контекстном меню контейнера следует выбрать пункт «Создать» → «inetOrgPerson».

4.5.5.1. Создание учетной записи пользователя

Для создания учетной записи пользователя в контекстном меню контейнера следует выбрать пункт «Создать» → «Пользователь». Окно мастера создания учетной записи пользователя (рис. 64).

AD Создать пользователя — ADMS

Имя: Михаил

Фамилия: Орлов

Полное имя: Орлов Михаил

Инициалы:

Имя для входа: orlov test.alt

Имя для входа (до Windows 2000): TEST\ orlov

Пароль:

Подтвердите пароль:

☐ Показывать пароль

Параметры учётной записи:

- ☒ Пользователь должен сменить пароль при следующем входе в систему
- ☐ Пользователь не может изменить пароль
- ☐ Пароль не истекает
- ☐ Учётная запись отключена

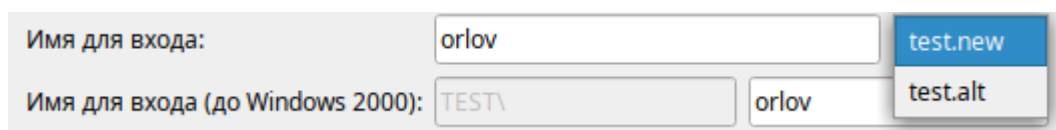
Отмена OK

Рис. 64 – Окно мастера создания учетной записи пользователя

При создании учетной 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 (рис. 65). Список содержит полное имя системы доменных имен (DNS) текущего домена и все альтернативные суффиксы UPN;



The image shows a Windows login dialog box. The 'Имя для входа:' (User name) field contains the text 'orlov'. Below it, the 'Имя для входа (до Windows 2000):' (User name (Windows 2000)) field is active, showing a dropdown menu. The dropdown menu displays 'TEST\' as the selected option, with 'orlov' and 'test.alt' as alternative options.

Рис. 65 – Ввод имени для входа

- «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 учетной записи пользователя не ограничен (по умолчанию срок действия пароля задан атрибутом minPwdAge);
- «Учетная запись отключена» – отключить учетную 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 учетной записи пользователя является DNS имя домена, которое содержит учетную запись пользователя. Для упрощения процессов администрирования и входа пользователя в систему, можно добавить альтернативные суффиксы UPN.

4.5.5.2. Изменение учетной записи пользователя

Для изменения учетной записи пользователя следует в контекстном меню пользователя выбрать соответствующее действие (рис. 66).

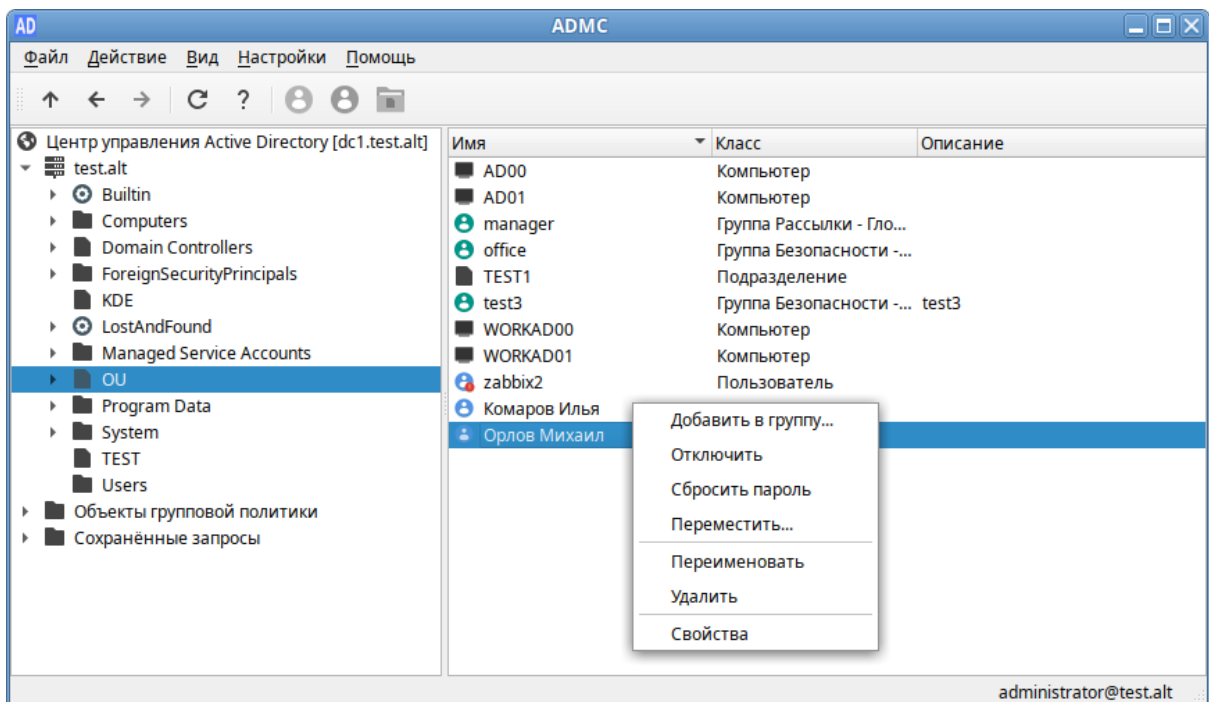


Рис. 66 – Контекстное меню учетной записи пользователя

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 учетную запись пользователя в качестве участника (рис. 67);

3) нажать кнопку «ОК».

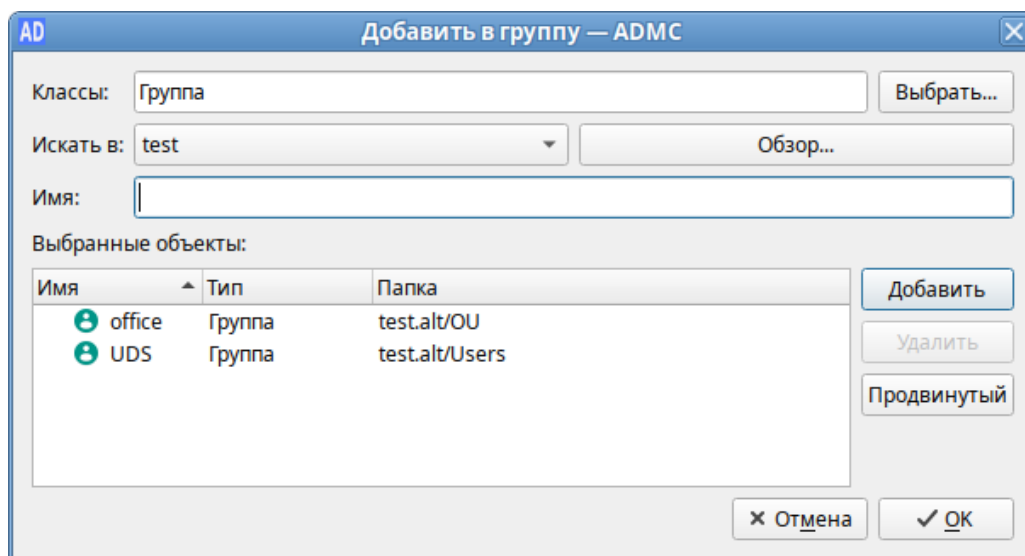


Рис. 67 – Добавление учетной записи пользователя

Для переименования пользователя:

- 1) в контекстном меню пользователя выбрать пункт «Переименовать»;
- 2) в открывшемся окне, если нужно, изменить соответствующие поля (рис. 68);
- 3) нажать кнопку «ОК» для сохранения изменений.

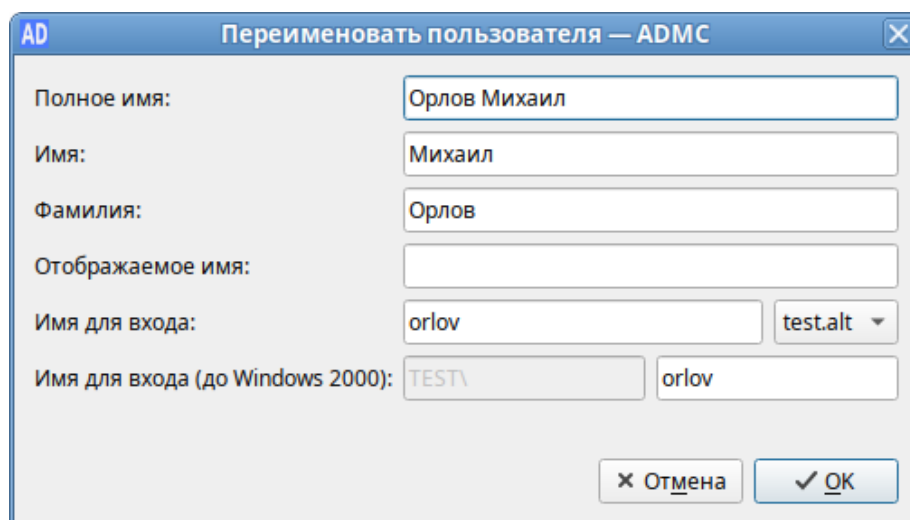


Рис. 68 – Переименование пользователя

Для изменения пароля пользователя:

- 1) в контекстном меню пользователя выбрать пункт «Сбросить пароль»;
- 2) в открывшемся окне ввести новый пароль и подтвердить его (рис. 69);

- 3) если нужно, 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 учетную запись», если нужно разблокировать учетную запись пользователя;
- 5) нажать кнопку «ОК» для сохранения изменений.

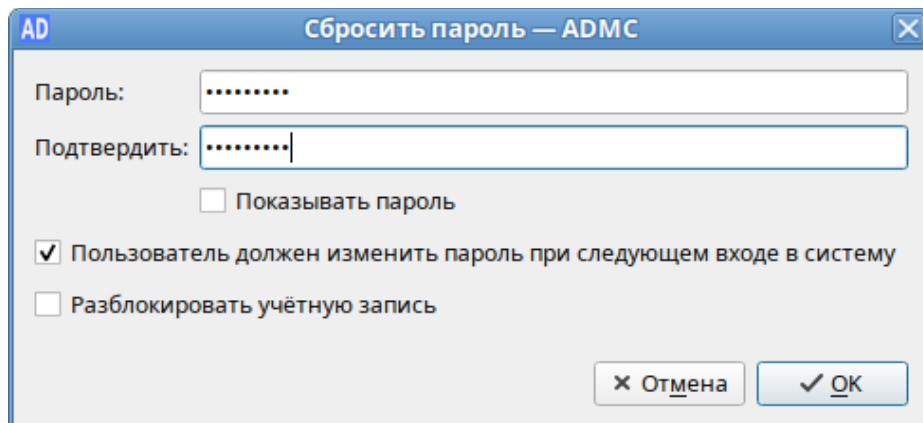


Рис. 69 – Подтверждение пароля

Для перемещения пользователя в другой контейнер:

- 1) в контекстном меню пользователя выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер, в который следует переместить учетную запись пользователя (рис. 63);
- 3) нажать кнопку «ОК».

Для включения/отключения учетной записи пользователя нужно в контекстном меню пользователя выбрать пункт «Отключить» или «Включить» (в зависимости от состояния учетной записи будет доступно одно из этих действий).

Чтобы разблокировать учетную запись пользователя:

- 1) в контекстном меню пользователя выбрать пункт «Свойства»;
- 2) в открывшемся окне на вкладке «Учетная запись» отметить пункт «Разблокировать учетную запись» (рис. 70);
- 3) нажать кнопку «ОК» или «Применить».

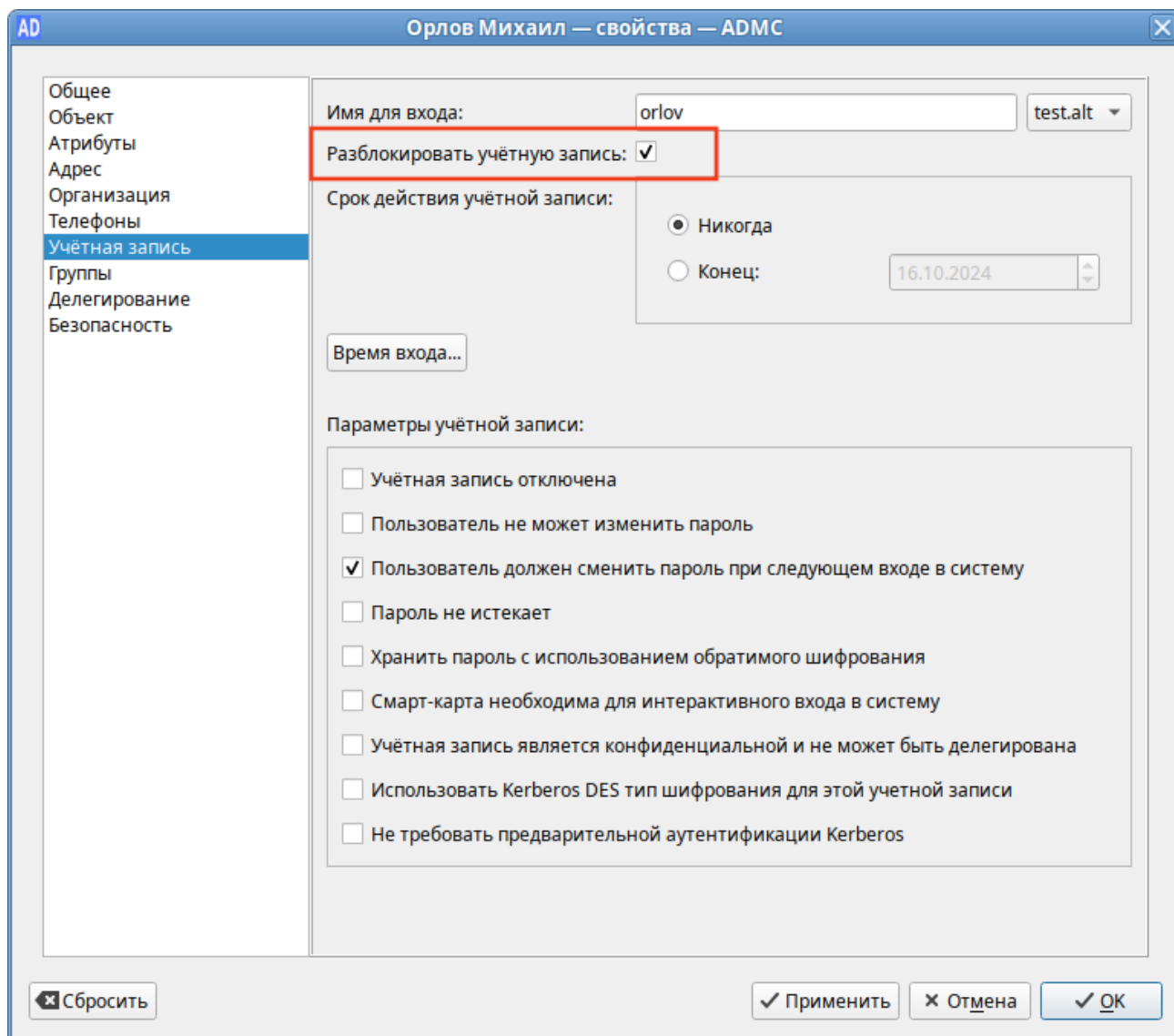


Рис. 70 – Пункт «Разблокировать учетную запись»

Для удаления учетной записи пользователя следует в контекстном меню пользователя выбрать пункт «Удалить».

⚠ Если в настройках ADMS 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» (рис. 71);
- 2) в открывшемся окне на вкладке «Группы» будут отображаться группы, в которые входит данный пользователь.

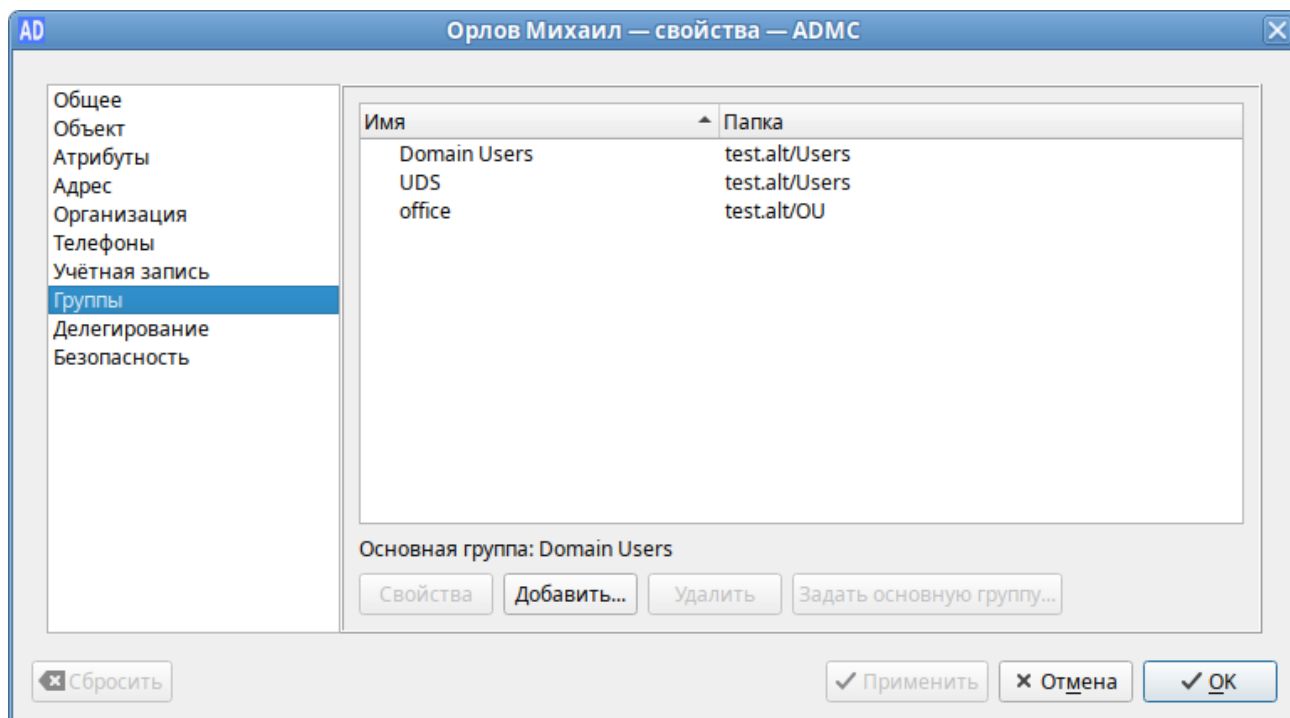


Рис. 71 – Вкладка «Группы»

4.5.6. Управление контактами

Контакт предназначен для хранения информации о пользователях, которым не требуется регистрация в домене.

4.5.6.1. Создание контакта

Для создания контакта в контекстном меню контейнера следует выбрать пункт «Создать» → «Контакт». Окно мастера создания контакта (рис. 72).

The screenshot shows a window titled 'Создать контакт — ADMS'. It contains several text input fields: 'Имя:' with 'Павел', 'Фамилия:' with 'Марков', 'Инициалы:' (empty), 'Полное имя:' with 'Марков Павел', and 'Отображаемое имя:' with 'Марков П.'. At the bottom right are buttons: 'Отмена' and 'ОК'.

Рис. 72 – 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 учетной записи.

4.5.6.2. Изменение свойств контакта

Для изменения учетной записи пользователя следует в контекстном меню контакта выбрать соответствующее действие (рис. 73).

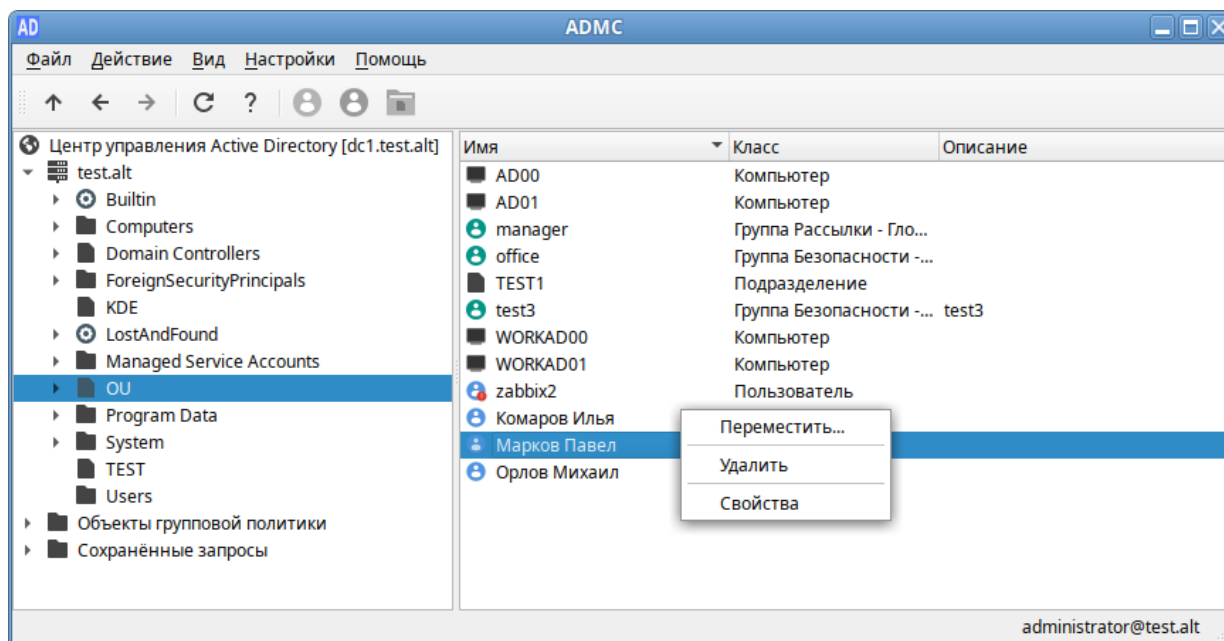


Рис. 73 – Контекстное меню учетной записи контакта

Вкладки «Общие», «Адрес», «Телефоны» и «Организация» в окне «Свойства» контакта идентичны соответствующим вкладкам окна «Свойства» учетной записи пользователя.

На вкладке «Группы» можно, по аналогии с учетными записями пользователей, указать, членом каких групп является контакт. Возможность членства в группах не дает 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.

4.5.7. Управление группами

Группа состоит из учетных записей пользователей и компьютеров, контактов и других групп и может управляться как единое целое. Пользователи и компьютеры, входящие в определенную 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).

4.5.7.1. Создание группы

Для создания группы следует в контекстном меню контейнера выбрать пункт «Создать» → «Группа». Окно мастера создания группы (рис. 74).

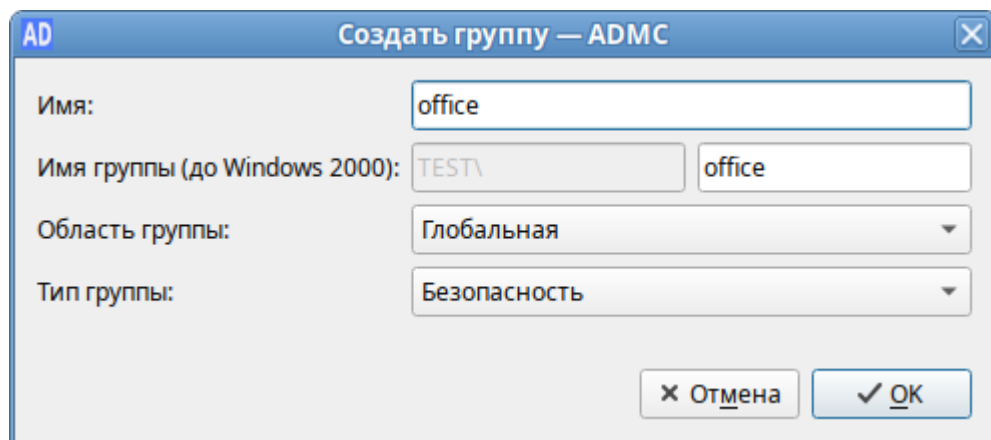


Рис. 74 – Окно мастера создания группы

При создании группы можно указать следующие параметры (атрибуты):

- 1) «Имя» – название группы;
- 2) «Имя группы (до Windows 2000)» – название группы для старых систем (пред-Windows 2000);
- 3) «Область группы» – область действия группы:
 - «Глобальная» – членами глобальной группы могут быть другие группы и учетные 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 учетные записи из любого домена дерева доменов или леса. Членам такой группы разрешения могут назначаться в любом домене дерева доменов или леса;

4) «Тип группы» – тип группы:

- «Безопасность» – используется для назначения разрешений доступа к общим ресурсам;
- «Рассылка» – используется для создания списков рассылки электронной почты.

4.5.7.2. Изменение группы

Для изменения группы следует в контекстном меню группы выбрать соответствующее действие (рис. 75).

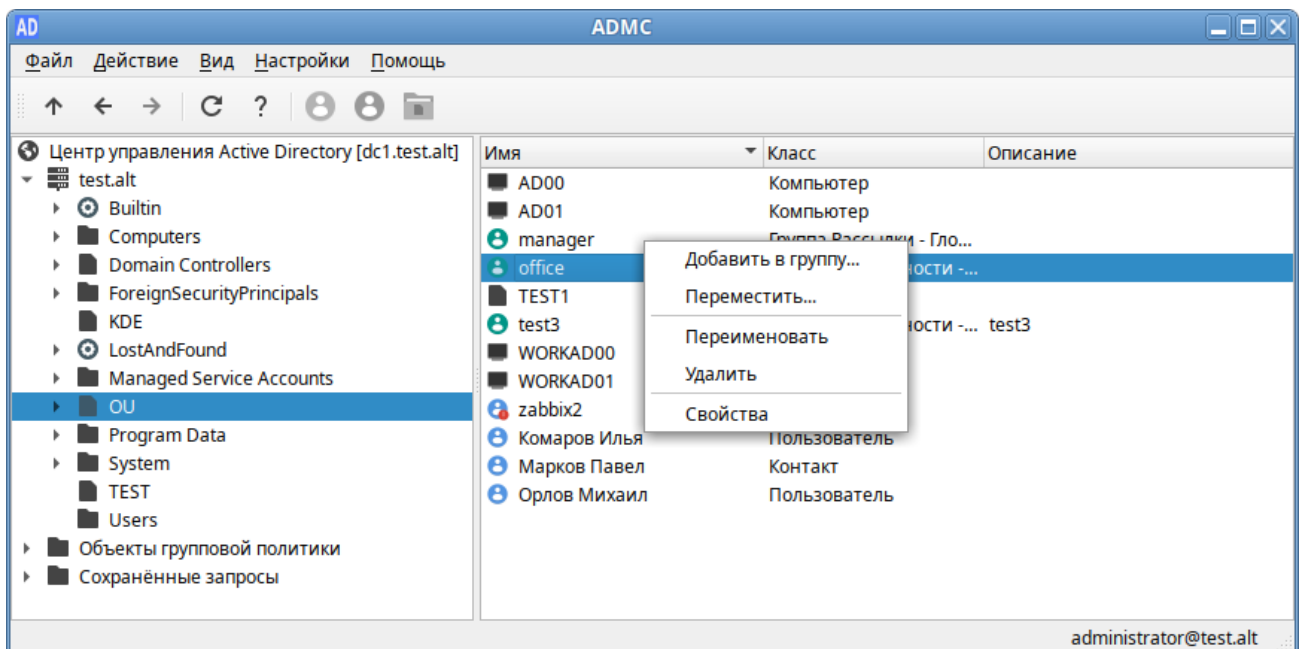


Рис. 75 – Контекстное меню группы

Для добавления группы в другую группу:

- 1) в контекстном меню группы выбрать пункт «Добавить в группу...»;

- 2) в открывшемся окне (рис. 76) выбрать группы, в которые следует добавить данную группу в качестве участника;
- 3) нажать кнопку «ОК».

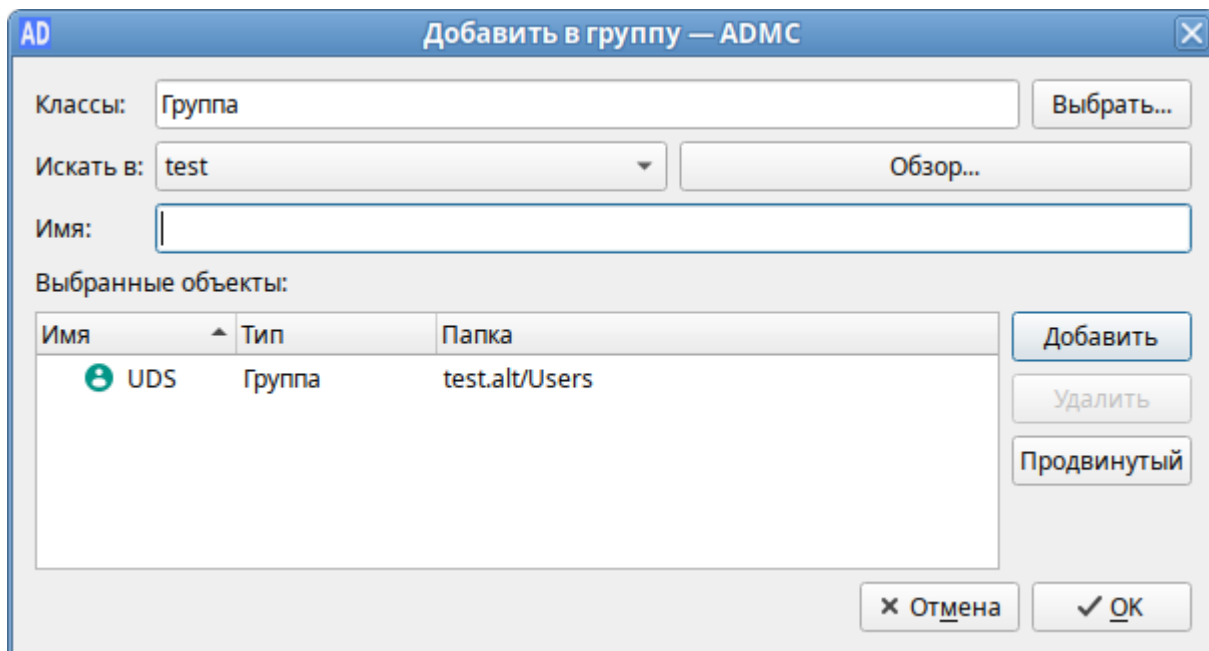


Рис. 76 – Добавление группы в другую группу

Для перемещения группы в другой контейнер:

- 1) в контекстном меню группы выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер (рис. 63), в который следует переместить группу;
- 3) нажать кнопку «ОК».

Для переименования группы:

- 4) в контекстном меню группы выбрать пункт «Переименовать»;
- 5) в открывшемся окне (рис. 77), если нужно, изменить соответствующие поля;
- 6) нажать кнопку «ОК» для сохранения изменений.

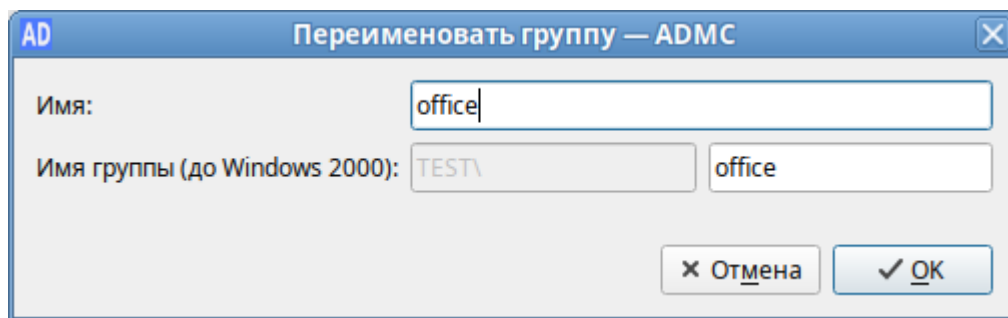


Рис. 77 – Переименование группы

Для удаления группы следует в контекстном меню группы выбрать пункт «Удалить».

⚠ Если в настройках ADMS 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...» (рис. 78);

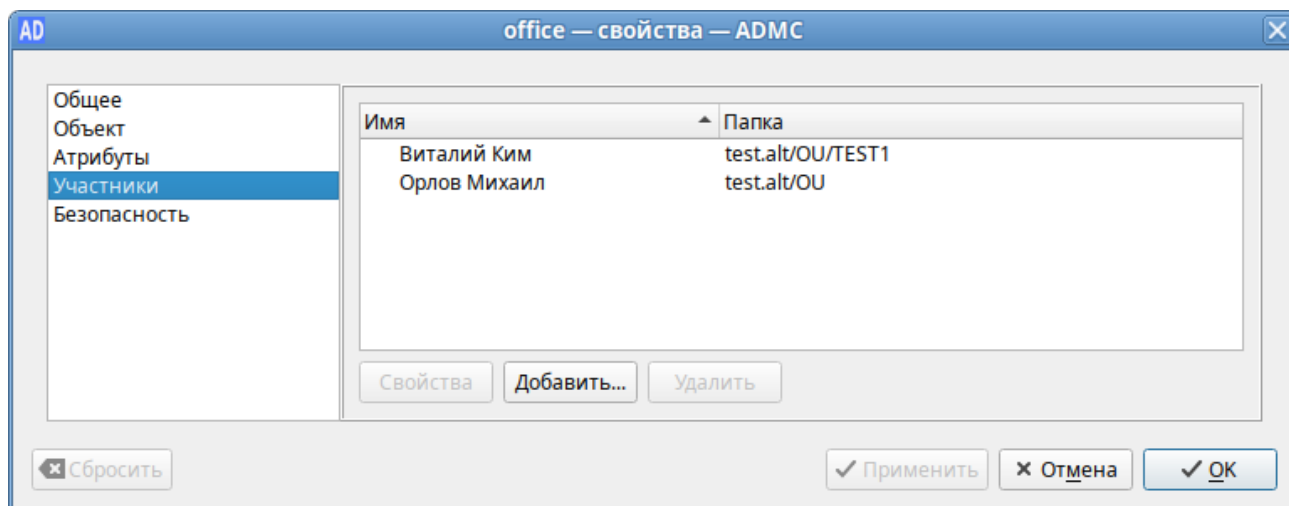


Рис. 78 – Добавление участников в группу

- 3) выбрать объекты, которые нужно добавить в группу (рис. 79);
- 4) нажать кнопку «ОК»;
- 5) нажать кнопку «ОК» или «Применить» для сохранения изменений.

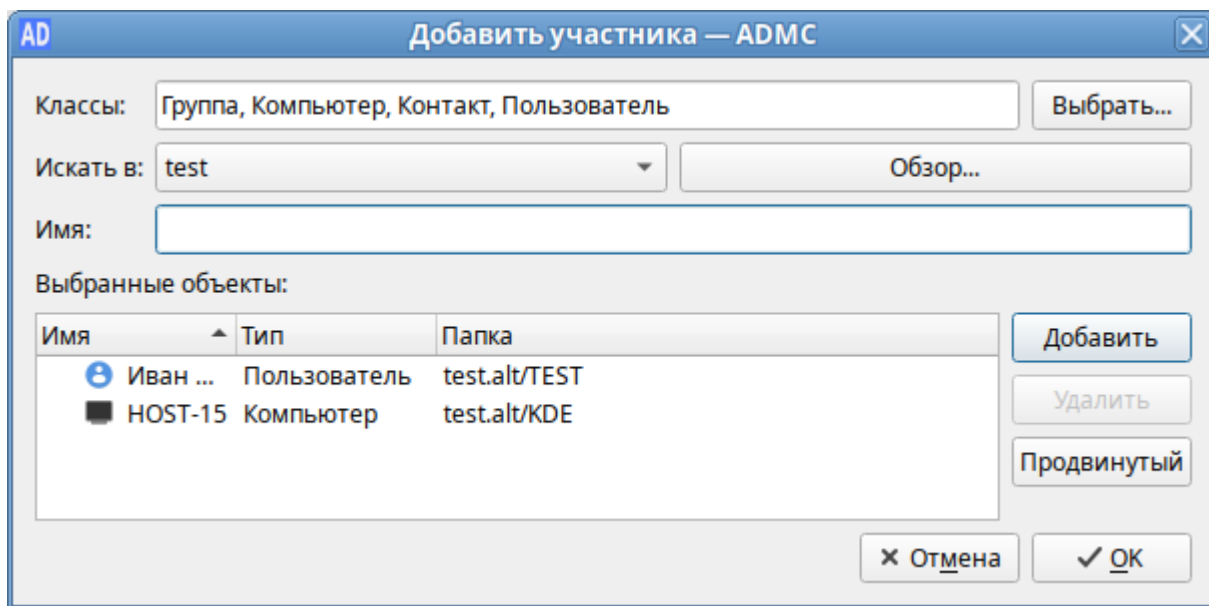


Рис. 79 – Выбор объектов, которые нужно добавить в группу

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 (рис. 80);
- 3) нажать кнопку «ОК» или «Применить» для сохранения изменений.

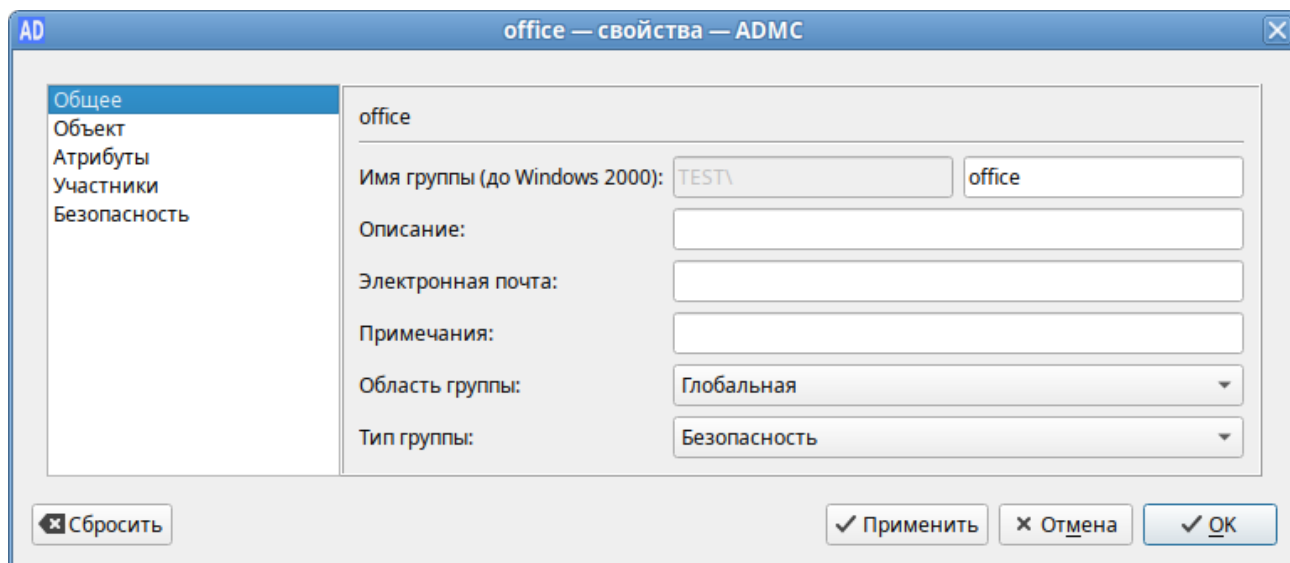


Рис. 80 – Изменение области действия/типа группы

4.5.8. Управление компьютерами

Учетные записи компьютеров представляют собой устройства, подключенные к «Альт Домен». Они хранятся в базе данных домена после того, как их подключат к домену.

4.5.8.1. Создание учетной записи компьютера

Учетная запись компьютера создается во время стандартной процедуры присоединения к домену.

Для создания вручную учетной записи компьютера следует в контекстном меню контейнера выбрать пункт «Создать» → «Компьютер».

При создании учетной записи компьютера (рис. 81) нужно указать название компьютера (поле «Имя») и название компьютера для старых систем (поле «Имя для входа (до Windows 2000)»).

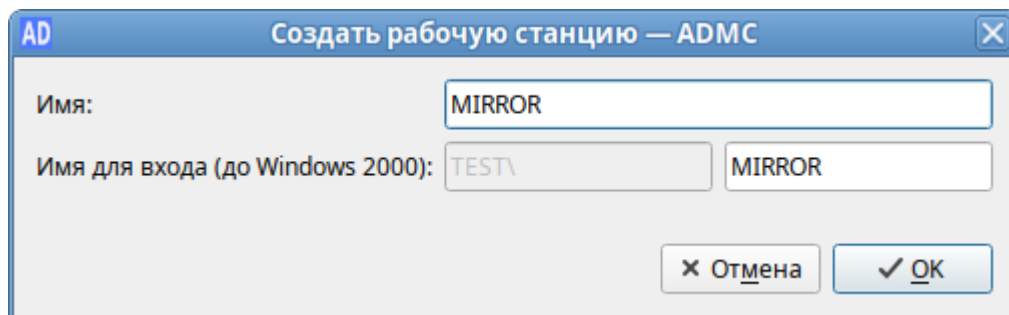


Рис. 81 – Создание учетной записи компьютера

4.5.8.2. Изменение учетной записи компьютера

Для изменения учетной записи компьютера следует в контекстном меню компьютера выбрать соответствующее действие (рис. 82).

Для включения/отключения учетной записи компьютера нужно в контекстном меню компьютера выбрать пункт «Отключить» или «Включить» (в зависимости от состояния учетной записи будет доступно одно из этих действий).

Для сброса учетной записи компьютера следует в контекстном меню компьютера выбрать пункт «Сбросить учетную запись». При этом учетная запись выбранного компьютера будет переустановлена. Переустановка учетной записи компьютера прекращает его подключение к домену и требует заново ввести данный компьютер в домен.

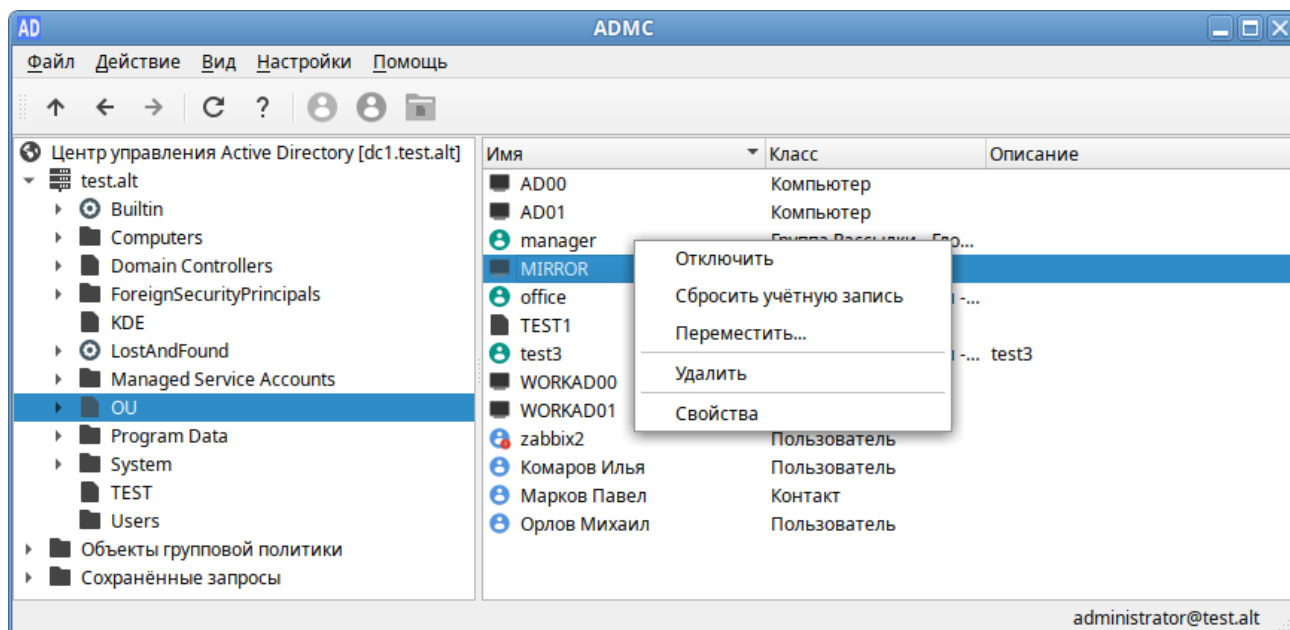


Рис. 82 – Контекстное меню учетной записи компьютера

Для перемещения компьютера в другой контейнер:

- 1) в контекстном меню компьютера выбрать пункт «Переместить...»;
- 2) в открывшемся окне выбрать контейнер (рис. 63), в который следует переместить учетную запись компьютера;
- 3) нажать кнопку «ОК».

Для удаления учетной записи компьютера следует в контекстном меню компьютера выбрать пункт «Удалить».

⚠ Если в настройках ADMC не отмечен пункт «Подтверждать действия», компьютер будет удален сразу после выбора пункта меню «Удалить».

4.5.9. Управление подразделениями

Организационная единица или подразделение (Organizational Unit, OU) – это субконтейнер в домене, в который можно помещать пользователей, группы, компьютеры и другие объекты домена. Подразделение – самая маленькая область или единица, для которой можно назначить параметры групповой политики. Подразделения могут быть вложенными.

4.5.9.1. Создание подразделения

Для создания подразделения следует в контекстном меню контейнера выбрать пункт «Создать» → «Подразделение».

При создании подразделения (рис. 83) нужно указать название подразделения (поле «Имя»).

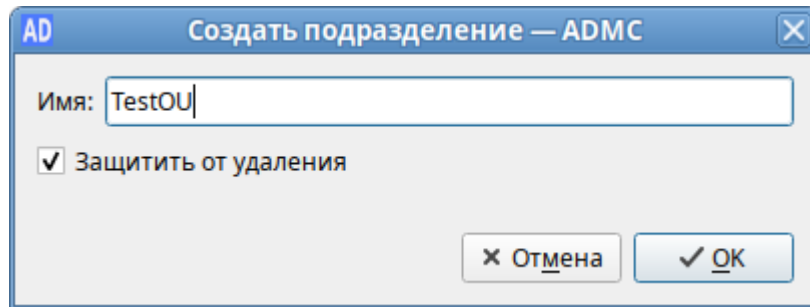


Рис. 83 – Окно мастера создания подразделения

Примечание. Если при создании подразделения отметить пункт «Защитить от удаления», то для удаления данного подразделения, нужно сначала снять данную отметку в окне свойств подразделения.

4.5.9.2. Изменение подразделения

Для изменения подразделения следует в контекстном меню подразделения выбрать соответствующее действие (рис. 84).

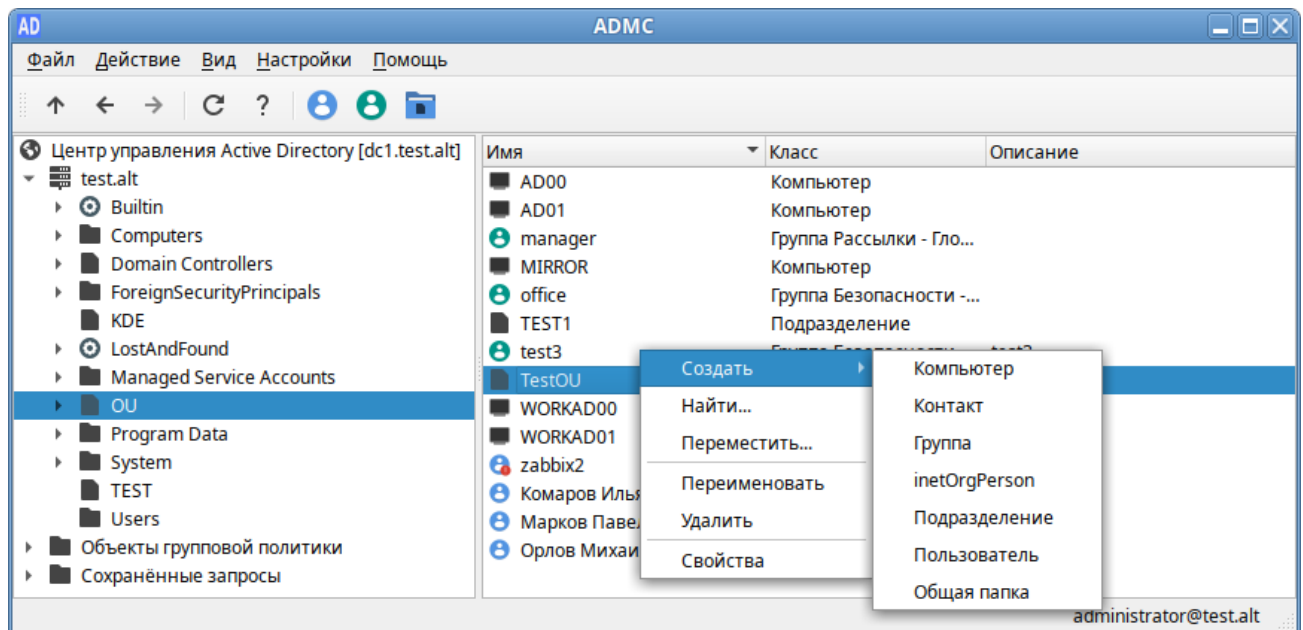


Рис. 84 – Контекстное меню подразделения

Для переименования подразделения:

- 1) в контекстном меню подразделения выбрать пункт «Переименовать»;
- 2) в открывшемся окне изменить имя подразделения (рис. 85);
- 3) нажать кнопку «ОК» для сохранения изменений.

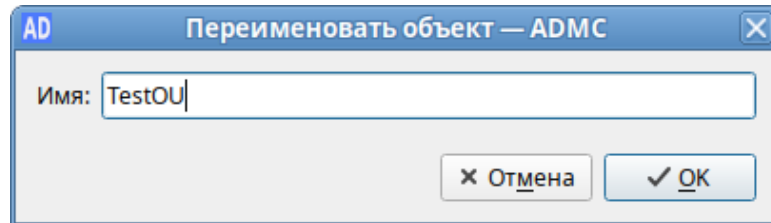


Рис. 85 – Переименование подразделения

Для удаления подразделения следует в контекстном меню подразделения выбрать пункт «Удалить».

⚠ Если при создании подразделения был отмечен пункт «Защитить от удаления», то сразу удалить подразделение не получится, нужно сначала снять данную отметку в окне свойств подразделения (рис. 86).

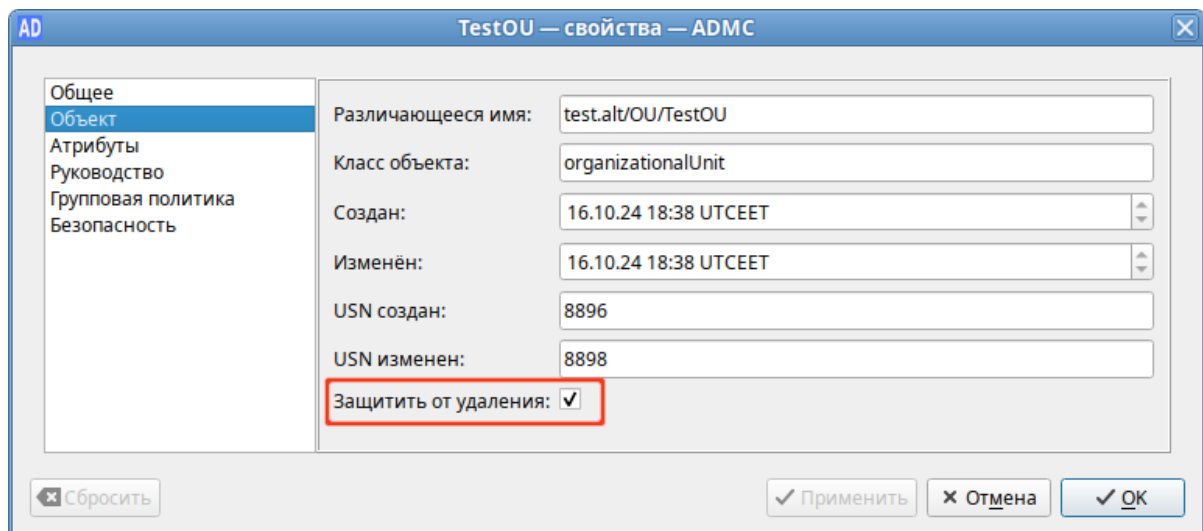


Рис. 86 – Свойства подразделения

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 (рис. 63);
- 3) нажать кнопку «ОК».

4.5.10. Управление объектами парольных настроек

Примечание. Для возможности работы с объектами парольных настроек необходимо в меню «Настройки» отметить пункт «Дополнительные возможности» (рис. 47).

4.5.10.1. 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» (рис. 87). Откроется окно мастера создания объекта парольных настроек (рис. 88).

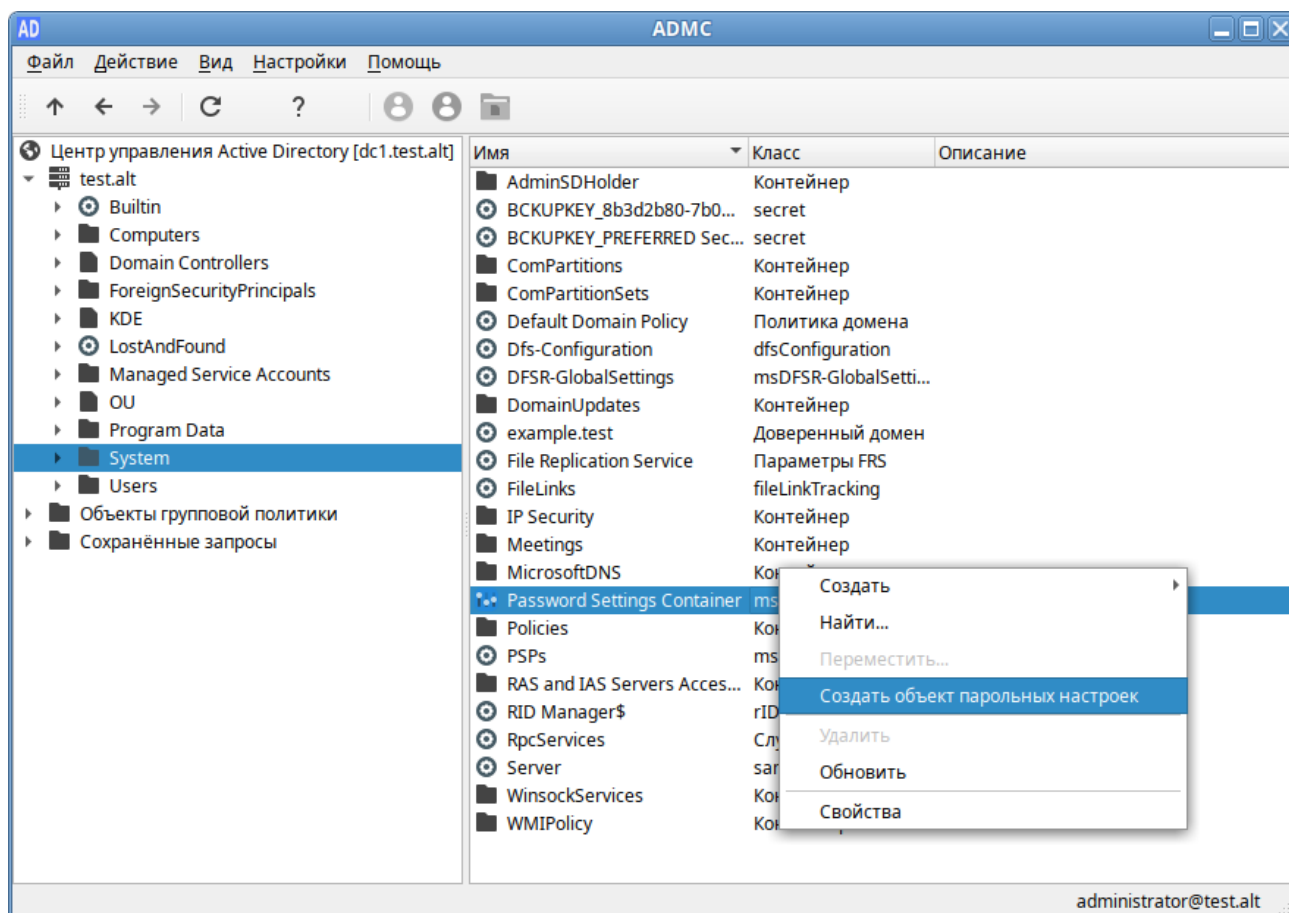


Рис. 87 – Контейнер «Password Settings Container»

AD Создание объекта парольных настроек — ADMS

Password Settings

Имя: PwPolicyUser

Приоритет: 1

Минимальная длина пароля: 10

Длина истории паролей: 24

Разрешено неудачных попыток входа: 0

Время до сброса блокировки (минуты): 30

Минимальный срок действия пароля (дни): 1

Максимальный срок действия пароля (дни): 42

Длительность блокировки учетной записи (минуты): 30

☒ Включить требования сложности

☐ Хранить пароли, используя обратимое шифрование

Применить к пользователю/группе

office

Добавить...

Удалить

☒ Защитить от удаления

Отмена ОК

Рис. 88 – Создание 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.

4.5.10.2. Изменение объекта парольных настроек

Для удаления объекта парольных настроек следует в контекстном меню объекта выбрать пункт «Удалить» (рис. 89).

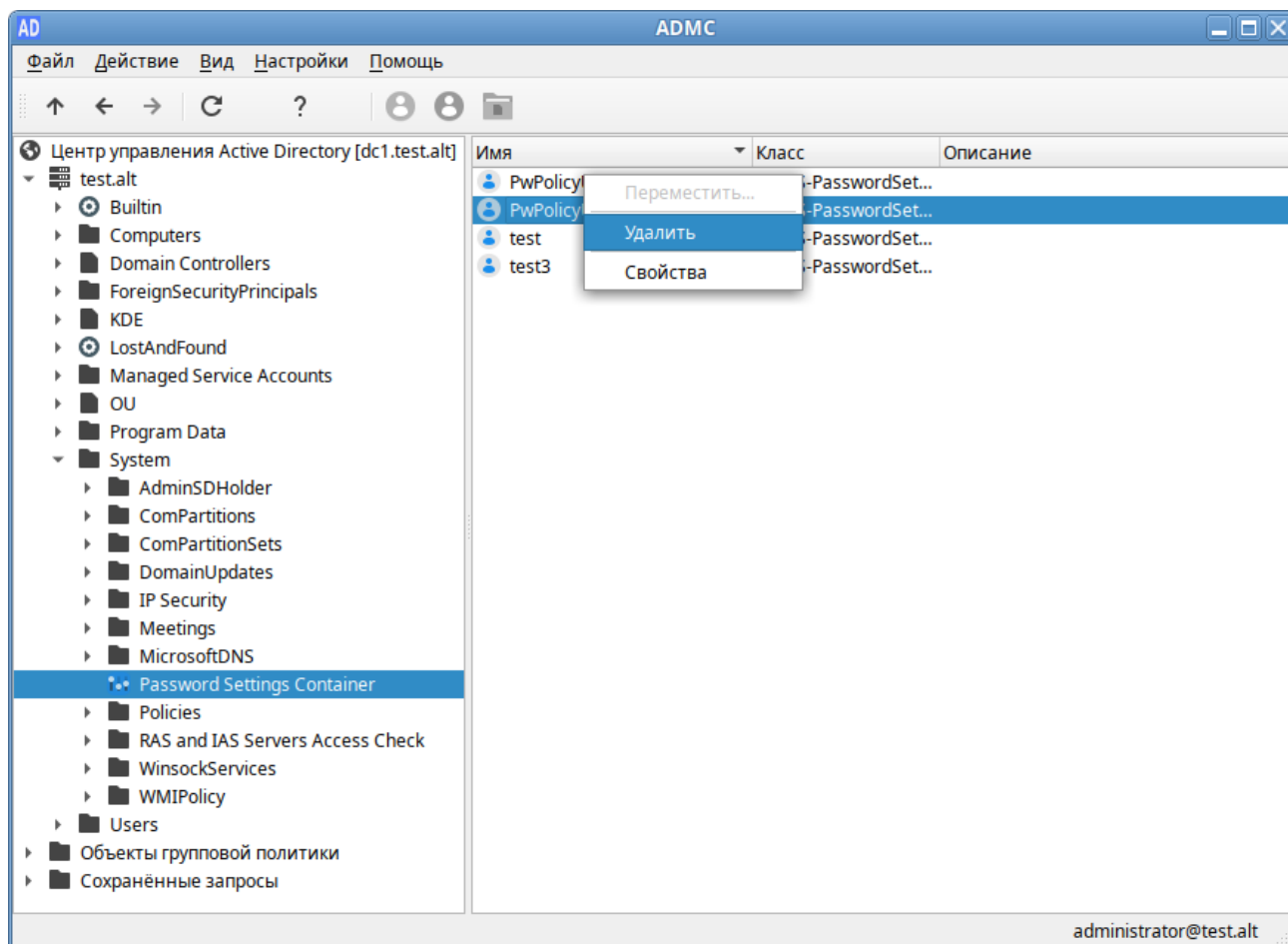


Рис. 89 – Контекстное меню объекта парольных настроек

Примечание. 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 (рис. 90).

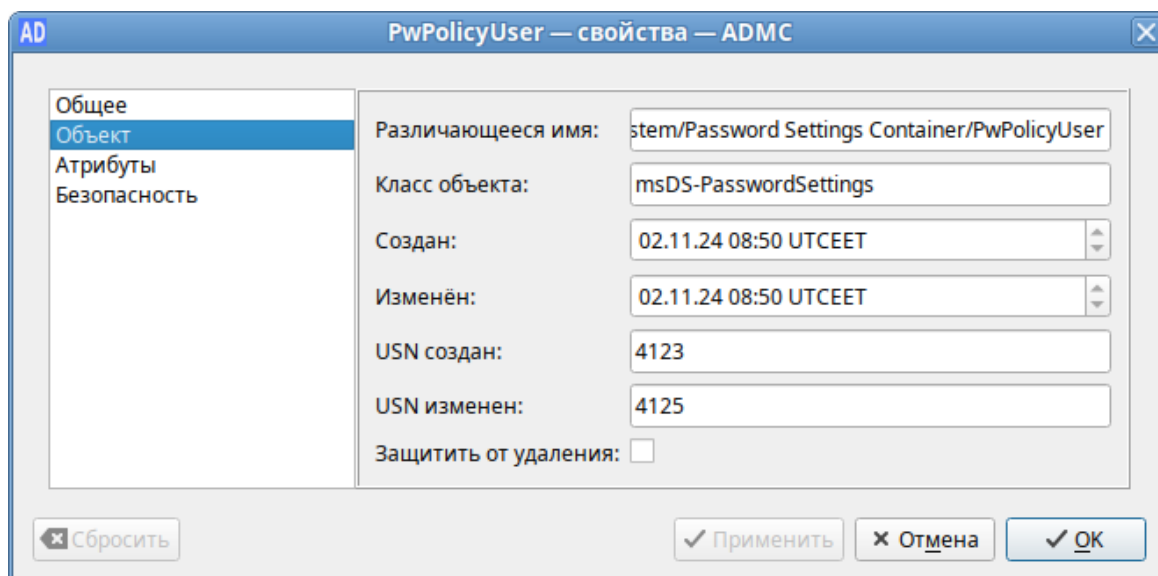


Рис. 90 – Свойства объекта парольных настроек

4.5.11. 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 (рис. 91).

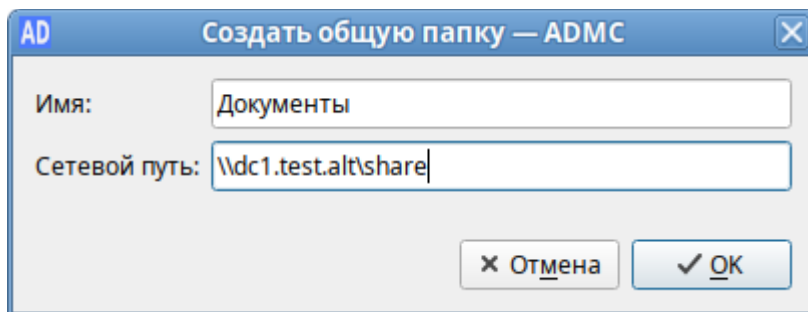


Рис. 91 – Создание общей папки

В поле «Имя» следует ввести название папки, под которым она будет отображаться в каталоге «Альт Домен», а в поле «Сетевой путь» – полный сетевой путь к общей папке.

Для изменения общей папки следует в контекстном меню общей папки выбрать соответствующее действие (рис. 92).

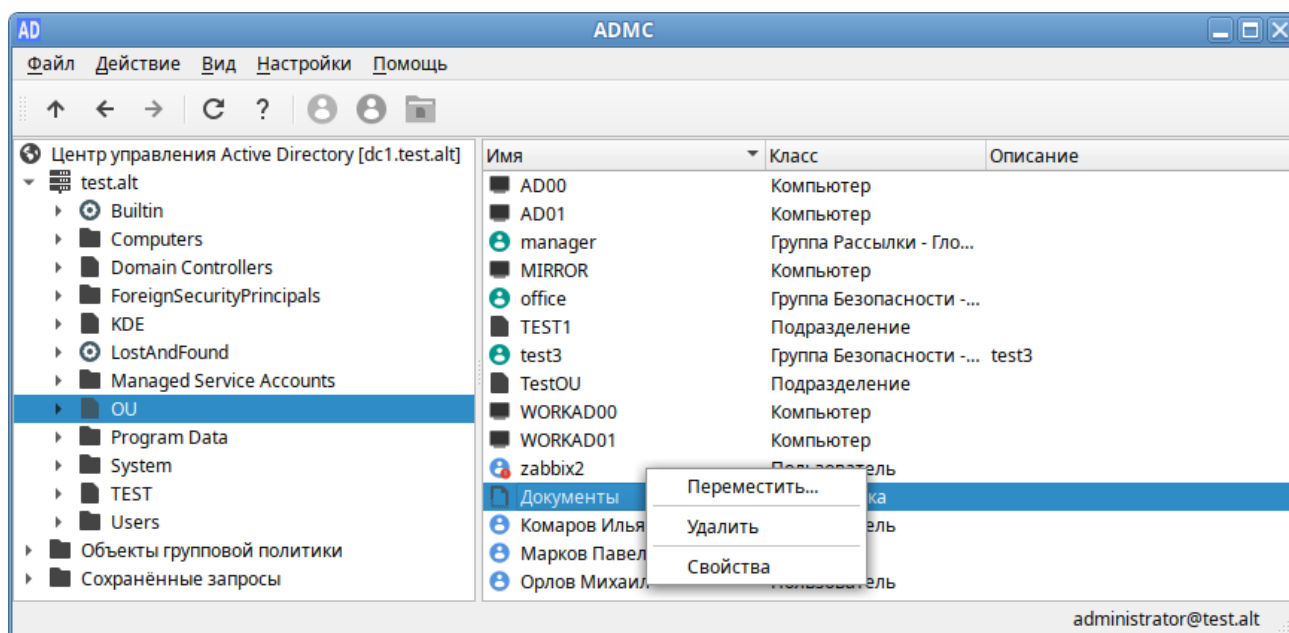


Рис. 92 – Изменение общей папки

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.

4.5.12. Управление объектами групповых политик

Групповая политика состоит из набора политик, называемых объектами групповой политики. Для вступления настроек в силу, объект групповой политики нужно связать с одним или несколькими контейнерами домена. 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» (рис. 93) отображаются групповые политики, которые назначены на различные OU (отображается вся структура OU). Полный список политик в текущем домене доступен в разделе «Все политики».

Примечание. В «Альт Домен» по умолчанию создаются два объекта групповой политики, которые действуют на все компьютеры и контроллеры домена соответственно:

- Default Domain Policy;
- Default Domain Controller Policy.

Примечание. Эти объекты групповой политики очень важны, поэтому не рекомендуется вносить в них изменения без крайней необходимости.

Групповые политики можно назначить на OU или весь домен. Чаще всего политики привязываются к OU с компьютерами или пользователями.

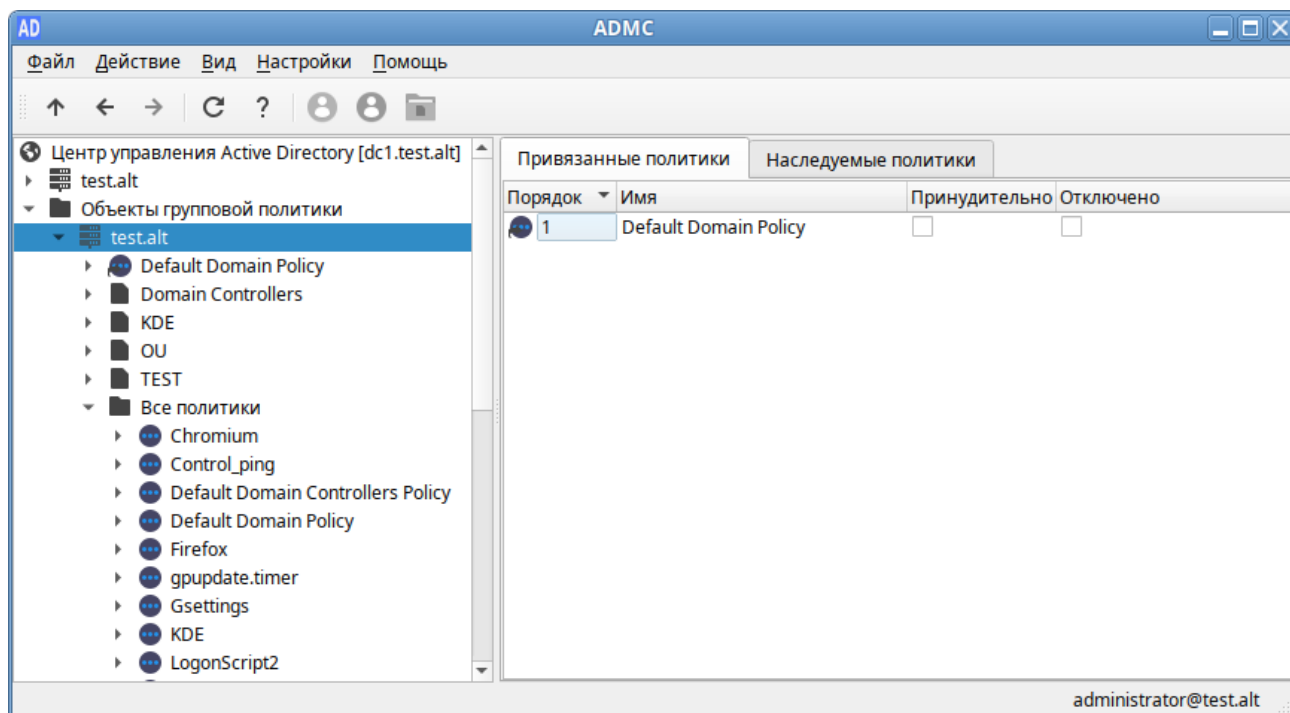


Рис. 93 – Объекты групповой политики

4.5.12.1. Создание объекта групповой политики

Для того чтобы создать новый объект групповой политики и сразу назначить его на OU нужно выполнить следующие действия:

- 1) в контекстном меню нужного контейнера выбрать пункт «Создать политику и связать с этим подразделением» (рис. 94);

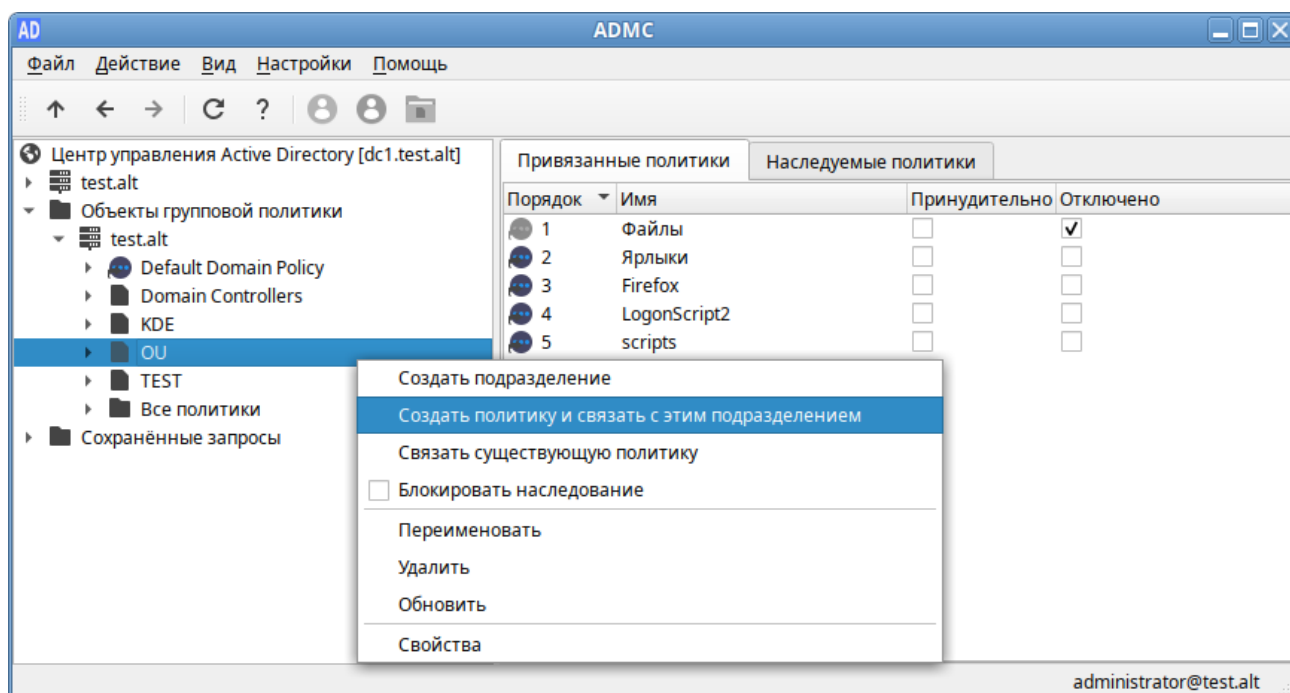


Рис. 94 – Контекстное меню контейнера

- 2) в открывшемся окне задать имя политики (рис. 95);
- 3) нажать кнопку «ОК».

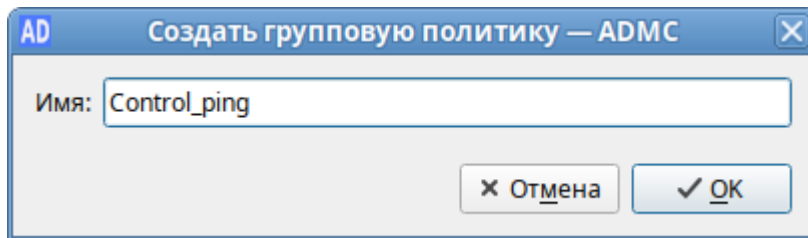


Рис. 95 – Создание объекта групповой политики

Для того чтобы создать новый объект групповой политики, не назначая его на OU, нужно выполнить следующие действия:

- 1) в контекстном меню папки «Все политики» выбрать пункт «Создать политику» (рис. 96);

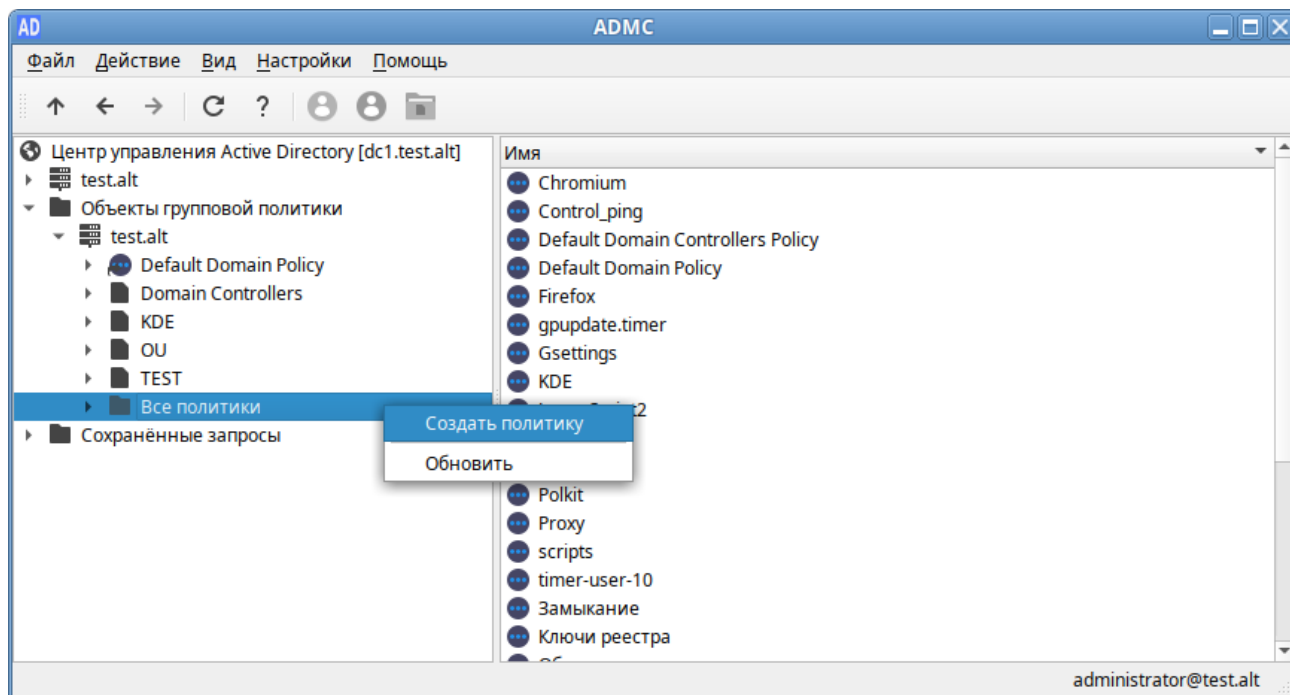


Рис. 96 – Контекстное меню папки «Все политики»

- 2) в открывшемся окне задать имя политики (рис. 95);
- 3) нажать кнопку «ОК».

Созданный объект групповой политики не будет задействован, пока не будет привязан к подразделению.

Примечание. Редактирование групповых политик реализуется в модуле редактирования настроек клиентской конфигурации (GPUI).

4.5.12.2. Изменение объекта групповой политики

Для изменения объекта групповой политики следует в контекстном меню политики выбрать соответствующее действие (рис. 97, рис. 98).

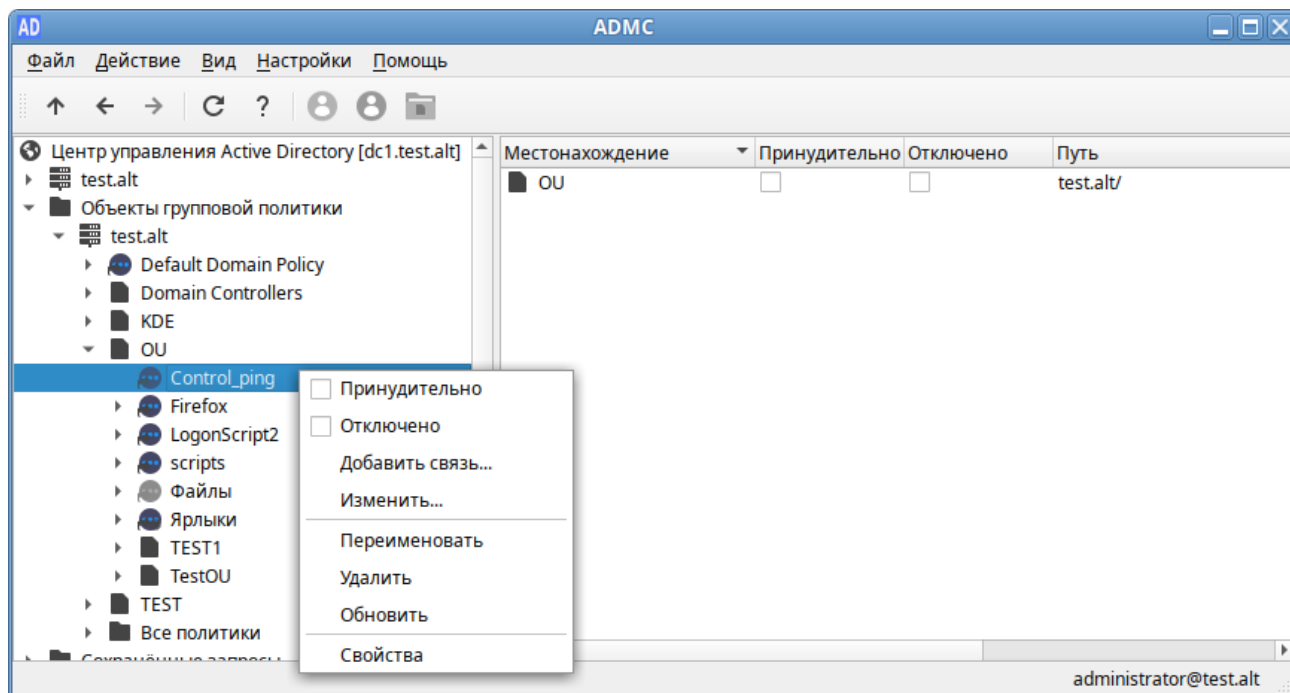


Рис. 97 – Контекстное меню объекта групповой политики

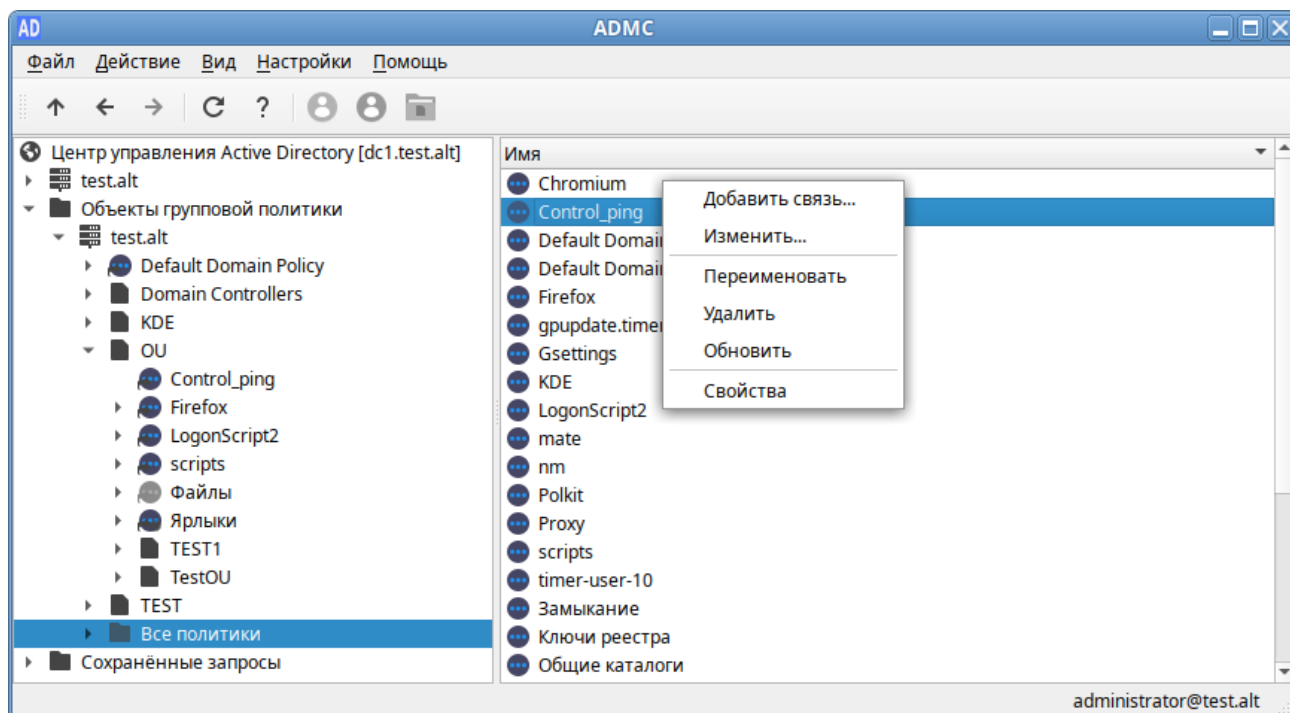


Рис. 98 – Контекстное меню объекта групповой политики

4.5.12.2.1. Переименование объекта групповой политики

Для переименования политики:

- 1) в контекстном меню политики выбрать пункт «Переименовать»;
- 2) в открывшемся окне ввести новое название (рис. 99);

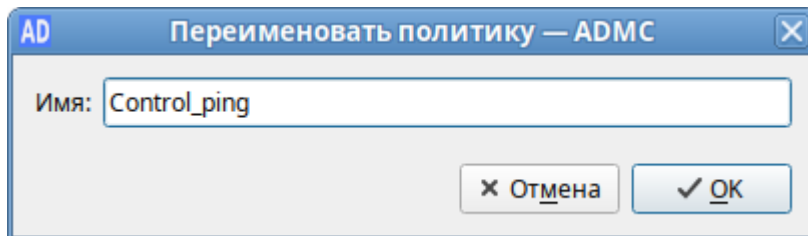


Рис. 99 – Переименование объекта групповой политики

- 3) нажать кнопку «ОК» для сохранения изменений.

4.5.12.2.2. Удаление объекта групповой политики

Для удаления политики:

- 1) в контекстном меню политики в разделе «Все политики» выбрать пункт «Удалить» (рис. 98);
- 2) подтвердить удаление, нажав кнопку «Да» (рис. 100).

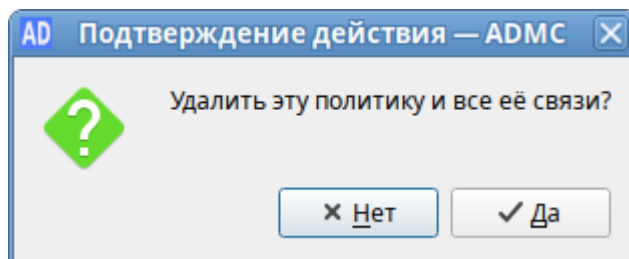


Рис. 100 – Подтверждение удаления

Примечание. Если выбрать пункт «Удалить» в контекстном меню политики в подразделении (см. рис. 97), на которое она назначена, будет удалена только связь между политикой и подразделением (рис. 101).

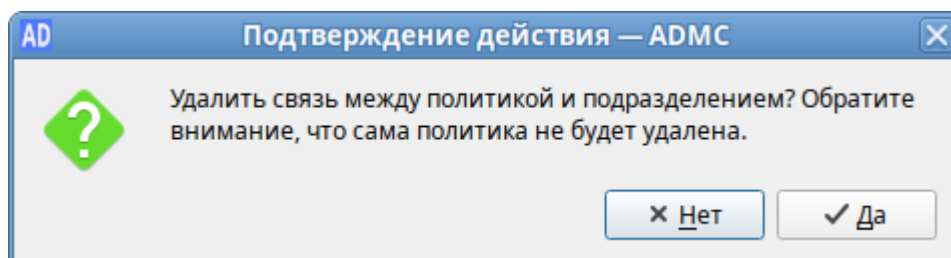


Рис. 101 – Подтверждение действия

4.5.12.2.3. Создание и удаление связи между политикой и подразделением

Для связи между политикой и подразделением (создания ссылки на политику):

- 1) в контекстном меню политики выбрать пункт «Добавить связь...»;
- 2) выбрать объекты, которые нужно связать с политикой;
- 3) нажать кнопку «ОК» (рис. 102).

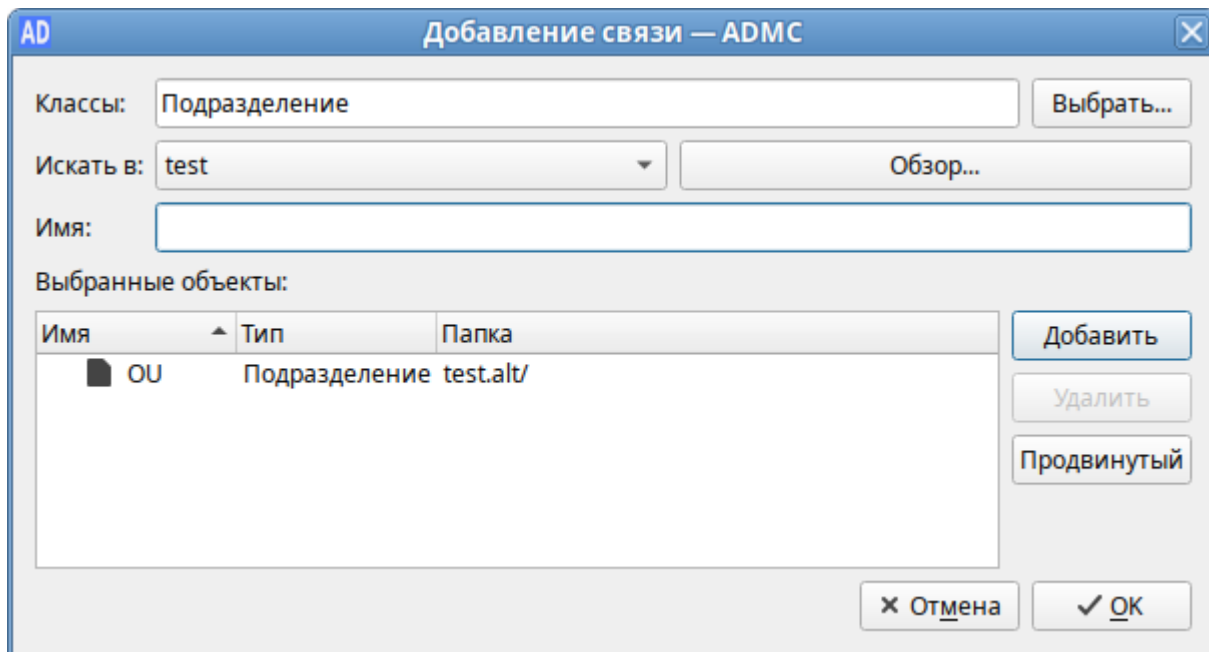


Рис. 102 – Добавление связи

Для удаления ссылки на объект групповой политики:

- выбрать политику, которую следует изменить (в папке «Все политики» или в папке соответствующего OU);
- в контекстном меню подразделения, связь с которым нужно отключить от политики, выбрать пункт «Удалить связь» (рис. 103).

Удалить связь между политикой и подразделением также можно, выбрав пункт «Удалить» в контекстном меню политики в подразделении, на которое она назначена (см. рис. 97).

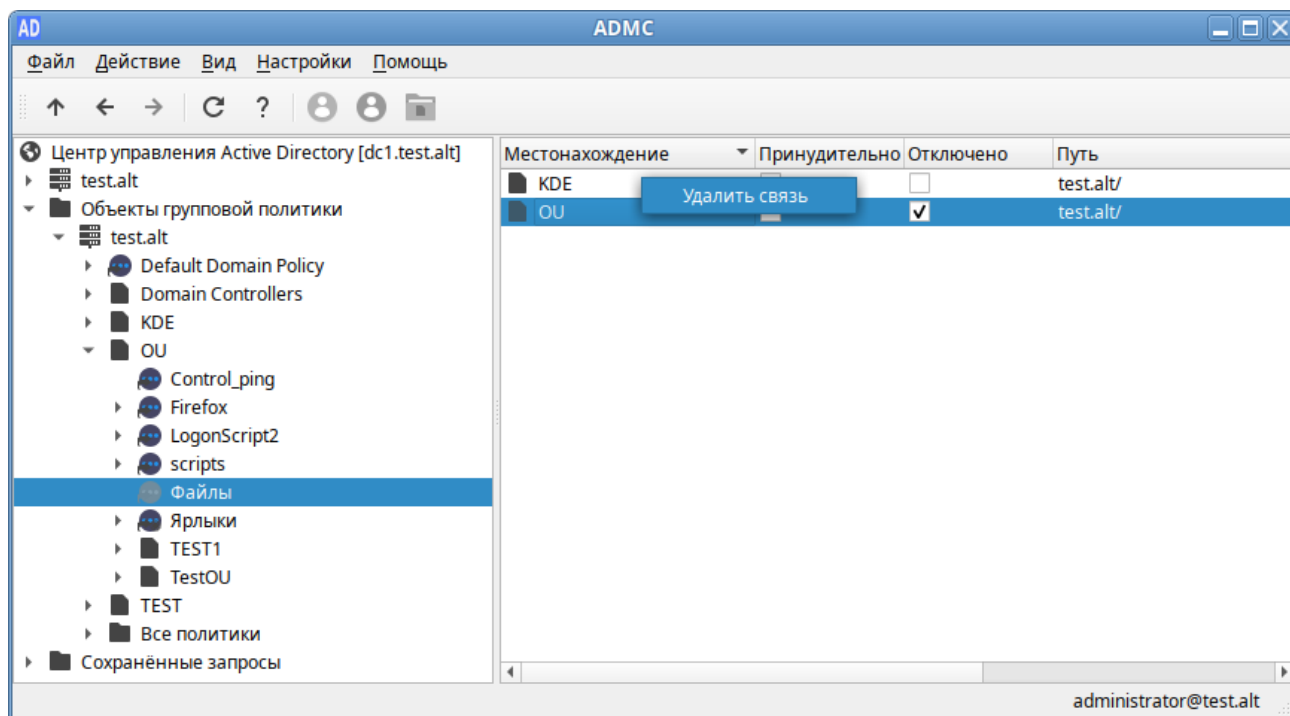


Рис. 103 – Пункт «Удалить связь»

В ADCM 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, нужно:

- 1) выбрать политику, которую следует отредактировать;
- 2) на панели результатов найти подразделение, для которого нужно изменить параметры ссылки (рис. 104);
- 3) включить опцию «Принудительно», чтобы запретить переопределение параметров политик (см. п. 4.5.12.3). Политика, с включенной опцией «Принудительно», отображается в списке политик с красным кружком;
- 4) включить опцию «Отключено», чтобы временно отключить действие политики. Отключенная политика, в списке политик отображается серым цветом.

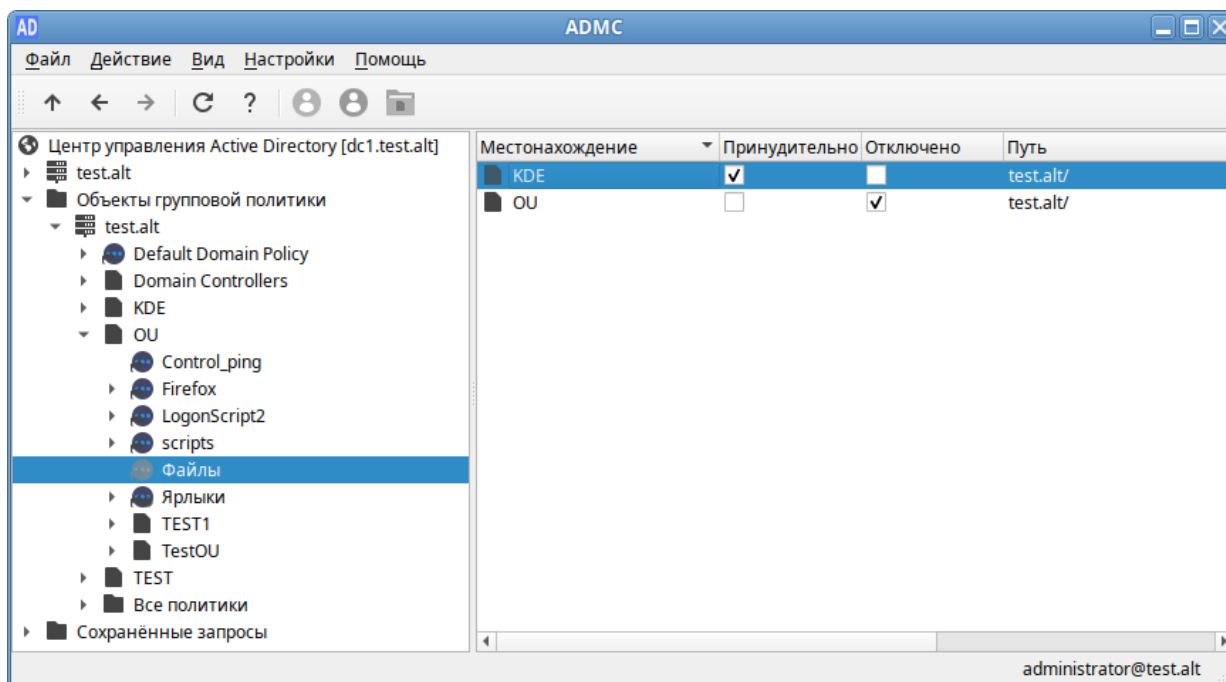


Рис. 104 – Редактирование параметров ссылки

Примечание. Если нужно, чтобы политика перестала действовать на клиентов в данном подразделении, можно либо удалить ссылку (при этом сама объект ГП не будет удален), либо временно отключить действие политики.

Включить/отключить опции «Принудительно» и «Отключено» также можно:

- в контекстном меню политики в подразделении (см. рис. 97);
- на вкладке «Привязанные политики» подразделения (рис. 105).

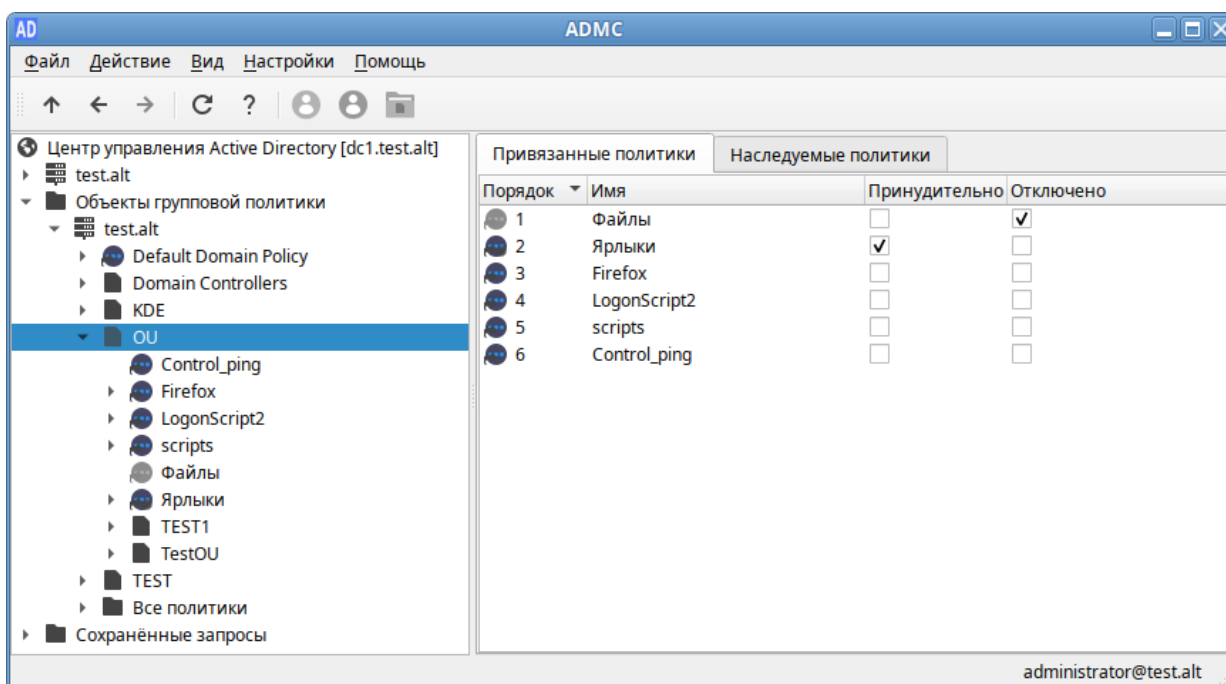


Рис. 105 – Опции «Принудительно» и «Отключено» на вкладке подразделения

4.5.12.2.4. 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 нужно 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 домена создается контейнер групповой политики (Group Policy Container, GPC). Для возможности просмотра контейнера групповой политики (это дочерний контейнер Policies контейнера System) в настройках ADMS должен быть отмечен пункт «Дополнительные возможности».

В «Альт Домен» контейнер групповой политики создается как тип groupPolicyContainer, причем его GUID можно увидеть в ADMS в столбце «Имя» (рис. 106).

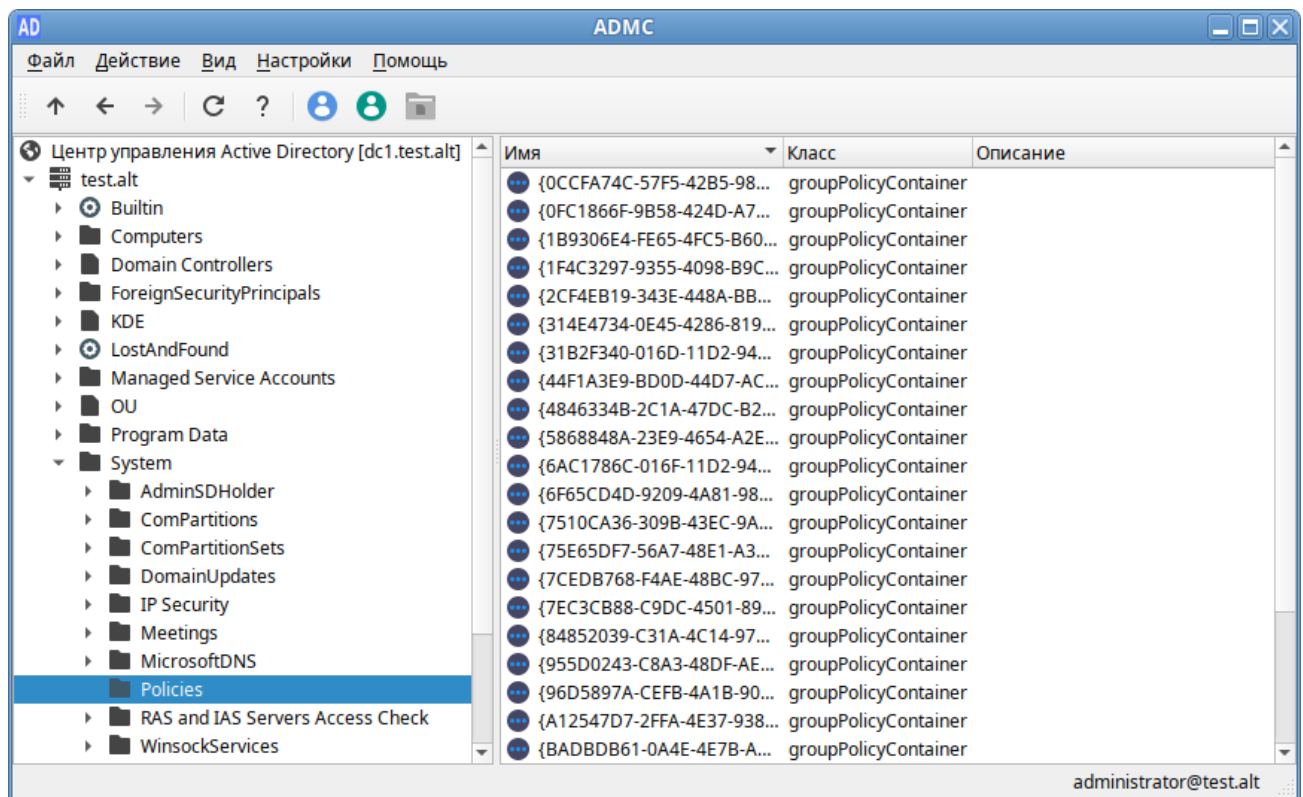


Рис. 106 – Контейнеры групповых политик

Ниже перечислены некоторые атрибуты, позволяющие описать различные типы данных объекта групповой политики (рис. 107):

- `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 ГП 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.

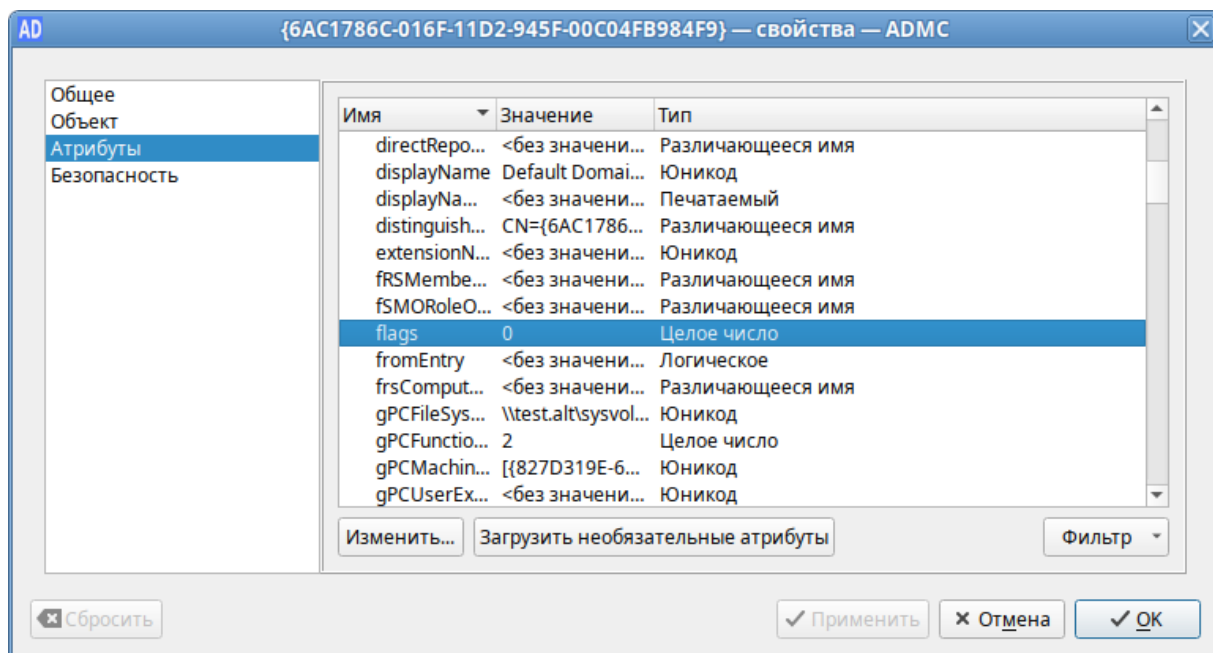


Рис. 107 – Атрибуты объекта групповой политики

4.5.12.3. Блокирование наследования

Для того чтобы параметры групповой политики, определенные на уровне вышестоящих контейнеров, не распространялись на содержимое конфигурируемого контейнера нужно выполнить одно из следующих действий:

- 1) в контекстном меню контейнера, к которому привязан объект групповой политики, установить отметку «Блокировать наследование» (рис. 108);

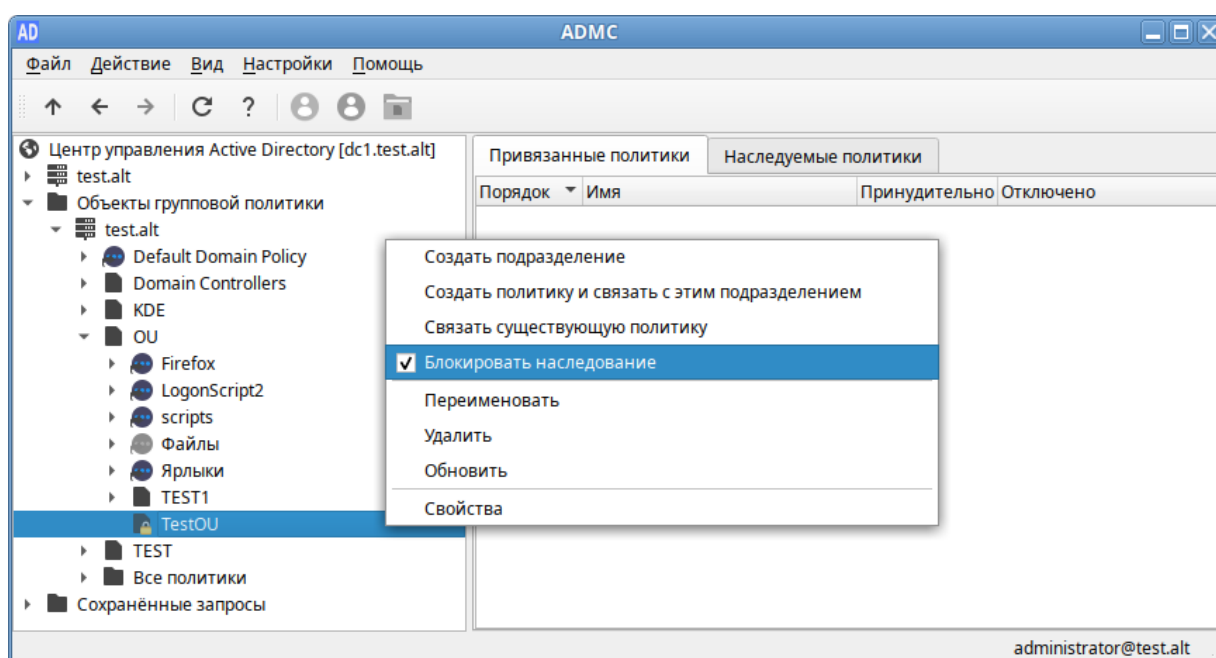


Рис. 108 – Отметка «Блокировать наследование»

- 2) в окне свойств контейнера, к которому привязан объект групповой политики, на вкладке «Групповая политика» установить отметку «Заблокировать наследование политик» (рис. 109);

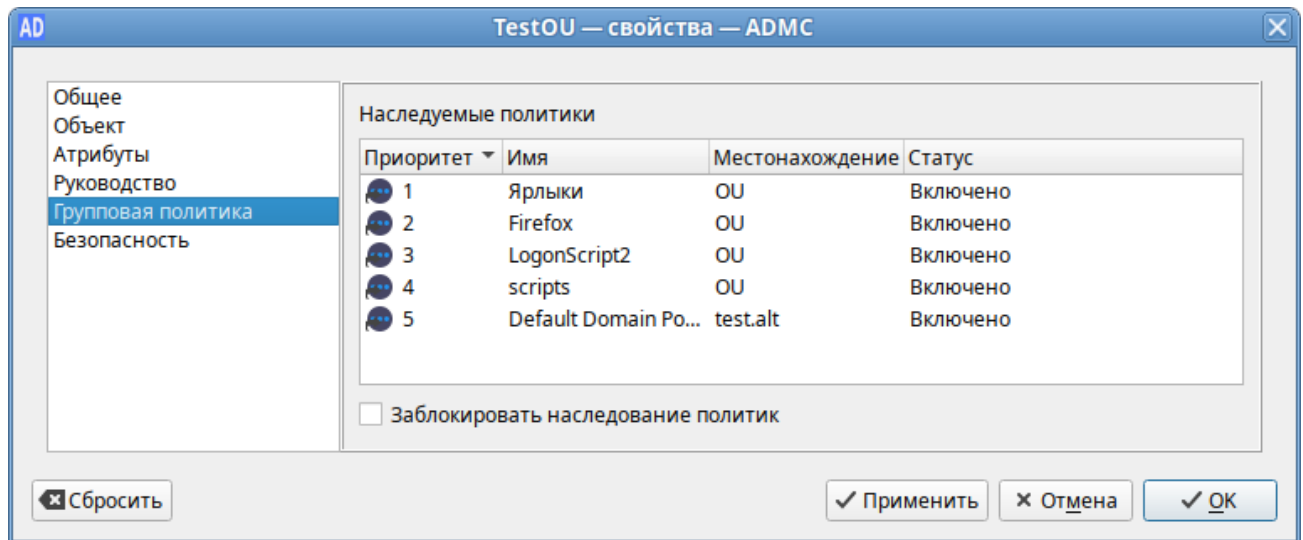


Рис. 109 – Окно свойств контейнера

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» (рис. 110).

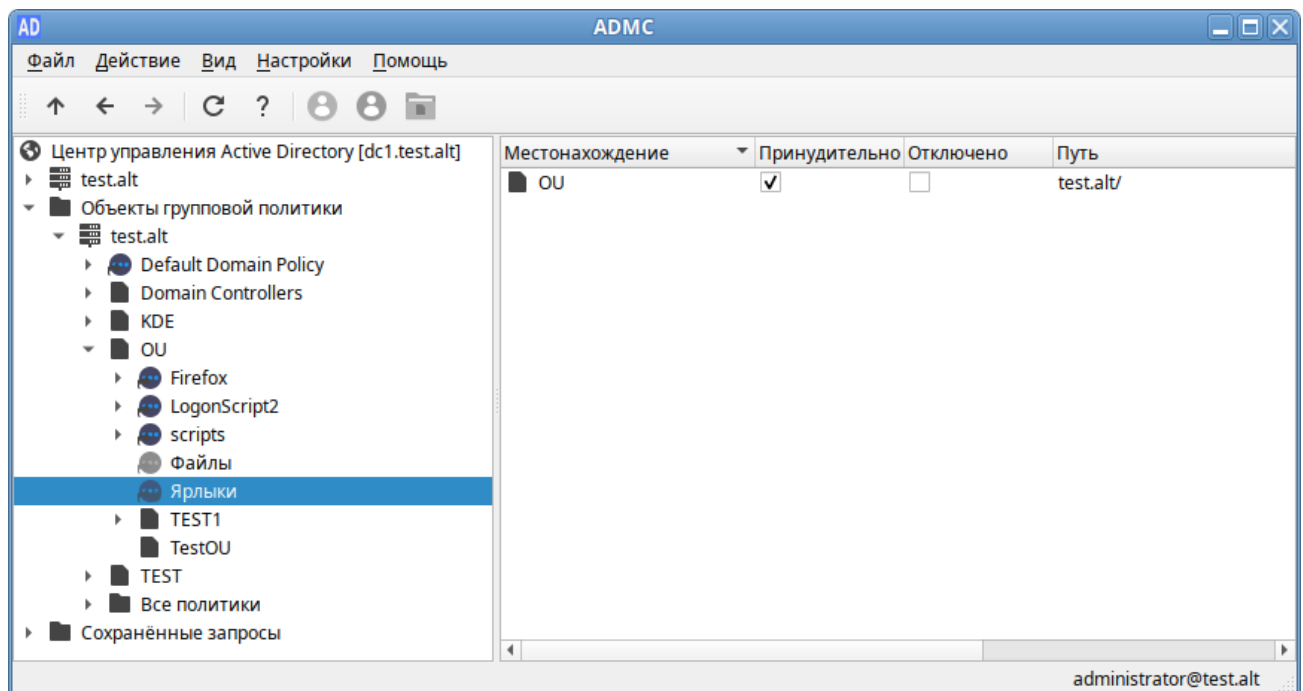


Рис. 110 – Переопределение параметров с помощью отметки «Принудительно»

Отметка в поле «Принудительно» означает, что связь установлена принудительно. Это приведет 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, при включении «Принудительно» у политики Default Domain Policy, она выигрывает у всех других групповых политик).

Примечание. Подразделение с заблокированным 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 (рис. 111).

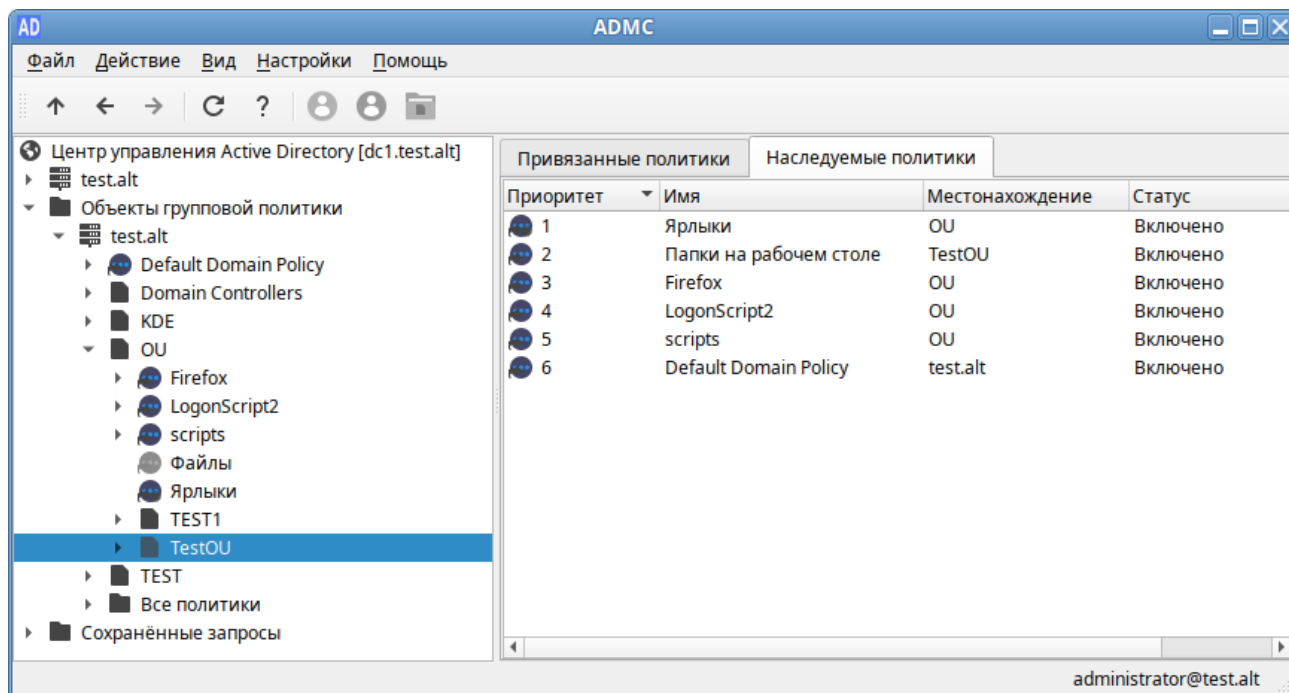


Рис. 111 – Вкладка «Наследуемые политики»

4.5.12.4. 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 ее 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» (рис. 112);
- 2) на вкладке «Безопасность» у группы «Authenticated Users» убрать разрешение на применение групповых политик (снять отметку с пункта «Применить групповые политики» в столбце «Разрешено») (рис. 113);
- 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» (рис. 114);
- 4) для добавленного объекта выставить разрешения «Читать» и «Применить групповые политики» (рис. 115) и нажать кнопку «Применить».

Примечание. Если выставить все разрешения, групповые политики применяться не будут.

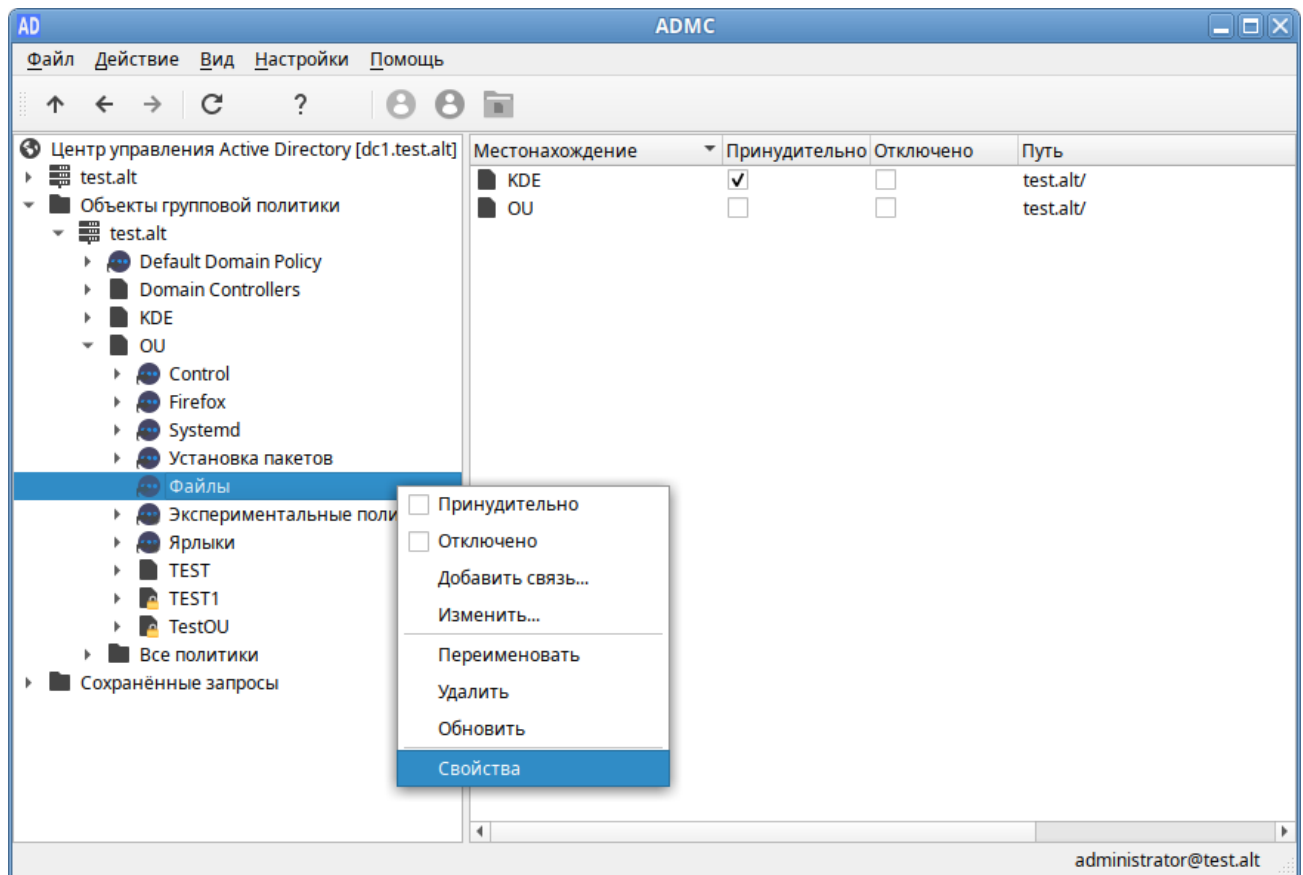


Рис. 112 – Контекстное меню групповой политики

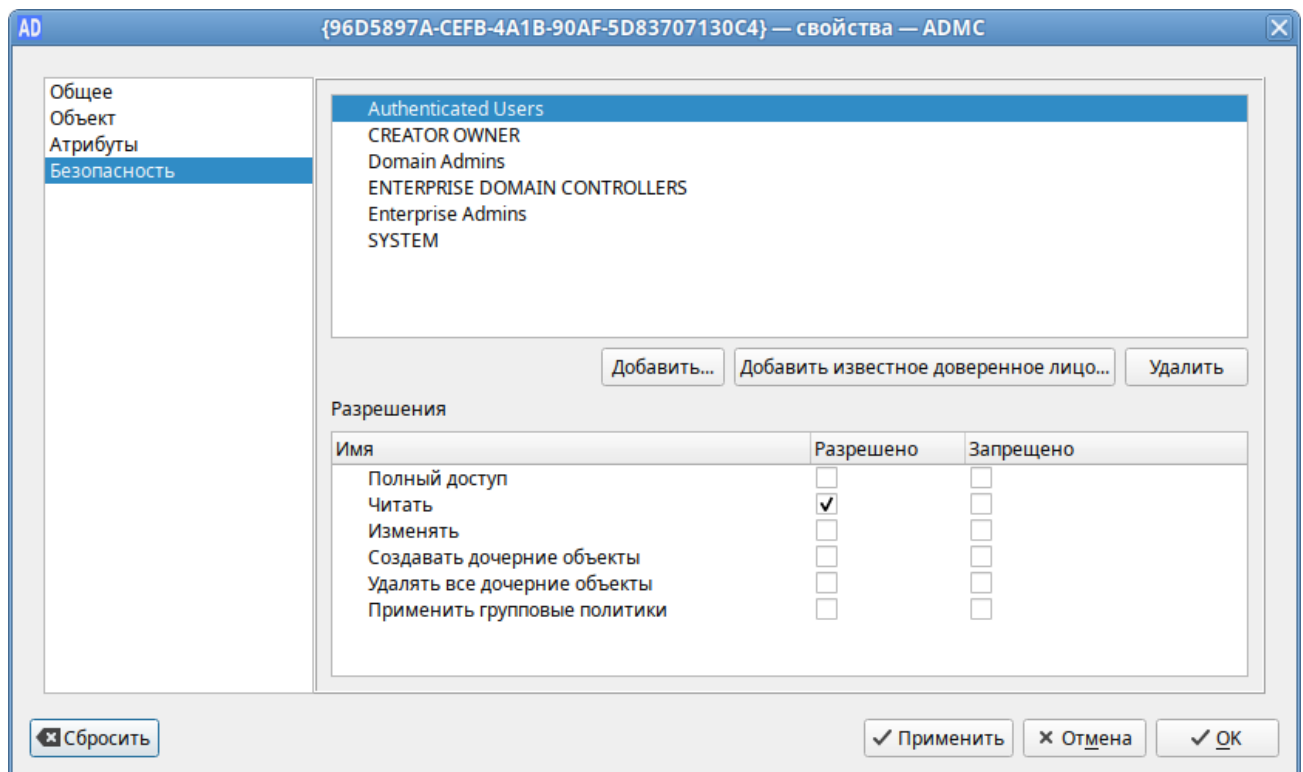


Рис. 113 – Вкладка «Безопасность» свойства групповой политики

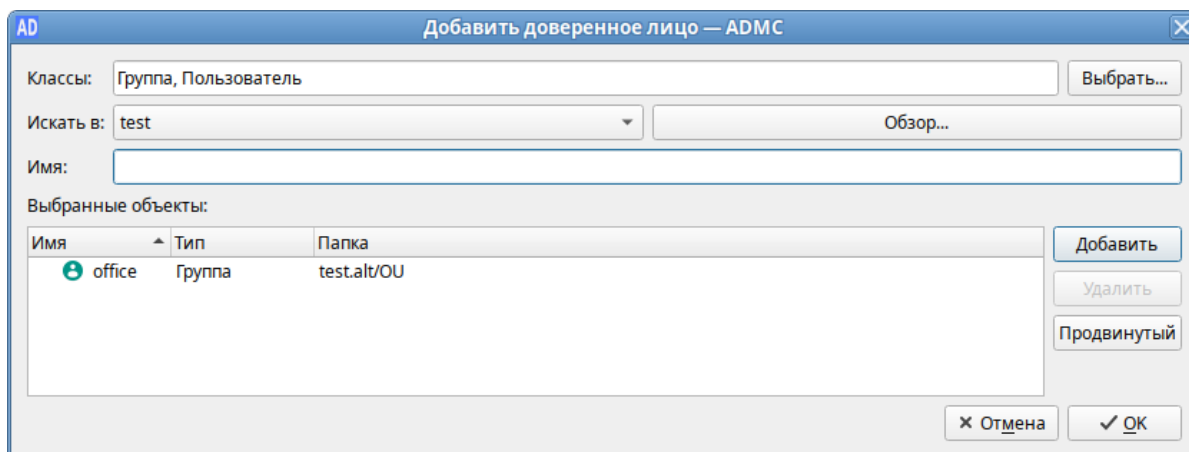


Рис. 114 – Добавление доверенного лица

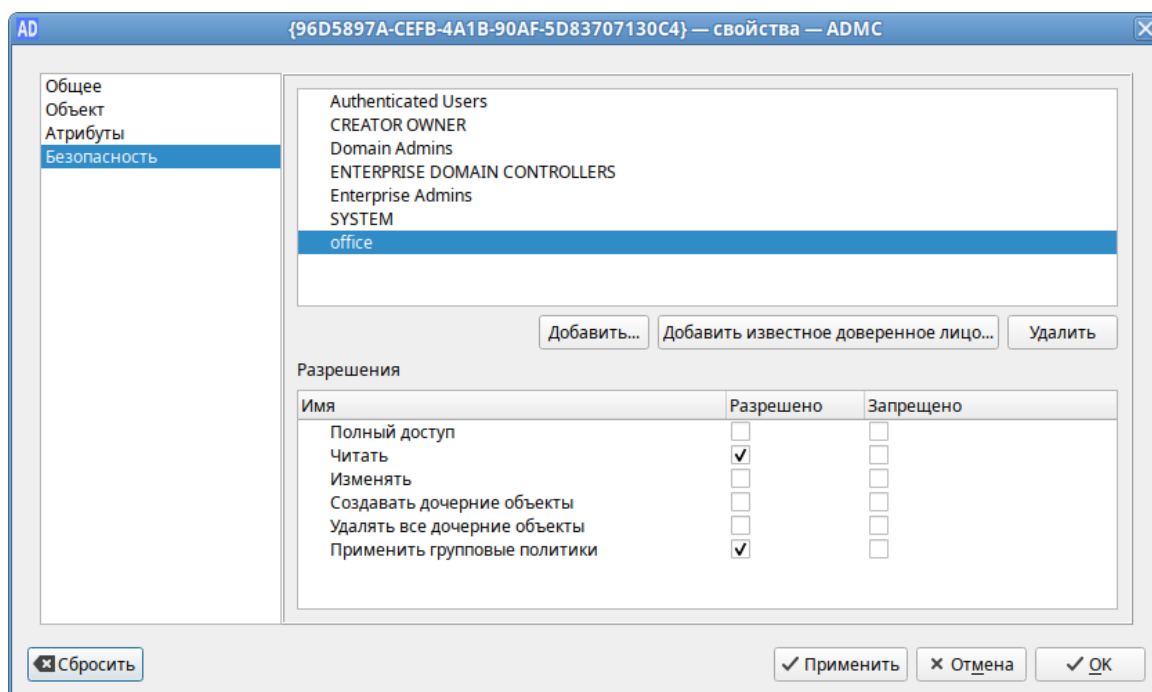


Рис. 115 – Разрешение на применение групповой политики

Чтобы определенному объекту запретить применение групповой политики, следует выполнить следующие действия:

- 1) в контекстном меню групповой политики выбрать пункт «Свойства» (см. рис. 112);
- 2) на вкладке «Безопасность» у группы «Authenticated Users» оставить разрешение на применение групповых политик (не снимать отметку с пункта «Применить групповые политики» в столбце «Разрешено» (рис. 116);

- 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» (рис. 117);
- 4) для добавленного объекта установить запрет применения групповых политик (установить отметку в пункте «Применить групповые политики» в столбце «Запрещено») и нажать кнопку «Применить» (рис. 118).

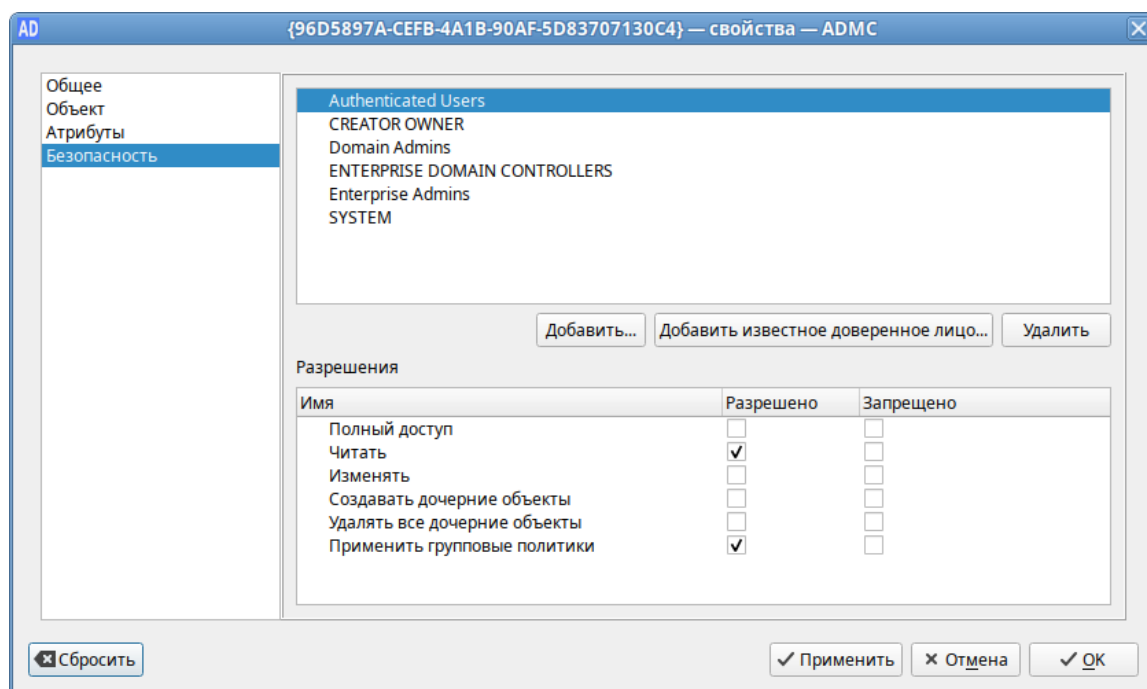


Рис. 116 – Вкладка «Безопасность» свойства групповой политики

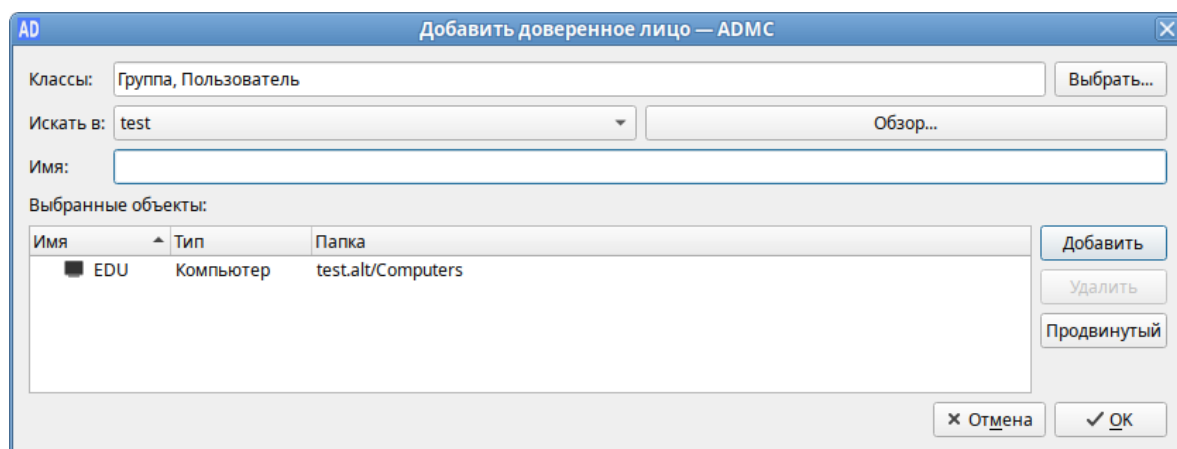


Рис. 117 – Добавить компьютер как доверенное лицо

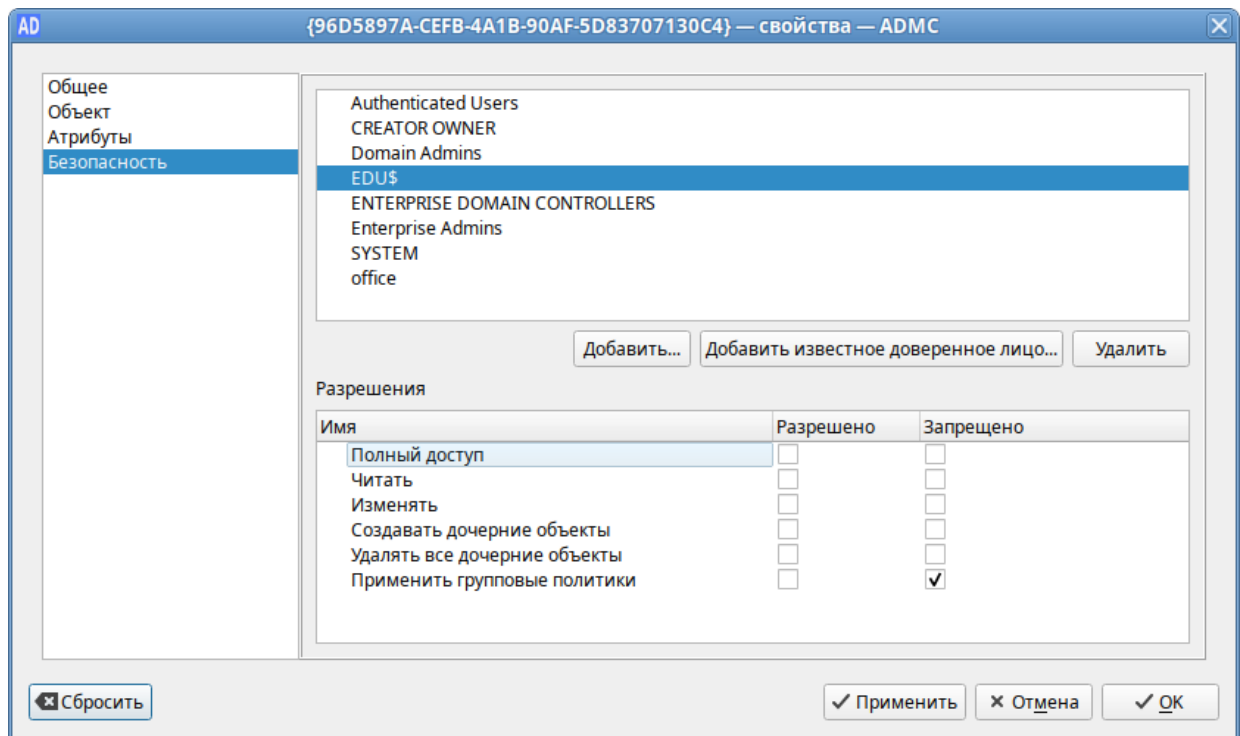


Рис. 118 – Запрет на применение групповых политик

4.5.13. 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 «Альт Домен»), test.alt – UPN-суффикс. По умолчанию в «Альт Домен» в качестве UPN-суффикса используется DNS имя домена. Добавление дополнительных имен доменов позволяет упростить процесс входа и повысить безопасность.

Для того чтобы добавить/удалить дополнительный UPN-суффикс, нужно выполнить следующие шаги:

- 1) в контекстном меню домена выбрать пункт «Изменить суффиксы UPN» (рис. 119);
- 2) в открывшемся диалоговом окне нажать кнопку «Добавить...» (рис. 120);

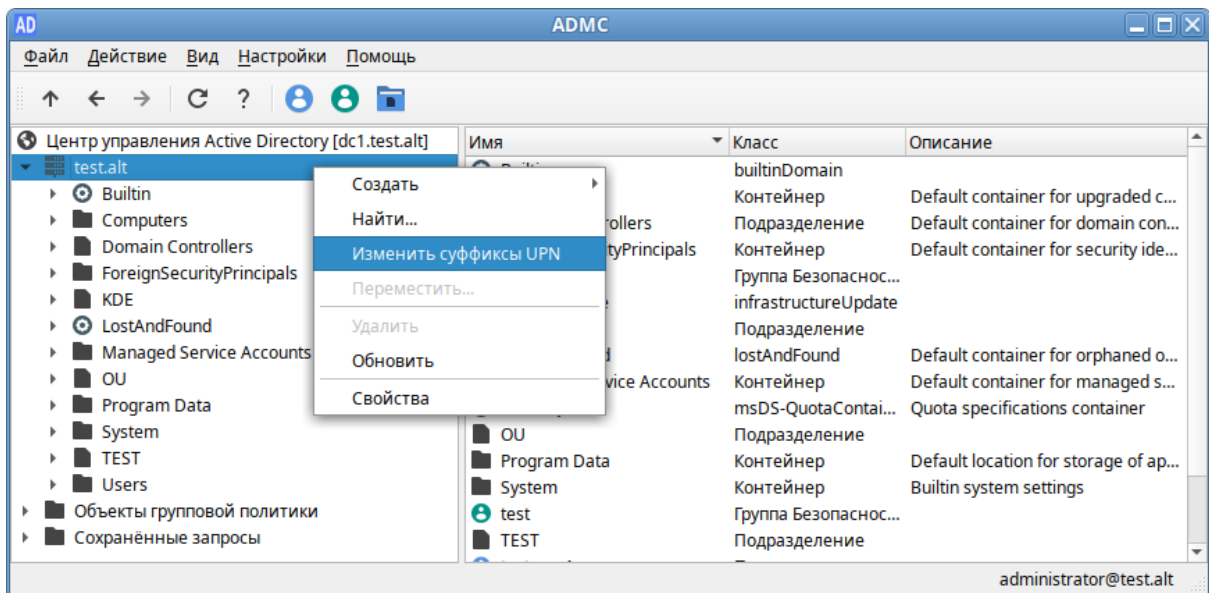


Рис. 119 – Пункт «Изменить суффиксы UPN»

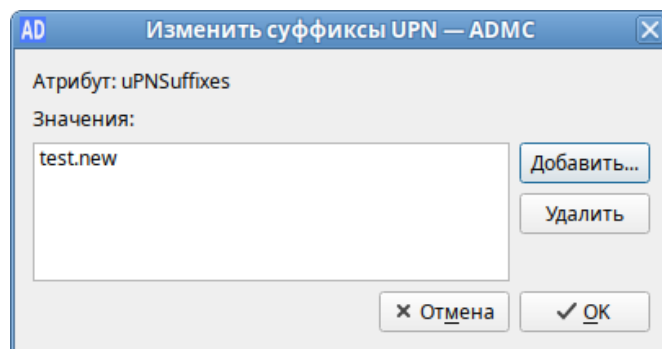


Рис. 120 – Кнопка «Добавить...»

- 3) ввести альтернативный суффикс (рис. 121). 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 «ОК», чтобы добавить новый суффикс в список.

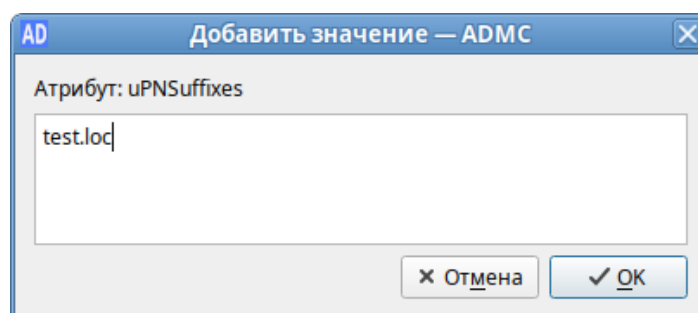


Рис. 121 – Введение альтернативного суффикса

Чтобы удалить существующий суффикс, нужно выбрать его в списке и нажать кнопку «Удалить» (рис. 122).

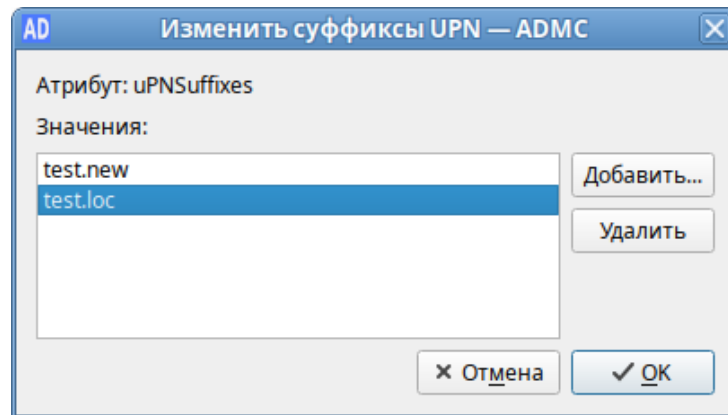


Рис. 122 – Удаление существующего суффикса

4.5.14. Роли 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 нужно выбрать пункт меню «Файл» → «Мастера Операций». В открывшемся окне в списке слева выбрать роль и в поле «Текущий мастер» будет показан владелец роли (рис. 123).

Список возможных ролей:

- «DNS домена» – Domain DNS Zone Master role;
- «DNS леса» – Forest DNS Zone Master role;
- «PDC эмуляция» – эмулятор PDC (PDC Emulator);
- «Схема» – хозяин схемы (Schema Master);
- «Имена домена» – хозяин именования доменов (Domain Naming Master);
- «Инфраструктура» – хозяин инфраструктуры (Infrastructure Master);
- «RID распределение» – хозяин RID (RID Master).

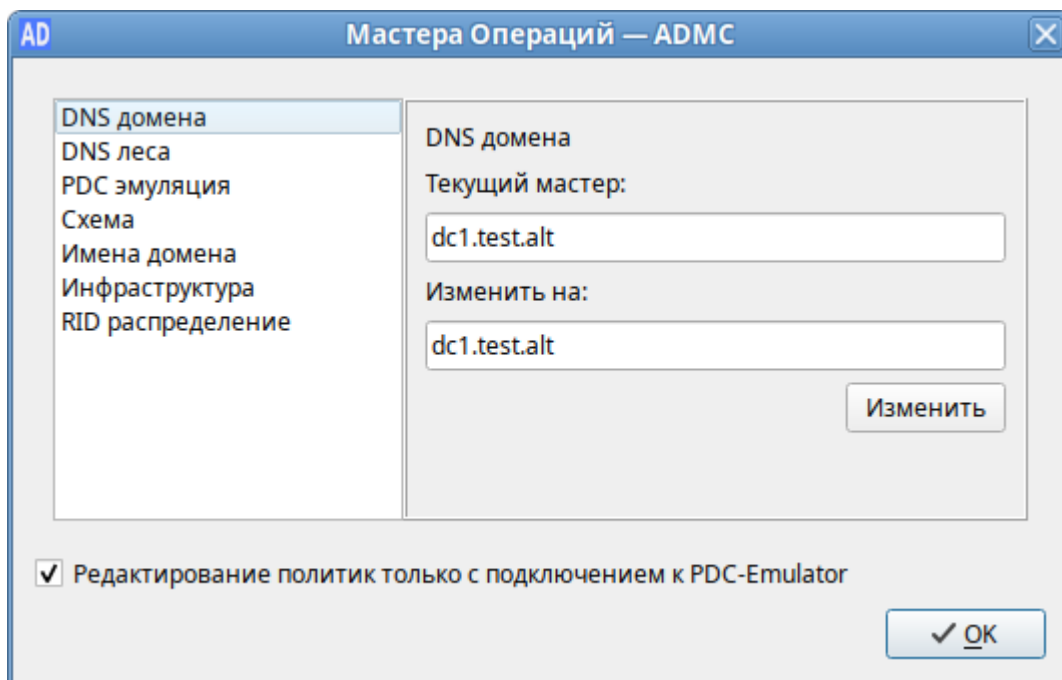


Рис. 123 – Просмотр текущего владельца роли

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, появится сообщение, показанное на рис. 124.

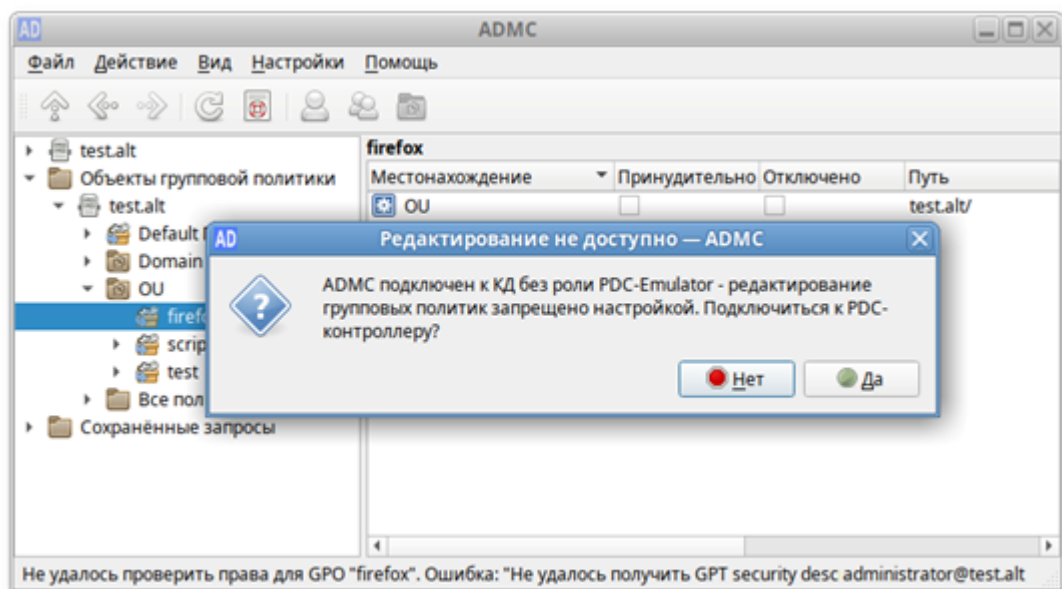


Рис. 124 – Окно «Редактирование не доступно»

Для штатной передачи роли нужно выполнить следующие действия:

- 1) в окне «Параметры подключения – ADMS» («Файл» → «Параметры подключения») выбрать контроллер домена, который должен стать новым владельцем роли, и нажать кнопку «ОК» (рис. 125);

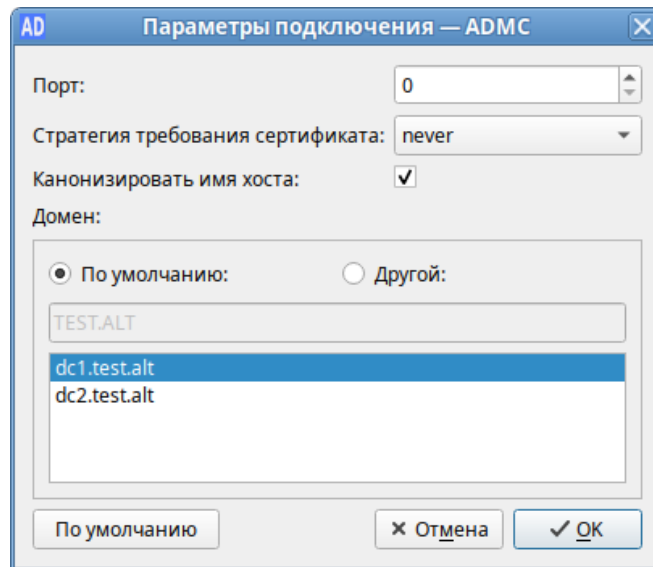


Рис. 125 – Окно «Параметры подключения – ADMS»

- 2) в окне «Мастера Операций – ADMS» («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» (рис. 126);

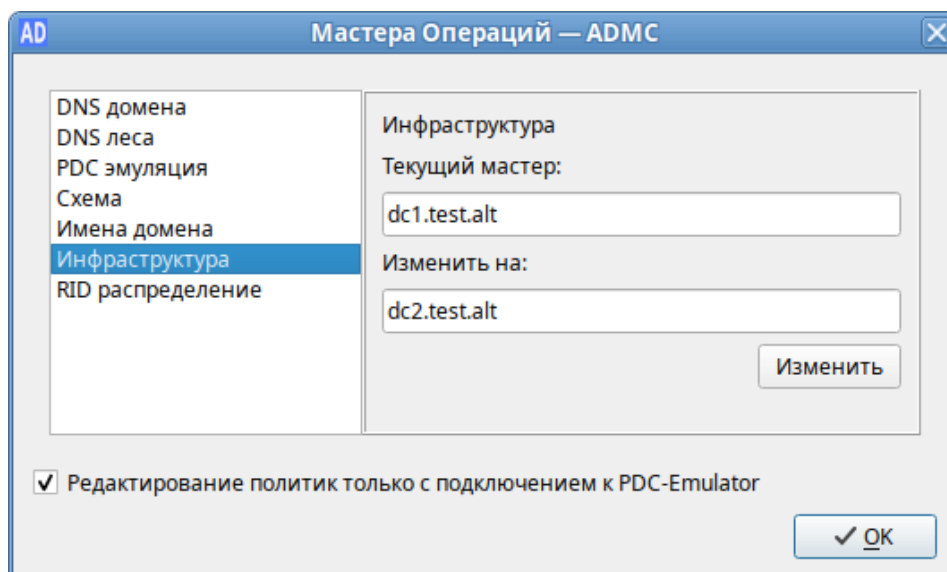


Рис. 126 – Передача роли на новый DC

3) владелец роли будет изменен (рис. 127).

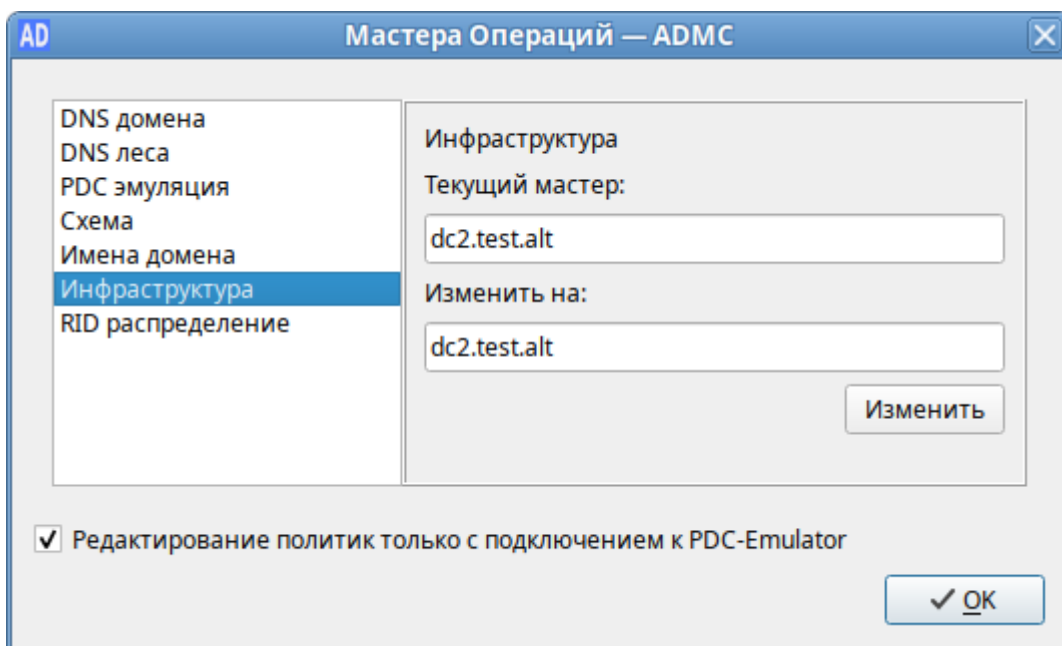


Рис. 127 – Новый владелец роли

4.5.15. Выбор объектов

Выбор объектов осуществляется в диалоговом окне «Выбрать объекты – ADMS» (рис. 128). Доступ к этому диалоговому окну можно получить из разных мест, например, при выборе действия «Добавить в группу...» в контекстном меню учетной записи пользователя.

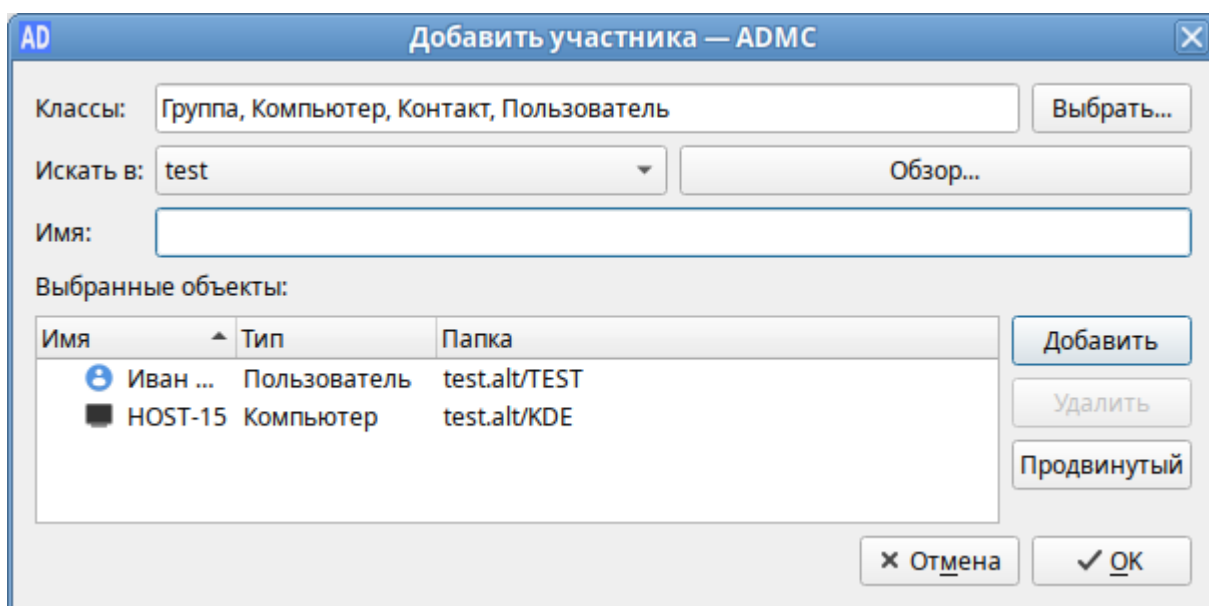


Рис. 128 – Диалоговое окно выбора объектов

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 (рис. 129);

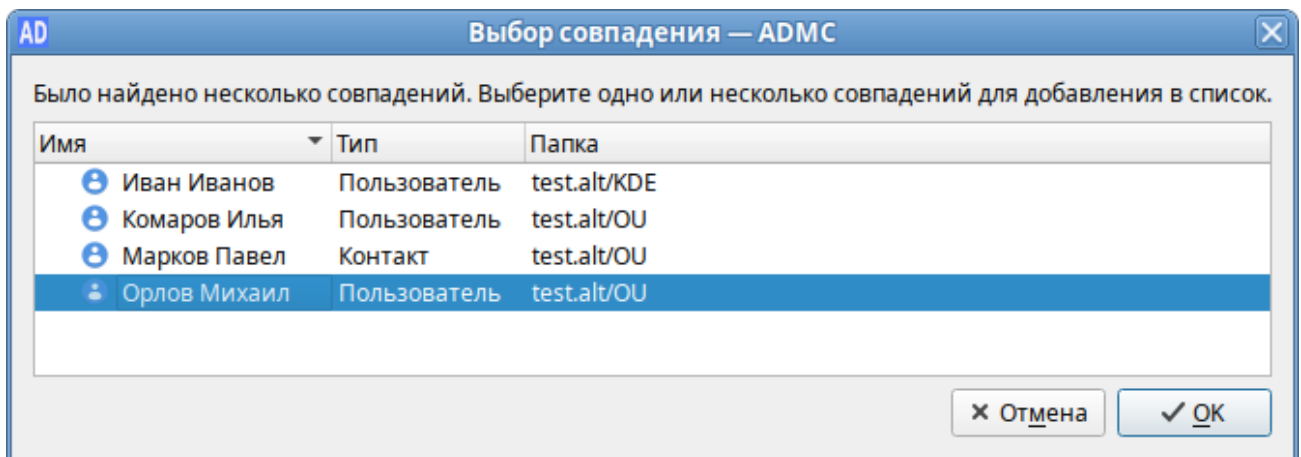


Рис. 129 – Выбор объектов из списка совпадений

- 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».

4.5.16. Поиск объектов

Поиск объектов осуществляется в диалоговом окне «Поиск объектов – ADMS» (рис. 130). Доступ к этому диалоговому окну можно получить, выбрав пункт «Найти...» в меню «Действие» или в контекстном меню контейнера.

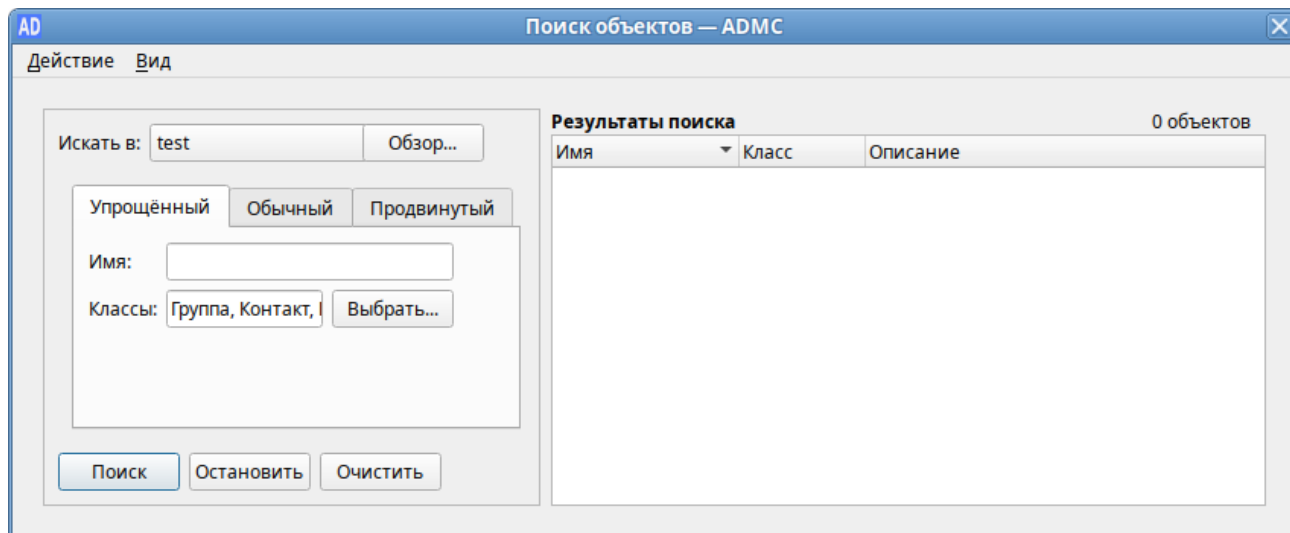


Рис. 130 – Поиск объектов

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 (рис. 131).

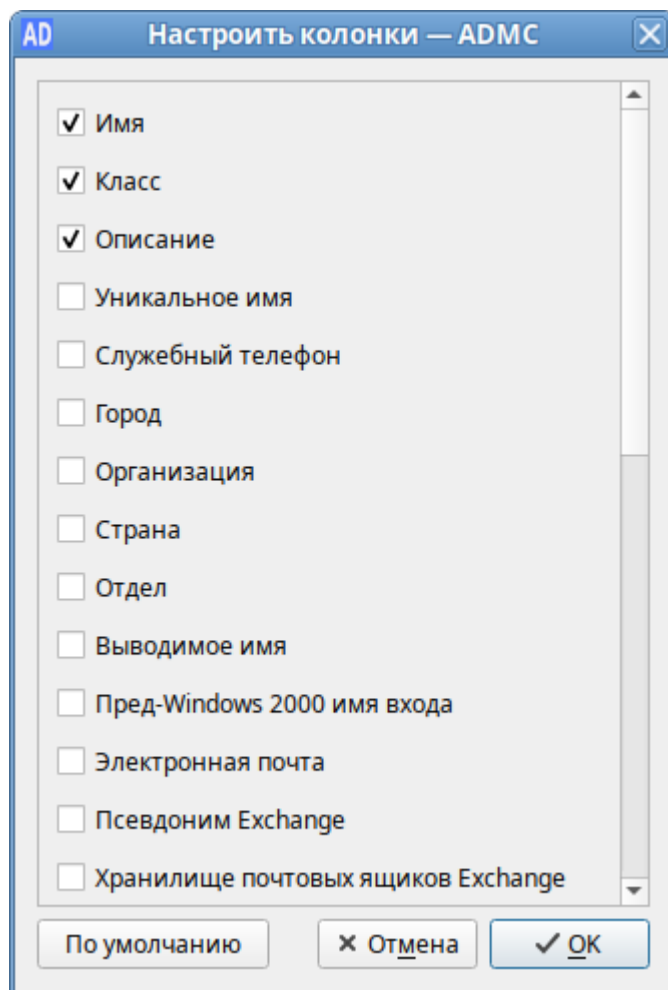


Рис. 131 – Поля, отображаемые в результатах

4.5.16.1. Простой поиск

Процедура простого поиска:

- 1) в диалоговом окне «Поиск объектов – ADMS» выбрать вкладку «Упрощенный» (см. рис. 130);
- 2) в поле «Классы», нажав кнопку «Выбрать...», выбрать классы объектов для поиска (рис. 132);

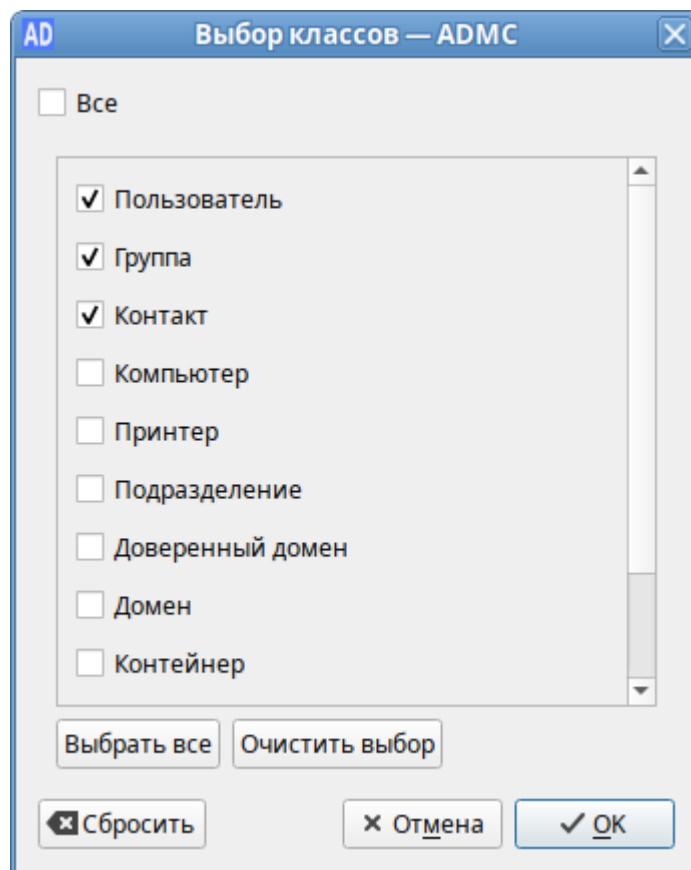


Рис. 132 – Выбор классов объектов для поиска

3) в поле «Имя» ввести имя объекта и нажать кнопку «Поиск» (рис. 133).

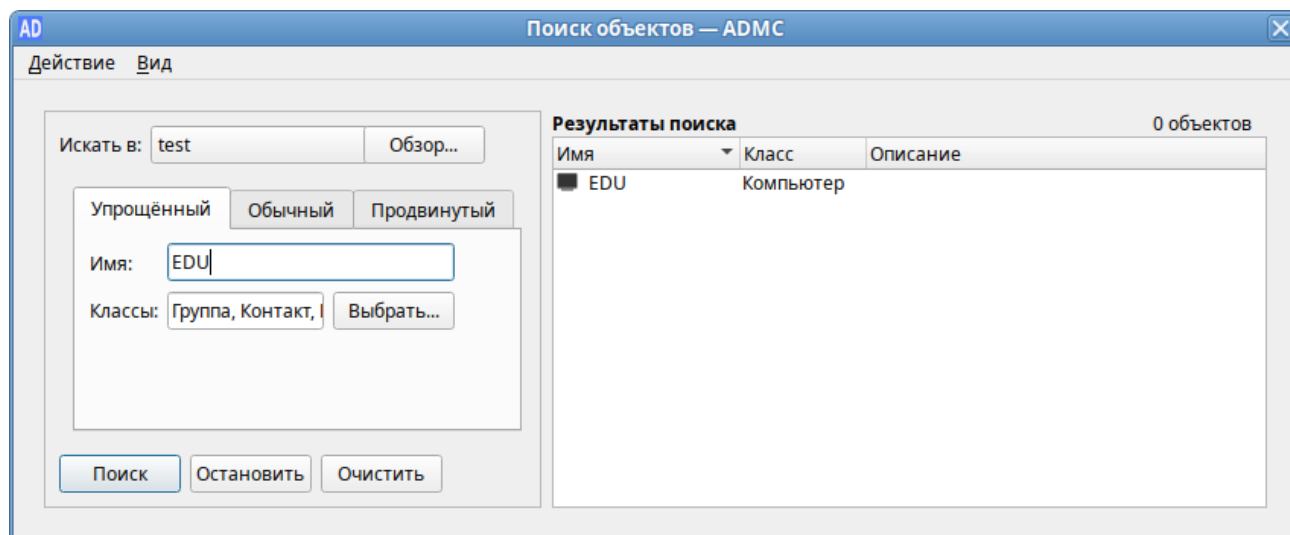


Рис. 133 – Простой поиск

4.5.16.2. Обычный поиск

При использовании обычного поиска создаются фильтры, определяющие критерии поиска:

- 1) в диалоговом окне «Поиск объектов – ADMS» (см. рис. 130) выбрать вкладку «Обычный»;
- 2) в поле «Классы», нажав кнопку «Выбрать...», выбрать классы объектов для поиска (рис. 132);
- 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 нужно 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 нужно удалить фильтр из списка;
- 7) нажать кнопку «Очистить», если нужно очистить список фильтров;
- 8) нажать кнопку «Поиск» (рис. 134).

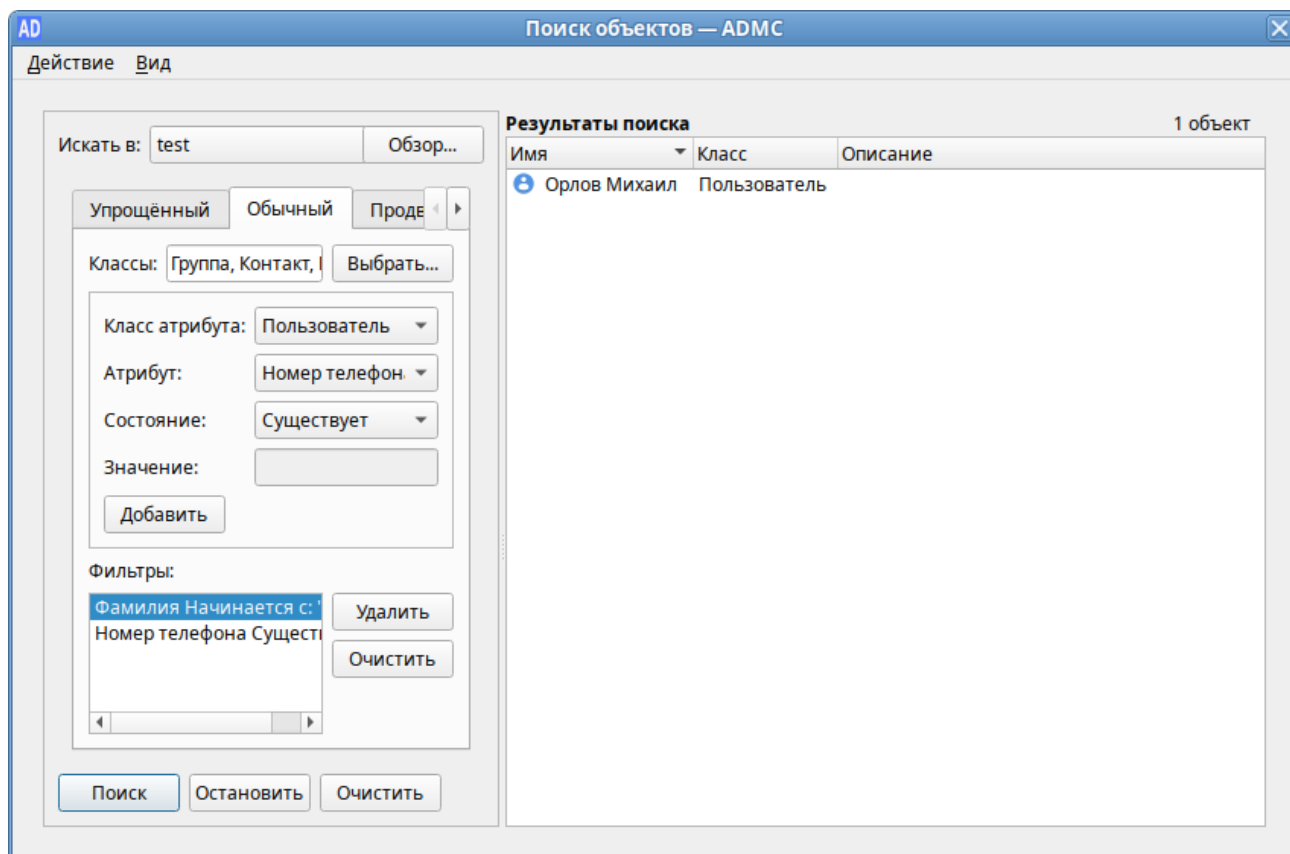


Рис. 134 – Обычный поиск

4.5.16.3. Продвинутый поиск

Продвинутый поиск предполагает использование LDAP-фильтров.

Использование LDAP-фильтров является наиболее эффективным способом поиска объектов в «Альт Домен».

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 – ADMS» (см. рис. 130) 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» (рис. 135).

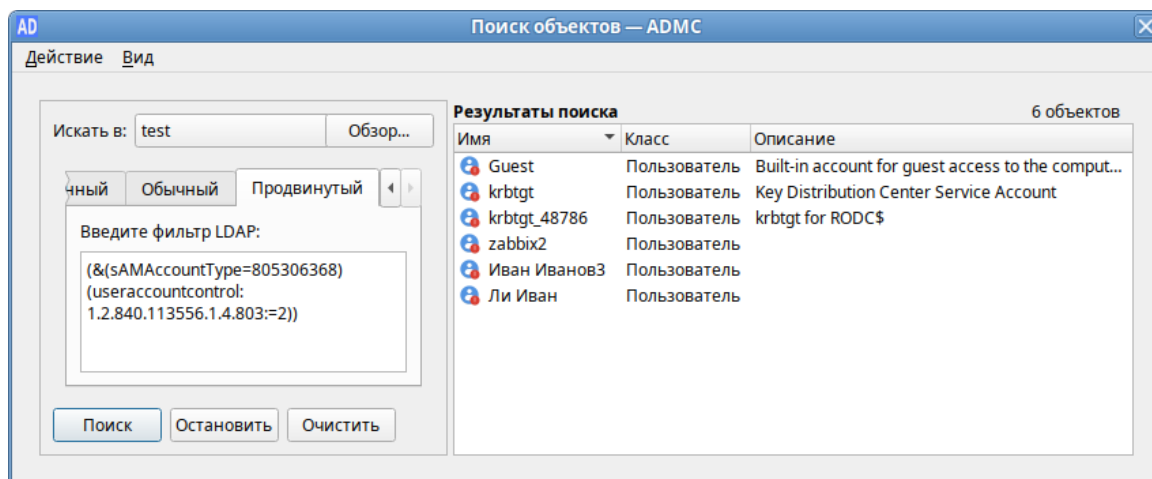


Рис. 135 – Продвинутый поиск

4.5.17. Использование сохраненных результатов поиска

Сохранение запросов (результатов поиска) – это удобный способ сохранять и воспроизводить поиск. Сохраненные запросы позволяют создавать различные LDAP-фильтры для выборки объектов домена. С помощью сохраненных запросов можно быстро и эффективно решать задачи поиска и выборки объектов по различным критериям.

При использовании сохраненных запросов администратор может выполнять групповые операции с объектами из разных OU домена. Например, можно выполнить массовую блокировку/разблокировку, удаление учетных записей, переименование.

Сохраненные запросы можно организовать в древовидную структуру (рис. 136).

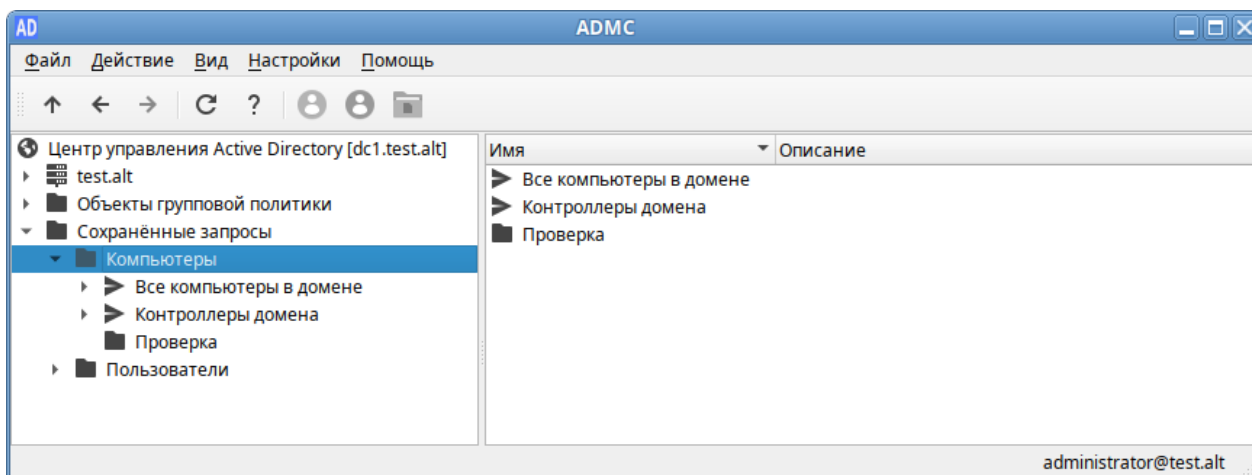


Рис. 136 – Структура сохраненных запросов

Создание папки запросов:

- 1) в контекстном меню папки «Сохраненные запросы» или ее подпапки выбрать пункт «Создать» → «Папка запросов» (рис. 137);

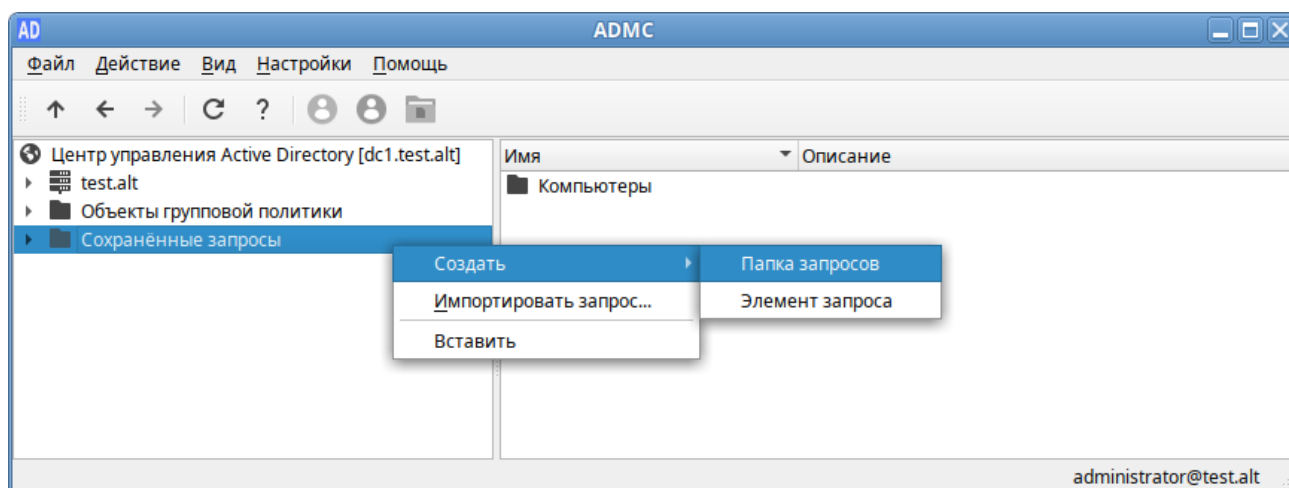


Рис. 137 – Контекстное меню папки «Сохраненные запросы»

- 2) в диалоговом окне «Создать папку запросов – ADMS» в поле «Имя» вести название папки, в поле «Описание» можно добавить описание папки (рис. 138);
- 3) нажать кнопку «ОК».

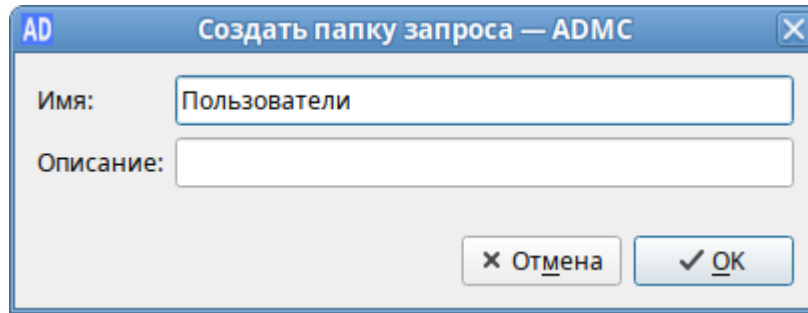


Рис. 138 – Создание папки запросов

Создание запроса:

- 1) в контекстном меню папки запроса выбрать пункт «Создать» → «Элемент запроса» (рис. 139);

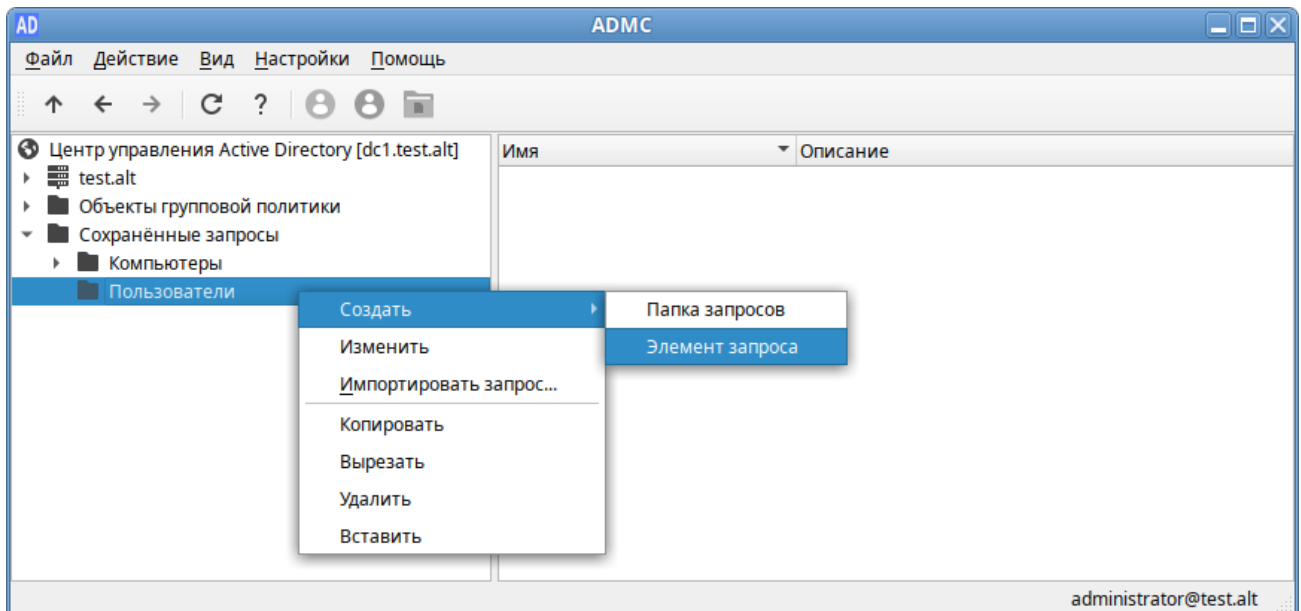


Рис. 139 – Контекстное меню папки запроса

- 2) в диалоговом окне создания запроса 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 (рис. 140);

- 3) нажать кнопку «Изменить фильтр», чтобы создать фильтр поиска (для получения информации о том, как создавать фильтры, см. п. 4.5.16);
- 4) после создания фильтра он будет отображаться в поле «Фильтр» (в формате LDAP);
- 5) нажать кнопку «ОК».

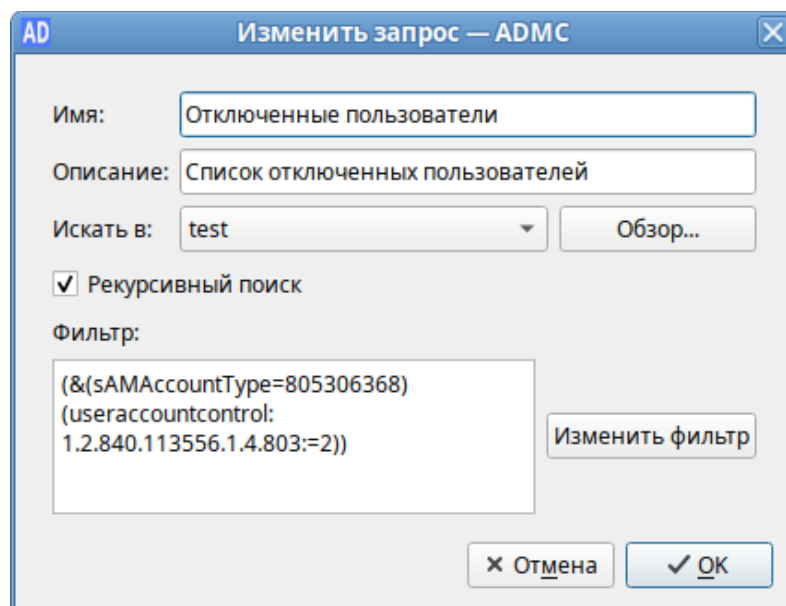


Рис. 140 – Диалоговое окно создания запроса

При выборе сохраненного запроса, в правом окне появится список объектов, который соответствует данному запросу (рис. 141).

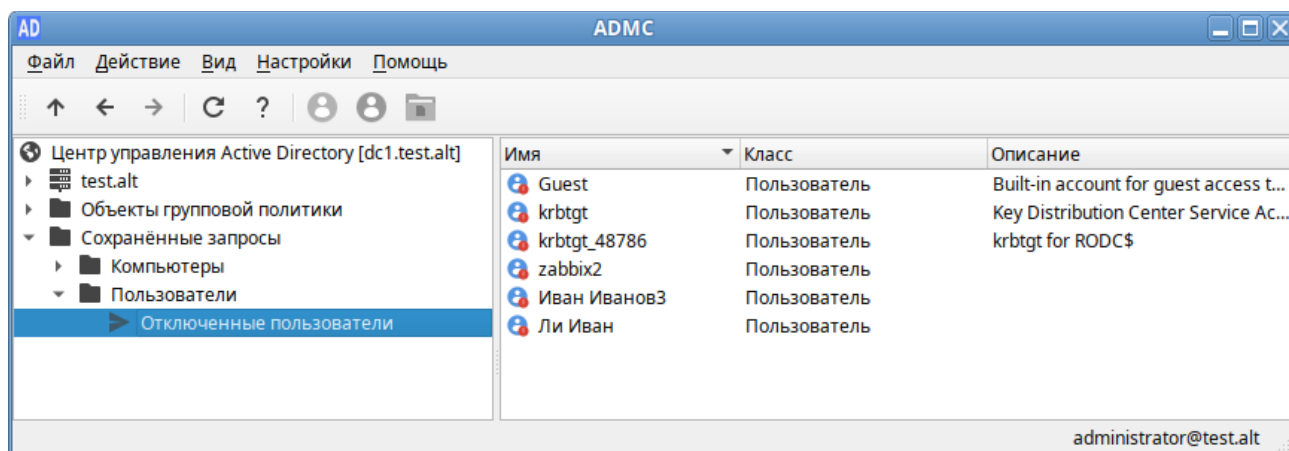


Рис. 141 – Результат выполнения запроса

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...» (рис. 142);
- 2) в открывшемся диалоговом окне выбрать экспортированный файл поиска;
- 3) нажать кнопку «Открыть».

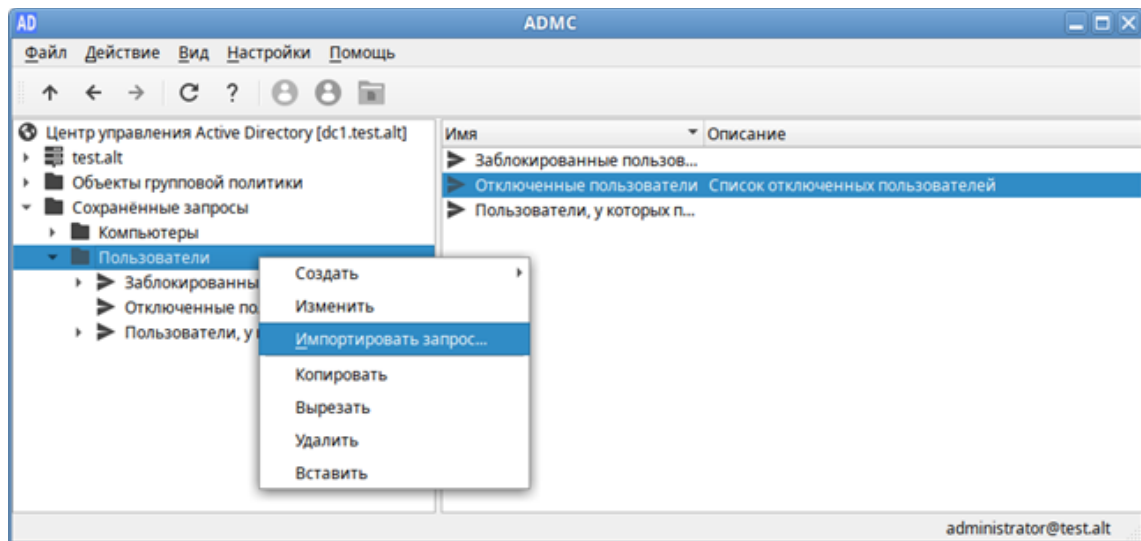


Рис. 142 – Импорт запроса

Для удаления запроса или папки запросов в контекстном меню объекта выбрать пункт «Удалить».

4.6. Модуль редактирования настроек клиентской конфигурации (GPUI)

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 домене.

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 ADMS.

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 находиться в одном из трех состояний: «Включено», «Отключено», «Не сконфигурировано». В состоянии «Отключено» 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.

4.6.1. Запуск GPUI для редактирования доменных политик

По умолчанию GPUI не редактирует никаких политик. Для того чтобы редактировать политику, GPUI нужно запустить либо из ADMS, выбрав в контекстном меню объекта групповой политики пункт «Изменить...» (рис. 143).

Те же действия можно произвести при помощи указания каталога групповой политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXXX}"
```

Ключ `-p` позволяет указать путь к шаблону групповой политики, который нужно редактировать, `dc1.test.alt` – имя контроллера домена, а `{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXXX}` – GUID шаблона групповой политики для редактирования. Можно указывать как каталоги `smb`, так и локальные каталоги.

Пример запуска GPUI для редактирования политики:

```
$ gpui-main -p "smb://dc1.test.alt/SysVol/test.alt/Policies/{2E80AFBE-BBDE-408B-B7E8-AF79E02839D6}"
```

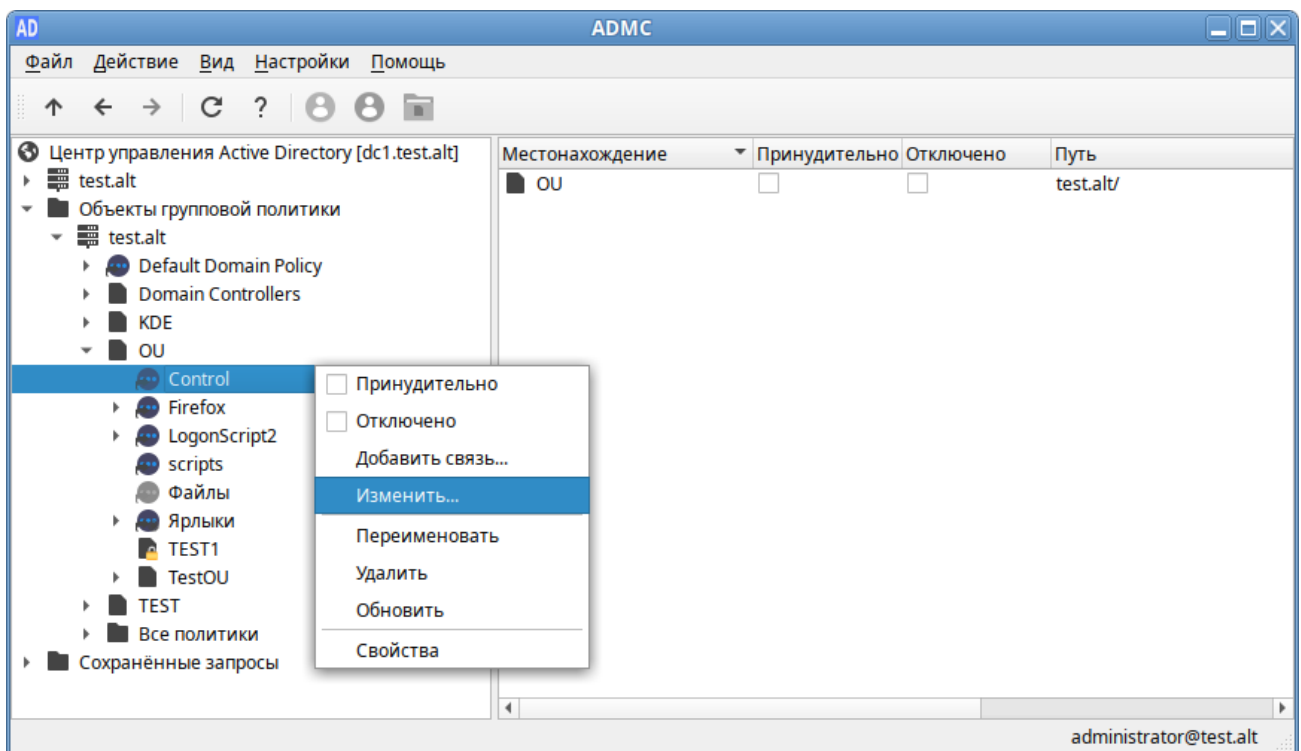


Рис. 143 – Запуск GPUI из ADMC

Примечание. GUID шаблона групповой политики можно узнать в ADMC (это дочерний контейнер `Policies` контейнера `System`), в настройках должен быть отмечен пункт «Дополнительные возможности» (рис. 144).

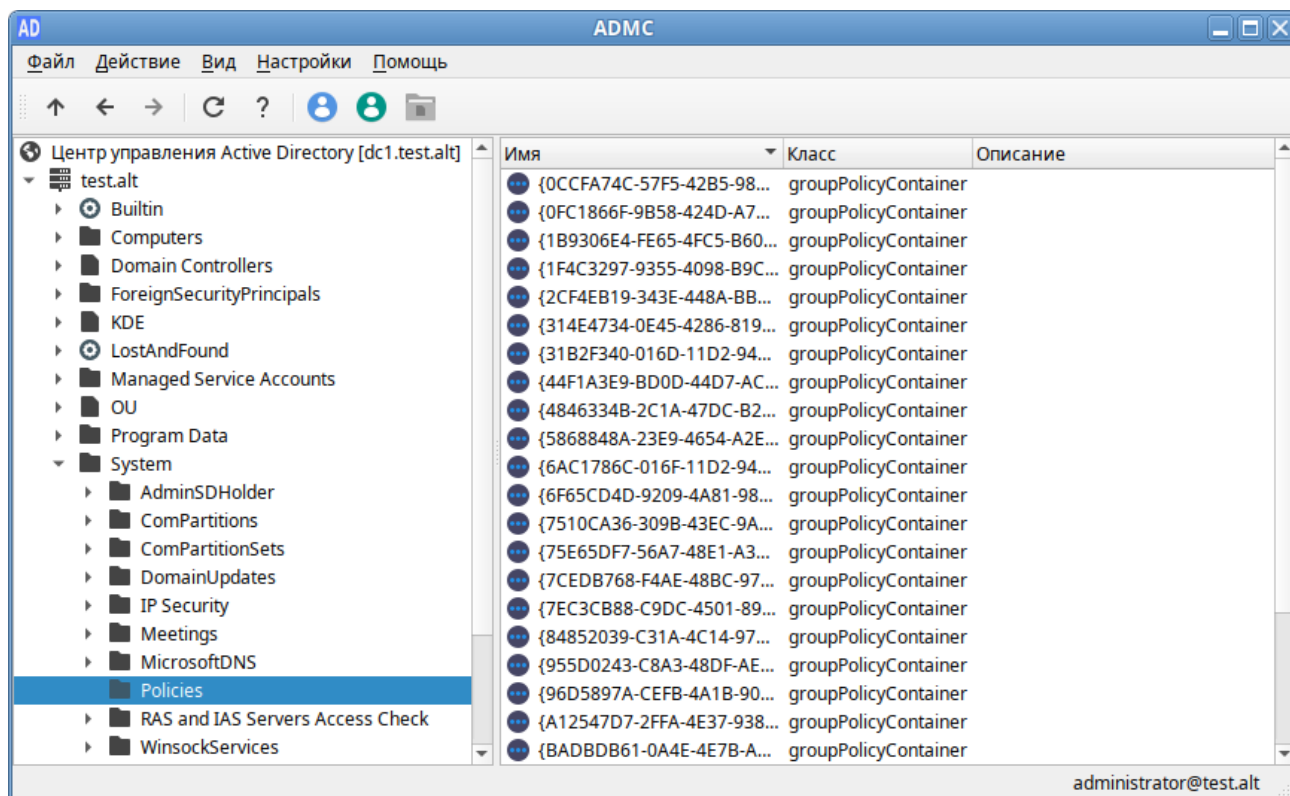


Рис. 144 – Контейнеры групповых политик

4.6.2. 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 можно также выбрать в графическом интерфейсе:

- 1) выбрать пункт меню «Файл» → «Открыть папку с ADMX файлами» (рис. 145);
- 2) открыть папку с шаблонами.

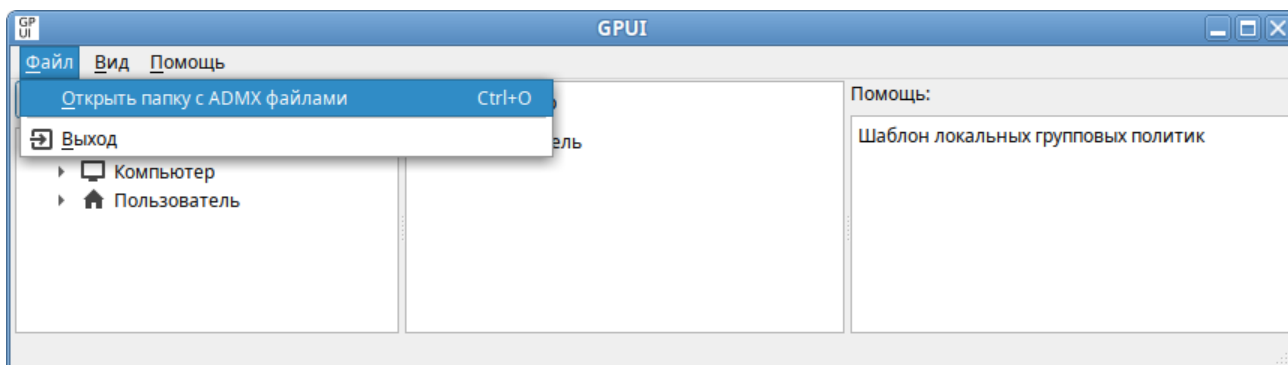


Рис. 145 – Подпункт «Открыть папку с ADMX файлами»

4.6.3. Интерфейс

Все настройки в GPUI разделены на два раздела:

- «Компьютер» («Machine») – раздел с настройками параметров компьютера;
- «Пользователь» («User») – раздел с настройками параметров пользователей домена (рис. 146).

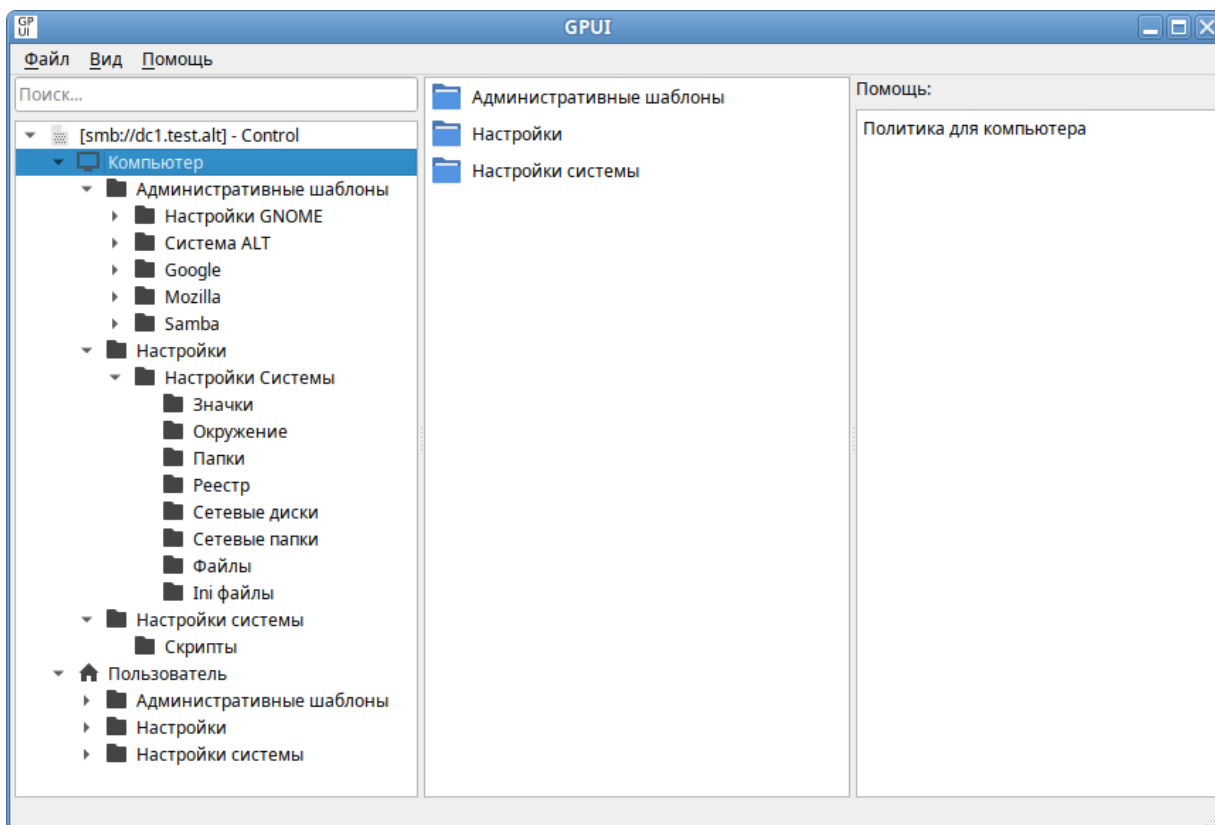


Рис. 146 – Интерфейс GPUI

Если параметр 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 СП 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.

4.6.3.1. 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 (рис. 147).

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).

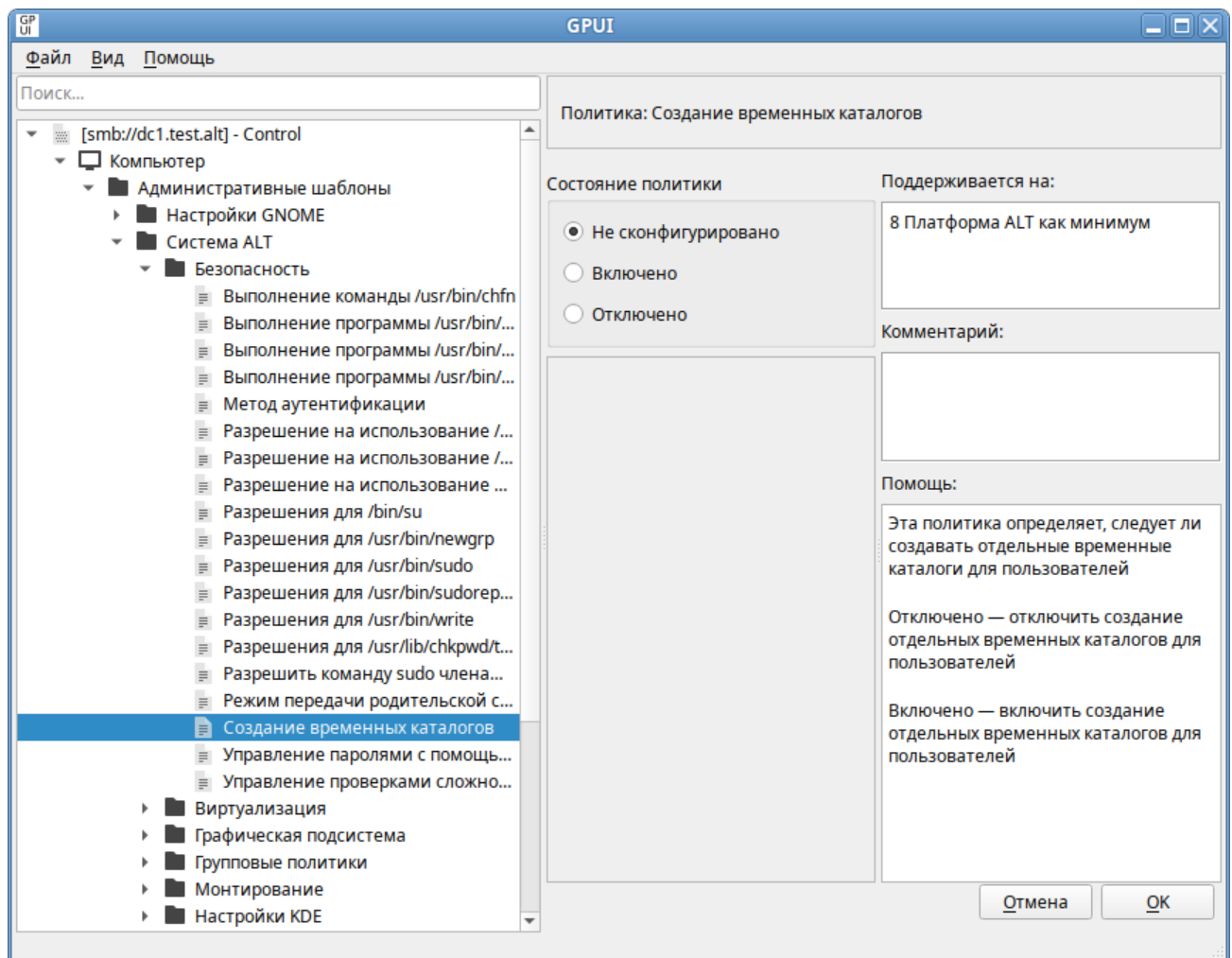


Рис. 147 – Состояние параметров политики

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 «ОК».

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 групповые политики, нужно включить политику и указать путь к файлу с изображением в поле «Файл» (рис. 148).

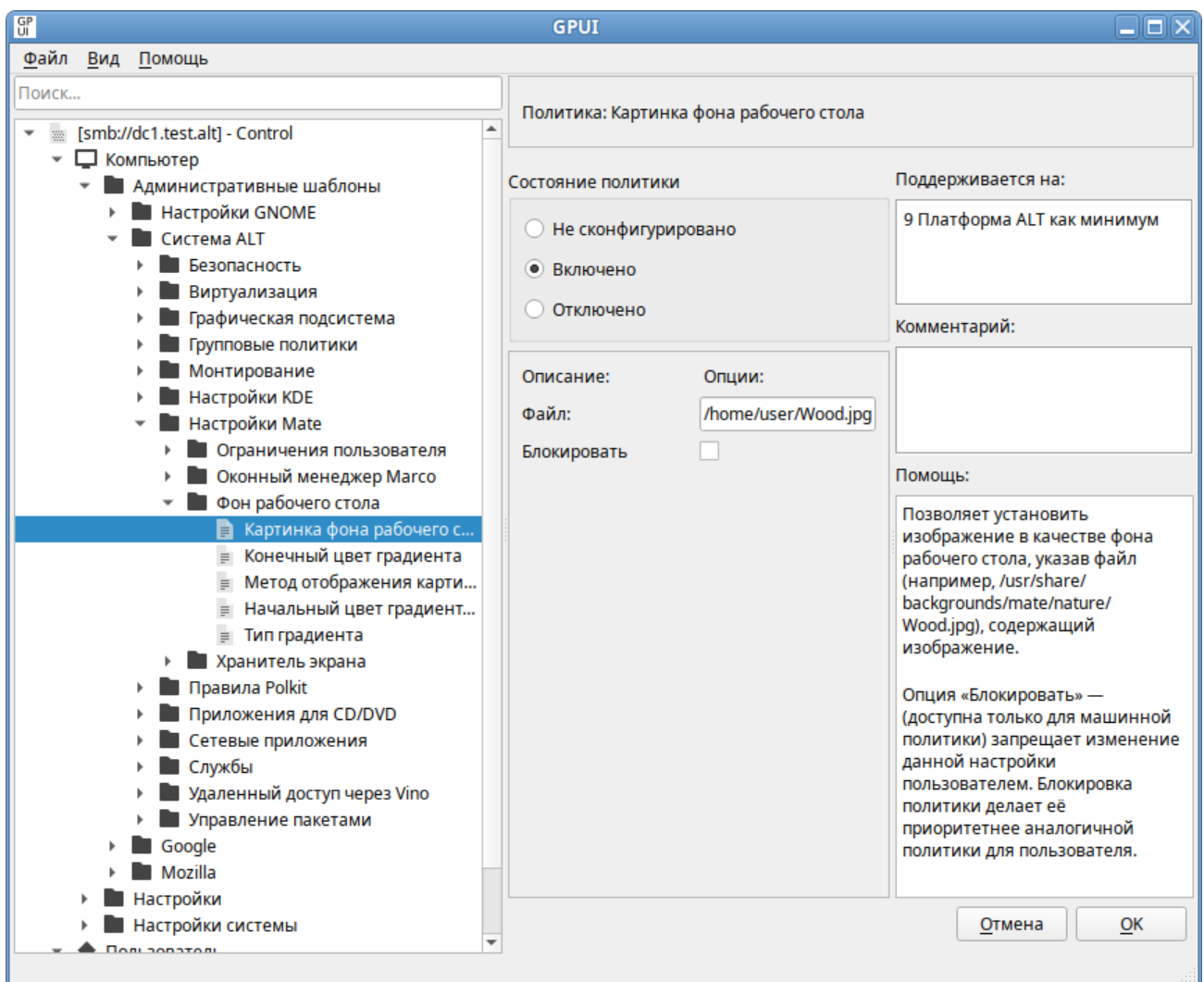


Рис. 148 – Установка изображения в качестве фона рабочего стола через групповые политики

В поле «Комментарий» можно указать примечание для групповой политики.

4.6.3.2. Фильтрация административных шаблонов

По умолчанию в GPUI отображаются все установленные административные шаблоны. Чтобы изменить отображение параметров политик административных шаблонов можно настроить фильтр административных шаблонов (рис. 149).

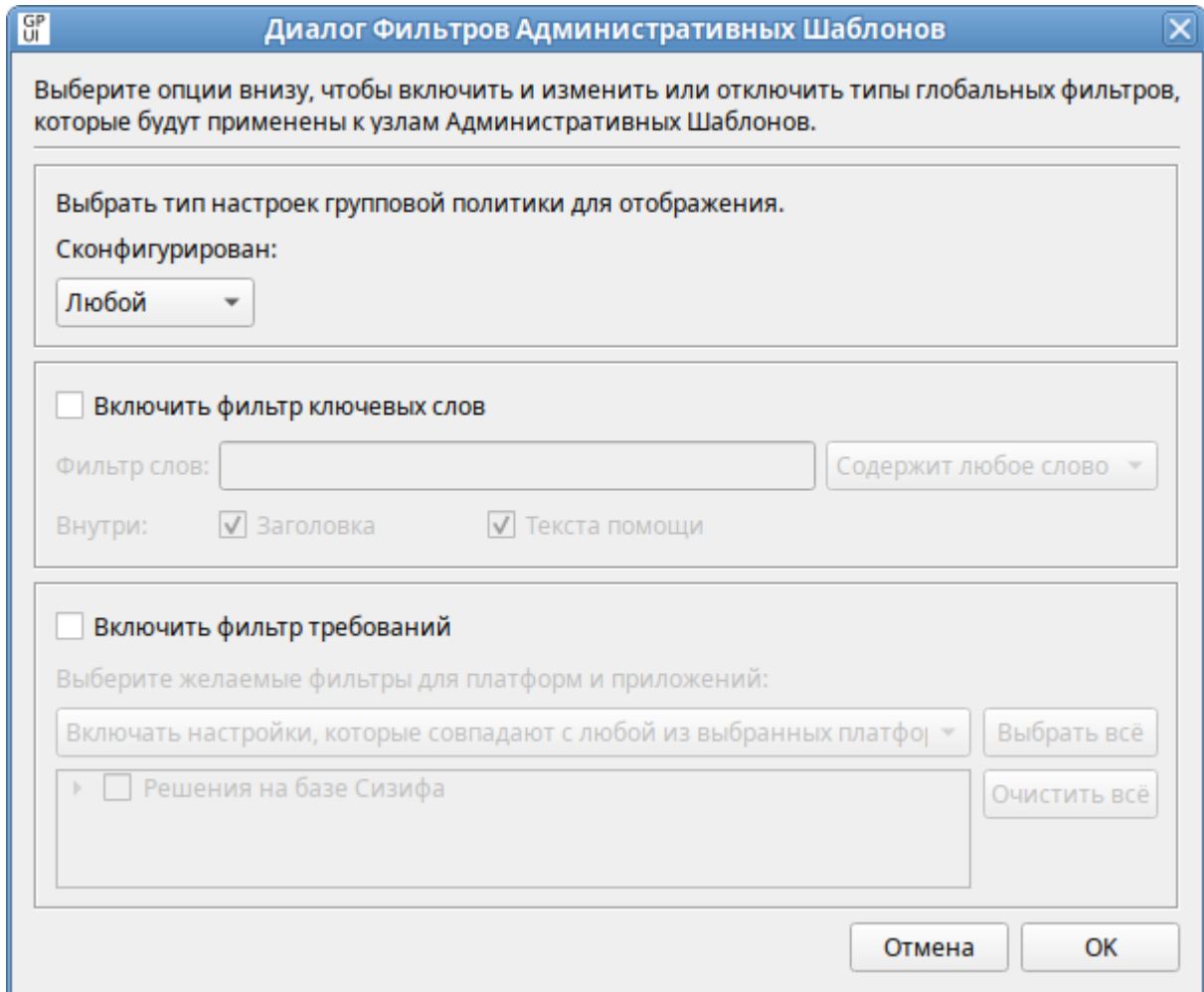


Рис. 149 – Диалог фильтров административных шаблонов

Фильтр административных шаблонов можно применять, если 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.

4.6.3.2.1. 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:

- 1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (рис. 150);

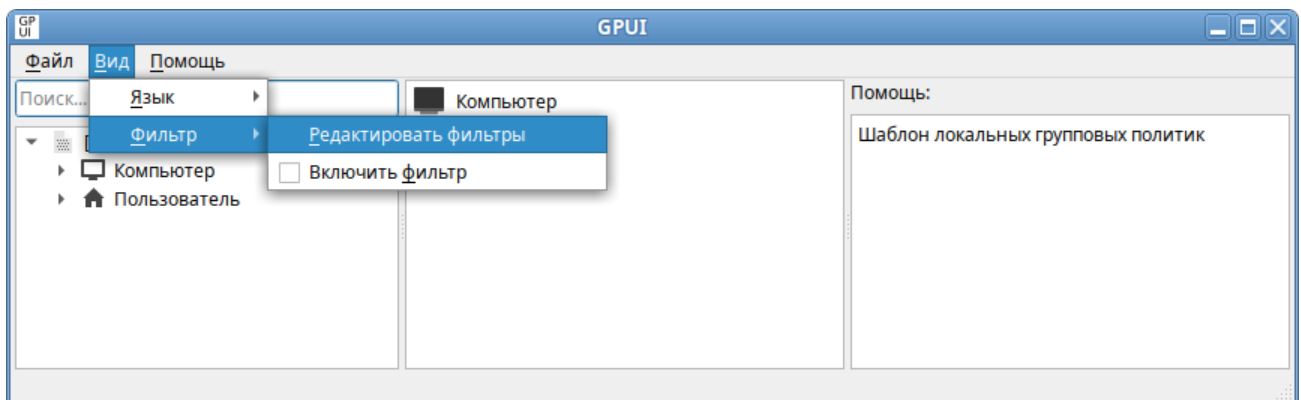


Рис. 150 – Фильтр по настроенным параметрам

- 2) в открывшемся окне в списке «Сконфигурирован» выбрать необходимый фильтр (рис. 151);
- 3) нажать кнопку «ОК», чтобы сохранить параметры фильтра;
- 4) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 152).

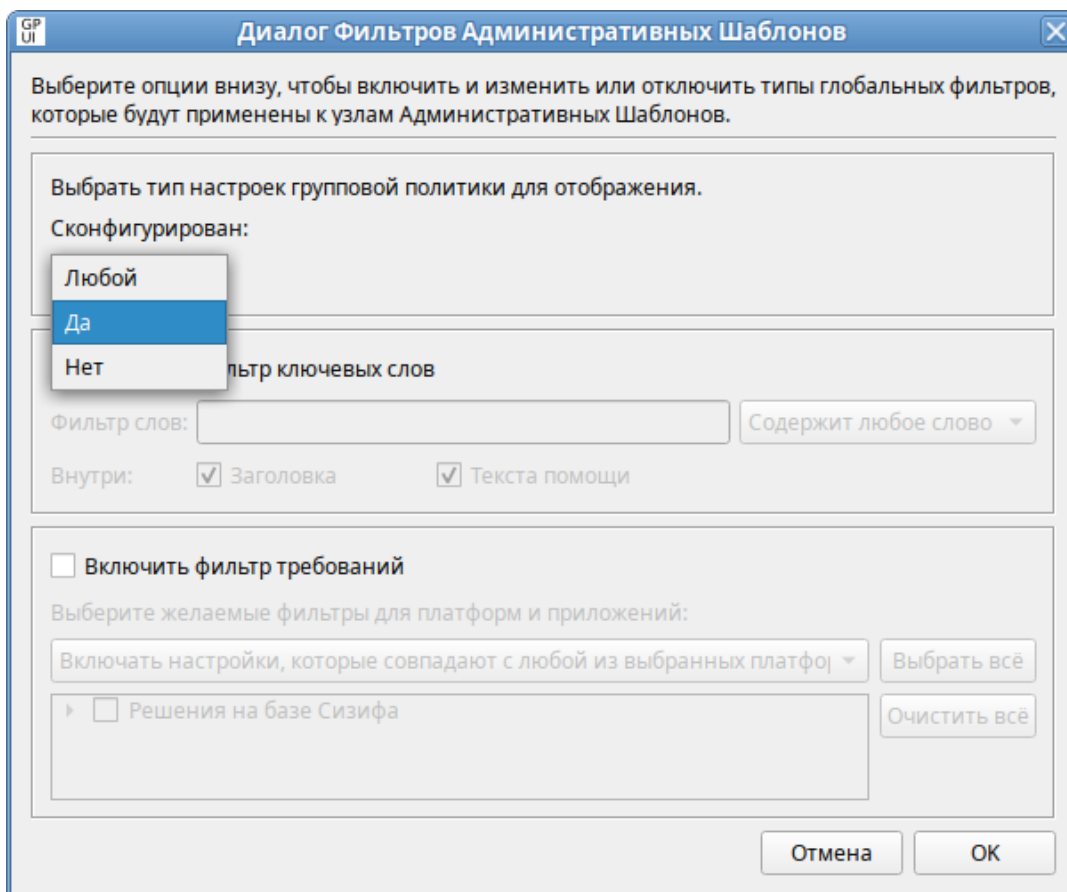


Рис. 151 – Фильтр по настроенным параметрам

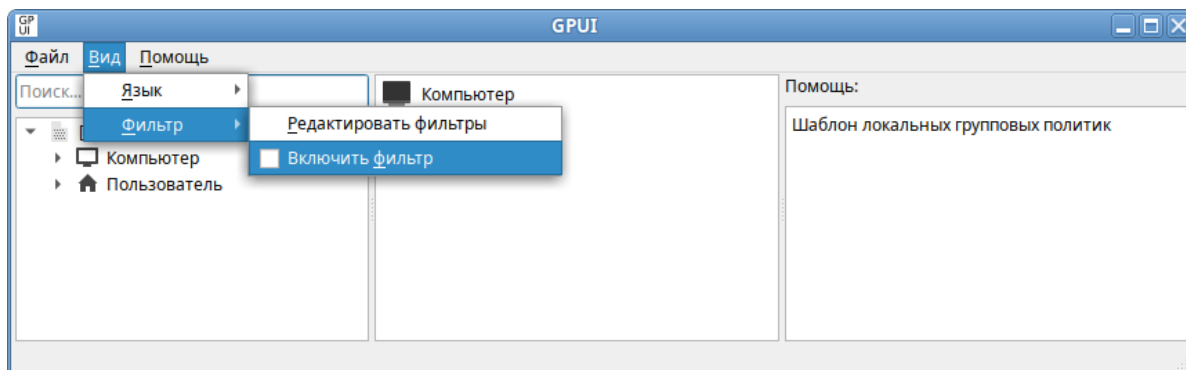


Рис. 152 – Включение фильтра административных шаблонов

4.6.3.2.2. Фильтр по ключевым словам

Для установки фильтра по ключевым словам:

- 1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (см. рис. 150);
- 2) в открывшемся окне установить отметку в поле «Включить фильтр ключевых слов» (рис. 153);

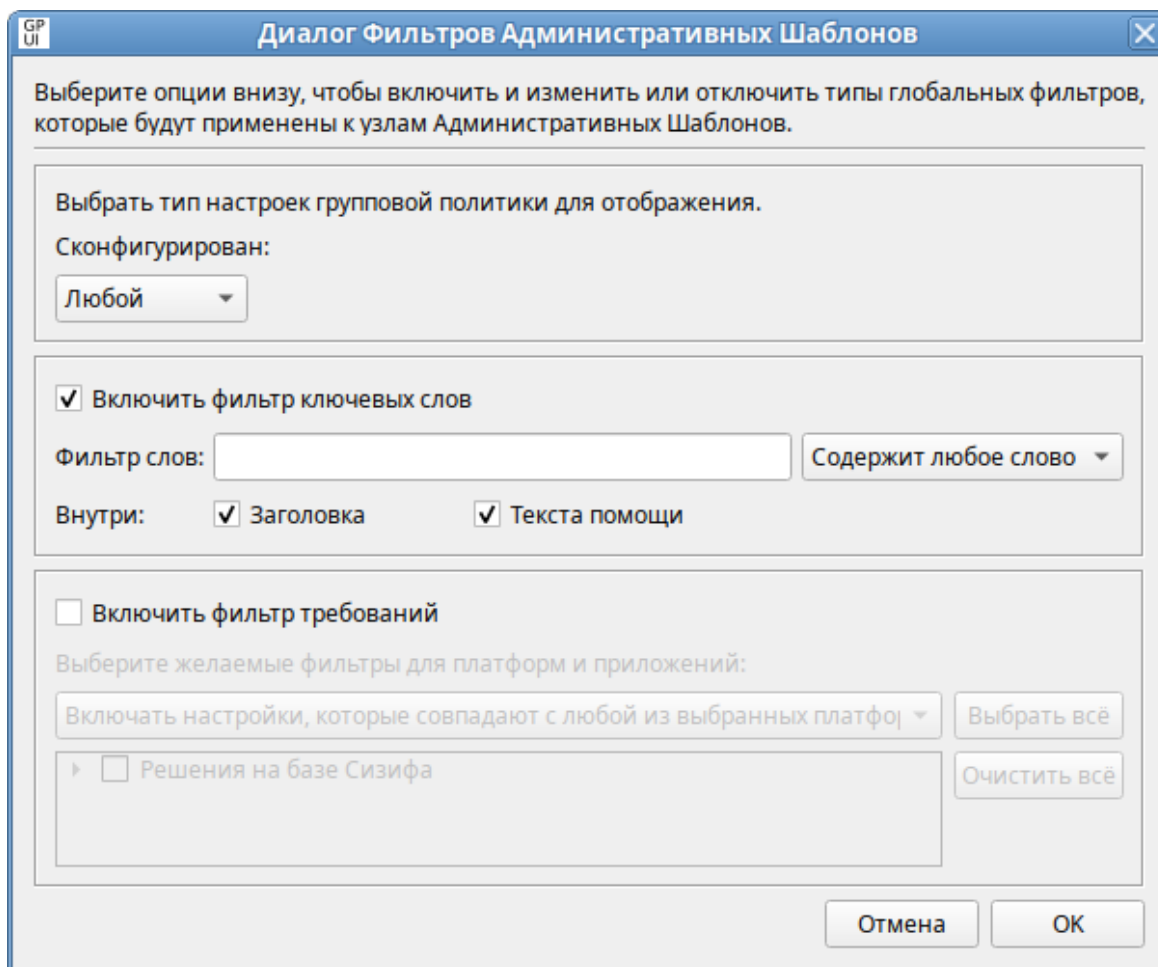


Рис. 153 – Отметка «Включить фильтр ключевых слов»

- 3) ввести одно или несколько ключевых слов в поле «Фильтр слов» и выбрать 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 «ОК», чтобы сохранить параметры фильтра (рис. 154);

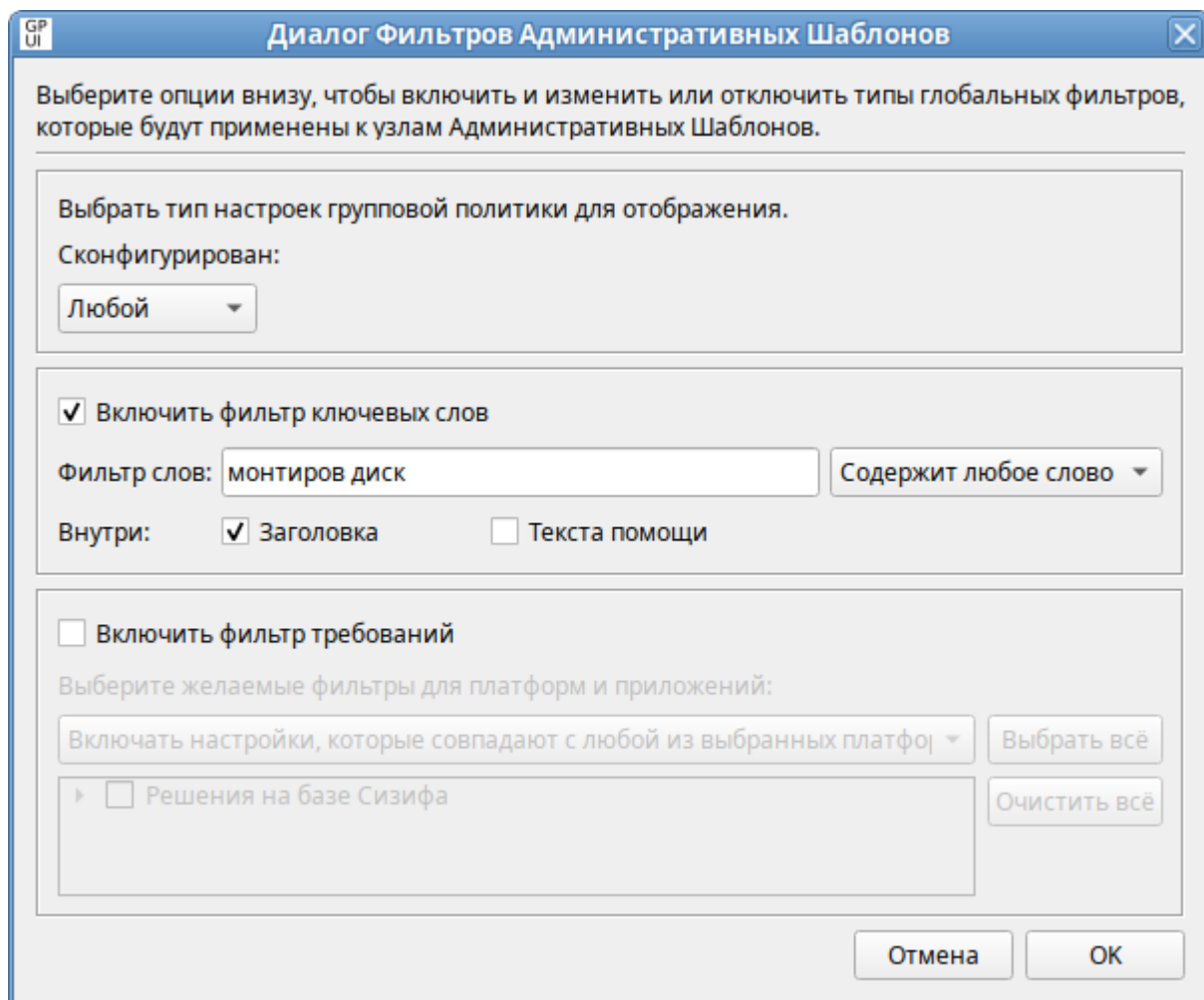


Рис. 154 – Настроенный фильтр ключевых слов

- б) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (см. рис. 152).

Результат применения фильтра по ключевым словам (рис. 155).

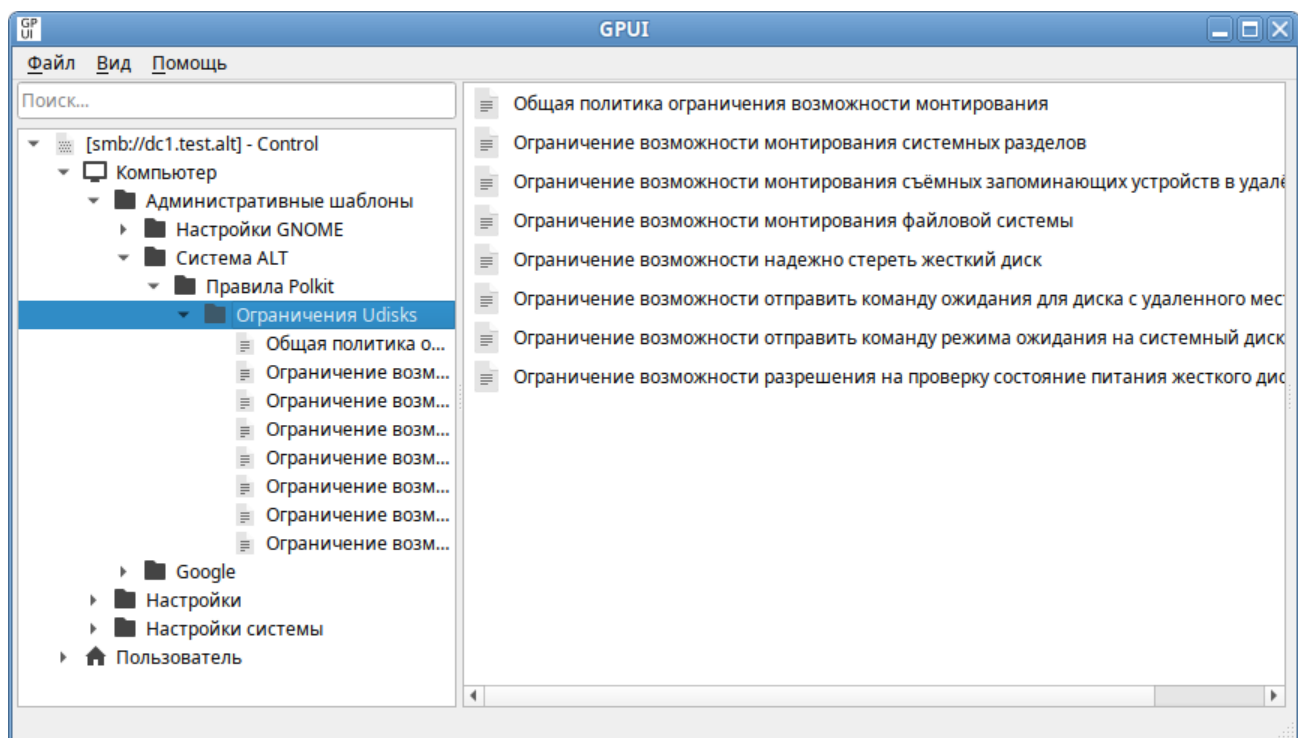


Рис. 155 – Результат применения фильтра по ключевым словам

4.6.3.2.3. 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:

- 1) в меню выбрать «Вид» → «Фильтр» → «Редактировать фильтр» (см. рис. 150);
- 2) в открывшемся окне установить отметку в поле «Включить фильтр ключевых требований»;
- 3) в списке «Выберите желаемые фильтры для платформы и приложений» выбрать фильтр:
 - включать настройки, которые совпадают с любой из выбранных платформ;
 - включить настройки, которые совпадают со всеми выбранными платформами;

- 4) выбрать необходимые платформы (рис. 156). Можно выбрать пункт «Решения на базе Сизифа», нажать кнопку «Выбрать все», чтобы выбрать все элементы в списке, или нажать кнопку «Очистить все», чтобы снять выделение всех элементов списка;

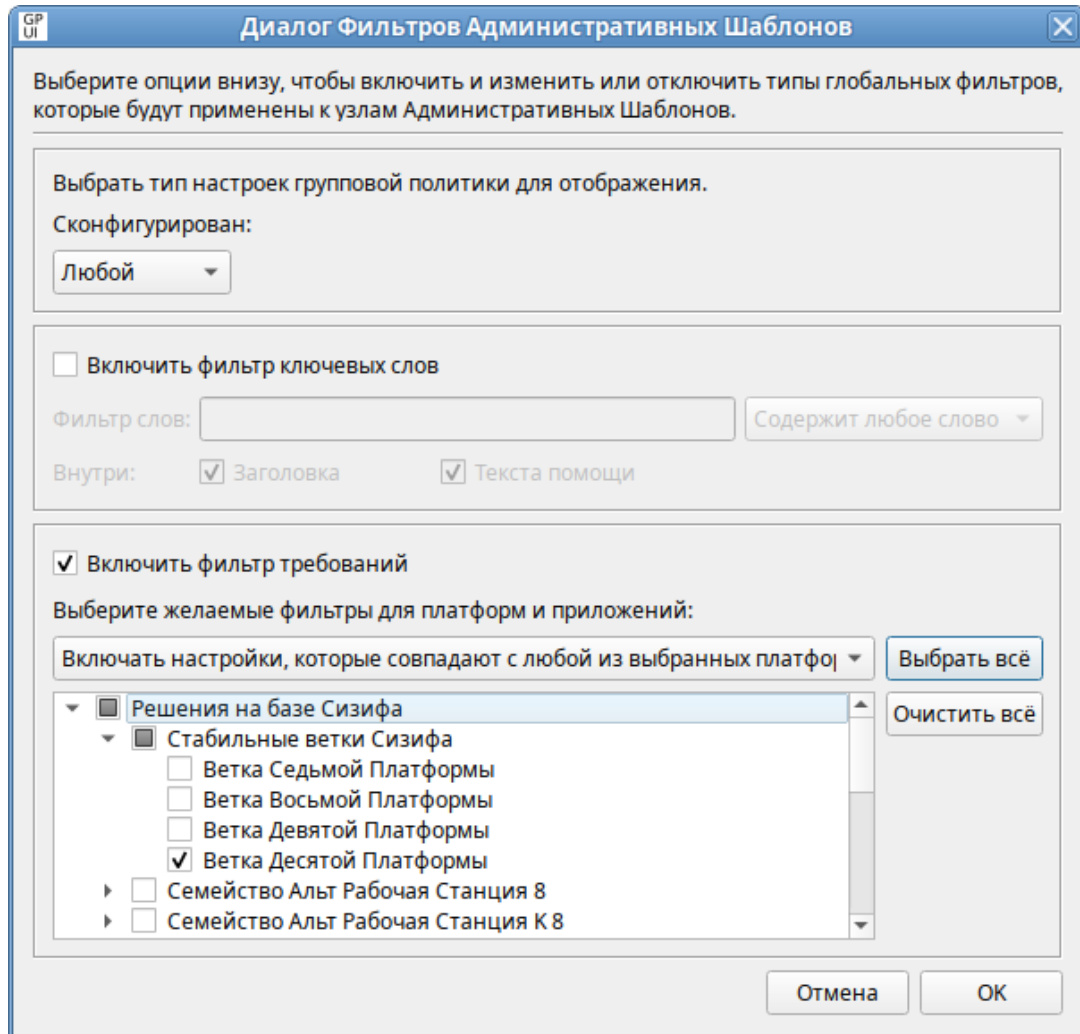


Рис. 156 – Настроенный фильтр по требованиям

- 5) нажать кнопку «ОК», чтобы сохранить параметры фильтра;
- 6) чтобы применить фильтр в меню выбрать «Вид» → «Фильтр» → «Включить фильтр» (рис. 152).

4.6.3.3. Работа с предпочтениями групповых политик

GPUI позволяет настраивать следующие предпочтения:

- «Значки» – создание, редактирование или удаление ярлыков;
- «Окружение» – создание, редактирование или удаление переменных среды;

- «Папки» – создание, редактирование или удаление папок;
- «Реестр» – копирование параметров реестра и их применение к другим компьютерам, создание, замена или удаление параметров реестра (для машин Windows);
- «Сетевые папки» – создание, удаление (скрытие из общего доступа) или редактирование общих ресурсов;
- «Сетевые диски» – создание, редактирование или удаление сопоставленных дисков и настройка видимости всех дисков;
- «Файлы» – копирование, замена, удаление или изменение атрибутов файлов;
- «INI-файлы» – 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») (рис. 157).

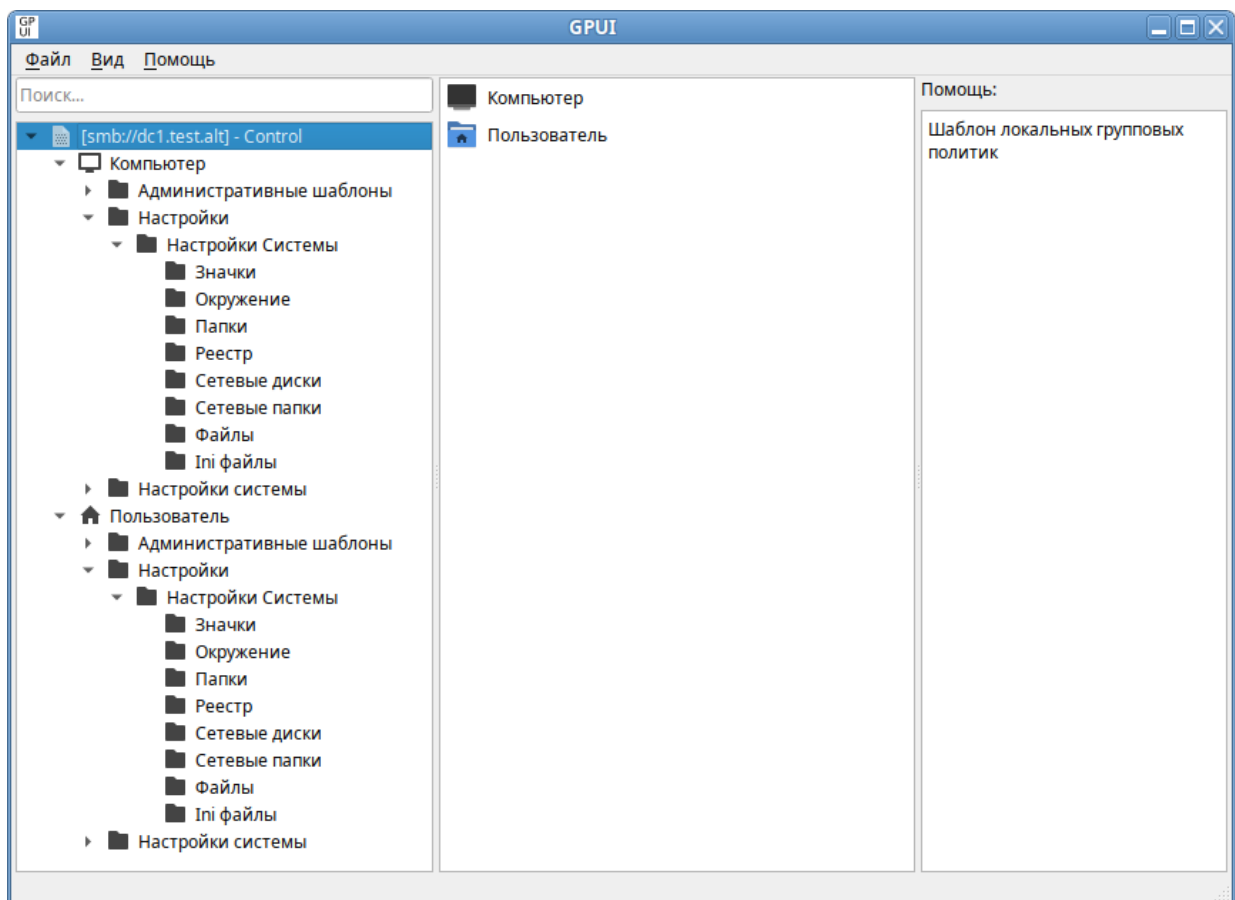


Рис. 157 – Управление предпочтениями

В каждом объекте групповой политики с каждым из расширений предпочтения можно создать несколько элементов предпочтения.

Для создания предпочтения нужно 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» нужно перейти в «Компьютер/Пользователь» → «Настройки» → «Настройки системы» → «Папки». В контекстном меню свободной области выбрать пункт «Новый» → «Папки» (рис. 158).

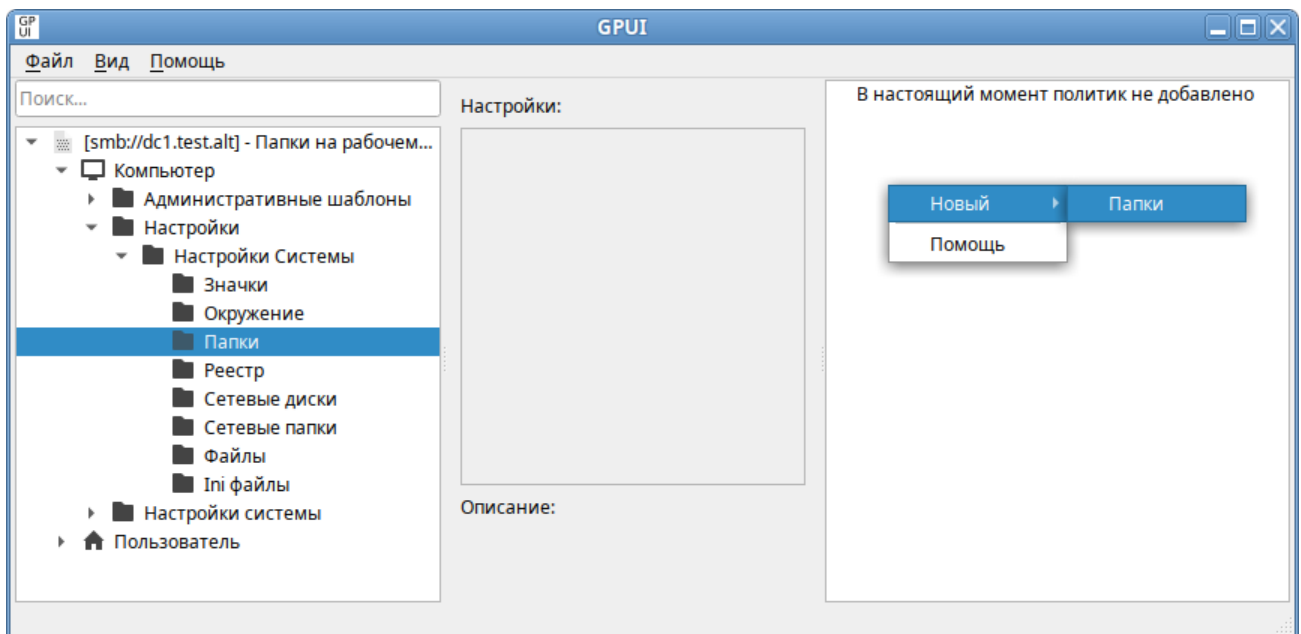


Рис. 158 – Создание новой политики «Папки»

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) (рис. 159).

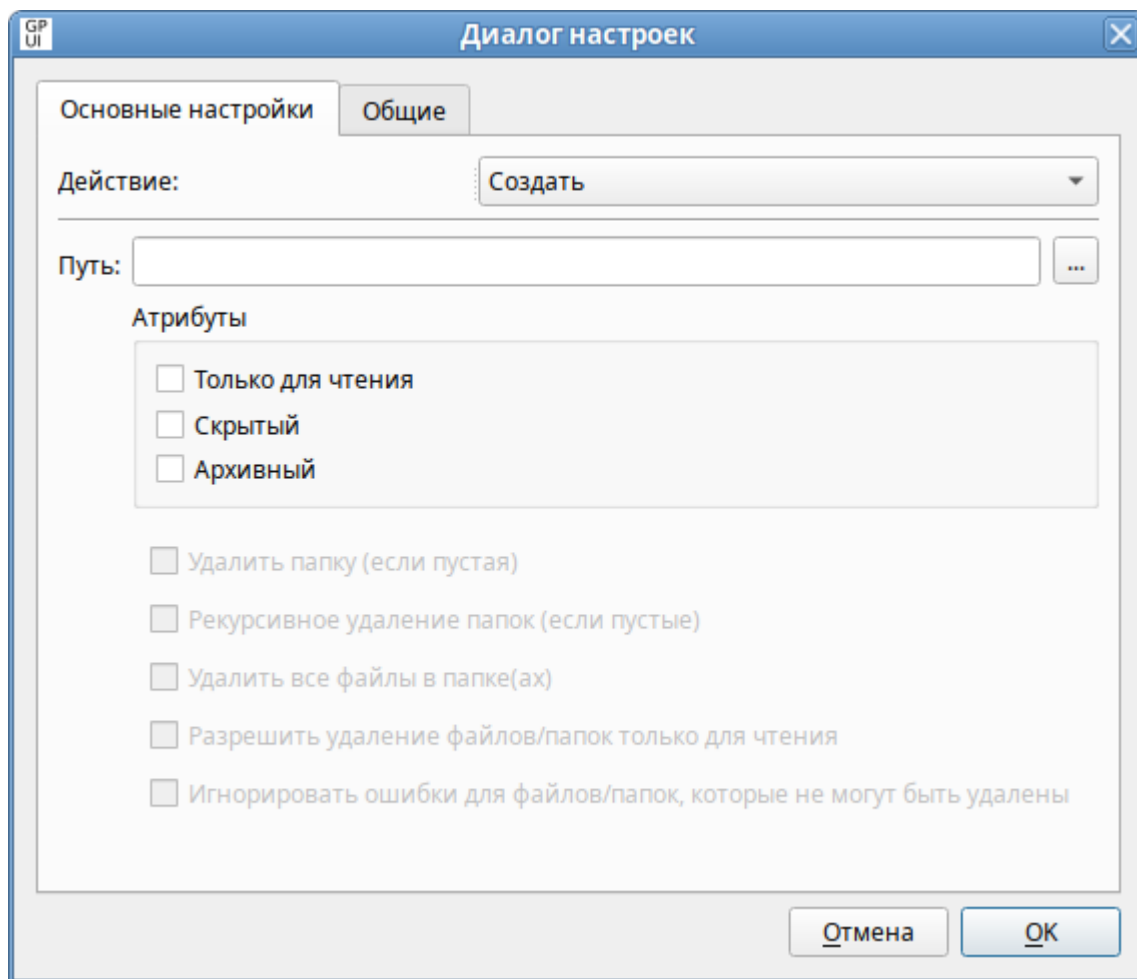


Рис. 159 – Вкладка «Основные настройки»

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» (рис. 160).

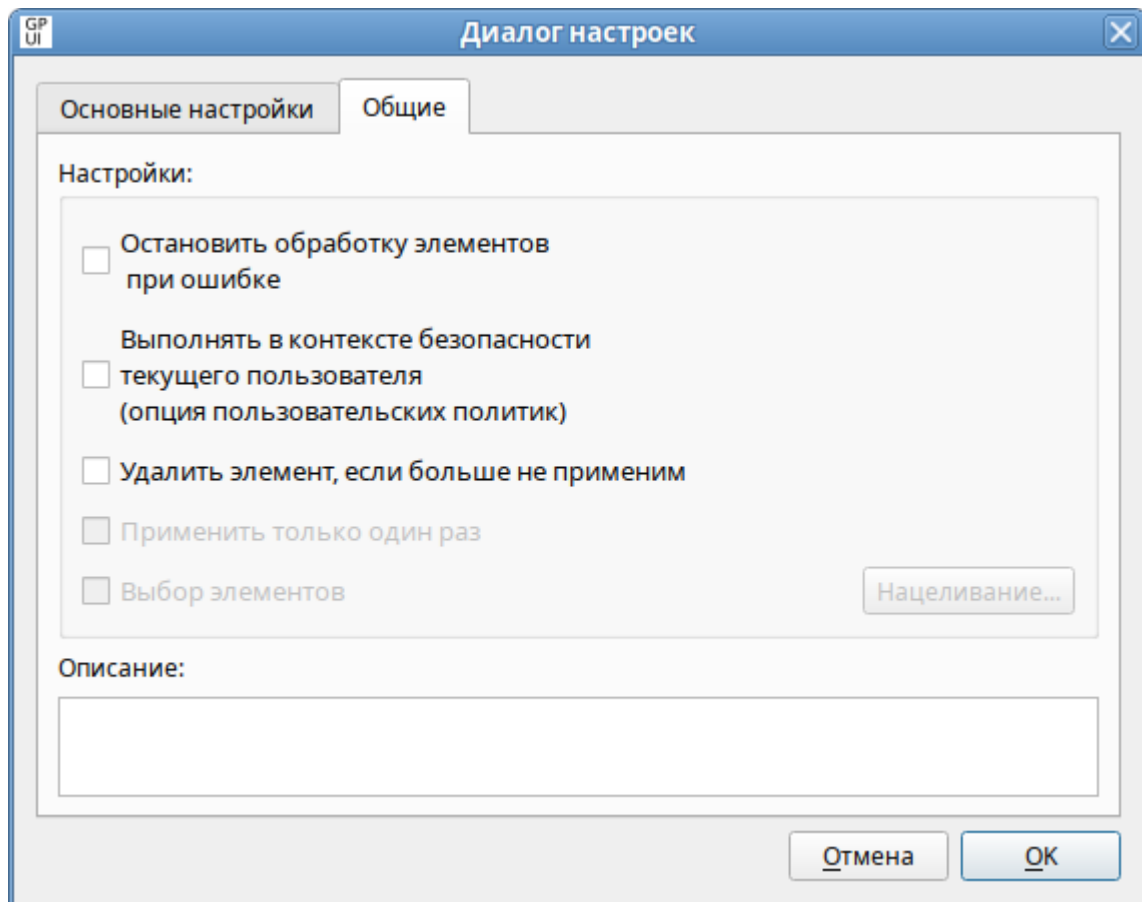


Рис. 160 – Вкладка «Общие»

Для редактирования элемента предпочтения следует дважды щелкнуть мышью по элементу (рис. 161) или в контекстном меню предпочтения выбрать пункт «Изменить элемент» (рис. 162).

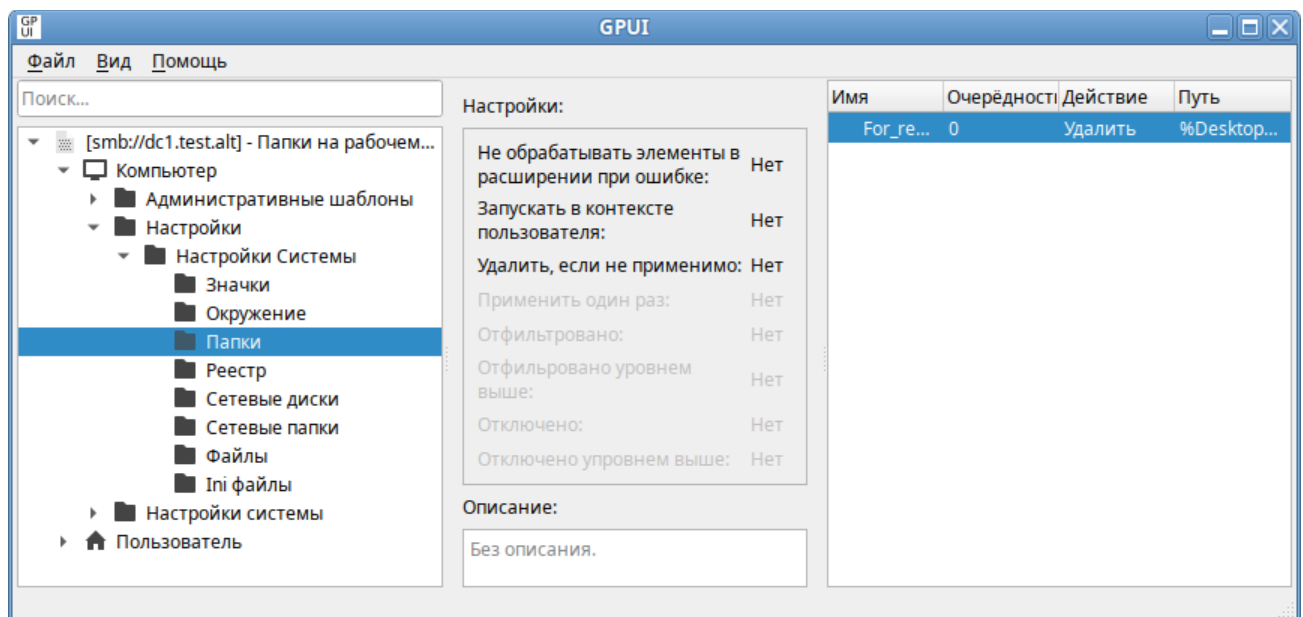


Рис. 161 – Элемент предпочтения

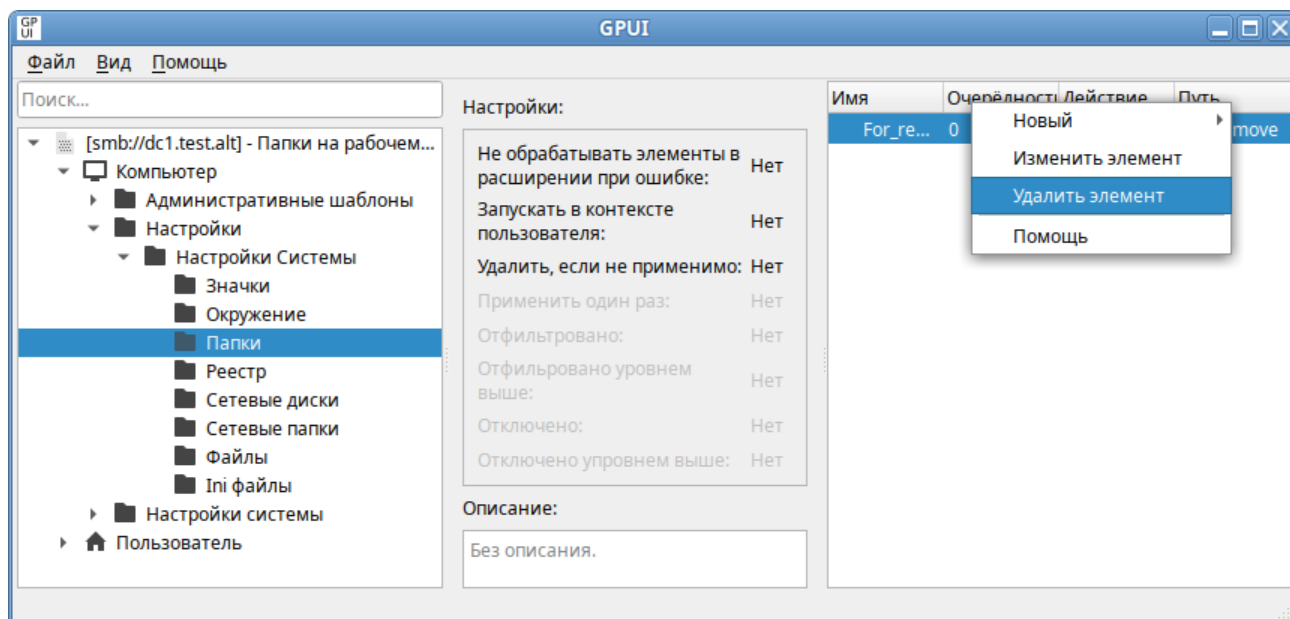


Рис. 162 – Контекстное меню элемента предпочтения

Откроется окно редактирования предпочтения (рис. 163).

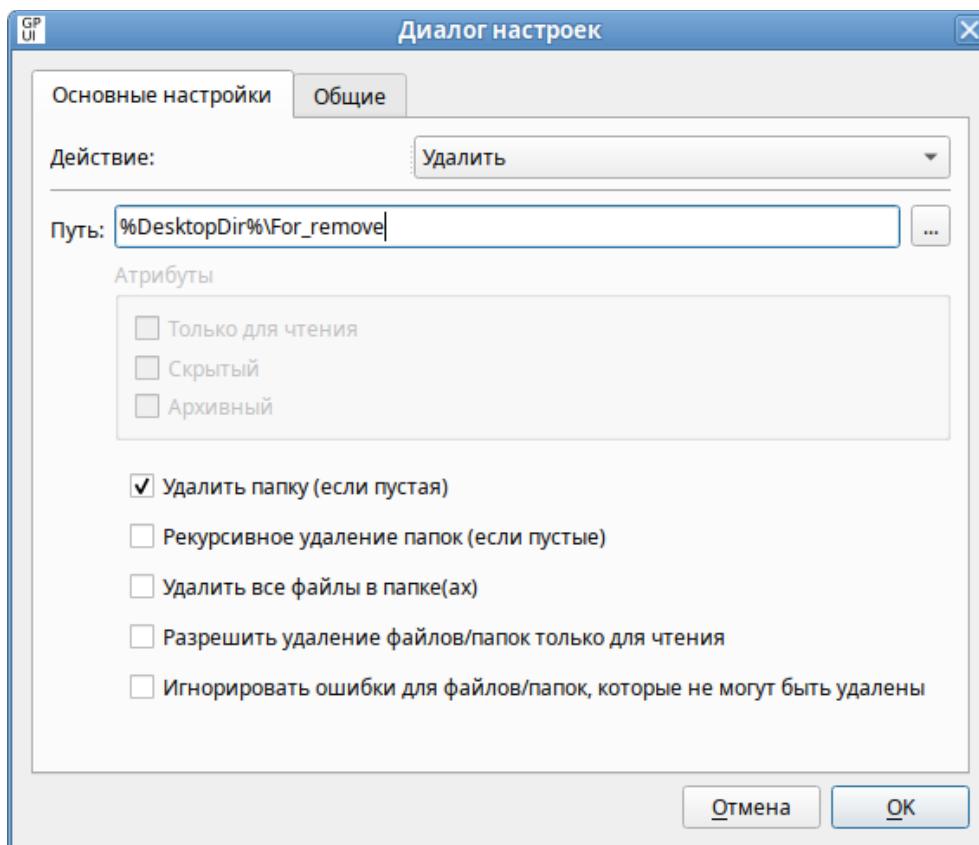


Рис. 163 – Редактирование предпочтения

Для удаления элемента следует в контекстном меню предпочтения выбрать пункт «Удалить элемент» (рис. 162).

4.6.3.4. Работа со скриптами

Работа со скриптами подробно описана в п. 4.6.6.

4.6.3.5. Смена языка

Для того чтобы изменить язык интерфейса, нужно в меню выбрать «Вид» → «Язык» (рис. 164).

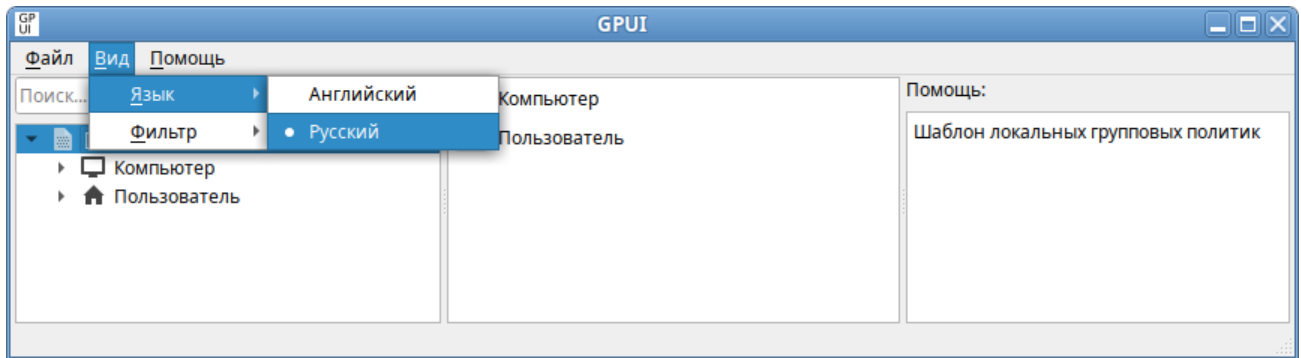


Рис. 164 – Выбор языка

4.6.4. Редактирование групповых политик

4.6.4.1. 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» (рис. 165).

При выборе политики, откроется диалоговое окно настройки политики (рис. 166).

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>`).

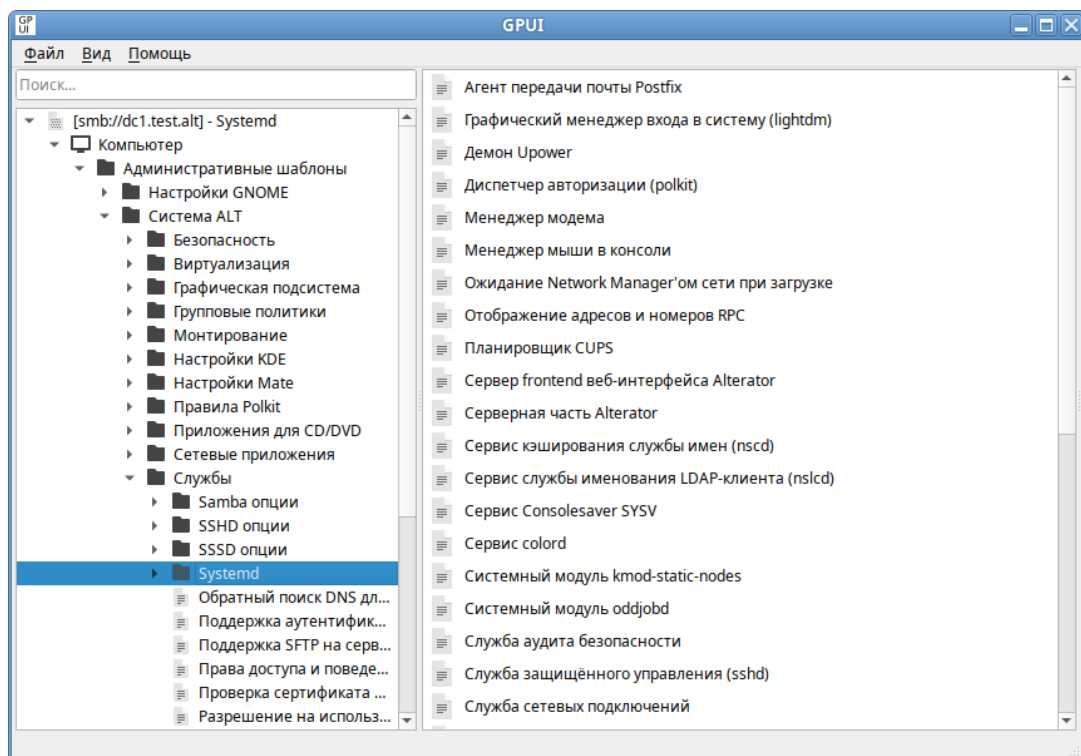


Рис. 165 – Список политик SystemdUnits

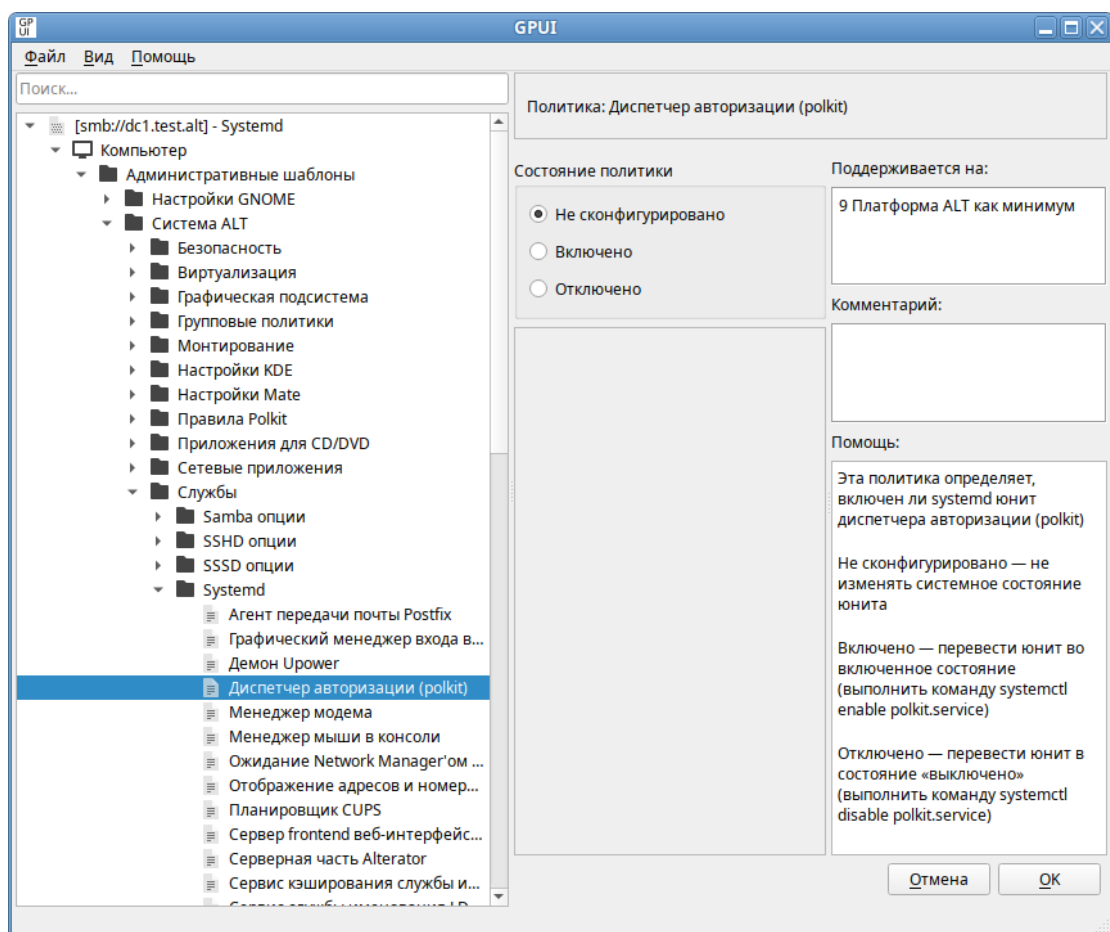


Рис. 166 – Диалоговое окно настройки политики

Список служб, состояние которых можно изменить, настроив соответствующую политику в GPUI, указан в таблице 18.

Т а б л и ц а 18 – 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	Политика определяет, включен ли systemd юнит «Network Manager»	NetworkManager.service
Служба учетных записей (accounts-daemon)	Политика определяет, включен ли systemd юнит службы учетных 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 frontend 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	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 (этот пакет загружает конфигурацию энергосбережения консоли)	consolesaver.service
Cpufreq-simple сервис	Политика определяет, включен ли systemd юнит службы Cpufreq-simple (загружает модули ядра, которые требуются для масштабирования cpufreq)	cpufreq-simple.service
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 кэширующий DNS-сервер, а также TFTP-сервер для поддержки загрузки по сети)	dnsmasq.service

Окончание таблицы 18

Служба	Описание	Сервис systemd
Менеджер мыши в консоли	Политика определяет, включен ли systemd юнит диспетчера мыши консоли	gpm.service
Системный модуль kmod-static-nodes	Политика определяет, включен ли systemd юнит kmod-static-nodes (создает список 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 кэширования службы имен (nscd)	Политика определяет, включен ли systemd юнит сервиса кэширования службы имен	nscd.service
Сервис службы именования LDAP-клиента (nslcd)	Политика определяет, включен ли systemd юнит сервиса служб именования клиента LDAP	nslcd.service
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 сервиса 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

4.6.4.2. Управление control framework

Через групповые политики реализовано управление настройками control.

control, использующийся в ОС Альт СП, 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 (рис. 167).

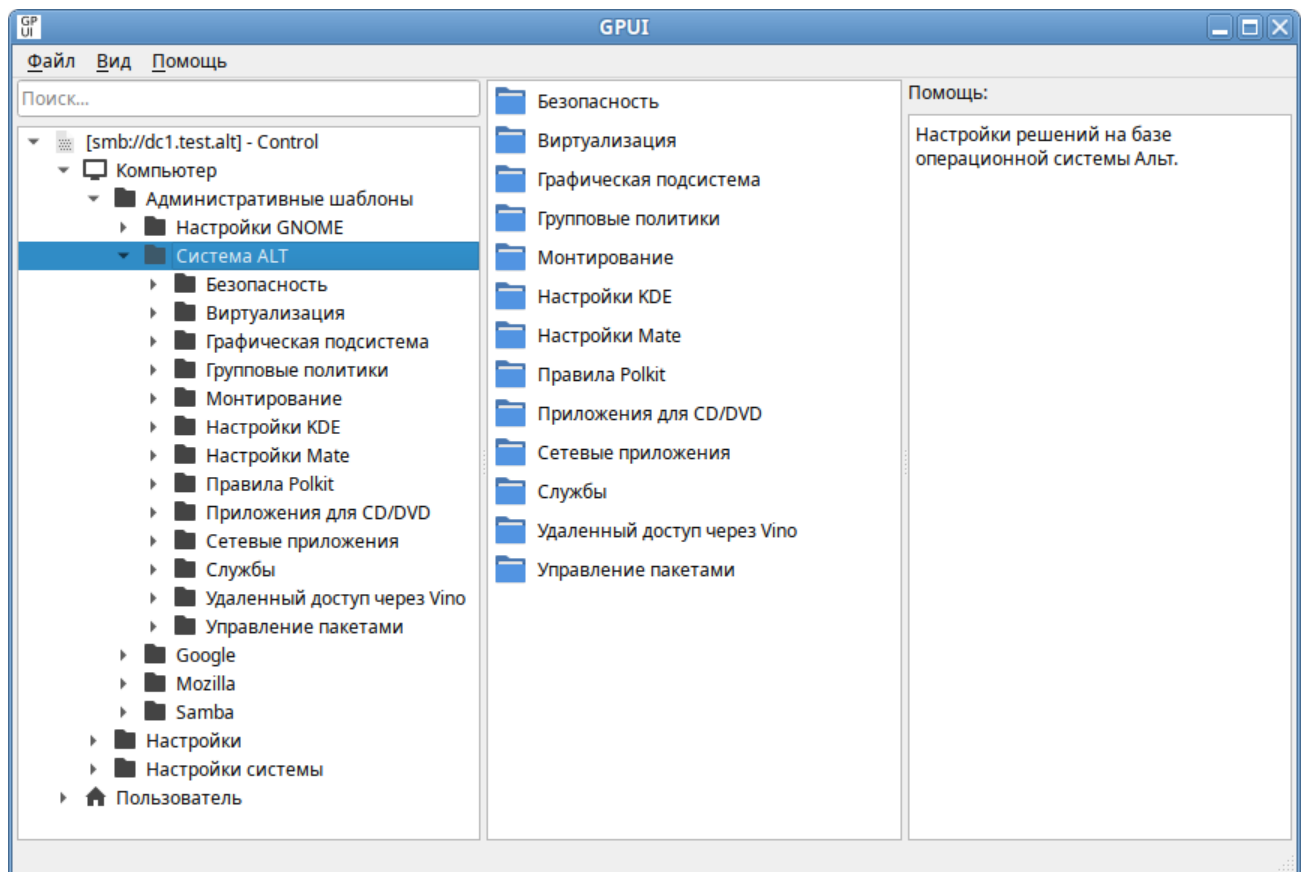


Рис. 167 – Политики настройки систем Альт

После выбора категории, в правом окне редактора отобразится список политик (рис. 168).

При выборе политики, откроется диалоговое окно настройки политики (рис. 169).

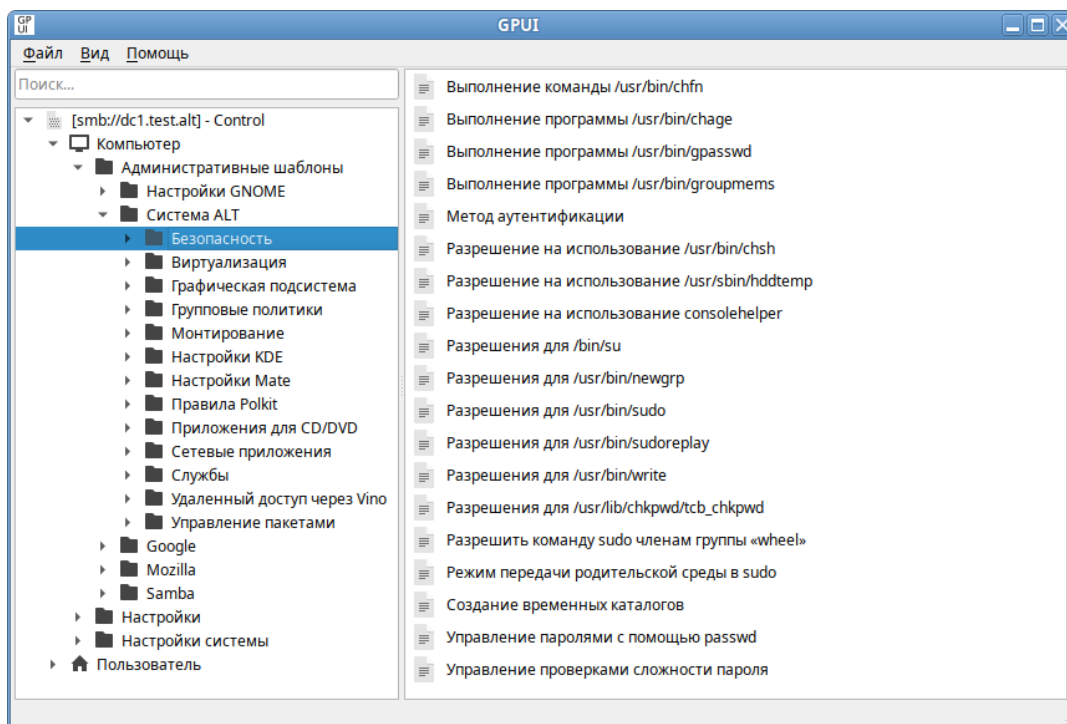


Рис. 168 – Список политик группы «Безопасность»

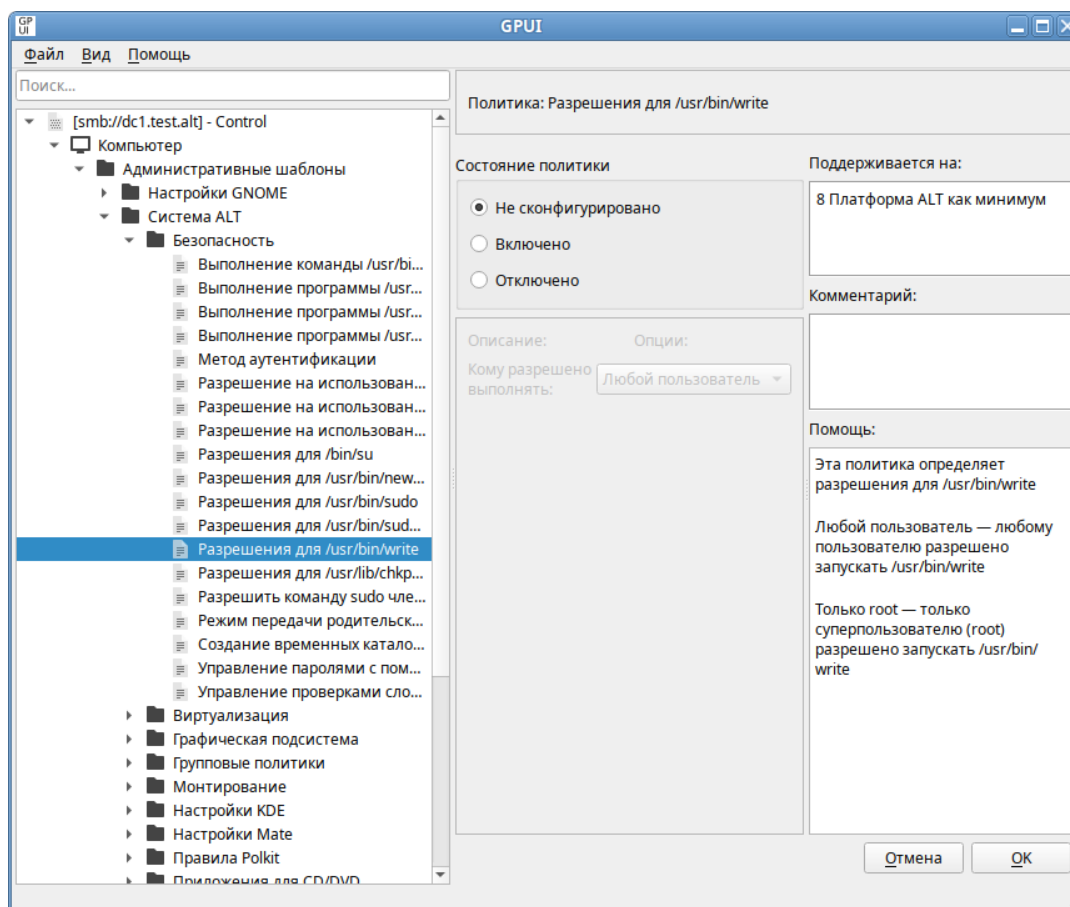


Рис. 169 – Диалоговое окно настройки политики

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 (рис. 170).

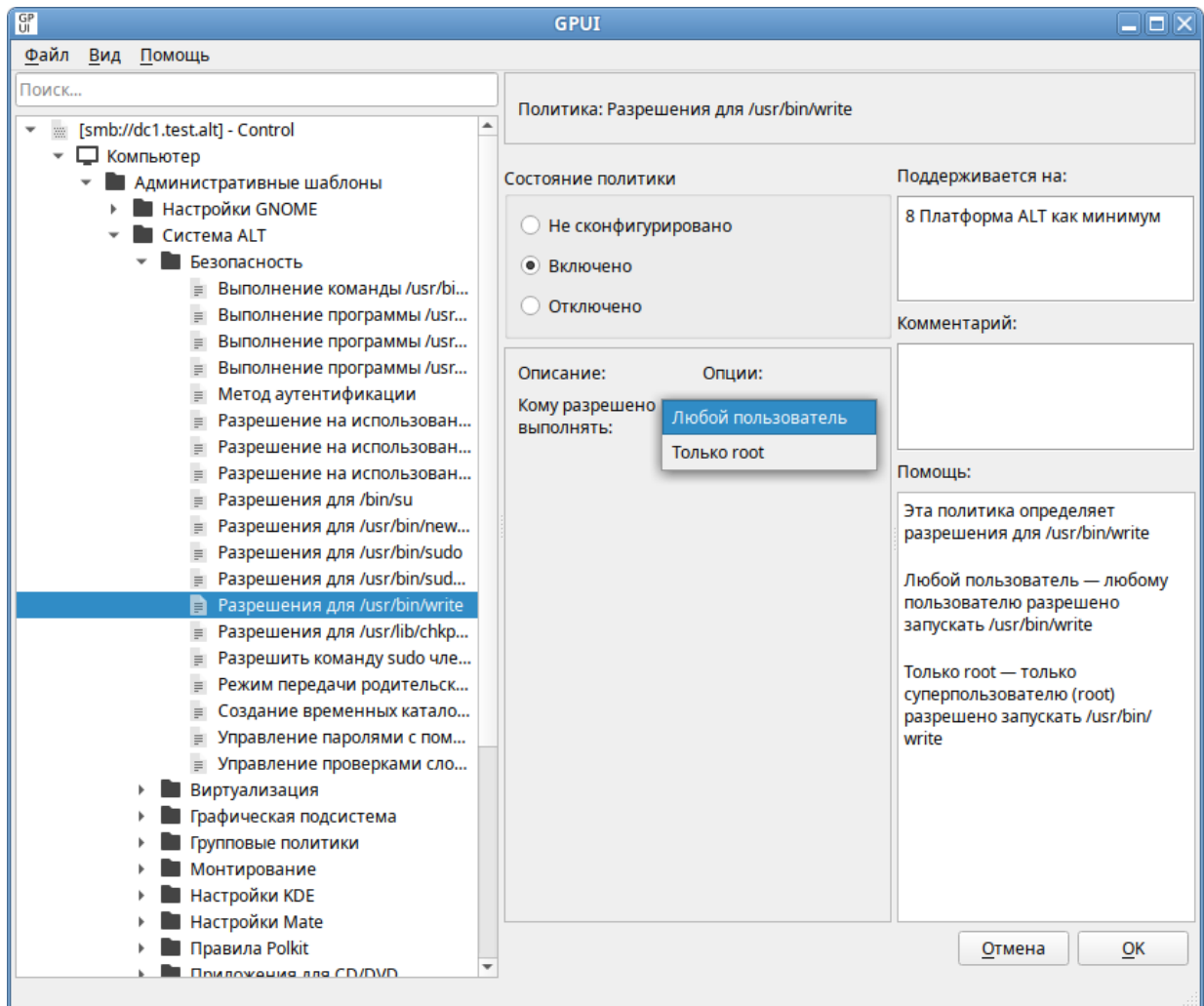


Рис. 170 – Выбор реeжима доступа для control

Все control в GPUI разделены на категории:

- «Безопасность» (см. таблицу 19);
- «Службы» (см. таблицу 20);
- «Сетевые приложения» (см. таблицу 21);
- «Приложения для CD/DVD» (см. таблицу 22);
- «Монтирование» (см. таблицу 23);
- «Виртуализация» (см. таблицу 24);
- «Графическая подсистема» (см. таблицу 25).

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`).

Т а б л и ц а 19 – Категория «Безопасность»

Политика	Control	Описание	Режимы
Выполнение программы <code>/usr/bin/chage</code>	<code>chage</code>	Политика позволяет контролировать доступ для выполнения программы <code>/usr/bin/chage</code>	«Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/chage</code> . «Любой пользователь» – любой пользователь может просмотреть, когда ему следует сменить свой пароль, используя команду <code>chage -l имя пользователя</code>
Выполнение программы <code>/usr/bin/chfn</code>	<code>chfn</code>	Политика позволяет контролировать поведение и права доступа к команде <code>chfn</code> (<code>/usr/bin/chfn</code>). Команда <code>chfn</code> может изменить полное имя пользователя, номер кабинета, номера офисного и домашнего телефона для учетной записи пользователя. Обычный пользователь может изменять поля только для своей учетной записи, с учетом ограничений в <code>/etc/login.defs</code> (конфигурация по умолчанию не позволяет пользователям менять свое полное имя)	«Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/chfn</code> . «Любой пользователь» – любой пользователь может использовать команду <code>/usr/bin/chfn</code>
Разрешение на использование Consolehelper	<code>consolehelper</code>	Определяет права доступа к инструменту <code>consolehelper</code> (<code>/usr/lib/consolehelper/priv/auth</code>), 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 <code>consolehelper</code>	«Любой пользователь» – любой пользователь может использовать <code>consolehelper</code> . «Только wheel» – только члены группы «wheel» могут использовать команду <code>consolehelper</code> . «Только root» – только суперпользователь (root) может использовать <code>consolehelper</code>

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Выполнение программы <code>/usr/bin/chsh</code>	chsh	Политика позволяет управлять правами доступа к команде <code>chsh</code> (<code>/usr/bin/chsh</code>). Команда <code>chsh</code> позволяет изменить командную оболочку (или интерпретатор командной строки), запускаемую по умолчанию при регистрации пользователя в текстовой консоли (по умолчанию используется <code>/bin/bash</code>). Обычный пользователь может изменить командную оболочку только для своей учетной записи (командная оболочка должна быть перечислена в файле <code>/etc/shells</code>). Суперпользователь может изменить настройки для любой учетной записи (могут быть указаны любые значения)	«Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/chsh</code> . «Все пользователи» – любой пользователь может использовать команду <code>/usr/bin/chsh</code>
Выполнение программы <code>/usr/bin/gpasswd</code>	gpasswd	Определяет права на запуск инструмента <code>/usr/bin/gpasswd</code>	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/gpasswd</code> . «Только wheel» – только члены группы «wheel» могут выполнять <code>/usr/bin/gpasswd</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/gpasswd</code>
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

Продолжение таблицы 19

Политика	Control	Описание	Режимы
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
Выполнение программы /usr/sbin/hddtemp	groupmems	Разрешение на использование инструмента /usr/sbin/hddtemp – отслеживание температуры жесткого 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

Продолжение таблицы 19

Политика	Control	Описание	Режимы
Управление паролями с помощью passwd	Passwd	Определяет политику управления паролями с помощью команды /usr/bin/passwd	«ТСВ» – 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. «Только root» – только суперпользователь (root) может запускать /bin/su

Продолжение таблицы 19

Политика	Control	Описание	Режимы
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/sudo replay	sudoreplay	Определяет разрешения для /usr/bin/sudo replay	«Любой пользователь» – любой пользователь может запускать /usr/bin/sudo replay. «Только wheel» – только пользователи из группы «wheel» могут запускать /usr/bin/sudo replay. «Только root» – только суперпользователь (root) может запускать /usr/bin/sudo replay
Разрешить команду sudo членам группы «wheel»	sudowheel	Эта политика разрешает или запрещает членам группы «wheel» применять команду sudo. Если политика включена, пользователи, входящие в группу «wheel» могут повысить системные привилегии через команду sudo. Если политика не настроена 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

Окончание таблицы 19

Политика	Control	Описание	Режимы
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. «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

Т а б л и ц а 20 – 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 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	«Разрешить» – выполнять обратный поиск DNS для запросов OpenLDAP. «Не разрешать» – не выполнять обратный поиск DNS для запросов OpenLDAP. «По умолчанию» – выполнять обратный поиск DNS для запросов OpenLDAP

Продолжение таблицы 20

Политика	Control	Описание	Режимы
Проверка сертификата при установлении соединений TLS OpenLDAP	ldap-tls-cert-chec	Политика определяет режим проверки сертификата при установке TLS соединений OpenLDAP	«По умолчанию» – установить соединение только с правильным сертификатом. «Разрешить» – установить соединение, даже если сертификат отсутствует или неверный. «Пробовать» – установить соединение, если нет или с действующим сертификатом. «Требовать» – установить соединение только с правильным сертификатом. «Никогда» – не выполнять никаких проверок
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/bin/postqueue	postqueue	Определяет разрешения для /usr/bin/postqueue	«Любой пользователь» – любому пользователю разрешено запускать /usr/bin/postqueue. «Группа mailadm» – пользователям из группы «mailadm» разрешено запускать /usr/bin/postqueue. «Только root» – только суперпользователю (root) разрешено запускать /usr/bin/postqueue
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

Продолжение таблицы 20

Политика	Control	Описание	Режимы
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 <code>usershare allow guests</code> в файле <code>/etc/samba/user shares.conf</code> .	«Включено» – разрешить предоставление гостевого доступа к общему ресурсу; разрешить создание общих каталогов с параметром доступа без авторизации (<code>usershare allow guests = yes</code>). «Отключено» – запретить предоставление гостевого доступа к общему ресурсу; запретить создание общих каталогов с параметром доступа без авторизации (<code>usershare allow guests = no</code>)
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 <code>usershare owner only</code> в файле <code>/etc/samba/user shares.conf</code> .	«Включено» – запретить предоставление общего доступа не владельцу каталога; запретить доступ к общим каталогам пользователей, без проверки владельца каталога (<code>usershare owner only = yes</code>). «Отключено» – разрешить предоставление общего доступа не владельцу каталога; разрешить доступ к общим каталогам пользователей, без проверки владельца каталога (<code>usershare owner only = no</code>)

Продолжение таблицы 20

Политика	Control	Описание	Режимы
Запрет на создание общих каталогов в системных каталогах	smb-conf-usershare-deny-list	Данная политика управляет параметром <code>usershare prefix deny list</code> в файле <code>/etc/samba/usershares.conf</code> – открывая или закрывая комментарием этот параметр. Параметр <code>usershare prefix deny list</code> 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 <code>usershare prefix deny list</code> заданы каталоги: <code>/etc, /dev, /sys, /proc</code>. Если настроен список запрещенных каталогов <code>usershare prefix deny list</code>, и список разрешенных каталогов <code>usershare prefix allow list</code>, сначала обрабатывается список запрета, а затем уже список разрешений.	«Включено» – включить список запрещенных каталогов (параметр <code>usershare prefix deny list</code> будет раскомментирован). «Отключено» – отключить список запрещенных каталогов (параметр <code>usershare prefix deny list</code> будет закомментирован)

Продолжение таблицы 20

Политика	Control	Описание	Режимы
Разрешение на создание общих каталогов в системных каталогах	smb-conf-usershare-allow-list	Данная политика управляет параметром <code>usershare prefix allow list</code> в файле <code>/etc/samba/useshares.conf</code> – открывая или закрывая комментарием этот параметр. Параметр <code>usershare prefix allow list</code> определяет каталоги в корневом каталоге (<code>/</code>), 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 <code>usershare prefix allow list</code> заданы каталоги: <code>/home, /srv, /mnt, /media, /var</code>. Если настроен список запрещенных каталогов <code>usershare prefix deny list</code>, и список разрешенных каталогов <code>usershare prefix allow list</code>, сначала обрабатывается список запрета, а затем уже список разрешений.	«Включено» – включить список разрешенных каталогов (параметр <code>usershare prefix allow list</code> будет раскомментирован). «Отключено» – отключить список разрешенных каталогов (параметр <code>usershare prefix allow list</code> будет закомментирован)

Продолжение таблицы 20

Политика	Control	Описание	Режимы
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
Доступ членам группы «users» к управлению общими каталогами	role-usershares	Политика управляет разрешением членам группы «users» 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 «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
Разрешение на создание пользовательских общих каталогов	smb-conf-usershare	Политика управляет возможностью создания пользовательских общих каталогов на компьютере.	«Включено» – включить возможность создания и использования общих каталогов пользователей (usershare max shares = 100).

Продолжение таблицы 20

Политика	Control	Описание	Режимы
		Данная политика управляет параметром <code>usershare max shares</code> в файле <code>/etc/samba/usershare s.conf</code> , который устанавливает предельное число общих каталогов.	«Отключено» – отключить возможность создания и использования общих каталогов пользователей (<code>usershare max shares = 0</code>)
SSHD опции			
Контроль доступа по группам к серверу OpenSSH	<code>ssh-gssapi-auth</code>	Эта политика включает в службу 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	<code>sshd-allow-groups-list</code>	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 удаленного доступа («wheel» и «remote») «Только wheel» – разрешить доступ к серверу OpenSSH только для группы администраторов («wheel») «Только remote» – разрешить доступ к серверу OpenSSH только для группы «remote»
Поддержка GSSAPI-аутентификации на сервере OpenSSH	<code>sshd-gssapi-auth</code>	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

Продолжение таблицы 20

Политика	Control	Описание	Режимы
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. «Запрещено» – суперпользователю запрещена аутентификация на сервере OpenSSH. «По умолчанию» – сбросить режим аутентификации для суперпользователя на значение по умолчанию в пакете
SSSD опции			
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. «По умолчанию» – настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию в пакете

Продолжение таблицы 20

Политика	Control	Описание	Режимы
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, ведется логирование. «Разрешающий режим» – правила управления доступом в SSSD основанные на GPO не выполняются, ведется только логирование. Такой режим требуется 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 сброшено на значение по умолчанию в пакете
Кэширование учетных данных пользователей	sssd-cache-credentials	Эта политика определяет, будут ли учетные данные удаленных пользователей сохраняться в локальном кеше SSSD	«Включить» – сохранение в локальном кеше SSSD учетных данных пользователей включено. «Отключить» – сохранение в локальном кеше SSSD учетных данных пользователей отключено. «По умолчанию» – настройка сохранения в локальном кеше SSSD учетных данных пользователей сброшена на значение по умолчанию в пакете

Окончание таблицы 20

Политика	Control	Описание	Режимы
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	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

Т а б л и ц а 21 – Категория «Сетевые приложения»

Политика	Control	Описание	Режимы
Разрешение на использование <code>/usr/bin/mtr</code>	mtr	Разрешение на использование сетевого инструмента <code>/usr/bin/mtr</code>	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/mtr</code> . «Группа netadmin» – только члены группы «netadmin» могут выполнять <code>/usr/bin/mtr</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/mtr</code>
Разрешения для <code>/usr/bin/ping</code>	ping	Эта политика определяет разрешения для <code>/usr/bin/ping</code>	«Любой пользователь» – любой пользователь может запускать <code>/usr/bin/ping</code> . «Группа netadmin» – пользователям из группы «netadmin» разрешено запускать <code>/usr/bin/ping</code> . «Только root» – только суперпользователь (root) может запускать <code>/usr/bin/ping</code> . «Любой пользователь (в контейнерах)» – любой пользователь может запускать <code>/usr/bin/ping</code> (в контейнерах). «Группа netadmin (в контейнерах)» – пользователям из группы «netadmin» разрешено запускать <code>/usr/bin/ping</code> (в контейнерах)
Разрешения для <code>/usr/sbin/pppd</code>	ppp	Эта политика определяет разрешения для <code>/usr/sbin/pppd</code>	«Только root» – только суперпользователю (root) разрешено запускать <code>/usr/sbin/pppd</code> . «Традиционный» – любой пользователь имеет право запустить <code>/usr/sbin/pppd</code> без повышения привилегий. «Группа uusr» – пользователям из группы «uusr» имеют право запускать <code>/usr/sbin/pppd</code> с правами суперпользователя. «Любой пользователь» – любой пользователь имеет право запускать <code>/usr/sbin/pppd</code> с правами суперпользователя
Разрешения для wireshark-capture (dumpcap)	wireshark-capture	Эта политика определяет функциональные возможности (режимы) разрешения для захвата wireshark (<code>/usr/bin/dumpcap</code>)	«Любой пользователь» – любой пользователь имеет право запустить <code>/usr/bin/dumpcap</code> , захват трафика включен. «Любой пользователь, без захвата трафика» – любой пользователь имеет право запустить <code>/usr/bin/dumpcap</code> , захват трафика отключен. «Группа netadmin» – пользователям из группы «netadmin» имеют право запускать <code>/usr/bin/dumpcap</code> . «Только root» – только суперпользователь (root) может запускать <code>/usr/bin/dumpcap</code>

Т а б л и ц а 22 – 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. «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. «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

Т а б л и ц а 23 – Категория «Монтирование»

Политика	Control	Описание	Режимы
Доступ к инструментам FUSE	fusermount	Эта политика определяет права доступа для монтирования файловой системы FUSE (выполнение программ <code>/usr/bin/fusermount</code> и <code>/usr/bin/fusermount3</code>)	«Любой пользователь» – любой пользователь может выполнить <code>/usr/bin/fusermount</code> и <code>/usr/bin/fusermount3</code> . «Только fuse» – только члены группы «fuse» могут выполнять <code>/usr/bin/fusermount</code> и <code>/usr/bin/fusermount3</code> . «Только wheel» – только члены группы «wheel» могут выполнять <code>/usr/bin/fusermount</code> и <code>/usr/bin/fusermount3</code> . «Только root» – только суперпользователь (root) может выполнить <code>/usr/bin/fusermount</code> и <code>/usr/bin/fusermount3</code>
Разрешения для <code>/bin/mount</code> и <code>/bin/umount</code>	mount	Эта политика определяет разрешения для <code>/bin/mount</code> и <code>/bin/umount</code>	«Любой пользователь» – любому пользователю разрешено запускать <code>/bin/mount</code> и <code>/bin/umount</code> . «Группа wheel» – пользователям из группы «wheel» разрешено запускать <code>/bin/mount</code> и <code>/bin/umount</code> . «Непривилегированный пользователь» – любой пользователь может запускать <code>/bin/mount</code> и <code>/bin/umount</code> для непривилегированных действий (не от имени root). «Только root» – только суперпользователь (root) может запускать <code>/bin/mount</code> и <code>/bin/umount</code>
Разрешения для <code>/sbin/mount.nfs</code>	nfsmount	Эта политика определяет разрешения для <code>/sbin/mount.nfs</code>	«Любой пользователь» – любому пользователю разрешено запускать <code>/sbin/mount.nfs</code> «Только wheel» – пользователям из группы «wheel» разрешено запускать <code>/sbin/mount.nfs</code> «Только root» – только суперпользователю (root) может запускать <code>/sbin/mount.nfs</code>
Правила подключения USB-накопителей	udisks2	Эта политика определяет правила подключения USB-накопителей	«По умолчанию» – подключить накопитель индивидуально (<code>/run/media/\$user/</code>) для каждого пользователя. «Общий» – подключить накопитель к общедоступной точке (<code>/media/</code>)

Т а б л и ц а 24 – 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

Т а б л и ц а 25 – 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	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» – всем 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

4.6.4.3. Управление настройками службы Polkit

Через групповые политики реализовано управление настройками службы Polkit (PolicyKit).

В настоящий момент реализованы следующие настройки:

- ограничения службы Login – формирование правил PolKit для управления службой Login;
- ограничения службы Machine – формирование правил PolKit для управления службой Machine;

- ограничения Udisks2 – формирование правил PolKit для монтирования файловых систем (демон udisks2);
- ограничения PackageKit – формирование правил PolKit для установки, удаления, обновления пакетов;
- ограничения Realmd – формирование правил PolKit для управления службой Realmd;
- ограничения NetworkManager – формирование правил PolKit для операций с сетевыми подключениями и настройкой сетевых интерфейсов;
- ограничения ModemManager – формирование правил PolKit для операций с ModemManager (взаимодействие с модемом или мобильным телефоном);
- 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 (рис. 171).

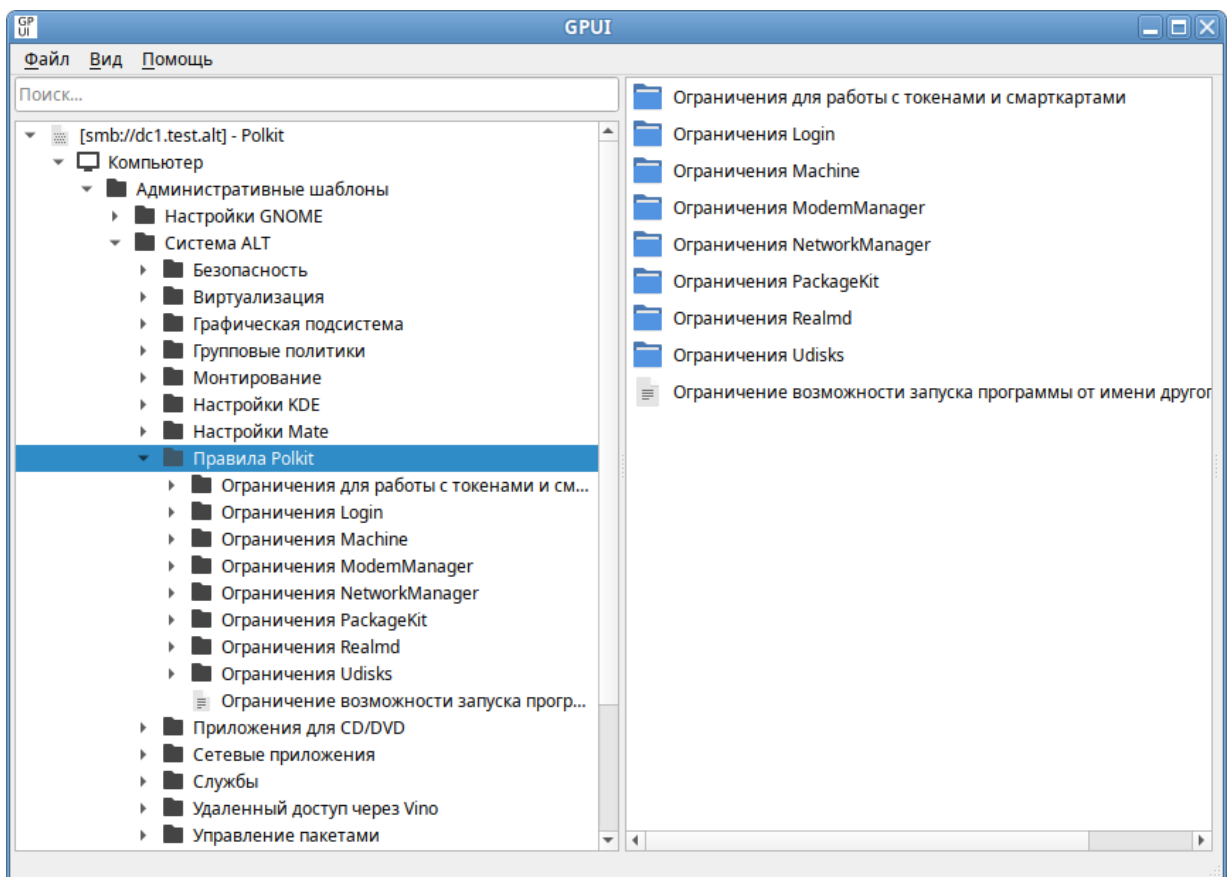


Рис. 171 – Список разделов Polkit

При выборе раздела, в правом окне редактора отобразится список политик (рис. 172).

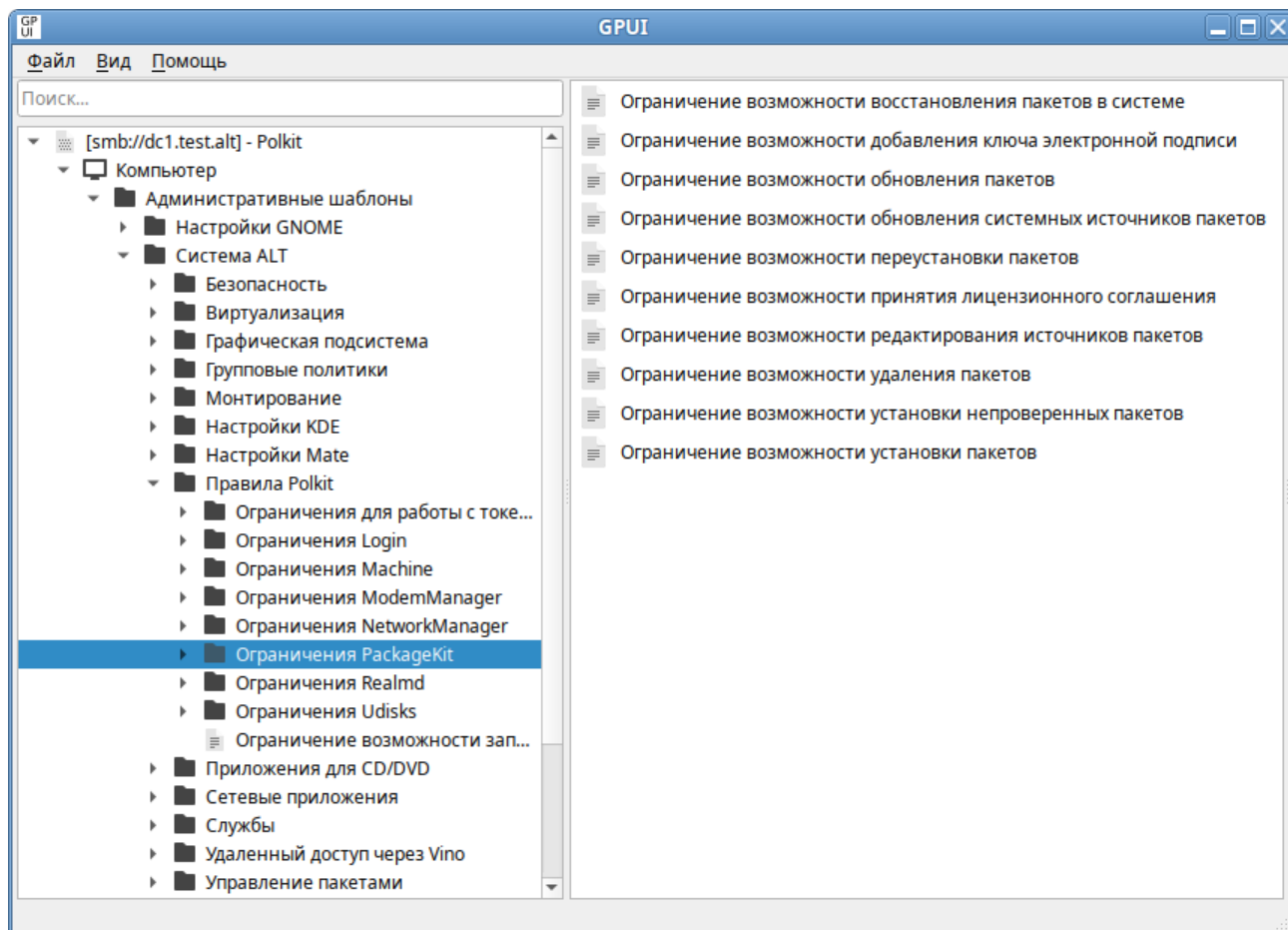


Рис. 172 – Список политик PackageKit

При выборе политики, откроется диалоговое окно настройки политики (рис. 173).

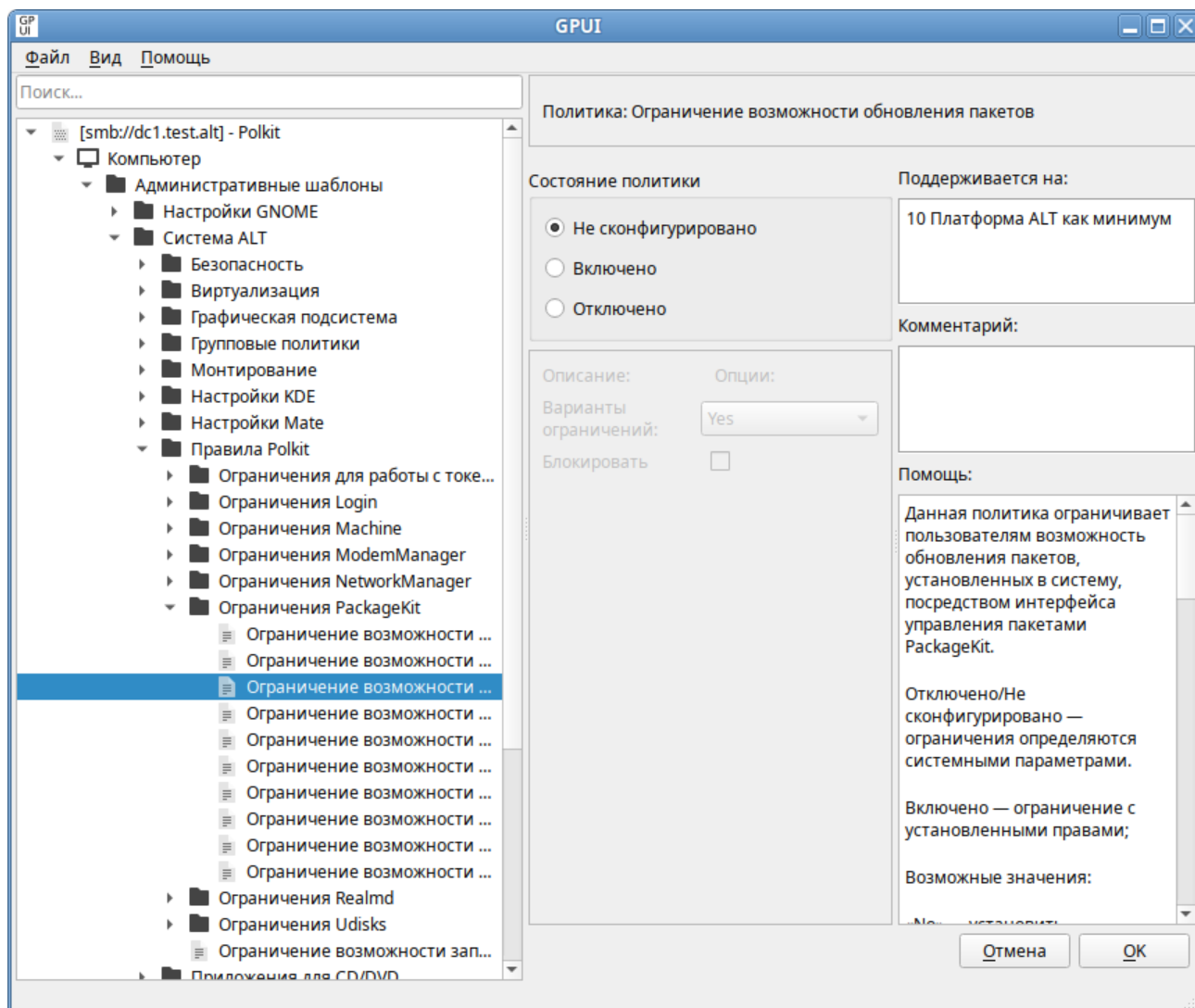


Рис. 173 – Диалоговое окно настройки ограничения Polkit

Можно не задавать настройку политики, включить или отключить. Если политика находится в состоянии «Отключено»/«Не сконфигурировано» разрешения определяются системными параметрами (по умолчанию — «Auth_admin»). Если выбрать параметр «Включено», в разделе «Опции» в выпадающем списке можно выбрать вариант ограничения для данного разрешения (рис. 174).

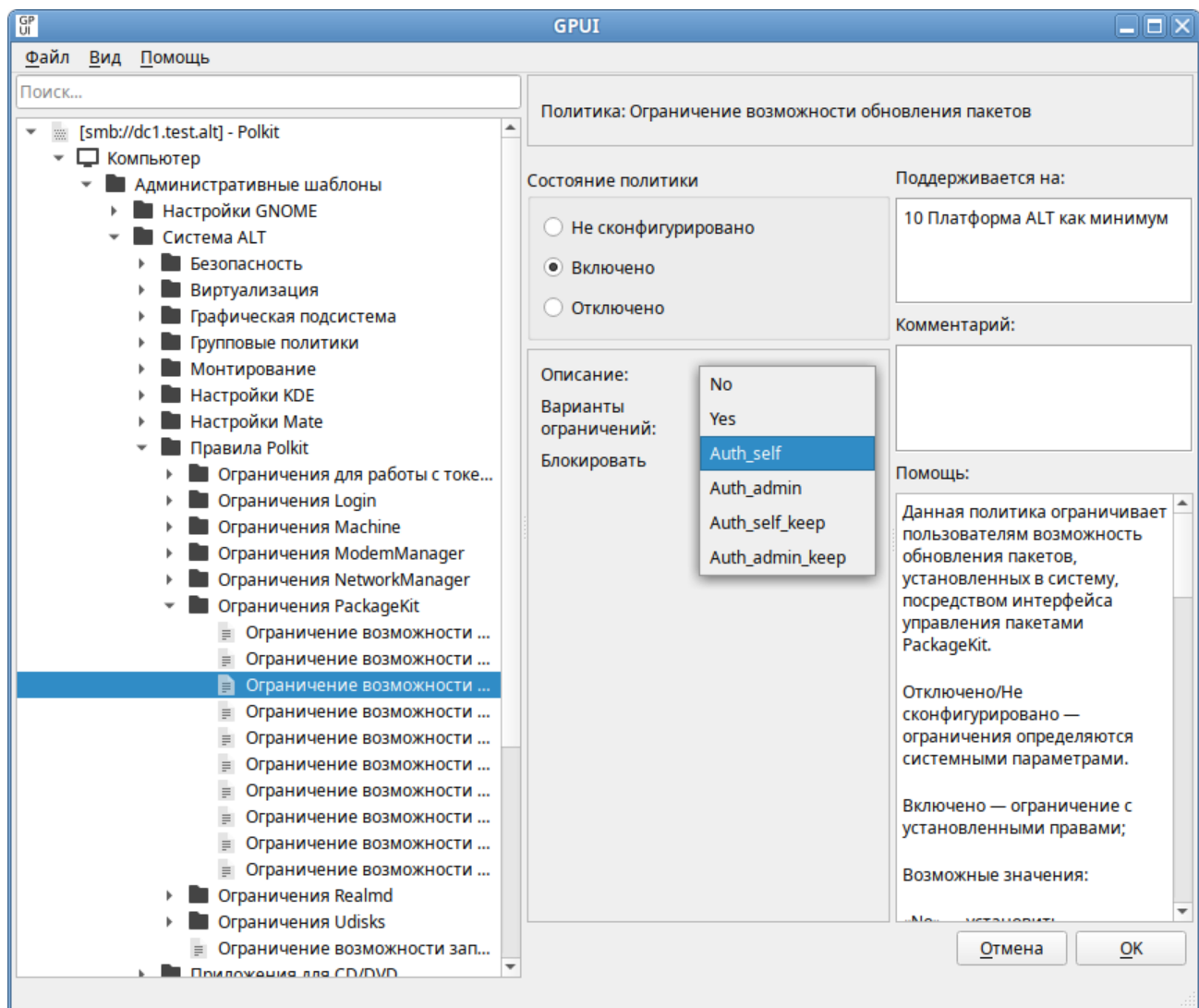


Рис. 174 – Настройка ограничения Polkit

Если выбран параметр «Включено», для каждой из этих политик доступны следующие разрешения:

- «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 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 СП определен 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`).

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.netwo
rk-control;;;Yes]
```

4.6.4.3.1. Ограничения для работы с токенами и смарт-картами

Список политик, настраивающих ограничения для работы с токенами и смарт-картами приведены в таблице 26.

Т а б л и ц а 26 – 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

4.6.4.3.2. Ограничения службы Login

Список политик, настраивающих ограничения службы Login приведены в таблице 27.

Т а б л и ц а 27 – 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

Продолжение таблицы 27

Политика	Описание	Правило Polkitd
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, когда 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 способа подключения устройств к рабочим местам)	Политика управляет ограничением возможности очистки устройства в месте привязки (изменение способа подключения устройств к рабочим местам)	org.freedesktop.login1.flush-devices
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

Продолжение таблицы 27

Политика	Описание	Правило Polkitd
Ограничение возможности приложениям запрещать автоматическое приостановление работы системы	Политика ограничивает возможность приложениям запрещать автоматическое приостановление работы системы	org.freedesktop.login1.inhibit-block-idle
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 обработку аппаратной клавиши приостановки системы	Политика ограничивает возможность приложениям запрещать низкоуровневую обработку аппаратной клавиши приостановки системы	org.freedesktop.login1.inhibit-handle-suspend-key
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

Окончание таблицы 27

Политика	Описание	Правило Polkitd
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
Ограничение возможности разрешения незалогиненному пользователю запускать программы	Политика ограничивает возможность разрешения незалогиненному пользователю запускать программы	org.freedesktop.login1.set-self-linger
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
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

4.6.4.3.3. Ограничения службы Machine

Список политик, настраивающих ограничения службы Machine приведены в таблице 28.

Т а б л и ц а 28 – 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 псевдотерминала (TTY) в локальном контейнере	Политика управляет ограничением возможности получения псевдотерминала (TTY) в локальном контейнере	org.freedesktop.machine1.open-pty
Ограничение возможности получения псевдотерминала (TTY) на локальном хосте	Политика управляет ограничением возможности получения псевдотерминала (TTY) на локальном хосте	org.freedesktop.machine1.host-open-pty
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

4.6.4.3.4. Ограничения службы NetworkManager

Список политик, настраивающих ограничения службы NetworkManager приведены в таблице 29.

Т а б л и ц а 29 – Ограничения службы 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 счетчика статистики устройства	org.freedesktop.NetworkManager.enable-disable-statistics
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 изменения общей конфигурации DNS	org.freedesktop.NetworkManager.settings.modify.global-dns
Ограничение возможности изменения персональных сетевых настроек	Данная политика управляет ограничением возможности изменения личных сетевых соединений	org.freedesktop.NetworkManager.settings.modify.own
Ограничение возможности изменения постоянного имени хоста	Данная политика управляет ограничением возможности изменения постоянного имени 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
Разрешение 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 на перевод NetworkManager в спящий режим или пробуждение из спящего режима (должна использоваться только для управления питанием системы)	org.freedesktop.NetworkManager.sleep-wake

Окончание таблицы 29

Политика	Описание	Правило Polkitd
Ограничение возможности отката конфигурации сетевых интерфейсов к контрольной точке	Политика управляет ограничением возможности создания контрольной точки сетевых интерфейсов или откату 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 защищенную 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 через открытую сеть Wi-Fi	org.freedesktop.NetworkManager.wifi.share.open

Разрешения 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
```

4.6.4.3.5. Ограничения службы ModemManager

Список политик, настраивающих ограничения службы ModemManager приведены в таблице 30.

Т а б л и ц а 30 – Ограничения службы 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
Ограничение возможности отправки, сохранения, изменения и удаления текстовых сообщений	Политика ограничивает возможность отправки или манипулирования текстовыми сообщениями устройства	org.freedesktop.ModemManager1.Messaging
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

4.6.4.3.6. Ограничения службы PackageKit

Список политик, настраивающих ограничения службы PackageKit приведены в таблице 31.

Т а б л и ц а 31 – Ограничения службы PackageKit

Политика	Описание	Правило Polkitd
Ограничение возможности восстановления пакетов в системе	Данная политика ограничивает пользователей 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 пользователей 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 пользователей 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 пользователей возможность обновления системных источников пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-refresh
Ограничение возможности переустановки пакетов	Данная политика ограничивает пользователей возможность переустановки пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-reinstall
Ограничение возможности принятия лицензионного соглашения	Данная политика ограничивает возможность принятия пользовательского соглашения программ посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-eula-accept
Ограничение возможности редактирования источников пакетов	Данная политика ограничивает пользователей возможность редактирования источников пакетов в системе посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.system-sources-configure
Ограничение возможности удаления пакетов	Данная политика ограничивает пользователей возможность удаления пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-remove
Ограничение возможности установки пакетов	Данная политика ограничивает пользователей возможность установки пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install
Ограничение возможности установки непроверенных пакетов	Данная политика ограничивает пользователей возможность установки ненадежных или непроверенных пакетов посредством интерфейса управления пакетами PackageKit	org.freedesktop.packagekit.package-install-untrusted

4.6.4.3.7. Ограничения Realmd

Список политик, настраивающих ограничения Realmd приведены в таблице 32.

Т а б л и ц а 32 – Ограничения Realmd

Политика	Описание	Правило Polkitd
Ограничение 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

4.6.4.3.8. Ограничения Udisks2

Список политик, настраивающих ограничения Udisks2 приведены в таблице 33.

Т а б л и ц а 33 – Ограничения Udisks2

Политика	Описание	Правило Polkitd
Общая политика ограничения возможности монтирования	Данная политика ограничивает возможность монтирования съемных запоминающих устройств, монтирования системных разделов, монтирования съемных запоминающих устройств в удаленных 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

Окончание таблицы 33

Политика	Описание	Правило Polkitd
Ограничение возможности запуска самопроверки SMART	Данная политика управляет ограничением возможности запуска самопроверки SMART	org.freedesktop.udisks2.ata-smart-selftest
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. Жесткий диск с установленной ОС относится к системным устройствам	org.freedesktop.udisks2.file-system-mount-system
Ограничение возможности монтирования съемных запоминающих устройств в удаленных сеансах	Данная политика ограничивает возможность монтирования съемных запоминающих устройств с устройства, подключенного к удаленному рабочему месту (например, на другом компьютере или удаленной сессии)	org.freedesktop.udisks2.file-system-mount-other-seat
Ограничение возможности монтирования файловой системы	Данная политика управляет ограничением возможности монтирования файловой системы устройства	org.freedesktop.udisks2.file-system-mount
Ограничение возможности надежно стереть жесткий диск	Данная политика управляет ограничением возможности надежно стереть жесткий 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 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 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
Ограничение возможности разрешения на проверку состояния питания жесткого диска	Данная политика управляет ограничением возможности разрешения на проверку состояния питания жесткого диска	org.freedesktop.udisks2.ata-check-power
Ограничение возможности установить данные SMART из большого двоичного объекта	Данная политика управляет ограничением возможности установить данные SMART из большого двоичного объекта	org.freedesktop.udisks2.ata-smart-simulate

4.6.4.3.9. Другие политики

Список политик Polkit, которые не относятся к вышеприведенным группам приведены в таблице 34.

Т а б л и ц а 34 – Другие политики Polkit

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

4.6.4.4. Политики доступа к съемным носителям

Эта групповая политика позволяет централизованно для компьютеров или пользователей настраивать доступ к съемным запоминающим устройствам (CD, DVD, USB и др.).

П р и м е ч а н и е . 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» (рис. 175).

П р и м е ч а н и е . 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 (рис. 176).

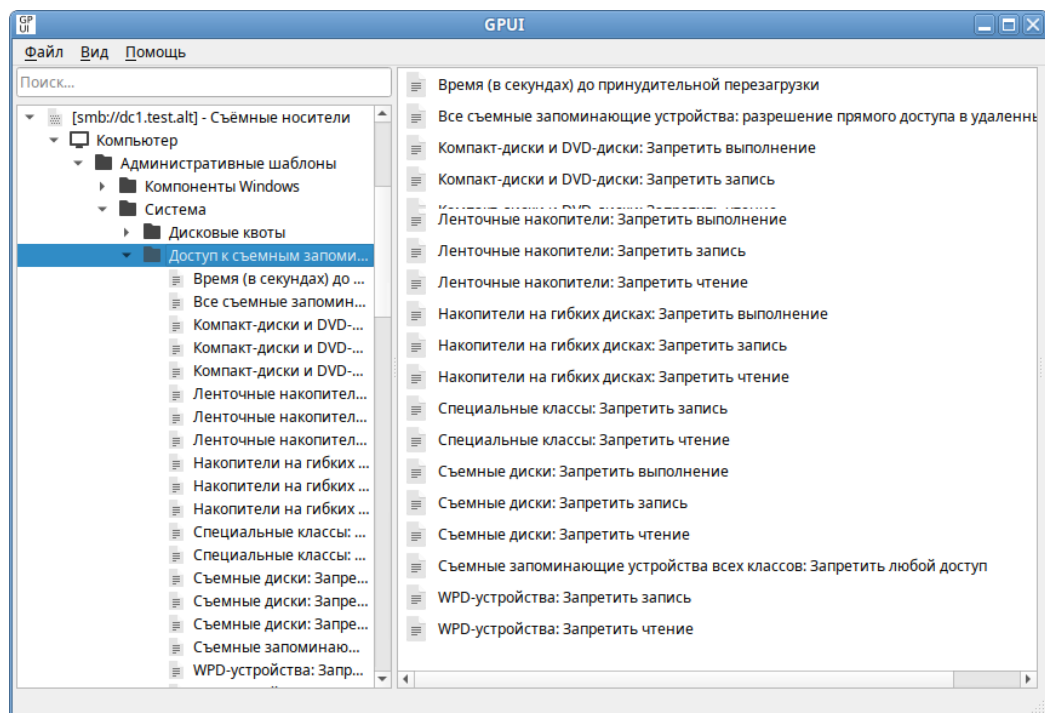


Рис. 175 – «Доступ к съемным запоминающим устройствам»

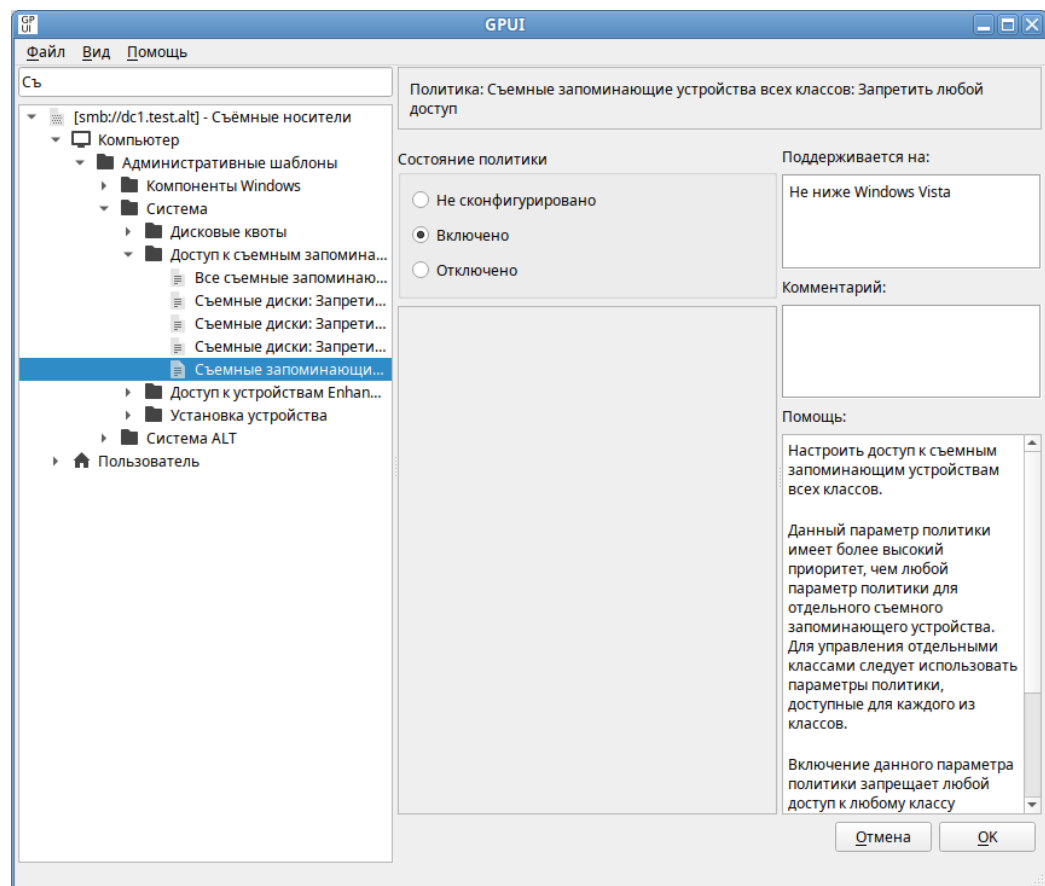


Рис. 176 – Настройки политики «Съемные запоминающие устройства всех классов: Запретить любой доступ»

Для включения запрета на доступ следует выбрать параметр «Включено», для отключения – «Отключено» или «Не сконфигурировано».

Настройки политики управления пакетами 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;;;]
```

4.6.4.5. 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 ограничений пользователя.

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 (рис. 177).

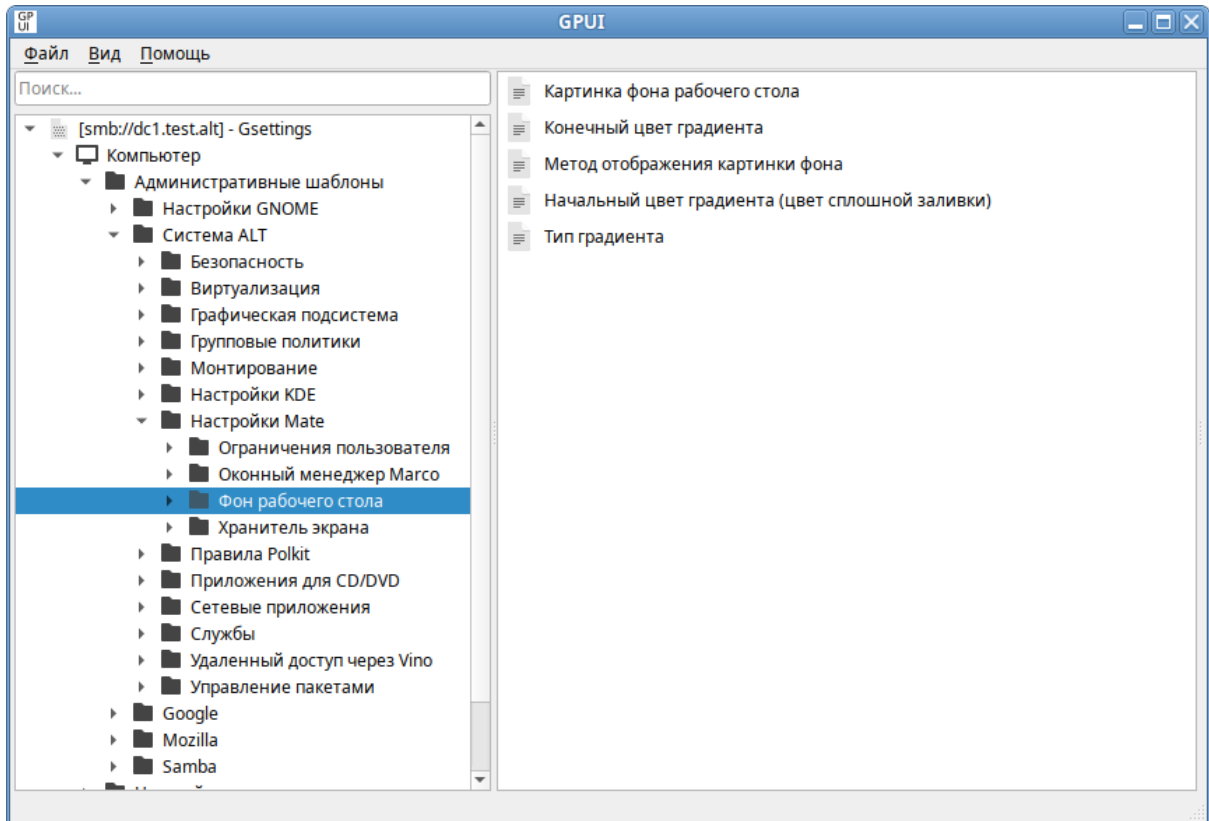


Рис. 177 – Управление настройками gsettings

При выборе политики, откроется диалоговое окно настройки политики (рис. 178).

Можно не задавать настройку политики, включить или отключить. Если выбрать параметр «Включено», в разделе «Параметры» в выпадающем списке можно указать настройки политики (рис. 179).

Политика, управляющая настройкой фона рабочего стола, изменяет ключ KEY в схеме org.mate.background. В реестре Windows 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.

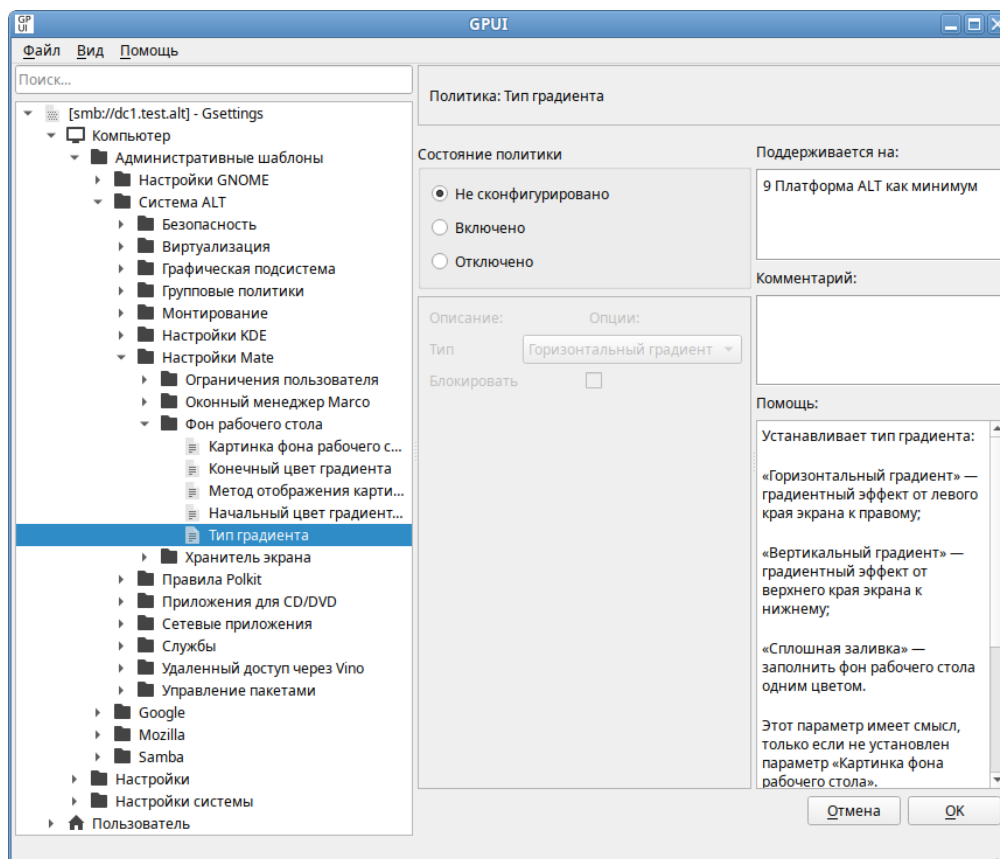


Рис. 178 – Диалоговое окно настройки политики «Тип градиента»

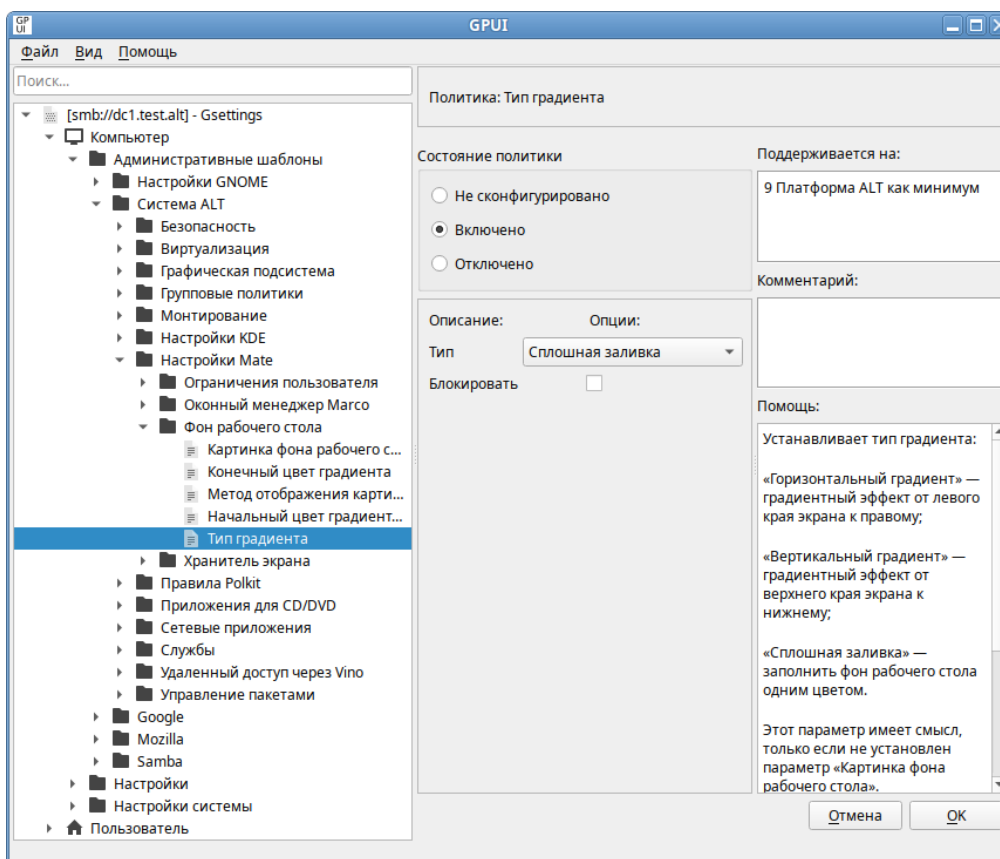


Рис. 179 – Установка градиента в политике «Тип градиента»

Настройки фона рабочего стола приведены в таблице 35.

Т а б л и ц а 35 – Настройки фона рабочего стола

Политика	Ключ	Описание	Значение
Картинка фона рабочего стола	picture-filename	Позволяет устанавливать изображение в качестве фона рабочего стола, задав имя файла, содержащего 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. «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. «Stretched» («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	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 краю. «Горизонтальный градиент» – градиентный эффект от левого края экрана к правому. «Сплошная заливка» – заполнить фон рабочего стола одним цветом

Окончание таблицы 35

Политика	Ключ	Описание	Значение
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 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.

Настройки хранителя экрана приведены в таблице 36.

Т а б л и ц а 36 – Настройки хранителя экрана

Политика	Ключ	Описание	Значение
Время смены тем	cycle-delay	Устанавливает интервал (в минутах) между сменами тем хранителя экрана. Этот параметр имеет смысл только при активированном параметре «Включение хранителя экрана» и если для параметра «Режим работы» установлено значение «Случайные темы»	Время в минутах
Время до блокировки паролем	lock-delay	Устанавливает количество минут, по истечении которых после активации хранителя экрана, компьютер будет заблокирован. 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». 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. 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	После некоторой задержки добавляет кнопку выхода из системы к диалогу разблокирования экрана. Время задержки указывается в настройке «Время выхода из сеанса». Имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера»	-
Переключить пользователя после блокировки	user-switch-enabled	Добавляет кнопку «Переключить пользователя» к диалогу разблокирования экрана. Имеет смысл только при активированном параметре «Включение хранителя экрана» и «Блокировка компьютера» (так как без блокировки не появляется диалог с кнопкой)	-

Окончание таблицы 36

Политика	Ключ	Описание	Значение
Режим работы	mode	Устанавливает режим работы хранителя экрана. Имеет смысл только при активированном параметре «Включение хранителя экрана»	Доступны следующие режимы: «Отключен» – режим отключен «Пустой экран» – не показывать никаких изображений, только черный экран; «Выбранная тема» – показывать одну (указанную) тему хранителя экрана; «Случайные темы» – выбрать тему хранителя экрана случайным образом
Включение хранителя экрана	idle-activation-enabled	Обеспечивает включение хранителя экрана при бездействии системы	-

Политика, управляющая настройкой ограничений пользователя, изменяет ключ KEY в схеме org.mate.lockdown. В реестре Windows 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.

Настройки ограничений пользователя приведены в таблице 37.

Т а б л и ц а 37 – 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 учетную 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 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.

Настройки ограничений пользователя приведены в таблице 38.

Т а б л и ц а 38 – 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 нужен пароль
Удаленный доступ	enabled	Разрешает удаленный доступ к рабочему столу с использованием протокола RFB и VNC	«Включено» – удаленный доступ разрешен. «Отключено» – удаленный доступ запрещен
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 удаленного 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	Включить прослушивание альтернативного порта для удаленных подключений (вместо порта по умолчанию 5 900). Порт указывается в параметре «Альтернативный порт»	«Включено» – включить прослушивание альтернативного порта. «Отключено» – не включать прослушивание альтернативного порта

Окончание таблицы 38

Политика	Ключ	Описание	Значение
Удаленное управление	view-only	Запрещает удаленное управление рабочим столом. Удаленным пользователям, разрешается только просматривать рабочий стол, но не управлять мышью и клавиатурой	«Включено» – удаленное управление разрешено. «Отключено» – удаленное управление запрещено

Политика, управляющая настройкой оконного менеджера Marco, изменяет ключ KEY в схеме org.mate.Marco.general. В реестре Windows 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.

Настройки оконного менеджера Marco приведены в таблице 39.

Т а б л и ц а 39 – 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
Действие по нажатию средней кнопки	action-middle-click-titlebar	Установка действия, выполняемого 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.

Продолжение таблицы 39

Политика	Ключ	Описание	Значение
			«Растянуть по вертикали» (<code><toggle_maximize_vertically></code>) – развернуть окно вертикально без изменения его ширины. «Растянуть по горизонтали» (<code><toggle_maximize_horizontally></code>) – развернуть окно горизонтально без изменения его высоты. «Свернуть» (<code><minimize></code>) – свернуть окно. «Показать меню» (<code><menu></code>) – показать меню окна. «Задвинуть» (<code><lower></code>) – поместить окно под другими. «Ничего не делать» (<code><none></code>) – никакого действия не производить. «Последнее действие» (<code><last></code>) – повторить предыдущее действие
Действие по нажатию правой кнопки	<code>action-right-click-titlebar</code>	Установка действия, выполняемого по нажатию правой кнопки мыши по заголовку окна	См. значение политики «Действие по нажатию средней кнопки»
Размер окна переключения Alt+Tab	<code>alt-tab-max-columns</code>	Устанавливает количество колонок в окне переключения приложений Alt+Tab	Количество колонок
Действие по двойному щелчку	<code>action-double-click-titlebar</code>	Установка действия, выполняемого по двойному щелчку левой кнопкой мыши по заголовку окна	См. значение политики «Действие по нажатию средней кнопки»
Изменение размеров при перетаскивании	<code>primary-color</code>	Включает изменение размеров окна при перетаскивании его в различные области экрана. Если включено, перетаскивание окна на границу экрана распаивает окно вертикально и изменяет горизонтальный размер до половины доступного пространства. Если активирован параметр «Распахнуть окно при перетаскивании к верхнему краю экрана», перетаскивание окна вверх разворачивает окно	-

Продолжение таблицы 39

Политика	Ключ	Описание	Значение
Разворачивание при перетаскивании	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 при перетаскивании»	-
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, 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	-

Продолжение таблицы 39

Политика	Ключ	Описание	Значение
Миниатюры при переключении окон	compositing-fast-alt-tab	Если включено, то вместо миниатюр предварительного просмотра в окне переключения Alt+Tab будут отображаться значки приложения	-
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
Режим активации окна	focus-mode	Режим переключения фокуса в окно определяет, как активируются окна	«Click» – для активации окна на нем надо щелкнуть. «Sloppy» – окно активируется, когда на него перемещается указатель мыши. «Mouse» – окно активируется, когда в него перемещается указатель мыши, и перестает быть активным, когда указатель мыши уходит из него
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	«Automatic» («Автоматически») – система выбирает местоположение на основе доступного пространства на рабочем столе, или располагает каскадом, если нет места. «Pointer» («Указатель») – новые окна размещаются в соответствии с положением указателя мыши. «Manual» («Ручной») – пользователь должен вручную расположить новое окно с помощью мыши или клавиатуры
Граница окна при переключении	show-tab-border	Выделять границу выбранного окна при переключении с помощью Alt+Tab	-

Окончание таблицы 39

Политика	Ключ	Описание	Значение
Тема оформления	theme	Устанавливает тему, отвечающую за отображение границ окон, заголовка и т. д.	Строка, содержащая название темы (например, Dorple)
Шрифт заголовка	titlebar-font	Устанавливает шрифт заголовков окон. Этот параметр игнорируется, если активирован параметр «Системный шрифт в заголовке окон»	Строка, содержащая название шрифта и через пробел, размер шрифта (например, Noto Sans Bold 10)
Системный шрифт в заголовке окон	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 ее же началу, и конец каждой колонки ведет к ее же началу

Политика, управляющая настройкой клавиатуры, изменяет ключ KEY в схеме org.mate.peripherals-keyboard. В реестре Windows 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.

Настройки клавиатуры приведены в таблице 40.

Т а б л и ц а 40 – 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
Повторять удерживаемую нажатой клавишу	repeat	Включить повтор нажатой и удерживаемой клавиши. Если нажать и удерживать клавишу при включенном повторе ввода, действие, соответствующее клавише, будет повторяться. Например, если нажать и удерживать клавишу с буквой, то эта буква будет многократно повторена.	-

4.6.4.6. 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 (рис. 180).

Для задания списка пакетов, которые нужно установить, щелкнуть левой кнопкой мыши на политике «Установка пакетов», откроется диалоговое окно настройки политики (рис. 181).

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 (рис. 182).

Для добавления/удаления строк можно воспользоваться соответствующими кнопками.

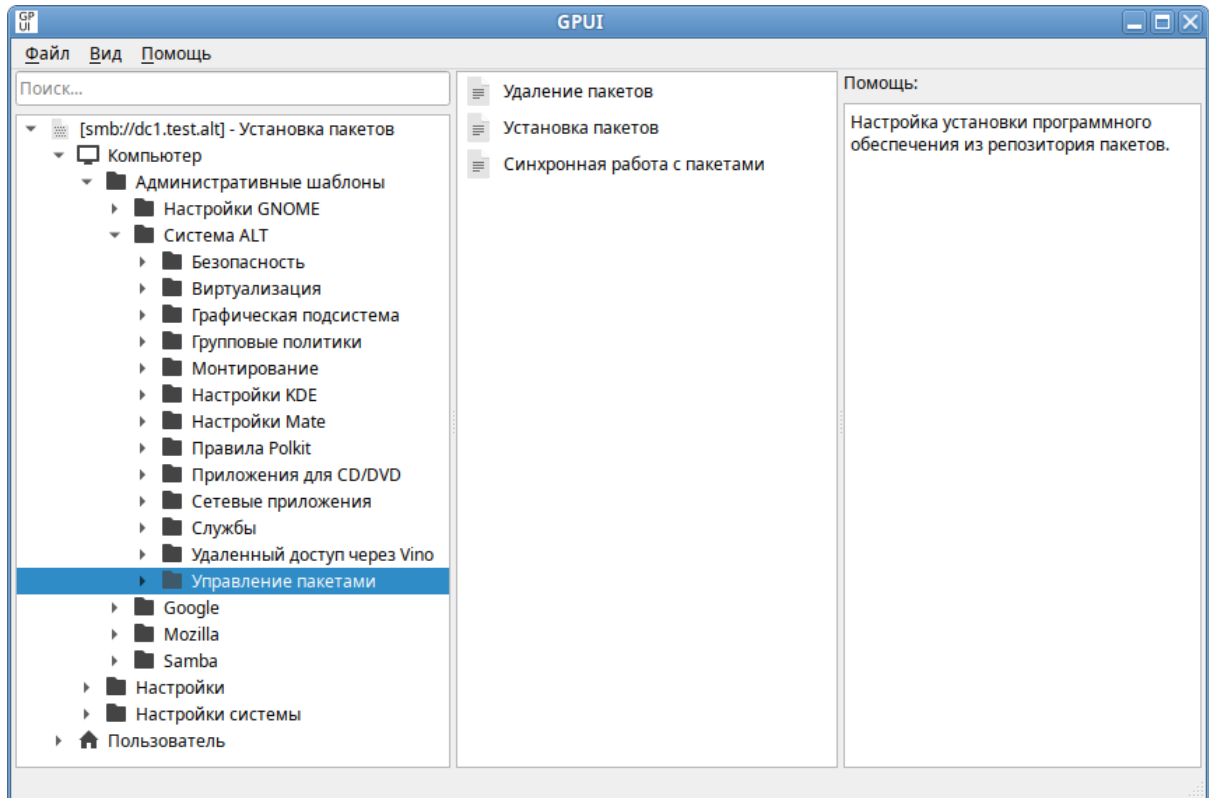


Рис. 180 – Раздел «Управление пакетами»

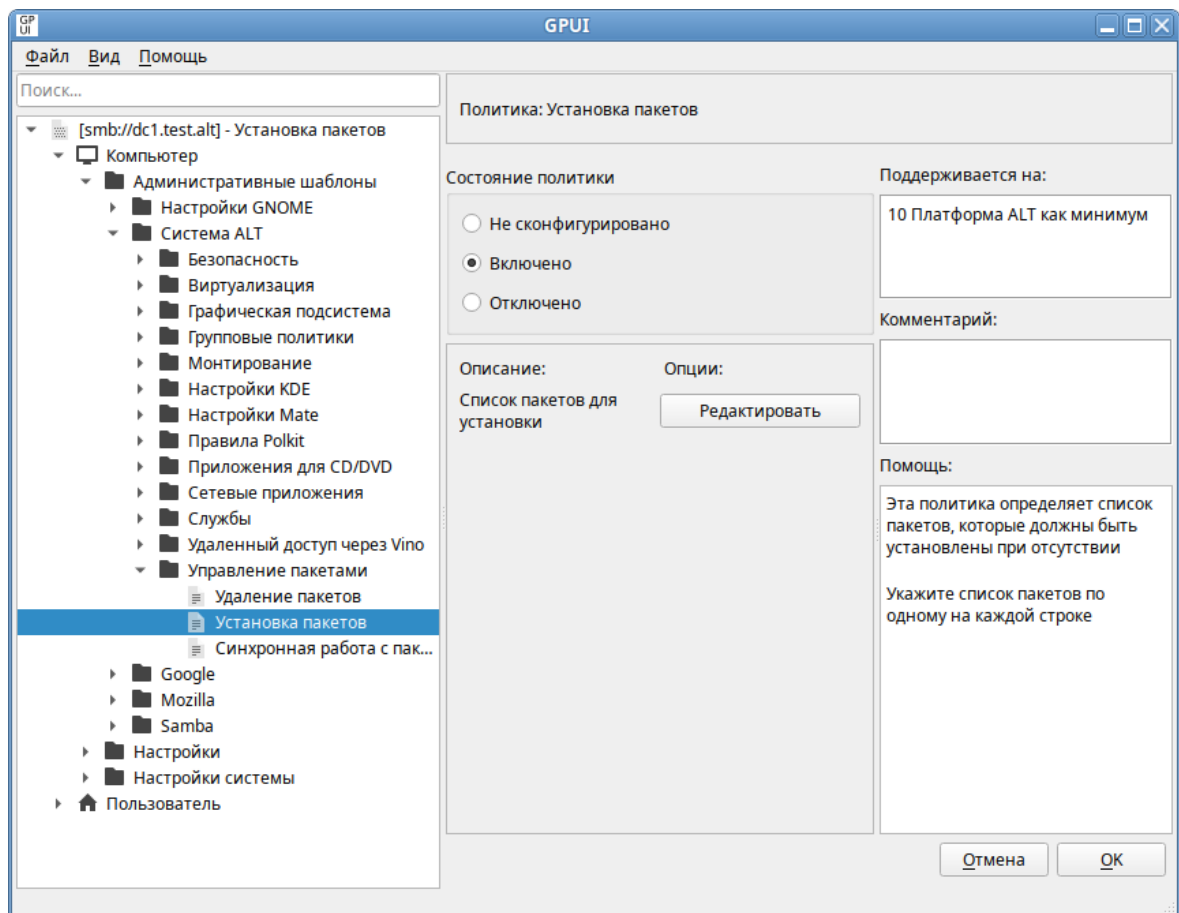


Рис. 181 – Диалоговое окно «Установка пакетов»

П р и м е ч а н и е . Для задания списка пакетов, которые нужно удалить, нужно выбрать политику «Удаление пакетов».

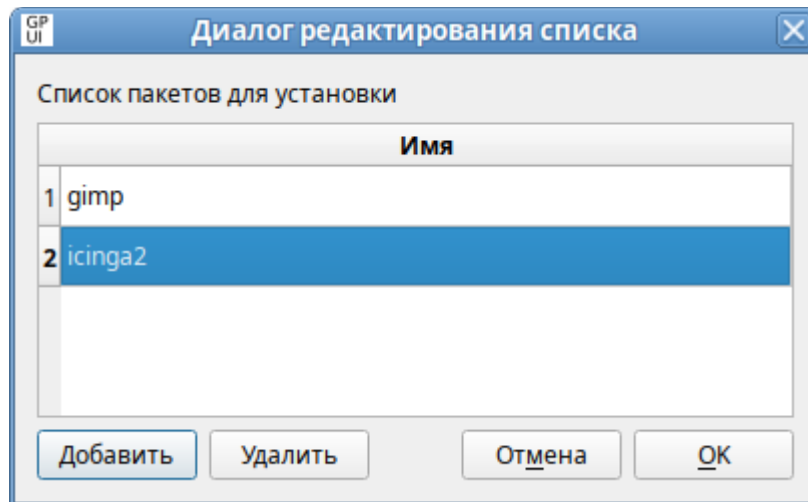


Рис. 182 – Список пакетов для установки

Можно также включить политику «Синхронная работа с политиками». 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 политиками» 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 «ОК», для сохранения изменений (рис. 183).

Политики управления пакетами относятся к экспериментальным, поэтому на машинах с ОС Альт СП, где они применяются, должны быть включены экспериментальные групповые политики (о том, как включить экспериментальные групповые политики указано в п. 4.6.4.7).

Все настройки политики управления пакетами хранятся в файлах {GUID GPT}/Machine/Registry.pol и {GUID GPT}/User/Registry.pol.

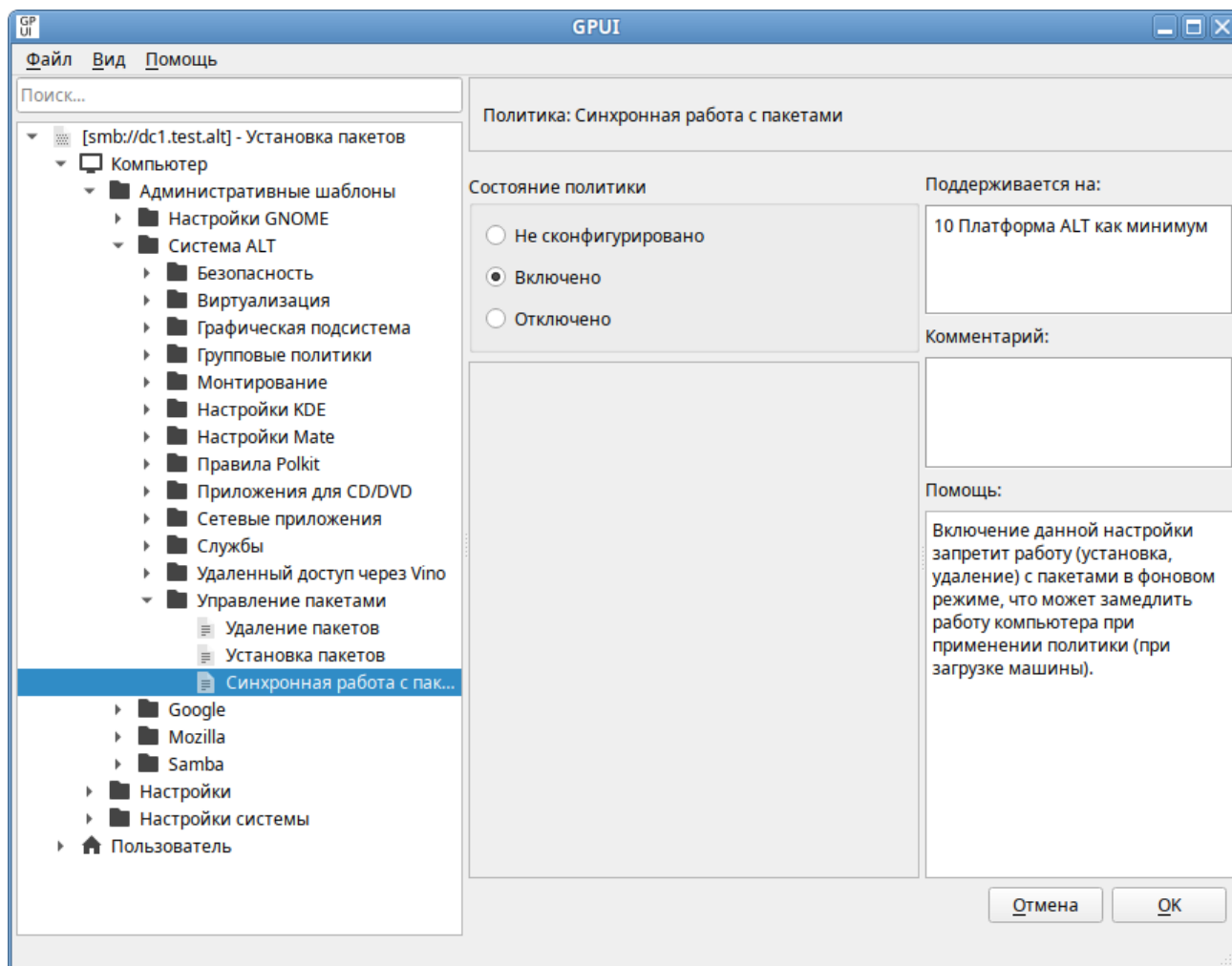


Рис. 183 – Политика «Синхронная работа с политиками»

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;icinga2;;; icinga2]
[Software\BaseALT\Policies\Packages\Remove;python3-
tools;;;python3-tools]
```

4.6.4.7. Экспериментальные групповые политики

На машинах с ОС Альт СП, где применяются экспериментальных политики, должны быть включены «Экспериментальные групповые политики».

Для включения экспериментальных групповых политик следует в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Групповые политики» выбрать пункт «Экспериментальные групповые политики» и установить в открывшемся окне отметку в поле «Включено» (рис. 184).

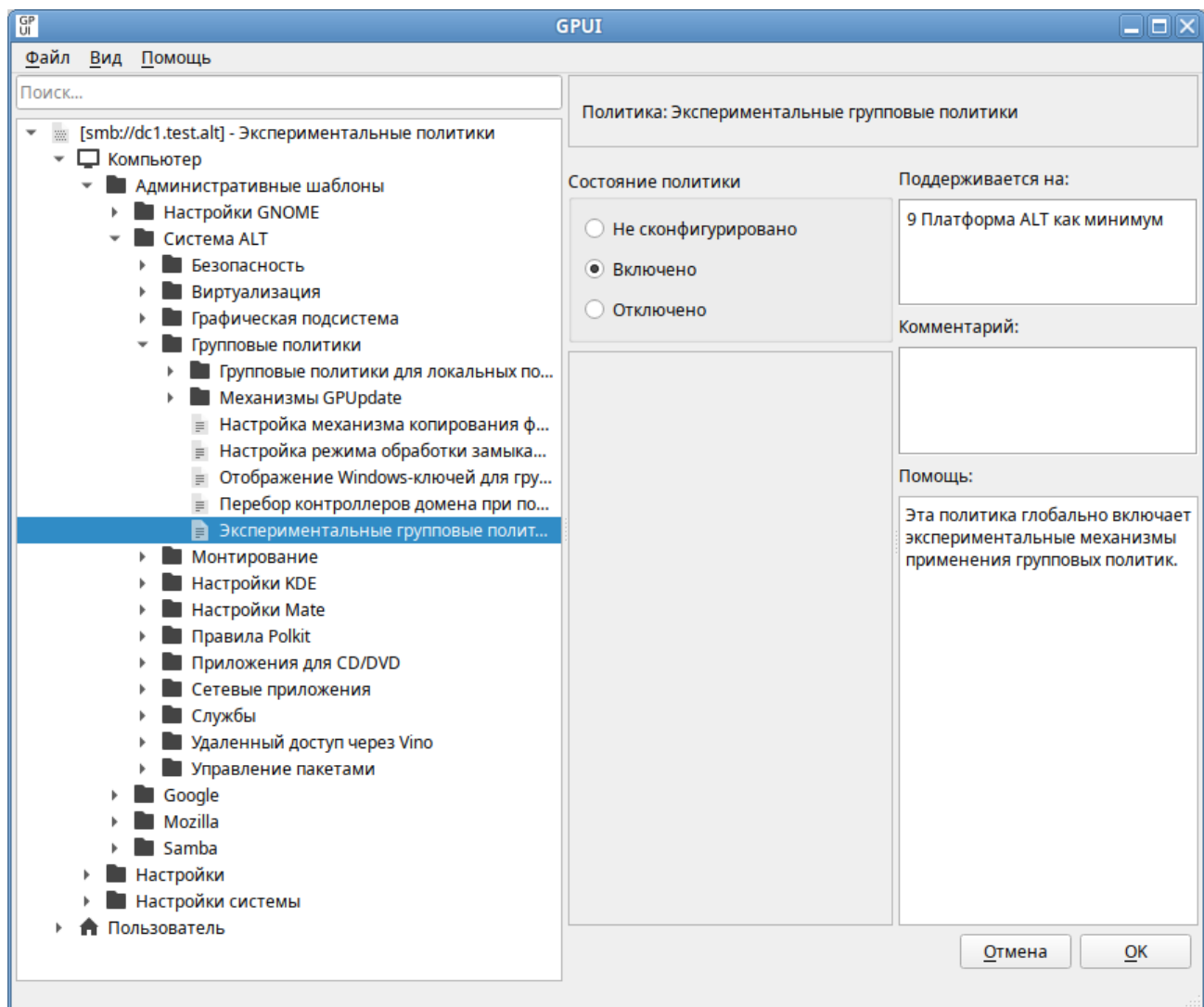


Рис. 184 – «Экспериментальные групповые политики»

4.6.4.8. Механизмы GPOupdate

Каждый механизм применения групповых политик можно отдельно включить или отключить. Для этого следует включить/отключить соответствующую политику в разделе «Компьютер»/«Пользователь» → «Административные шаблоны» → «Система ALT» → «Групповые политики» → «Механизмы GPOupdate».

Например, включить/отключить механизм групповых политик управления пакетами (Packages) можно, включив/отключив политики «Установка и удаление программ» или «Установка и удаление программ для пользователей» (рис. 185).

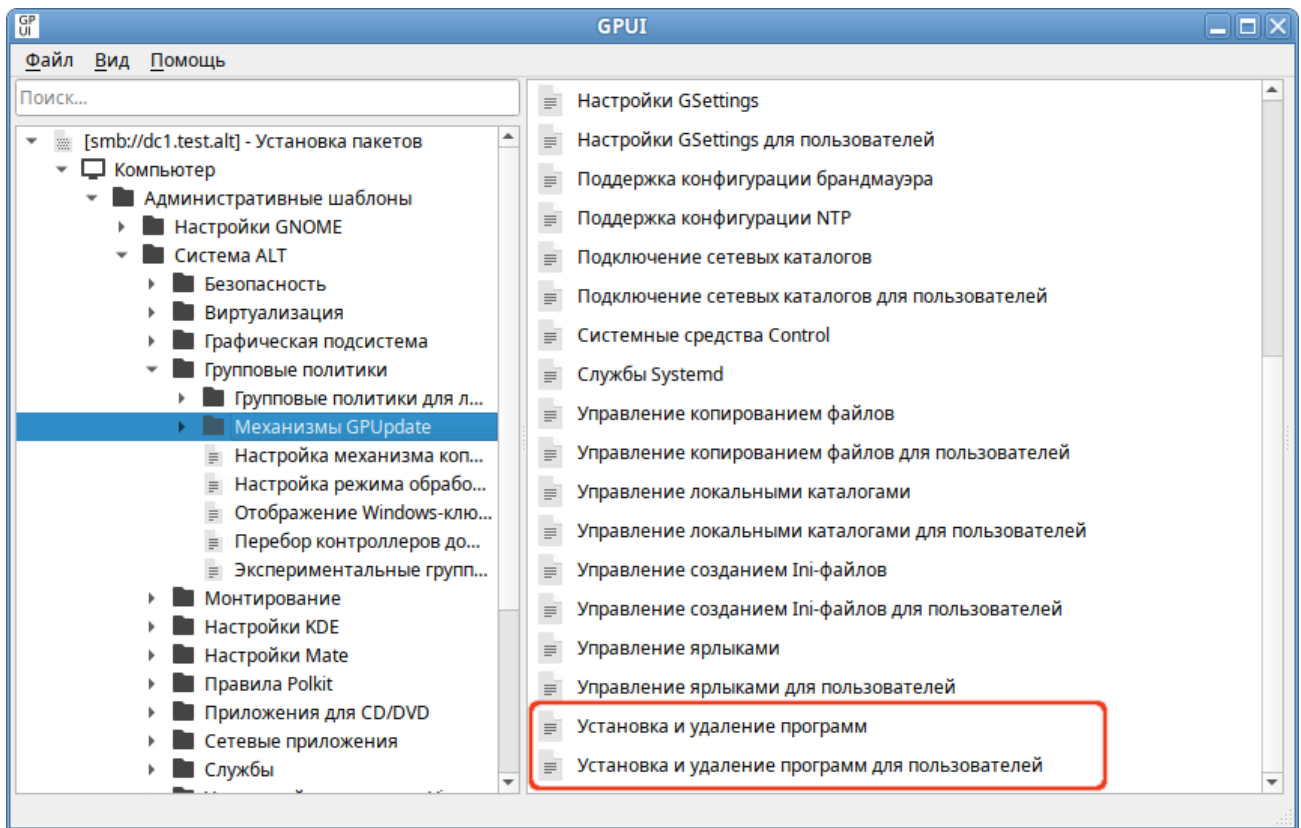


Рис. 185 – Механизм применения групповых политик

4.6.4.9. Управление политиками веб-браузера Chromium

Эти групповые политики позволяют централизованно для компьютеров управлять настройками интернет-браузера Google Chromium.

Механизм Chromium в составе пакета gupdate формирует JSON-файл для веб-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 веб-браузерами в любом дистрибутиве «Альт» с установленным окружением рабочего стола.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-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` (рис. 186).

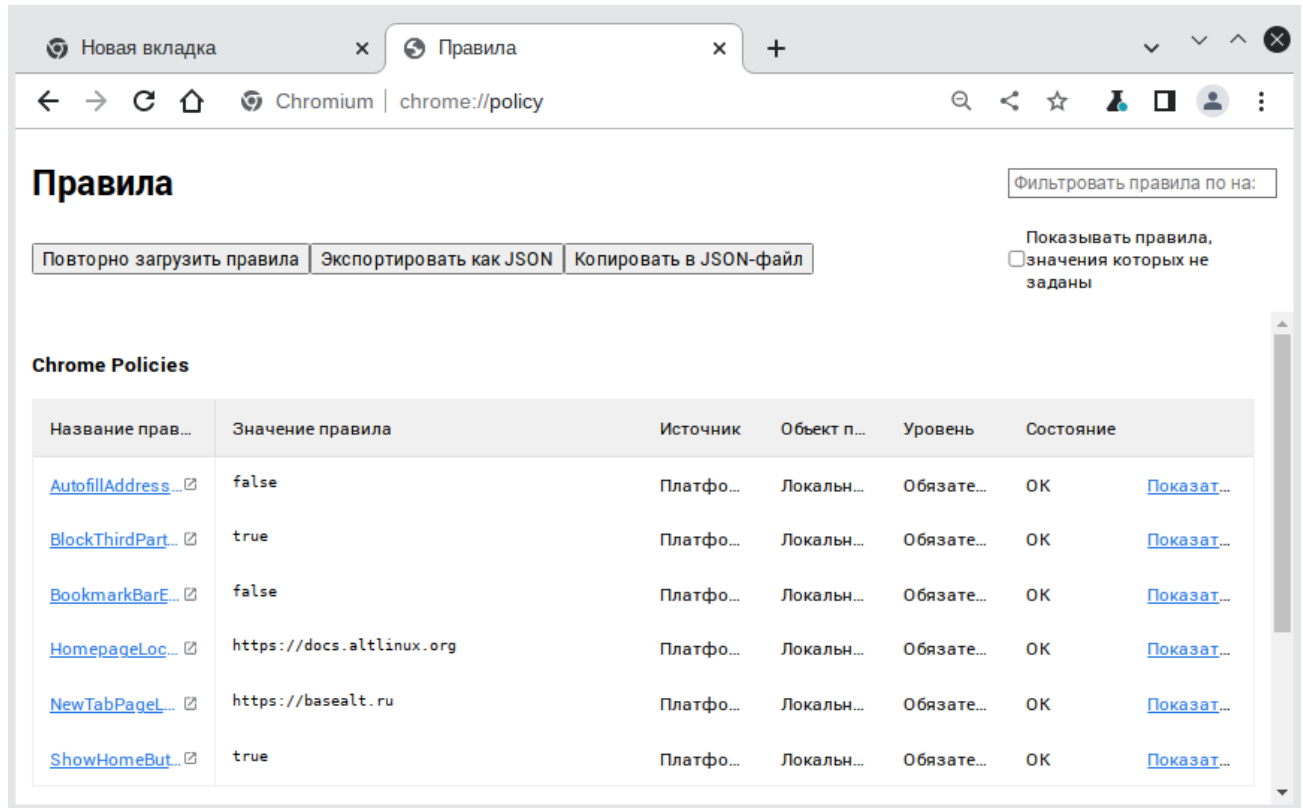


Рис. 186 – Активные политики веб-браузера Chromium

В качестве примера ниже рассмотрена политика установки URL домашней страницы.

Для редактирования политик веб-браузера Chromium следует перейти в «Компьютер» → «Административные шаблоны» → «Google» → «Google Chrome». Отобразится список политик (рис. 187).

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 «Описание» ввести URL и нажать кнопку «ОК» (рис. 188).

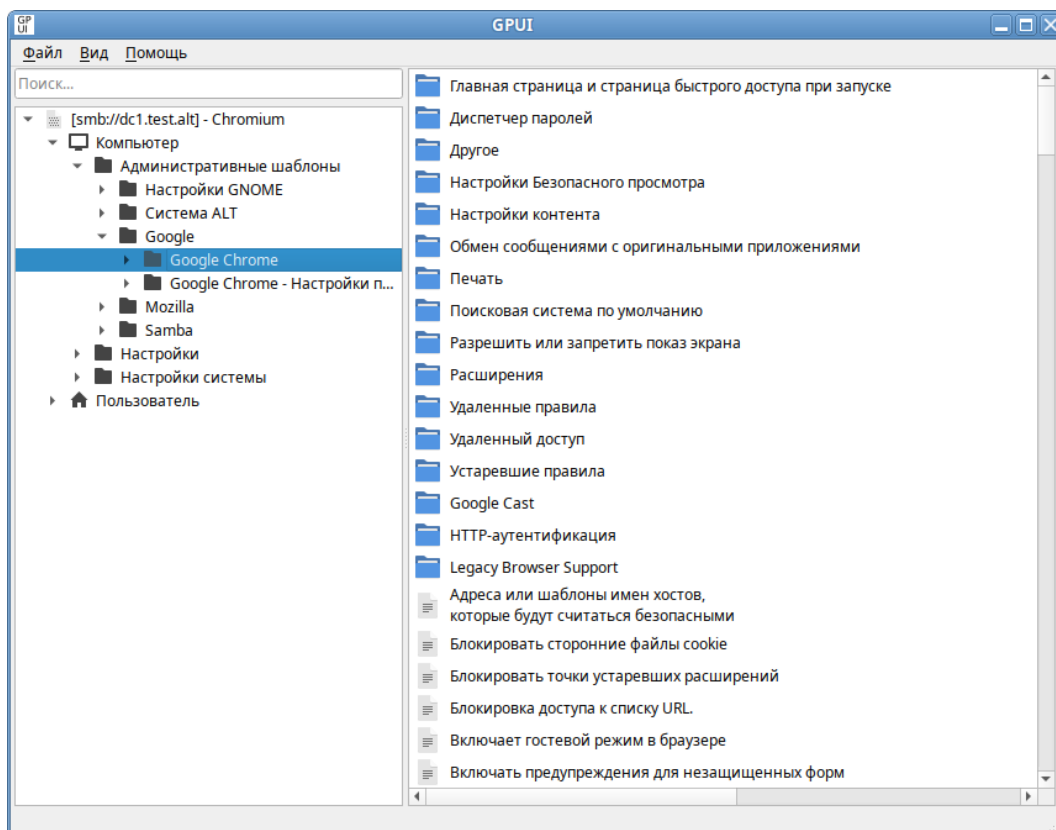


Рис. 187 – Политики настройки веб-браузера Chromium

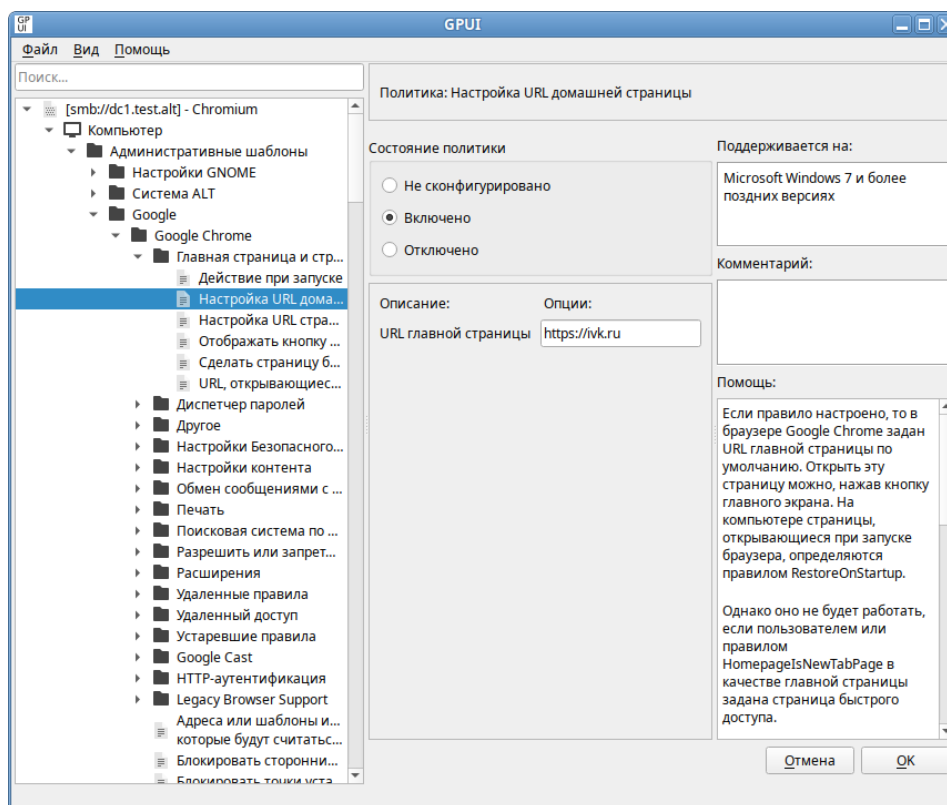


Рис. 188 – Установка URL домашней страницы Chromium

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 189).

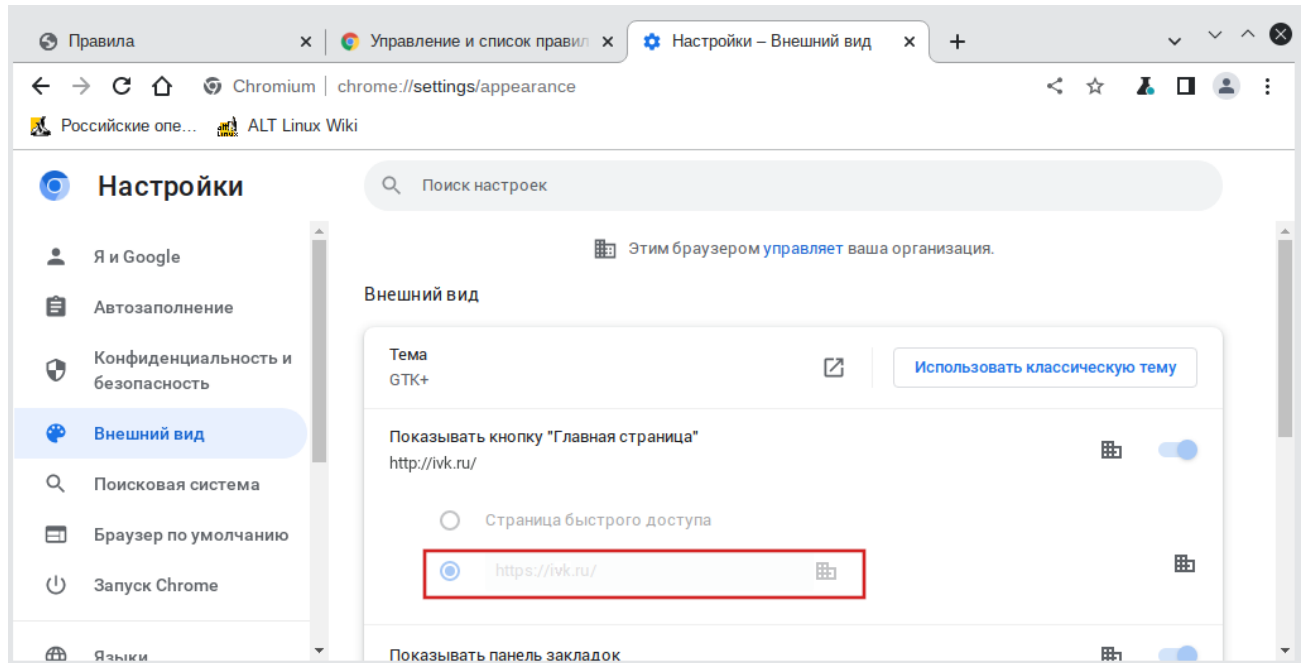


Рис. 189 – Настройки веб-браузера Chromium

Все настройки политики веб-браузера Chromium хранятся в файле {GUID GPT}/Machine/Registry.pol.

Пример файла Registry.pol:

```
PReg[Software\Policies\Google\Chrome;HomepageLocation;;;https://ivk.ru]
```

В таблице 41 описаны только некоторые политики. Полный список политик и их описание можно найти в веб-браузере Chromium, указав в адресной строке URL: `chrome://policy` и установив отметку на пункте «Показывать правила, значения которых не заданы».

Т а б л и ц а 41 – Примеры политик управляющих настройками 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 веб-браузере или сессионных файлов cookie при завершении работы. Если для политики указано значение «Открыть список URL и восстановить последний сеанс», веб-браузер будет восстанавливать предыдущий сеанс и открывать URL, заданные в политике «URL, открываемые 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
Настройка URL страницы быстрого доступа	NewTabPageLocation	Позволяет установить URL страницы быстрого доступа по умолчанию и запрещает пользователям его изменять. Страница быстрого доступа появляется, когда пользователь открывает новую вкладку или окно.

Продолжение таблицы 41

Политика	Ключ	Описание
		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 <code>chrome://newtab</code> . Если эта политика настроена, пользователи не смогут изменить главную страницу в Chromium. Если политика не настроена, они 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

Продолжение таблицы 41

Политика	Ключ	Описание
Включить сохранение паролей	PasswordManagerEnabled	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 ее 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

Продолжение таблицы 41

Политика	Ключ	Описание
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. URL поисковой системы Google можно указать так: <pre>'{google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:searchClient}{google:sourceId}ie={inputEncoding}'</pre>
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 ее 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 изображение задано. В противном случае применяются персональные настройки пользователя

Продолжение таблицы 41

Политика	Ключ	Описание
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», веб-браузер не блокирует URL. 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 веб-браузер Chromium сохраняет скачиваемые файлы. Данный каталог используется, даже если пользователь выбрал каталог для сохранения или установил флаг, позволяющий выбирать каталог при каждом скачивании файла. Эта политика отменяет действие политики DefaultDownloadDirectory.

Продолжение таблицы 41

Политика	Ключ	Описание
		Если политика находится в состоянии «Не сконфигурировано», веб-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
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 веб-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

Продолжение таблицы 41

Политика	Ключ	Описание
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. 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 ее. Если политика не настроена, 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 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

Продолжение таблицы 41

Политика	Ключ	Описание
Включить анонимный сбор данных	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
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 <pre>[{"name": "Документация", "url": "docs.altlinux.org"}, {"name": "Wiki", "url": "altlinux.org"}]</pre> По умолчанию папка называется «Управляемые закладки». Чтобы изменить это название, нужно добавить в правило дополнительный словарь с единственным ключом toplevel_name и названием папки в качестве значения. Также можно задать подпапку для закладок. Для этого вместо ключа url следует использовать ключ children, а в качестве его значения указать список вложенных закладок или папок <pre>[{"toplevel_name": "ALT"}, {"name": "BaseALT", "url": "basealt.ru"}, {"name": "ALT docs", "children": [{"name": "Документация", "url": "docs.altlinux.org"}, {"name": "Wiki", "url": "altlinux.org"}]}]</pre> 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

Продолжение таблицы 41

Политика	Ключ	Описание
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 веб-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 веб-браузере не разрешается использовать гостевые профили
Удаление данных о работе в веб-браузере при выходе	ClearBrowsingDataOnExitList	Политика позволяет настроить список данных о работе в веб-браузере, которые должны удаляться, когда пользователь закрывает все окна веб-браузера. Можно указать следующие типы данных: - browsing_history (история веб-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 кэше); - password_signin (пароли); - autofill (автозаполнение); - site_settings (настройки сайтов); - hosted_app_data (данные размещенных приложений).

Продолжение таблицы 41

Политика	Ключ	Описание
		У этой политики нет приоритета над политикой «Удаление истории просмотров и загрузок веб-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 веб-браузера или ОС), данные о работе в веб-браузере удаляются при следующей загрузке профиля. Если политика находится в состоянии «Отключено», то данные о работе, при закрытии веб-браузера, не удаляются
Задать объем кэша в байтах	DiskCacheSize	Если для политики задано значение «None», Chromium использует объем кэша по умолчанию для хранения кэшированных файлов на диске. В этом случае пользователи не могут изменить правило. Если политика находится в состоянии «Включено», Chromium будет использовать указанный размер кэша независимо от того, указали ли пользователи значение экспериментального параметра <code>--disk-cache-size</code>. Объем кэша задается в байтах, например, чтобы задать размер кэша 300 МБ, нужно 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 кэша с помощью экспериментального параметра <code>--disk-cache-size</code>. Указанное в правиле значение используется различными подсистемами в веб-браузере как справочное. Поэтому фактический объем используемого дискового пространства может превышать указанное значение, но будет иметь такой же порядок

Продолжение таблицы 41

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 веб-браузера). Названия серверов нужно разделять запятыми. Допустимы подстановочные знаки (*)
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.

Продолжение таблицы 41

Политика	Ключ	Описание
		Пример значения: <pre>{ "hdokiejnpimakedhajhdlcegeplioahd": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" }, "pioclpoplcbdaefihamjohnefbikjilc": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" } }</pre> Параметры политики: 1) <code>allowed_types</code> – типы приложений и расширений, которые пользователям разрешено устанавливать в веб-браузере (допустимые строки: «<code>extension</code>», «<code>hosted_app</code>», «<code>legacy_packaged_app</code>», «<code>platform_app</code>», «<code>theme</code>», «<code>user_script</code>»). Используется только для настройки конфигурации по умолчанию со значением *; 2) <code>blocked_install_message</code> – уведомление (не более 1000 символов), которое будет появляться на устройствах пользователей при попытке установить запрещенные расширения; 3) <code>blocked_permissions</code> – запрещает пользователям устанавливать и запускать расширения, требующие разрешений API (список доступных разрешений указан в манифесте расширения); 4) <code>installation_mode</code> – указывает, разрешено ли добавлять заданные расширения. Допустимые режимы: - <code>allowed</code> – пользователи могут установить это расширение (поведение по умолчанию); <code>blocked</code> – пользователи не могут установить это расширение;

Продолжение таблицы 41

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 нужно указать ссылку для скачивания расширения (параметр update_url); - автоматически – пользователи могут его удалить. В этом режиме нужно указать ссылку для скачивания расширения (параметр update_url); 5) install_sources – список URL страниц, с которых разрешено загружать и устанавливать расширения. Нужно разрешить URL расположения CRX-файла и страницы, с которой начинается скачивание (то есть URL перехода); 6) 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; 7) update_url – определяет, откуда загружается расширение. Можно указать URL интернет-магазина Chrome, Орега или использовать XML-файл: - если расширение размещено в интернет-магазине Chrome, следует указать <code>https://clients2.google.com/service/update2/crx</code> - если расширение размещено в интернет-магазине Орега, следует указать <code>https://extension-updates.opera.com/api/omaha/update/</code> 8) override_update_url – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля update_url или update в политике ExtensionInstallForcelist. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения;

Окончание таблицы 41

Политика	Ключ	Описание
		9) <code>verified_contents_url</code> – указывает путь до файла «<code>extension.verified_contents</code>». С его помощью расширение проверяется на доверие (используется, если нет доступа в интернет); 10) <code>normal_Installed</code> – расширение устанавливается <code>runtime_allowed_hosts</code> – разрешает взаимодействие расширений с указанными сайтами, даже если они указаны в поле <code>runtime_blocked_hosts</code>. Можно указать до 100 сайтов; 11) <code>toolbar_pin</code> – определяет, закреплён ли значок расширения на панели инструментов. Возможные значения: - <code>force_pinned</code> – значок расширения закреплён на панели инструментов и постоянно виден. Пользователь не может скрыть его в меню расширения; - <code>default_unpinned</code> – расширение скрыто в меню расширений (по умолчанию), пользователь может закрепить его на панели инструментов.

4.6.4.10. Управление политиками веб-браузера Firefox

Эти групповые политики позволяют централизованно для компьютеров управлять настройками веб-браузера Mozilla Firefox.

Механизм Firefox в составе пакета `groupupdate` формирует JSON-файл для веб-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 веб-браузерами в любом дистрибутиве «Альт» с установленным окружением рабочего стола.

Путь к файлу `policies.json`, в зависимости от версии веб-браузера Mozilla Firefox:

- `/etc/firefox/policies` – новые версии;
- `/usr/lib64/firefox/distribution` – старые версии.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-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` (рис. 190).

В качестве примера ниже рассмотрена политика установки URL домашней страницы.

Для редактирования политик веб-браузера Mozilla Firefox следует перейти в «Компьютер» → «Административные шаблоны» → «Mozilla» → «Firefox» (рис. 191).

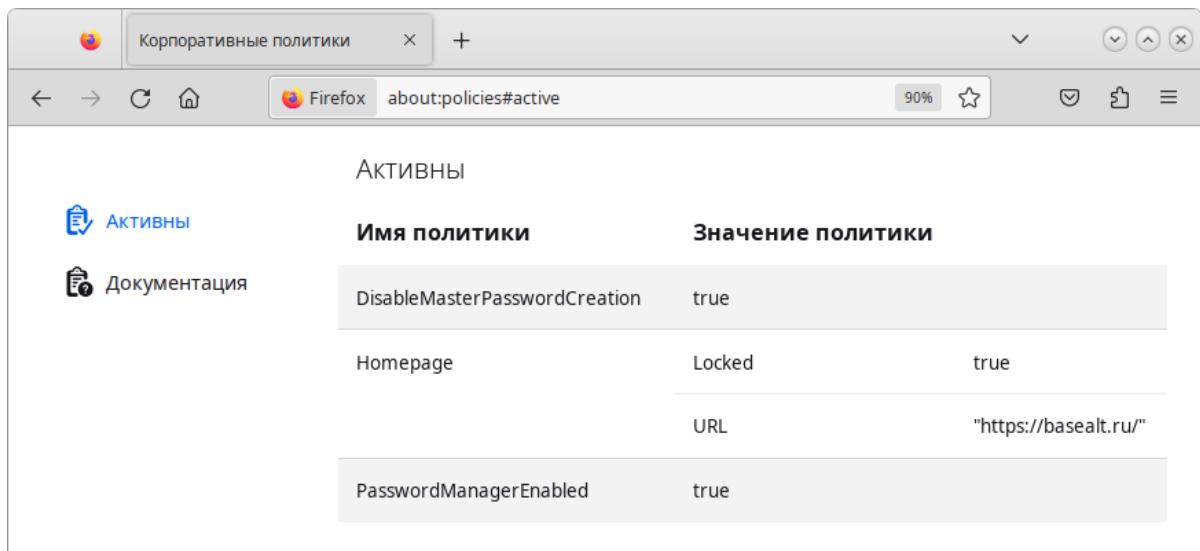


Рис. 190 – Активные политики веб-браузера Mozilla Firefox

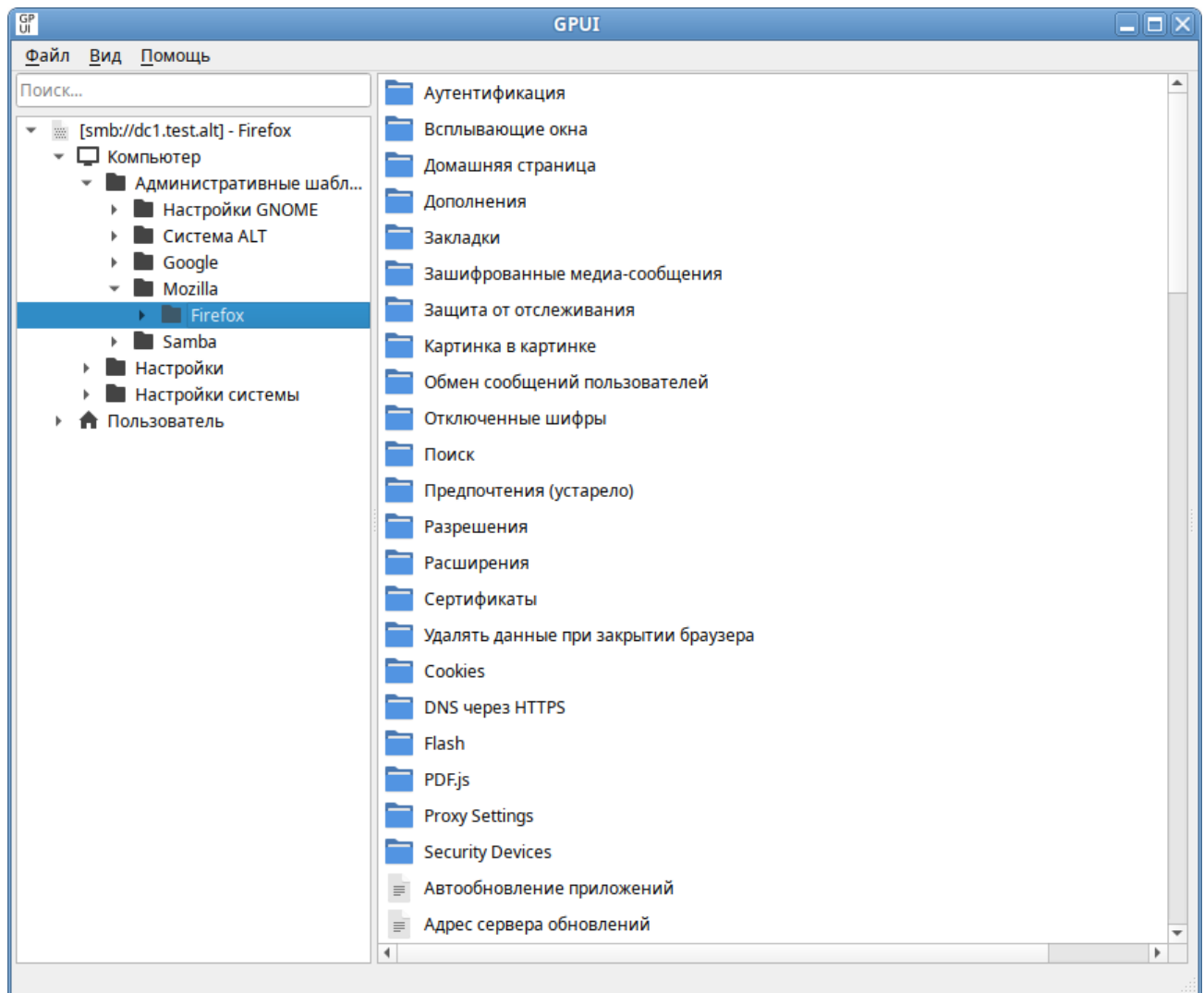


Рис. 191 – Политики настройки веб-браузера Mozilla Firefox

Раскрыть группу «Домашняя страница», щелкнуть левой кнопкой мыши на политике «URL для домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Описание» ввести URL и нажать кнопку «ОК» (рис. 192).

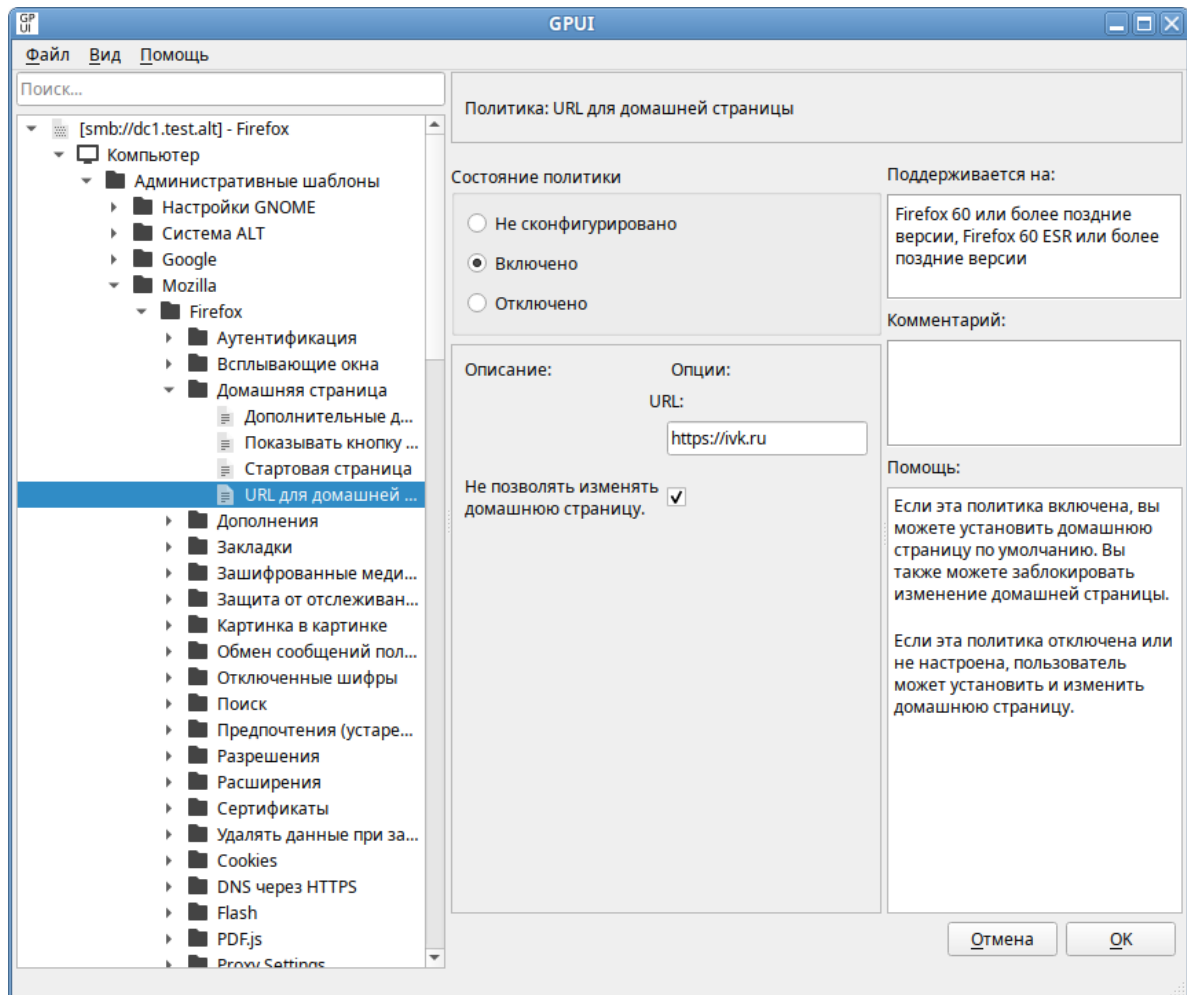


Рис. 192 – Диалоговое окно «URL для домашней страницы»

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 193).

Все настройки политики веб-браузера Mozilla Firefox хранятся в файле {GUID GPT}/Machine/Registry.pol.

Пример файла Registry.pol:

```
PReg[Software\Policies\Mozilla\Firefox\Homepage;URL;;;https://ivk.ru]
[Software\Policies\Mozilla\Firefox\Homepage;Locked;;;]
```

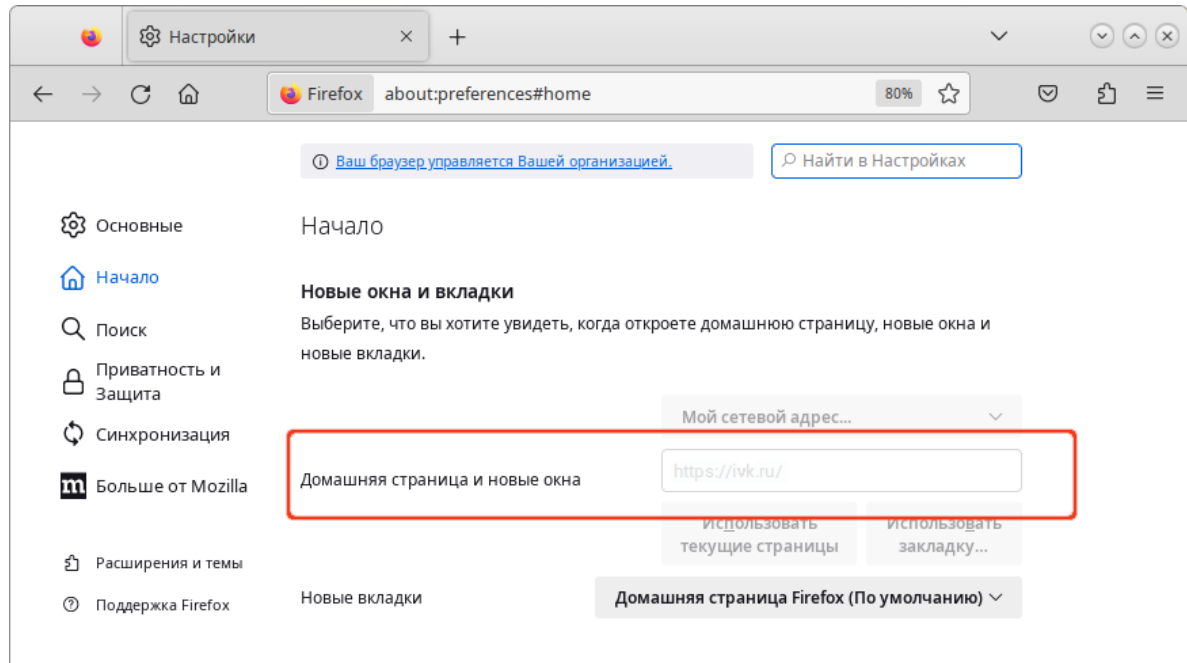


Рис. 193 – Настройки веб-браузера Mozilla Firefox

Примеры политик управляющих настройками веб-браузера Mozilla Firefox представлены в таблице 42. Полный список политик и их описание можно найти в веб-браузере Mozilla Firefox, указав в адресной строке URL:

`about:policies#documentation`

Т а б л и ц а 42 – Примеры политик управляющих настройками 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 сохраненные 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

Продолжение таблицы 42

Политика	Ключ	Описание
Отключить инструменты разработчика	DisableDeveloperTools	Позволяет управлять доступом к инструментам 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	Спрашивает, куда сохранять файлы при загрузке. 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.

Продолжение таблицы 42

Политика	Ключ	Описание
		Если политика находится в состоянии «Не сконфигурировано», пользователю будет выдаваться запрос на сохранение файла, но он может изменить значение по умолчанию
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 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).

Продолжение таблицы 42

Политика	Ключ	Описание
		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. П р и м е ч а н и е . Веб-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 проверки поддержки активного сетевого соединения IPv6. Отключение этой функциональности уменьшает количество автоматических подключений и может немного ускорить запуск веб-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».

Продолжение таблицы 42

Политика	Ключ	Описание
		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 скриншоты 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. Для получения дополнительной информации см. https://support.mozilla.org/en-US/kb/shield и https://wiki.mozilla.org/Firefox/Shield/Heartbeat

Продолжение таблицы 42

Политика	Ключ	Описание
Отключить кнопку «Забыть»	DisableForgetButton	Закрывает доступ к кнопке «Забыть». Если политика находится в состоянии «Включено», кнопка «Забыть о части истории веб-серфинга» недоступна. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», кнопка «Забыть о части истории веб-серфинга» доступна
Запретить показывать пароли в сохраненных логинах	DisablePasswordReveal	Не позволяет просматривать пароли у сохраненных 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-серфинга
Отключить импорт профиля	DisableProfileImport	Отключает команду меню для импорта данных из другого веб-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

Продолжение таблицы 42

Политика	Ключ	Описание
Отключить обновление профиля	DisableProfileRefresh	Отключает кнопку «Обновить Firefox» на странице about:support. Если политика находится в состоянии «Включено», кнопка «Обновить Firefox» будет недоступна на странице about:support. Если эта политика отключена или не настроена, кнопка «Обновить Firefox» доступна
Отключить безопасный режим	DisableSafeMode	Отключает функцию для перезапуска в безопасном режиме. Если политика находится в состоянии «Включено», пользователь не может перезапустить веб-браузер в безопасном режиме. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», безопасный режим разрешен
Не проверять веб-браузер по умолчанию	DontCheckDefaultBrowser	Отключает проверку веб-браузера по умолчанию при запуске. Если политика находится в состоянии «Включено», Firefox не проверяет, является ли он веб-браузером по умолчанию при запуске. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Firefox при запуске проверяет, является ли он веб-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	Требовать или не давать использовать мастер-пароль. Если политика находится в состоянии «Отключено», пользователи не могут создать основной пароль.

Продолжение таблицы 42

Политика	Ключ	Описание
		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. 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

Продолжение таблицы 42

Политика	Ключ	Описание
Показывать кнопку «Домашняя страница Firefox» на панели инструментов	ShowHomeButton	Включает кнопку «Домашняя страница Firefox» на панели инструментов. Если политика находится в состоянии «Отключено», кнопка «Домашняя страница Firefox» не будет отображаться на панели инструментов. Если политика находится в состоянии «Включено», кнопка «Домашняя страница Firefox» 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)
URL для домашней страницы	Homepage	Устанавливает URL домашней страницы при старте веб-браузера и, если нужно, блокирует ее смену. 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

Продолжение таблицы 42

Политика	Ключ	Описание
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 веб-браузера. Если политика находится в состоянии «Включено», указанным веб-сайтам разрешается использовать аутентификацию SPNEGO в веб-браузере. Записи в списке имеют формат altlinux.org или https://altlinux.org
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 флаги отмечены), SPNEGO или NTLM будут включены для неполных доменных имен (Non FQDN)
Отключить историю форм	DisableFormHistory	Отключает запоминание истории поиска и данных форм. Если политика находится в состоянии «Включено», Firefox не запоминает историю форм или поиска. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», Firefox будет помнить историю форм и поиска
Не разрешать изменять настройки аутентификации	Authentication Locked	Блокирует настройки аутентификации от изменений пользователем. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь не может изменить параметры проверки подлинности. Если политика находится в состоянии «Включено» (и флаги отмечены), пользователь может изменить параметры проверки подлинности

Продолжение таблицы 42

Политика	Ключ	Описание
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. 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 нужно задавать в формате *.xpi (например, https://addons.mozilla.org/firefox/downloads/file/3450175/adapter_rutoken_plugin-1.0.5.0.xpi). Также можно указать путь на локальный каталог, в который, политикой копирования файлов (см.п. 4.6.5.5), 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 установить расширение и посмотреть идентификатор на странице about:support в разделе «Расширения».

Продолжение таблицы 42

Политика	Ключ	Описание
		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: <pre>{ "*": { "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", "install_url": "https://addons.mozilla.org/.../plugin.xpi" } }</pre> Конфигурация для каждого расширения – это еще один словарь, который может содержать следующие поля: - <code>installation_mode</code> – режим установки расширения. Допустимые значения: а) <code>allowed</code> – разрешает установку расширения пользователем (поведение по умолчанию). Поле <code>install_url</code> не используется и будет автоматически определено на основе идентификатора; б) <code>blocked</code> – блокирует установку расширения и удаляет его, если оно уже установлено;

Продолжение таблицы 42

Политика	Ключ	Описание
		в) <code>force_installed</code> – расширение устанавливается автоматически и не может быть удалено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует <code>install_url</code>; г) <code>normal_installed</code> – расширение устанавливается автоматически, но может быть отключено пользователем. Этот параметр недействителен для конфигурации по умолчанию и требует <code>install_url</code>; - <code>install_url</code> – сопоставляется с URL-адресом, указывающим, откуда Firefox может загрузить расширение (при <code>force_installed</code> или <code>normal_installed</code>). При установке из локальной файловой системы следует использовать URL-адрес <code>file:///</code>. При установке с сайта <code>addons.mozilla.org</code> можно использовать URL-адрес в виде <code>https://addons.mozilla.org/firefox/downloads/file/3450175/adaptor_rutoken_plugin-1.0.5.0.xpi</code>; - <code>install_sources</code> – 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; - <code>minimum_version_required</code> – отключает расширения (в том числе установленные принудительно) более ранних версий, чем определено этим параметром. Формат строки версии аналогичен формату, который используется в манифесте расширения; <code>allowed_types</code> – белый список разрешенных типов расширений/приложений, которые можно установить в Firefox. Значение представляет собой список строк

Окончание таблицы 42

Политика	Ключ	Описание
		(допустимые строки: «extension», «theme», «dictionary», «locale»). Этот параметр можно использовать только для конфигурации по умолчанию; - <code>override_update_url</code> – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля <code>update_url</code> или <code>update</code> в политике <code>ExtensionInstallForcelist</code>. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - <code>override_update_url</code> – указывает, что для всех последующих обновлений расширения будет использоваться URL из поля <code>update_url</code> или <code>update</code> в политике <code>ExtensionInstallForcelist</code>. Если это политика не настроена или отключена, будет использоваться URL из манифеста расширения; - <code>blocked_install_message</code> – сообщение об ошибке, которое будет отображаться для пользователей, если им заблокирована установка расширения. Этот параметр можно использовать только для конфигурации по умолчанию; - <code>restricted_domains</code> – массив доменов, на которых нельзя запускать сценарии контента. Этот параметр можно использовать только для конфигурации по умолчанию; - <code>updates_disabled</code> – логическое значение, указывающее, следует ли отключать автоматические обновления для отдельного расширения; - <code>default_area</code> – указывает, где должен быть размещен значок расширения. Возможные значения: <code>navbar</code> и <code>menupanel</code>

4.6.4.11. Управление политиками веб-браузера «Яндекс.Браузера»

Эти групповые политики позволяют централизованно для компьютеров управлять настройками «Яндекс.Браузера».

Механизм Yandex в составе пакета groupupdate формирует JSON-файл для веб-браузера из шаблонов групповых политик.

Во время запуска веб-браузер «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 веб-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.

Примечание. Данный механизм реализован только для машинных политик.

Примечание. Настройка политик для веб-браузера «Яндекс.Браузера» требует дополнительной установки ADMX-файлов Yandex (пакет `adm-x-yandex-browser`).

Результат применения параметров групповой политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: `browser://policy` (рис. 194).

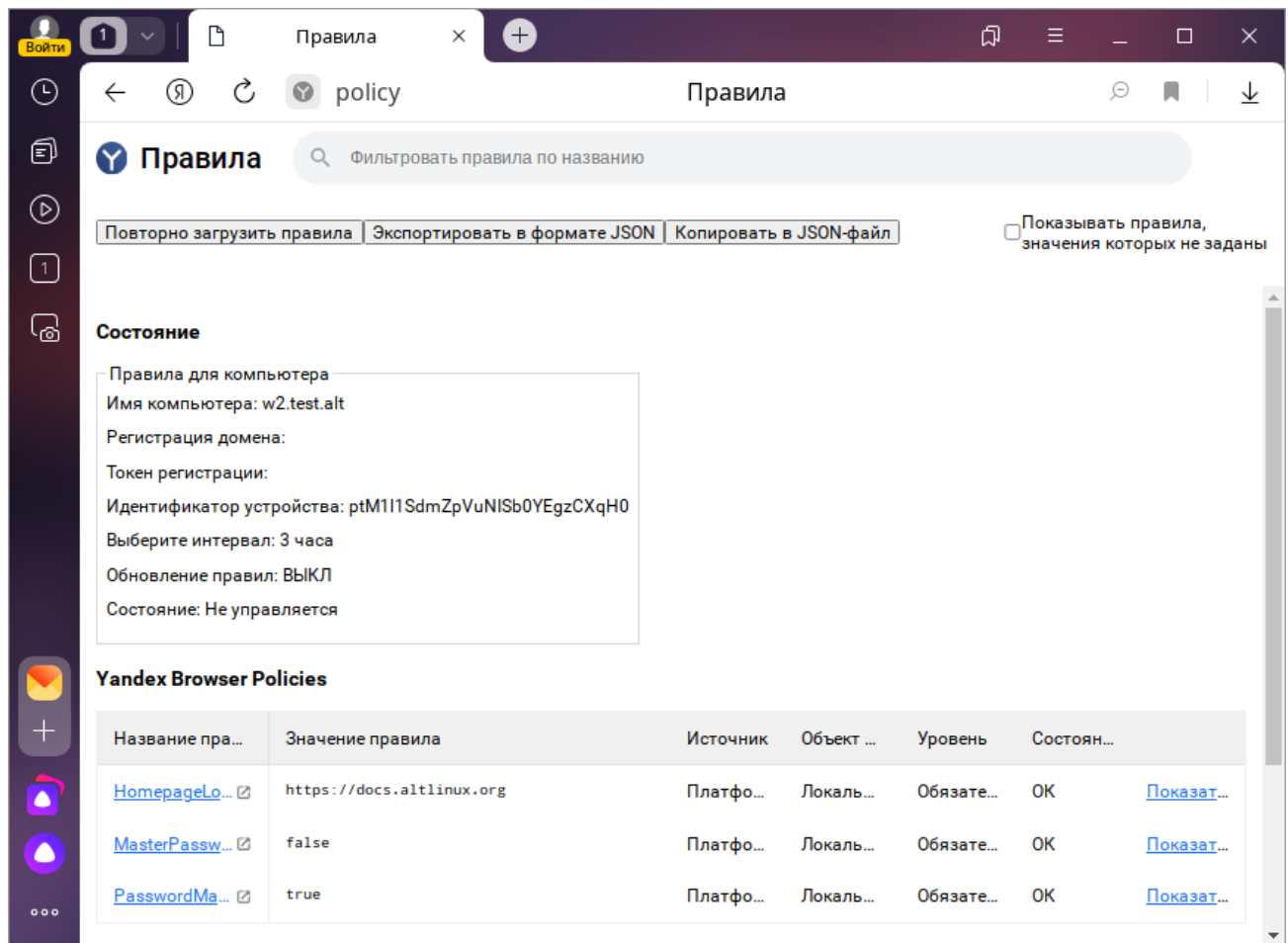


Рис. 194 – Активные политики «Яндекс.Браузера»

В качестве примера ниже рассмотрена политика установки URL домашней страницы.

Для редактирования политик веб-браузера «Яндекс.Браузера» следует перейти в «Компьютер» → «Административные шаблоны» → «Яндекс» → «Яндекс.Браузер». Отобразится список политик (рис. 195).

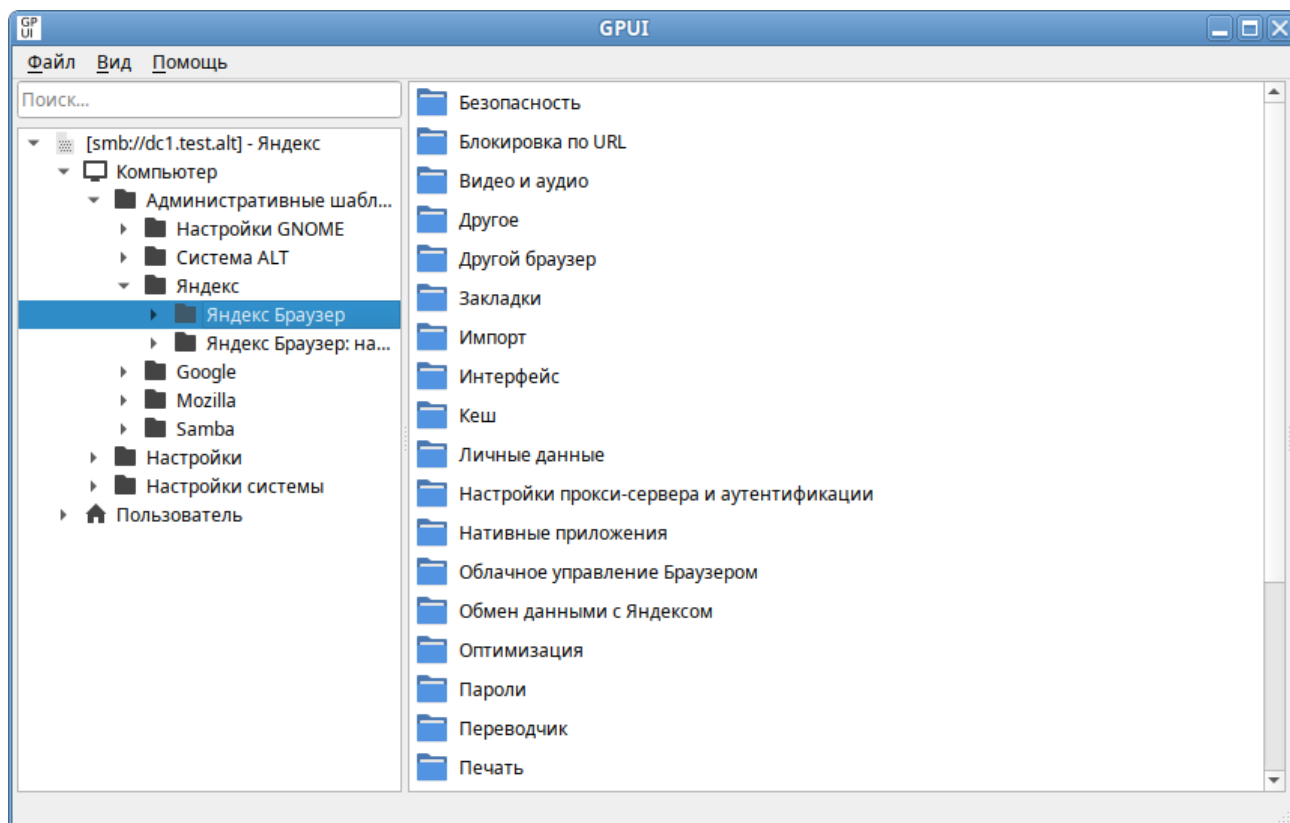


Рис. 195 – Политики настройки «Яндекс.Браузера»

Для установки URL домашней страницы следует выбрать пункт «Поведение», щелкнуть левой кнопкой мыши на политике «Задать URL домашней страницы», откроется диалоговое окно настройки политики. Выбрать параметр «Включено», в разделе «Описание» ввести URL и нажать кнопку «ОК» (рис. 196).

В результате применения данной политики будет установлена домашняя страница по умолчанию, а также будет заблокирована возможность изменения домашней страницы пользователем (рис. 197).

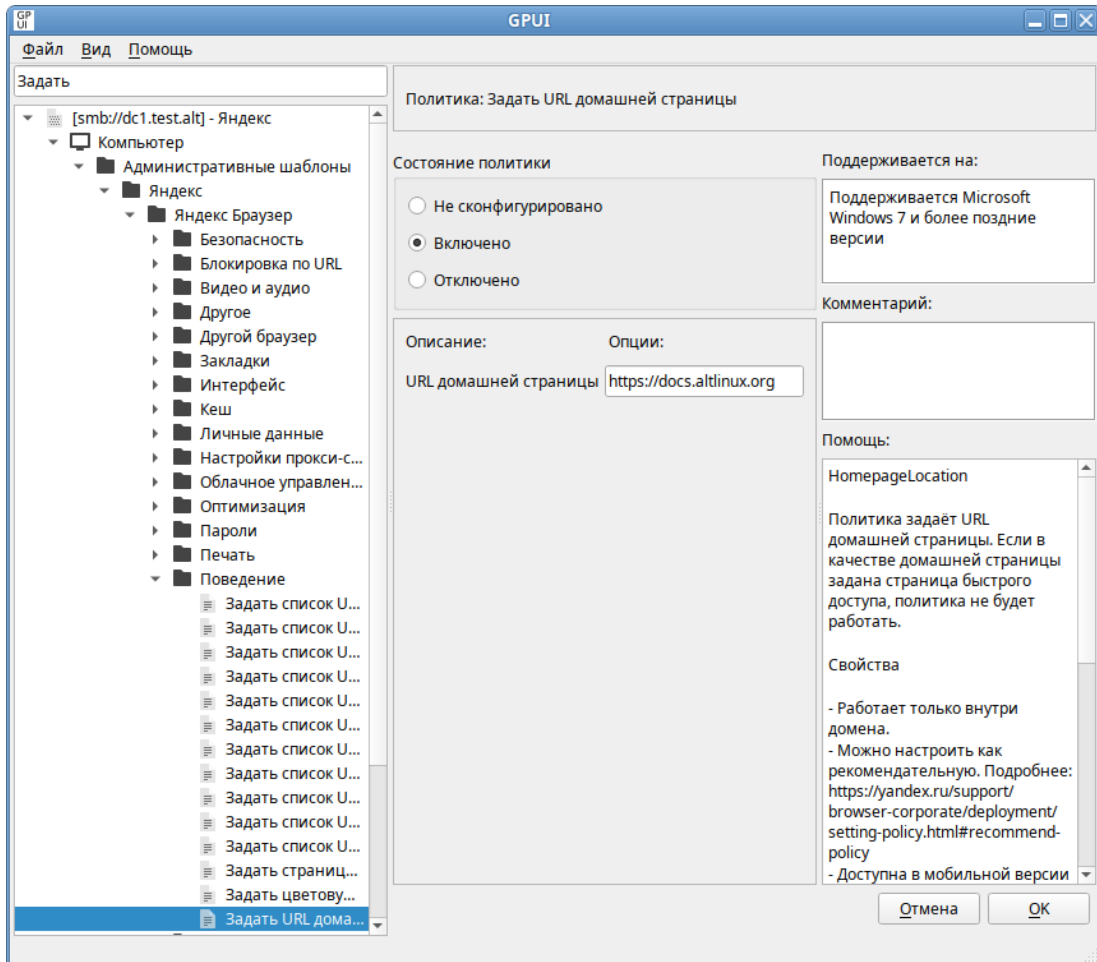


Рис. 196 – Установка URL домашней страницы «Яндекс.Браузера»

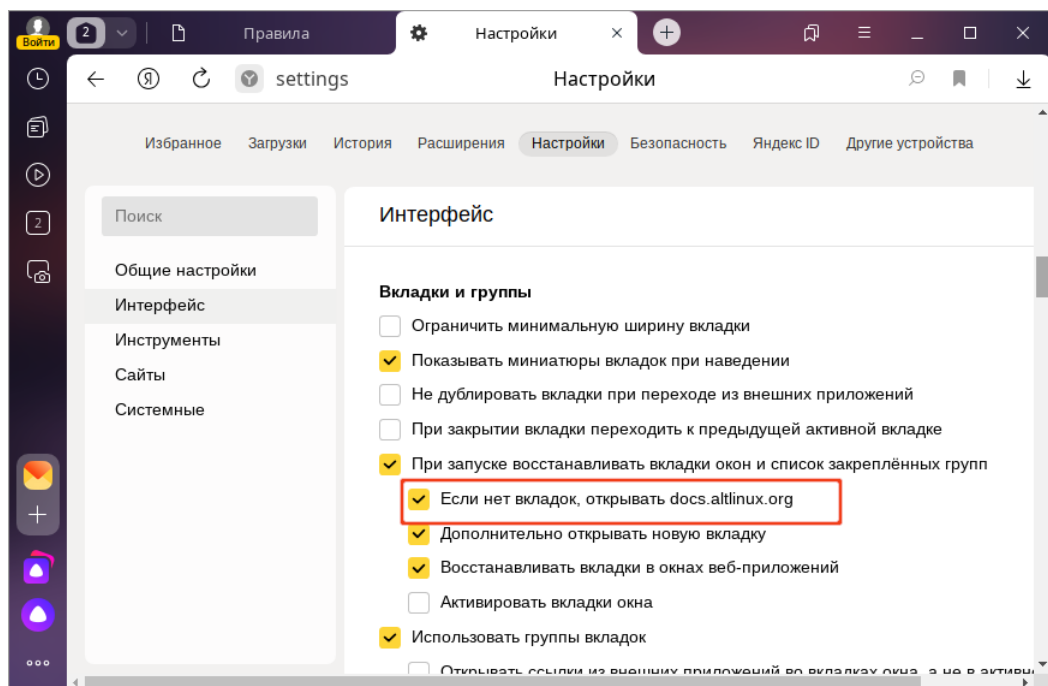


Рис. 197 – Настройки «Яндекс.Браузера»

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 43 описаны только некоторые политики. Полный список политик и их описание можно найти в «Яндекс.Браузере», указав в адресной строке URL: `browser://policy/` и установив отметку на пункте «Показывать правила, значения которых не заданы».

Т а б л и ц а 43 – Примеры политик управляющих настройками «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. 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, 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»)

Продолжение таблицы 43

Политика	Ключ	Описание
Запретить открывать файлы офисных форматов в веб-браузере	CloudDocumentsDisabled	Политика запрещает пользователям открывать файлы офисных форматов в веб-браузере. Если политика находится в состоянии «Отключено» или «Не сконфигурировано», пользователь может открывать в веб-браузере файлы офисных форматов. Если политика находится в состоянии «Включено», пользователю запрещено открывать в веб-браузере файлы офисных форматов
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 веб-браузера
Разрешить полноэкранный режим	FullscreenAllowed	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 клавишу <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

Продолжение таблицы 43

Политика	Ключ	Описание
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 веб-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 веб-браузер был закрыт без вкладок или сочетанием клавиш <Alt> + <Home>. Пользователи не могут менять домашнюю страницу в веб-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.

Продолжение таблицы 43

Политика	Ключ	Описание
Отображать боковую панель	SidePanelMode	Политика позволяет настроить режим отображения боковой панели и запретить пользователям его менять. 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

Продолжение таблицы 43

Политика	Ключ	Описание
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. Если политика находится в состоянии «Включено», мастер-пароль в веб-браузере отключен
Разрешить сохранять пароли	PasswordManagerEnabled	Политика разрешает сохранять пароли в веб-браузере и автоматически подставлять их при авторизации на сайтах. Если политика находится в состоянии «Не сконфигурировано», сохранение паролей в веб-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 веб-браузера. Вкладки и Табло синхронизируются с сервером Яндекса. Если политика находится в состоянии «Включено», история посещенных страниц не сохраняется в журнале веб-браузера. Пользователи не могут включить сохранение истории посещенных страниц. Только Табло синхронизируются с сервером Яндекса. Возможность переноса истории вручную отключена

Продолжение таблицы 43

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», веб-браузер использует папку по умолчанию, однако пользователи могут ее изменить с помощью параметра disk-cache-dir. Если политика находится в состоянии «Включено», веб-браузер хранит кеш на диске в заданной администратором папке. Пользователи не могут ее изменить с помощью параметра disk-cache-dir
Задать объем кеша в байтах	DiskCacheSize	Политика позволяет задать объем кеша в байтах. Значение используется различными подсистемами в веб-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», веб-браузер использует объем кеша по умолчанию. Если политика находится в состоянии «Включено», веб-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», веб-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

Продолжение таблицы 43

Политика	Ключ	Описание
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», веб-браузер не блокирует URL. 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)

Продолжение таблицы 43

Политика	Ключ	Описание
Задать исключения для политики URLBlocklist	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»
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.). Также пользователи 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

Продолжение таблицы 43

Политика	Ключ	Описание
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. 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.

Продолжение таблицы 43

Политика	Ключ	Описание
		Пример значения: <pre>{ "hdokiejnpimakedhajhdicegeplioahd": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" }, "pioclpoplcldbaefihamjohnefbikjilc": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" } }</pre> Параметры политики: - allowed_types – типы приложений и расширений, которые пользователям разрешено устанавливать в веб-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: а) allowed – пользователи могут установить это расширение (поведение по умолчанию); б) blocked – пользователи не могут установить это расширение;

Продолжение таблицы 43

Политика	Ключ	Описание
		в) removed – пользователи не могут установить это расширение. Если расширение было установлено, оно будет удалено; г) force_installed – расширение устанавливается автоматически. Пользователи не могут его удалить. В этом режиме необходимо указать ссылку для скачивания расширения (параметр update_url); д) 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; - 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);

Окончание таблицы 43

Политика	Ключ	Описание
		- 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

4.6.4.12. Политика замыкания

Описание политики замыкания см. в п. 4.8.4.

Для настройки этой политики следует перейти в «Компьютер/Пользователь» → «Административные шаблоны» → «Система» → «Групповая политика» (рис. 198).

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 (рис. 199).

Примечание. Для быстрого доступа к политике можно ввести в поле «Поиск...» ключевое слово.

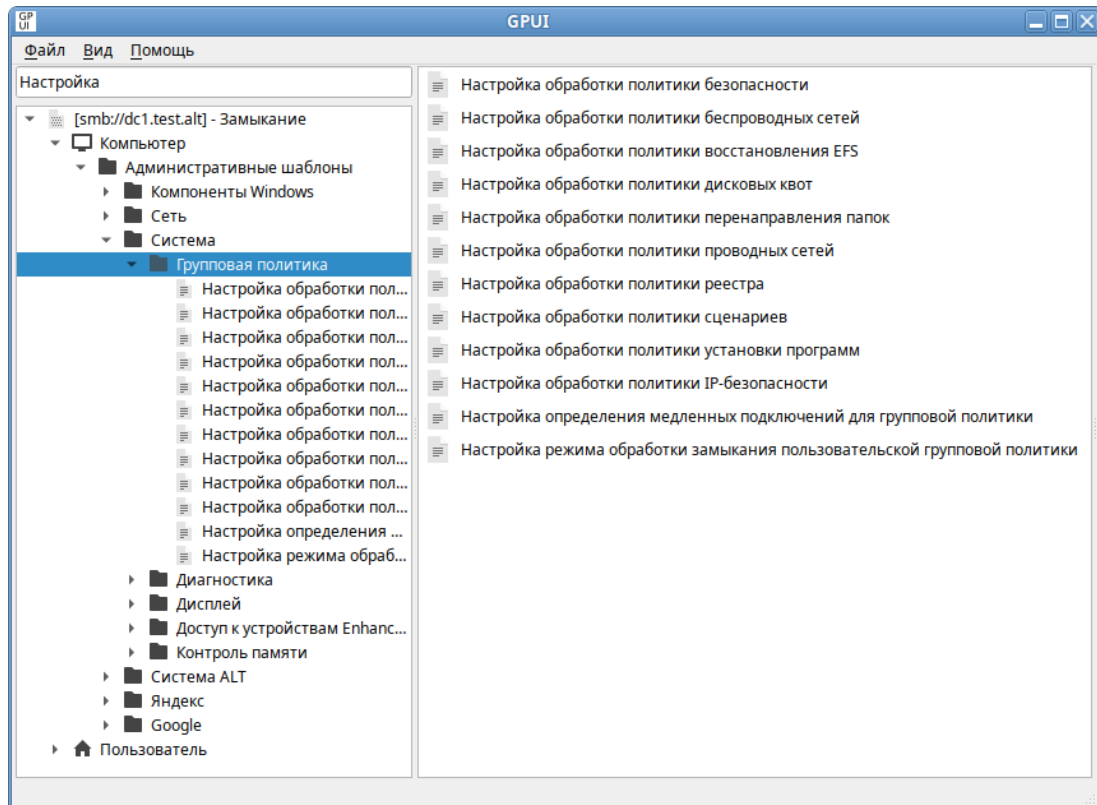


Рис. 198 – Политики ОС

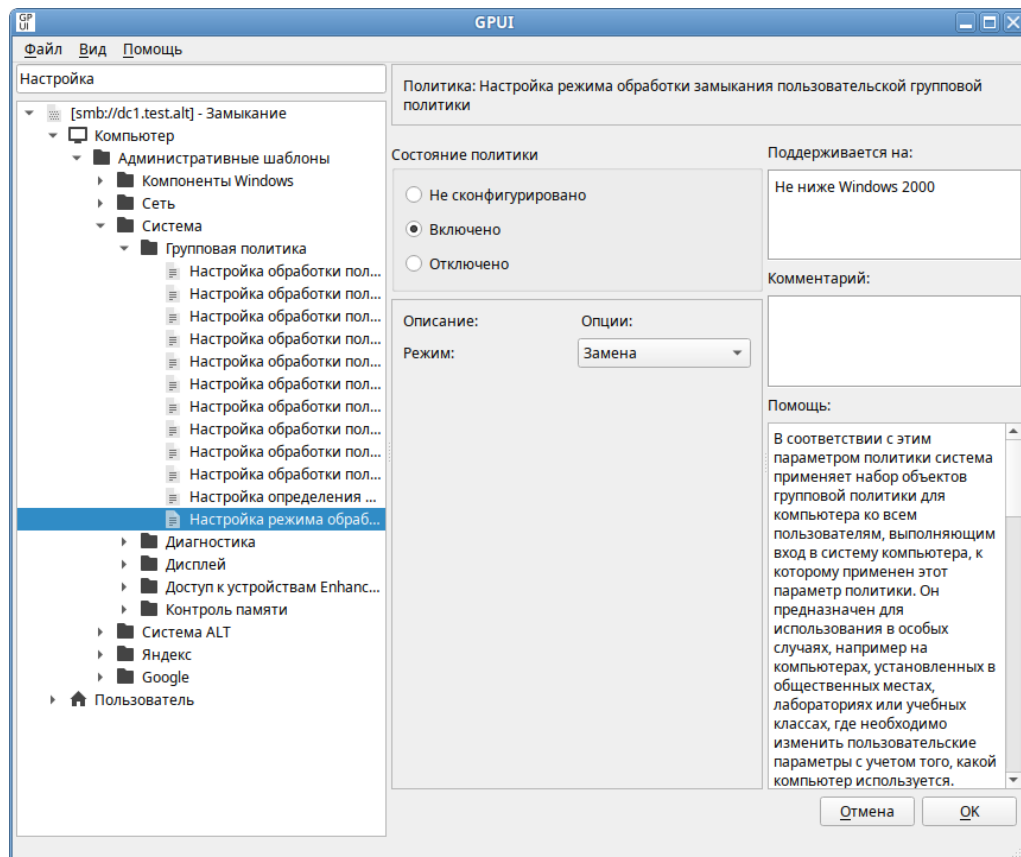


Рис. 199 – Политика «Настройка режима обработки замыкания пользовательской групповой политики»

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.

4.6.5. Редактирование предпочтений

Если предпочтение настраивается в секции «Компьютер», групповая политика должна быть привязана к ОУ с компьютерами. Соответственно, если настраиваемый параметр относится к конфигурации пользователя, нужно назначить политику на ОУ с пользователями. Также следует убедиться, что объект, к которому должна применяться политика находится в нужном ОУ с компьютерами или пользователями.

4.6.5.1. 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» (рис. 200).

В открывшемся диалоговом окне «Диалог настроек» задать настройки политики (рис. 201).

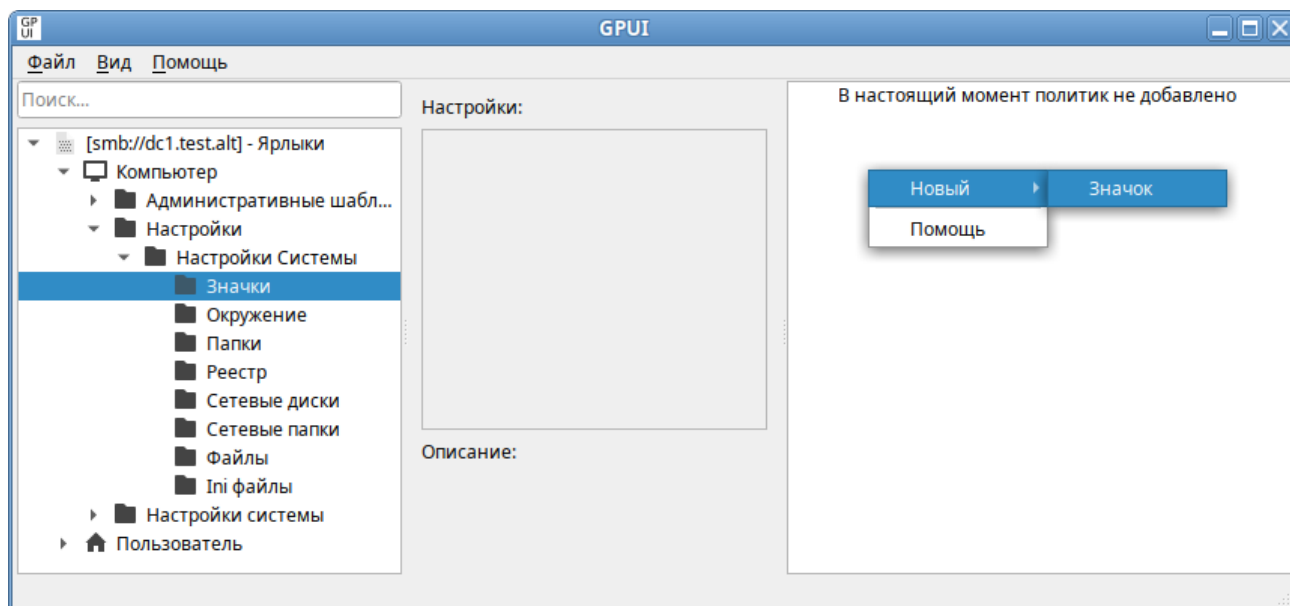


Рис. 200 – Создание новой политики «Значки»

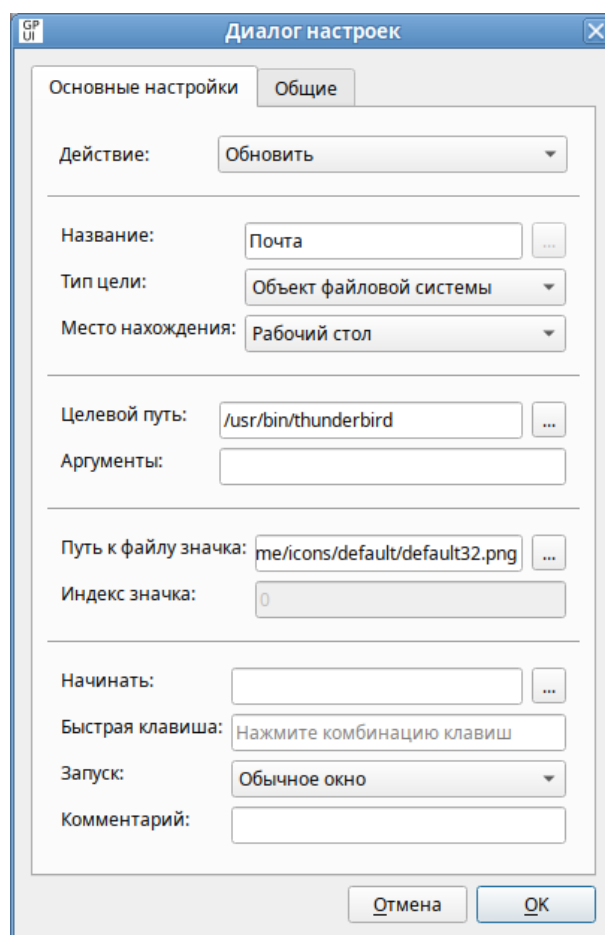


Рис. 201 – Диалоговое окно настройки политики «Значки»

Опции доступные на вкладке «Основные настройки»:

- 1) «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;
- 2) «Название» – отображаемое имя для ярлыка. При изменении или удалении ярлыка имя должно совпадать с именем существующего ярлыка;
- 3) «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;
- 4) «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 File», нужно

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», нужно ввести Ярлыки/Почта в поле «Название» и выбрать «Рабочий стол» в поле «Место нахождения» (рис. 202);

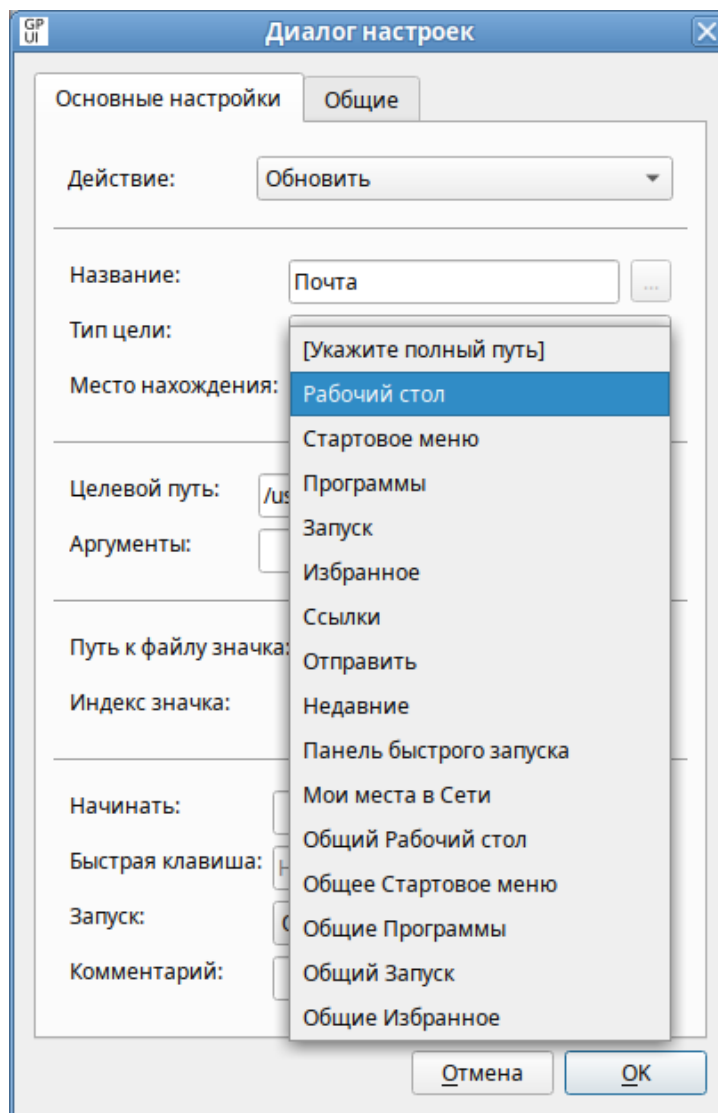


Рис. 202 – Диалог настроек

- 5) «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»;

- 6) «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»;
- 7) «Путь к файлу значка» и «Индекс значка» – значок для ярлыка. Для указания значка, отличного от значка по умолчанию нужно 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»;
- 8) «Начинать» – рабочий каталог, содержащий файлы, которые требуются для конечного объекта. Это поле принимает переменные. Поле доступно в случае, если выбрано действие «Создать», «Заменить» или «Обновить»;
- 9) «Быстрая клавиша» – сочетание клавиш для запуска ярлыка. Чтобы назначить сочетание клавиш следует установить курсор в поле «Быстрая клавиша» и нажать комбинацию клавиш. Чтобы удалить сочетание клавиш, можно нажать клавишу <CTRL> или <ALT>, или нажать на значок, расположенный справа от сочетания клавиш. Это поле недоступно, если выбрано действие «Удалить»;
- 10) «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»;
- 11) «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».

⚠ Чтобы ярлыку назначались корректные права (для пользовательской политики), нужно установить отметку в пункте «Выполнять в контексте безопасности текущего пользователя» на вкладке «Общие».

Все настройки политики для ярлыков 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>
```

4.6.5.2. 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» (рис. 203).

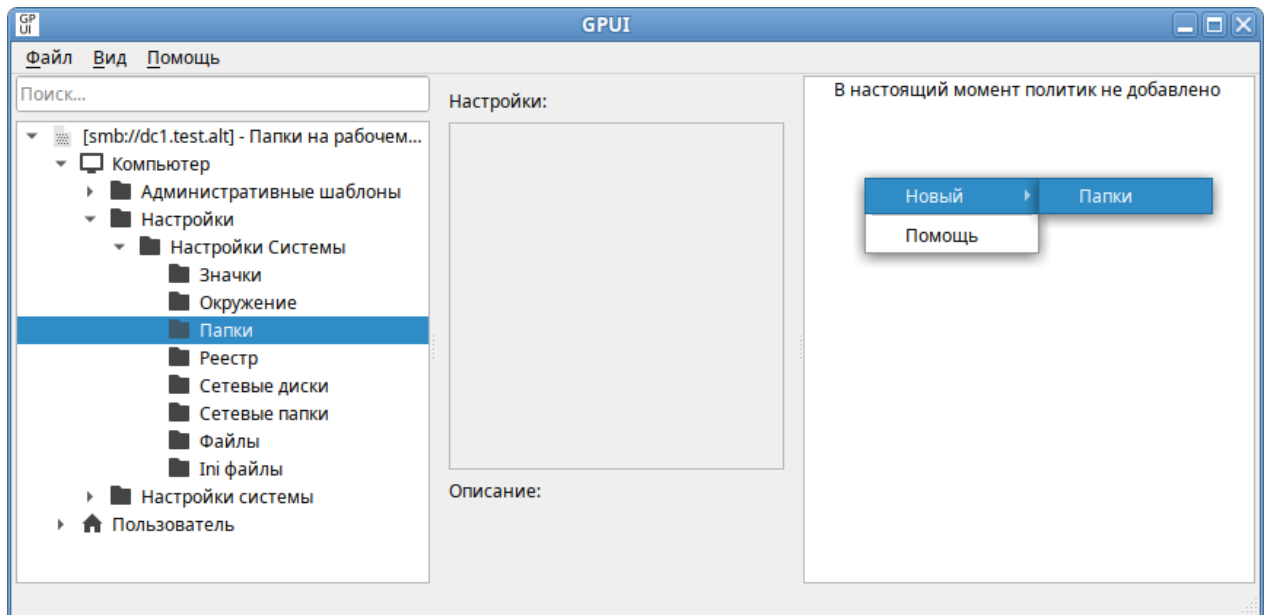


Рис. 203 – Создание новой политики «Папки»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 204).

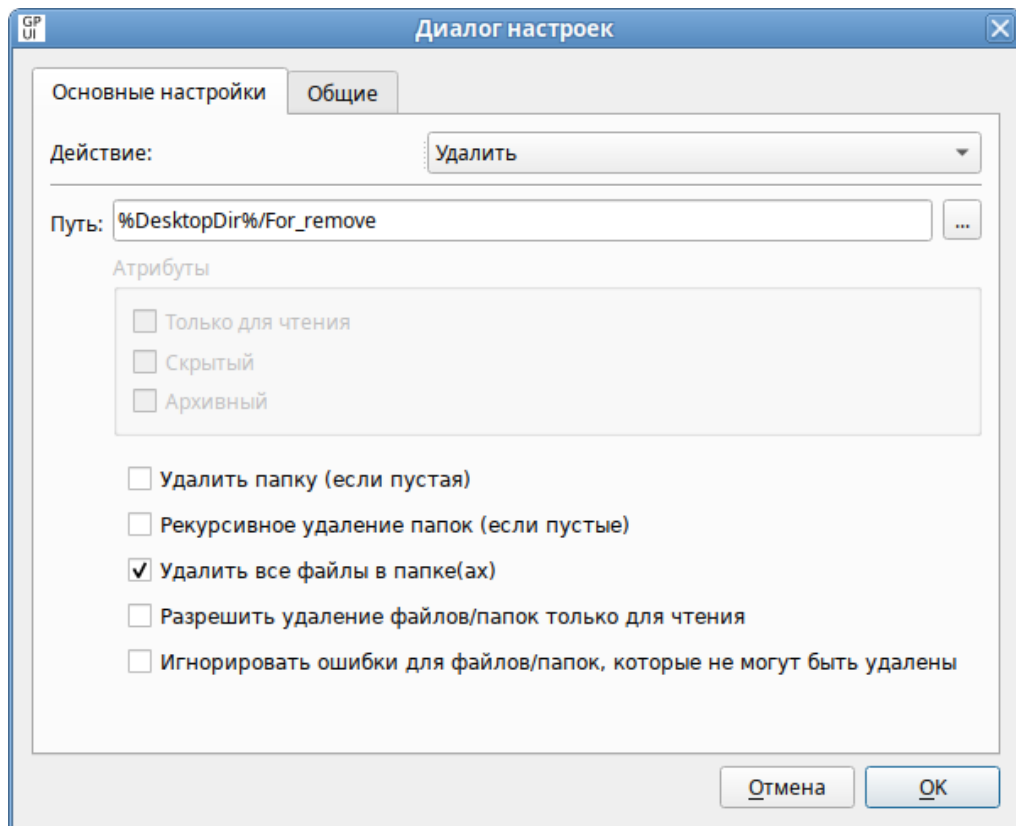


Рис. 204 – Диалоговое окно настройки политики «Папки»

Опции доступные на вкладке «Основные настройки»:

1) «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;

2) «Путь» – путь к папке (с точки зрения клиента). Это поле может содержать переменные (не следует вводить кавычки и завершающую косую черту);

3) «Атрибуты» – атрибуты файловой системы для папки (недоступны для действия «Удалить»):

- «Только для чтения»;
- «Скрытый»;
- «Архивный»;

4) 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. Будет ли эта папка пустой, 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 ее невозможно отключить;
- «Рекурсивное удаление папок (если пустые)» – если включена эта опция, самый низкий уровень вложенных папок удаляется, если они пусты, повторяется для каждой родительской папки до достижения папки,

указанной в поле «Путь». Пустые подпапки оцениваются после того, как опция «Удалить все файлы в папке(ах)» была обработана;

- «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» отключается для удаляемых файлов и папок;
- «Игнорировать ошибки для файлов/папок, которые не могут быть удалены» – если включена эта опция, подавляются любые сообщения об ошибках, возникающие из-за невозможности удаления файлов или папок. Если эта опция не включена, возвращается ошибка, 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.

Примечание. Атрибуты «Архивный», «Скрытый» и «Только для чтения» применимы только для Windows систем.

Все настройки политики для 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>

```

4.6.5.3. 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» (рис. 205).

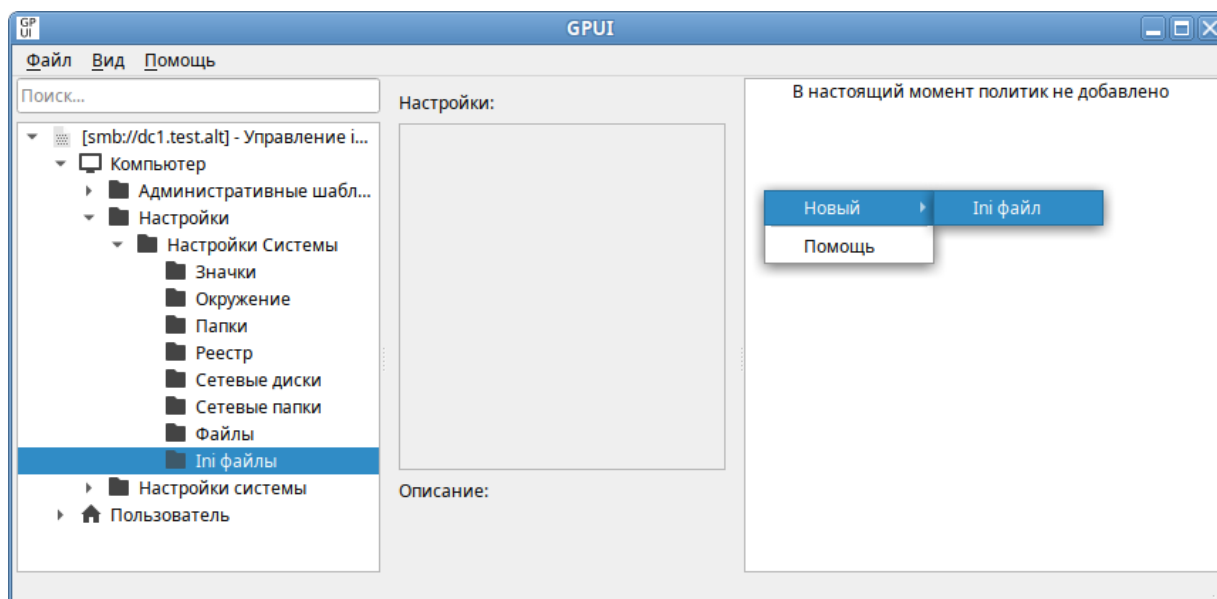


Рис. 205 – Создание новой политики «INI файл»

В открывшемся диалоговом окне «Диалог настроек» задать настройки политики (рис. 206).

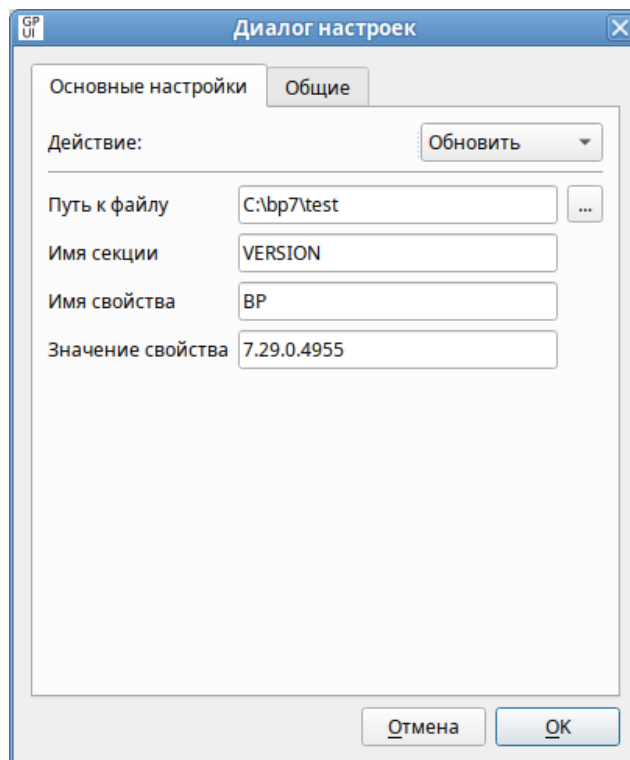


Рис. 206 – Настройки политики «INI файл»

Опции доступные на вкладке «Основные настройки»:

1) «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»);

- 2) «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;
- 3) «Имя секции» – имя раздела в файле, свойство которого нужно настроить или удалить. Чтобы удалить INI-файл целиком, следует оставить это поле пустым;
- 4) «Имя свойства» – имя свойства, которое нужно настроить или удалить. Чтобы удалить целиком раздел файла или весь файл, следует оставить это поле пустым;
- 5) «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 СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 4.6.4.7).

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>
```

4.6.5.4. Управление переменными среды

Групповая политика «Управление переменными среды» позволяет централизованно для компьютеров или пользователей:

- 1) создать постоянные пользовательские или системные переменные среды;
- 2) удалить переменные среды;
- 3) 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» (рис. 207).

В открывшемся диалоговом окне «Диалог настроек» задать настройки политики (рис. 208).

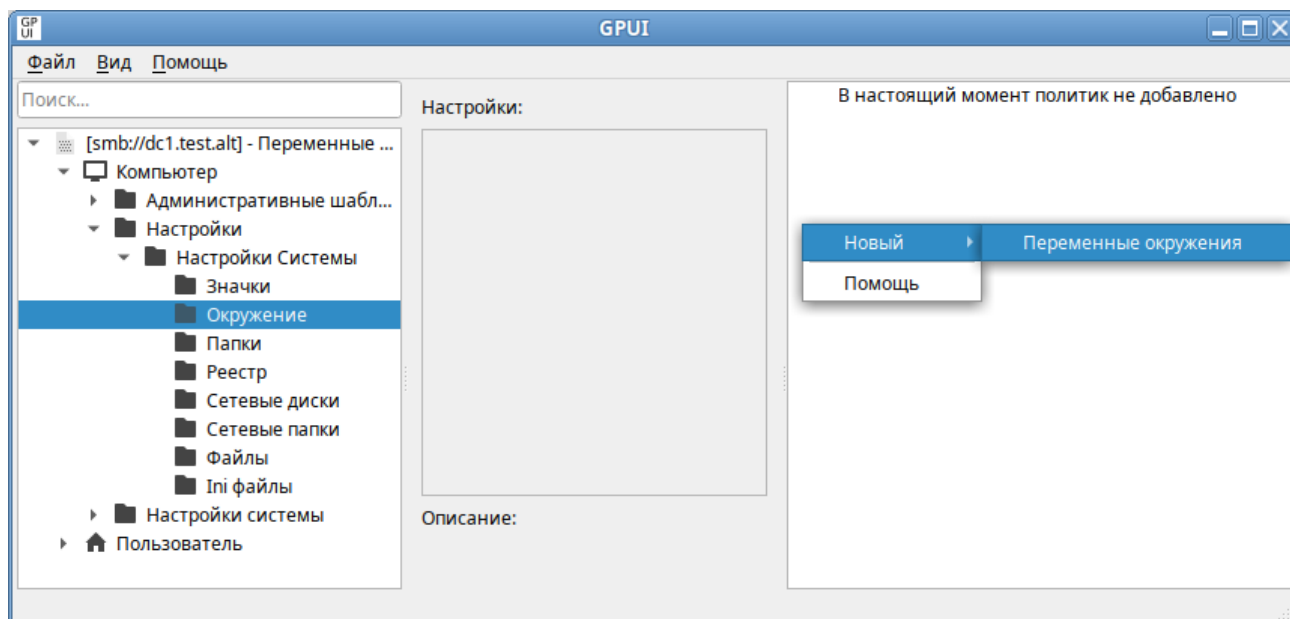


Рис. 207 – Новая политика «Переменные окружения»

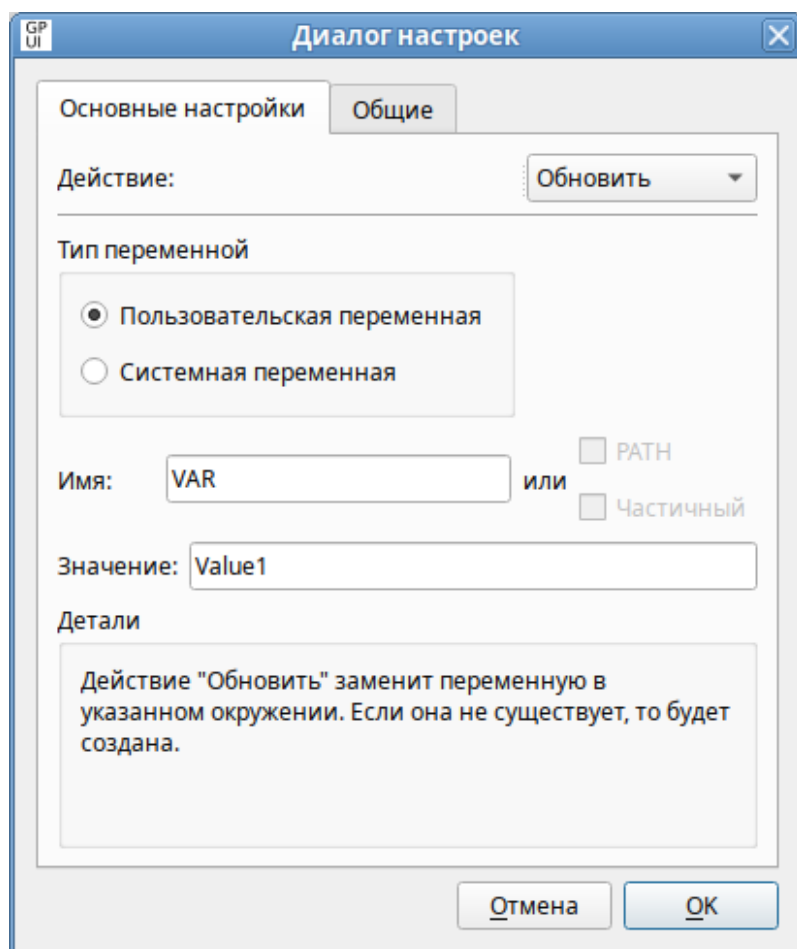


Рис. 208 – Настройки политики «Переменные окружения»

Опции доступные на вкладке «Основные настройки»:

- 1) «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 ее 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 создает 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;
- 2) «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;
- 3) «Системная переменная» – переменная среды будет влиять на всех пользователей компьютера. Переменная среды будет храниться в реестре в разделе HKEY_LOCAL_MACHINE;
- 4) «Имя» – имя переменной среды, к которой применяется действие. Чтобы выбрать переменную PATH, следует оставить это поле пустым;

- 5) «Значение» – значение переменной среды. В это поле можно вводить переменные;
- 6) «РАТН» – действие будет применяться к переменной РАТН: можно создать/заменить значение переменной РАТН или добавить/удалить сегмент значения переменной РАТН. В поле «Имя» будет отмечено значение «РАТН» и оно не будет доступно для редактирования. Эта опция доступна только в том случае, если выбран параметр «Системная переменная»;
- 7) «Частичный» – добавить или удалить один сегмент переменной РАТН. Эта опция доступна только в том случае, если выбраны «Системная переменная» и «РАТН».

Все настройки политики управления INI-файлами 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) нужно 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
```

4.6.5.5. 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 определенным расширением в одном каталоге;
- изменить атрибуты, заменить или удалить все файлы в определенном 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» (рис. 209).

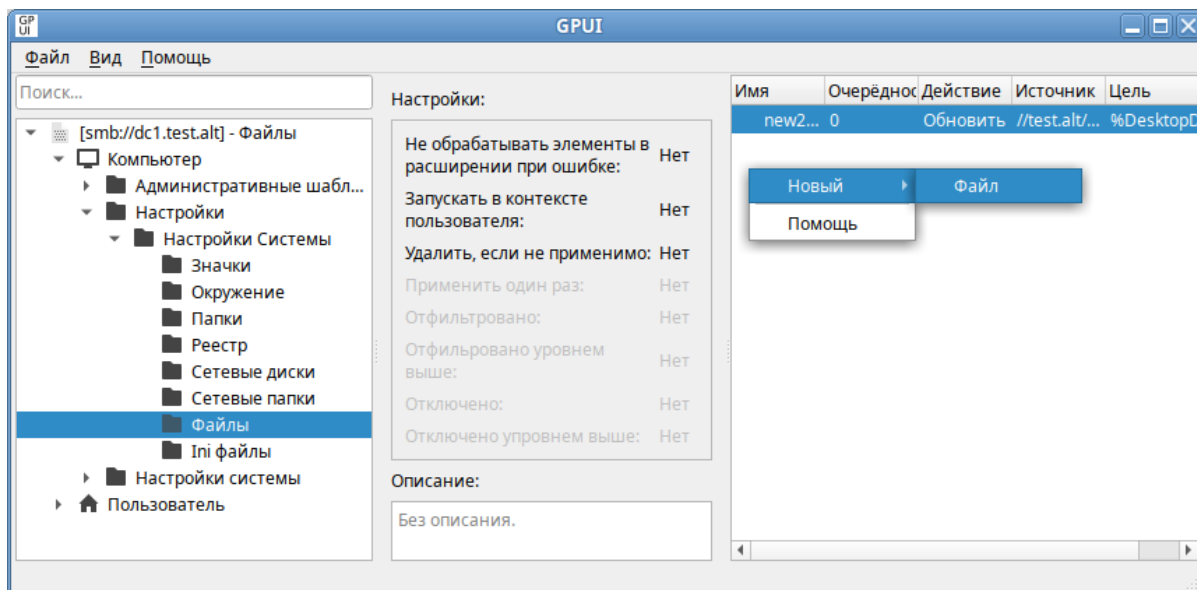


Рис. 209 – Создание новой политики «Файл»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 210).

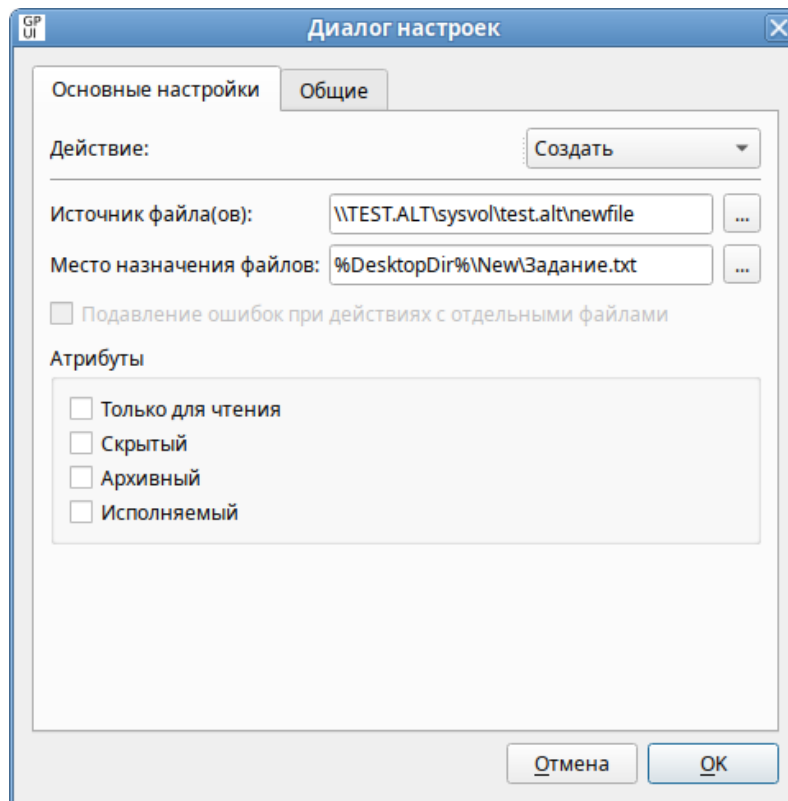


Рис. 210 – Настройки политики «Файл»

Опции доступные на вкладке «Основные настройки»:

1) «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;

2) «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. В настоящее время в ОС Альт СП можно использовать подстановочный знак (*) только для копирования всех файлов из папки (рис. 211).

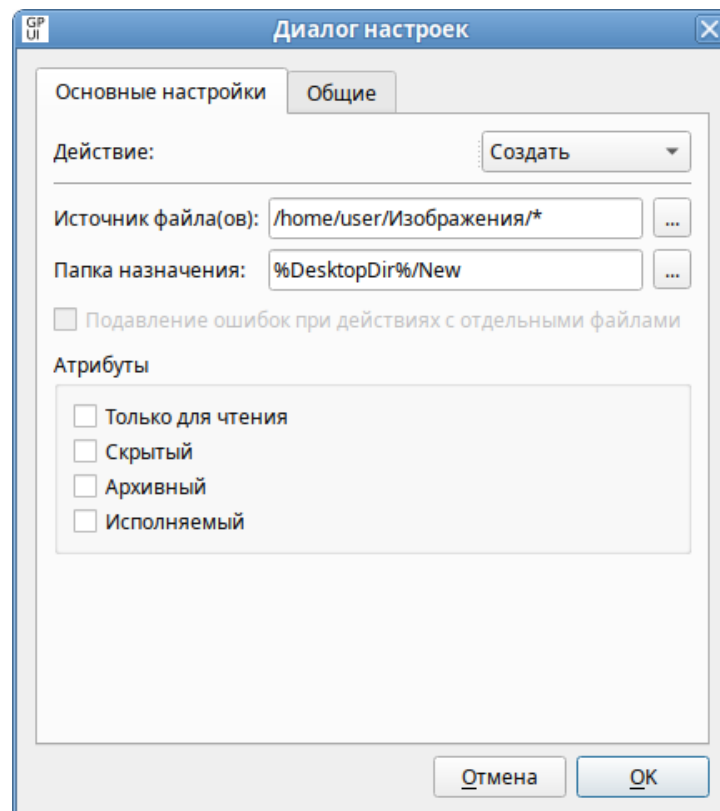


Рис. 211 – Копирование всех файлов из папки

- 3) «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. Нужно 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;
- 4) «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;
- 5) «Удалить файл(ы)» – путь к файлу (с точки зрения клиента), который требуется удалить. Чтобы удалить несколько файлов из одной папки нужно 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» (рис. 212).

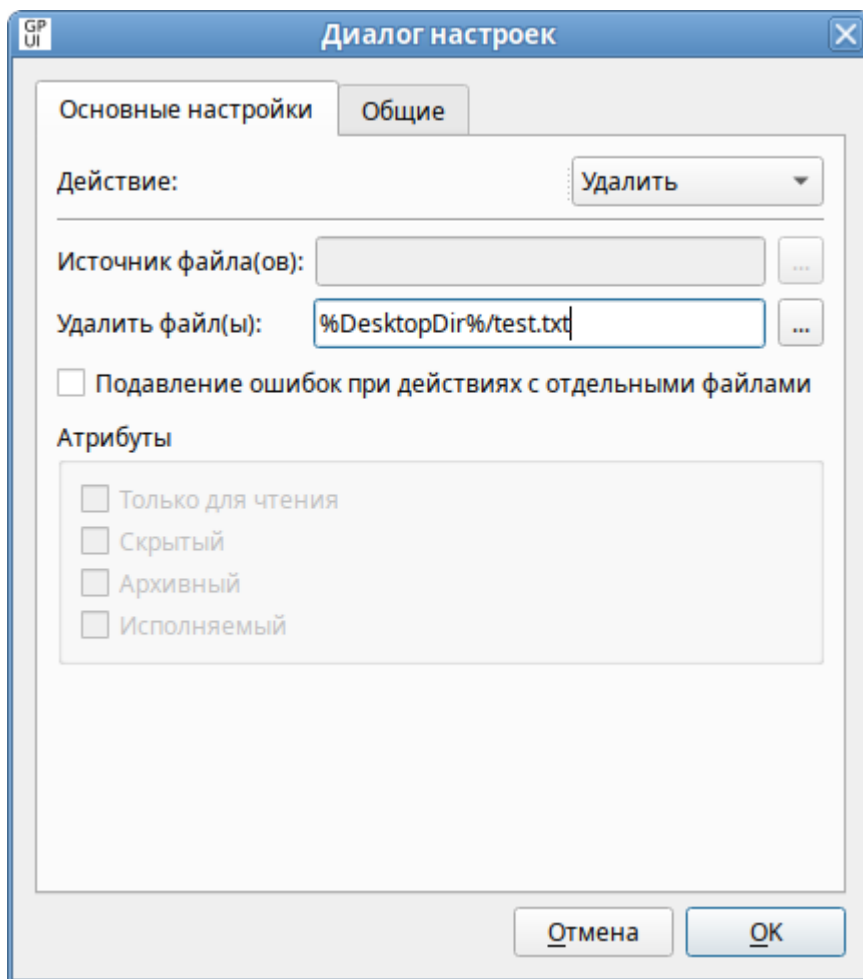


Рис. 212 – Настройка политики «Удаление файла»

- 6) «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»;
- 7) «Атрибуты» – атрибуты файловой системы для папки (недоступны для действия «Удалить»):
- «Только для чтения»;

- «Скрытый»;
- «Архивный»;
- «Исполняемый».

П р и м е ч а н и е . Атрибуты «Архивный», «Скрытый» и «Только для чтения» применимы только для Windows систем.

Политики управления файлами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 4.6.4.7).

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» выбрать пункт «Настройка механизма копирования файлов». В открывшемся окне установить отметку в поле «Включено» (рис. 213).

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 (рис. 214).

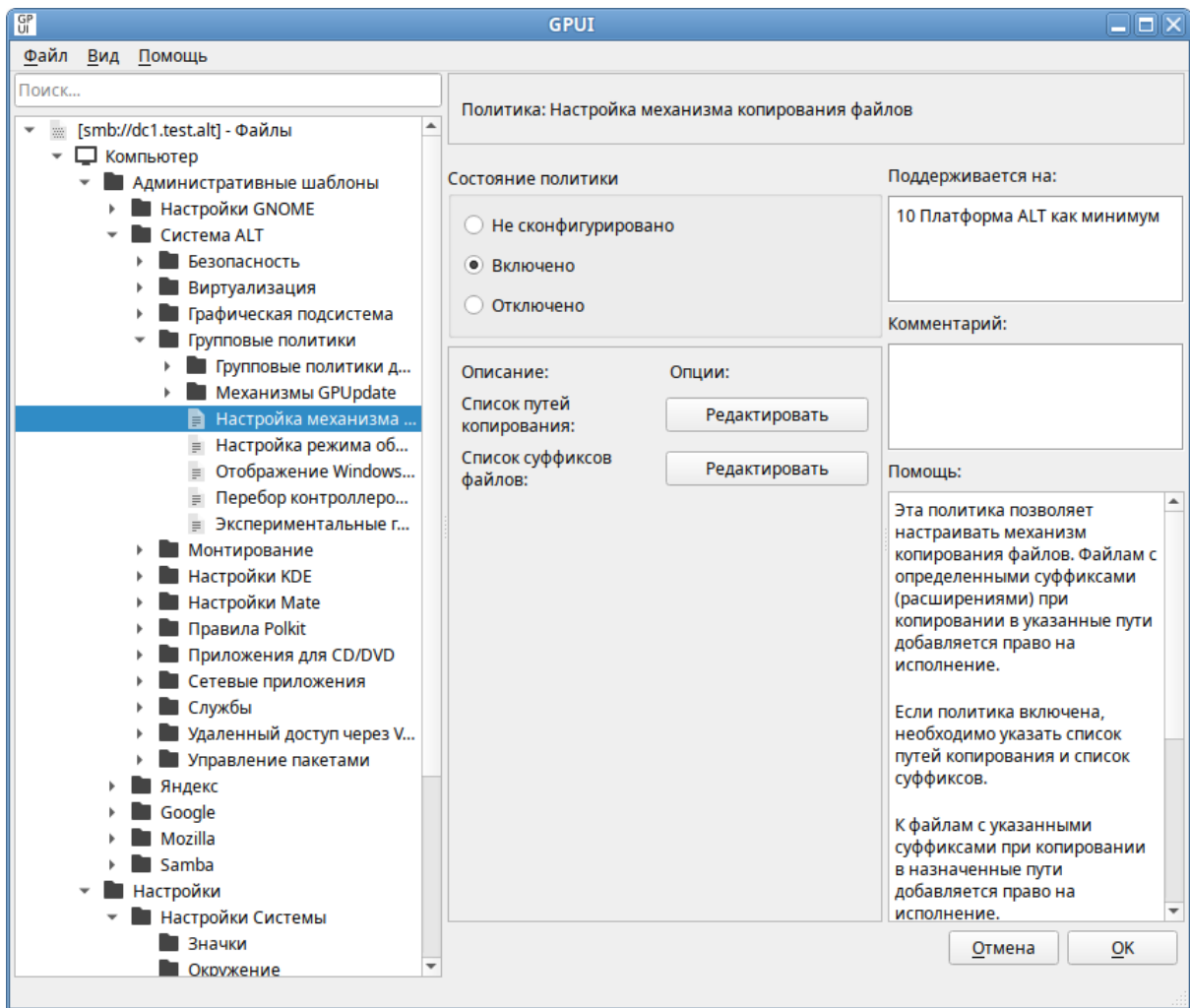


Рис. 213 – Политика «Настройка механизма копирования файлов»

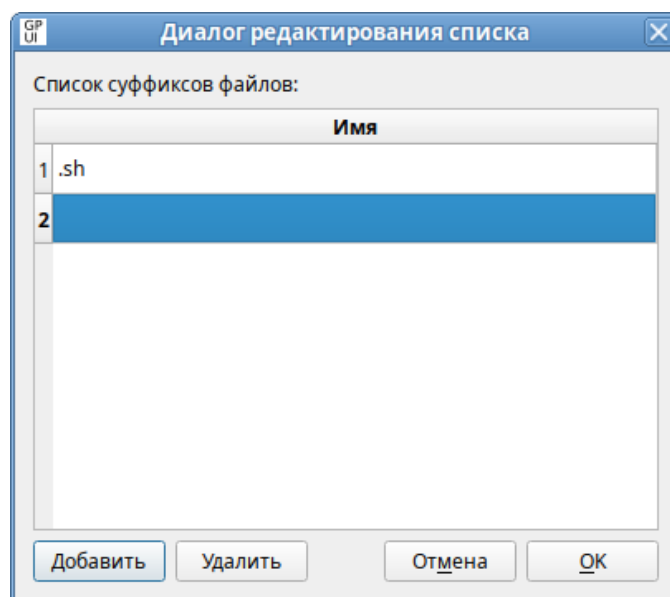


Рис. 214 – Список суффиксов файлов

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 (рис. 215).

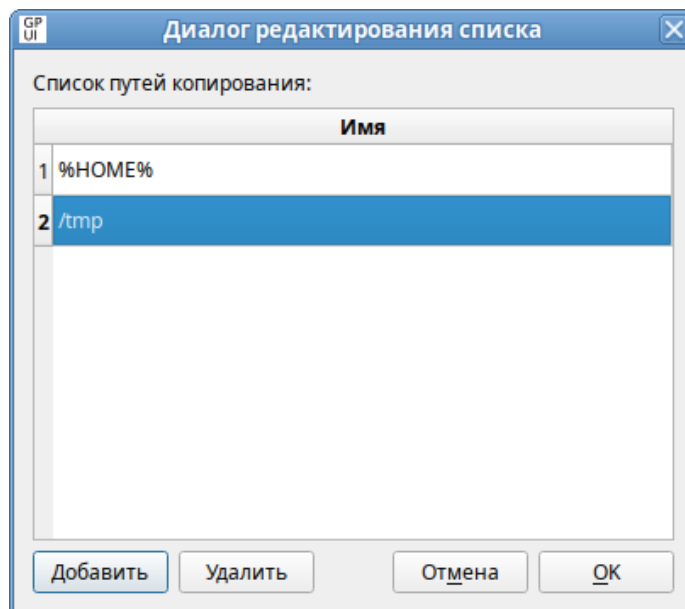


Рис. 215 – Список путей копирования

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>
```

4.6.5.6. Управление общими каталогами

Групповая политика «Управление общими каталогами» позволяет:

- 1) создать общие ресурсы и настроить их свойства;
- 2) изменить путь к папке общего ресурса путем замены ресурса;
- 3) удалить (вывести из общего доступа) или изменить лимит пользователей, функцию перечисления на основе доступа и комментариев 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 ее 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» (рис. 216).

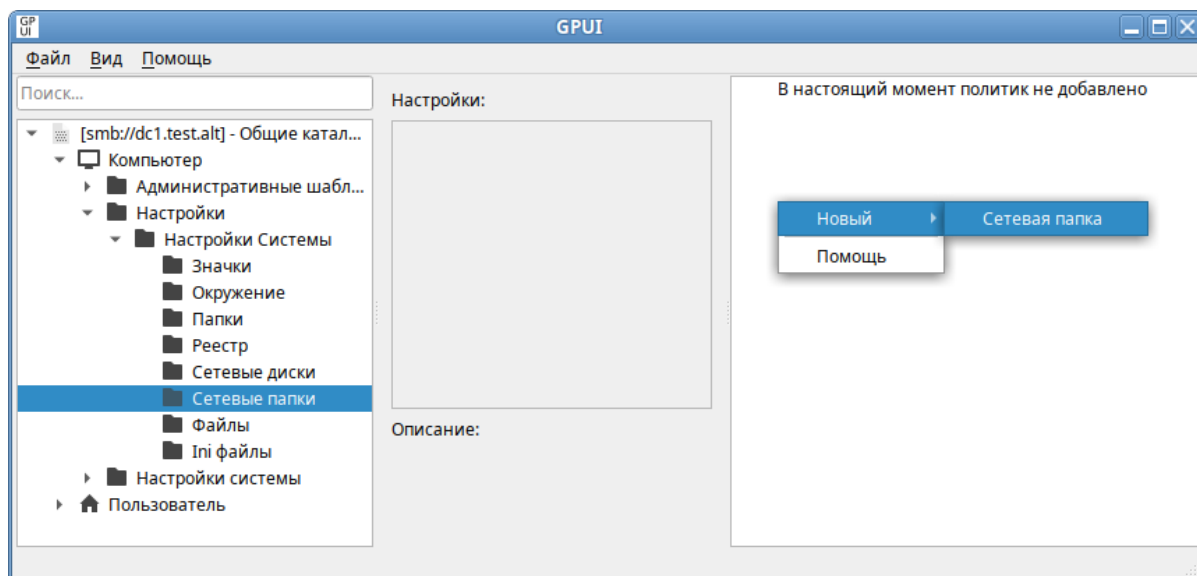


Рис. 216 – Создание новой политики «Сетевая папка»

В диалоговом открывшемся окне «Диалог настроек» задать настройки политики (рис. 217).

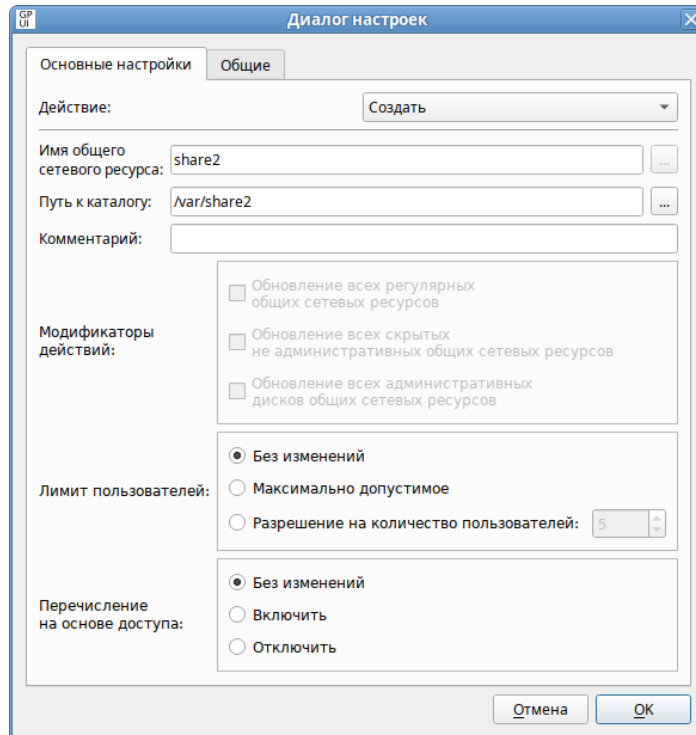


Рис. 217 – Настройки политики «Сетевая папка»

Опции доступные на вкладке «Основные настройки»:

1) «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 создает новый сетевой ресурс;

- «Обновить» – изменение параметров существующего сетевого ресурса. Если сетевого ресурса не существует, то это действие создает сетевой ресурс. Это действие отличается от «Заменить» тем, что не удаляет сетевой ресурс, а только обновляет параметры сетевого ресурса, определенные в элементе настройки;

2) «Имя общего сетевого ресурса» – имя общего ресурса. В этом поле можно указывать переменные;

- 3) «Путь к каталогу» – путь к существующей папке, на которую будет указывать общий ресурс. В этом поле можно указывать переменные;
- 4) «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»;
- 5) «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 \$);
- 6) «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);
- 7) «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 СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 4.6.4.7).

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>
```

4.6.5.7. 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 ОС Альт СП:

- /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.

Для настройки этой политики следует перейти в «Компьютер»/«Пользователь» → «Настройки» → «Настройки системы» → «Сетевые диски». В контекстном меню свободной области выбрать пункт «Новый» → «Сетевой диск» (рис. 218).

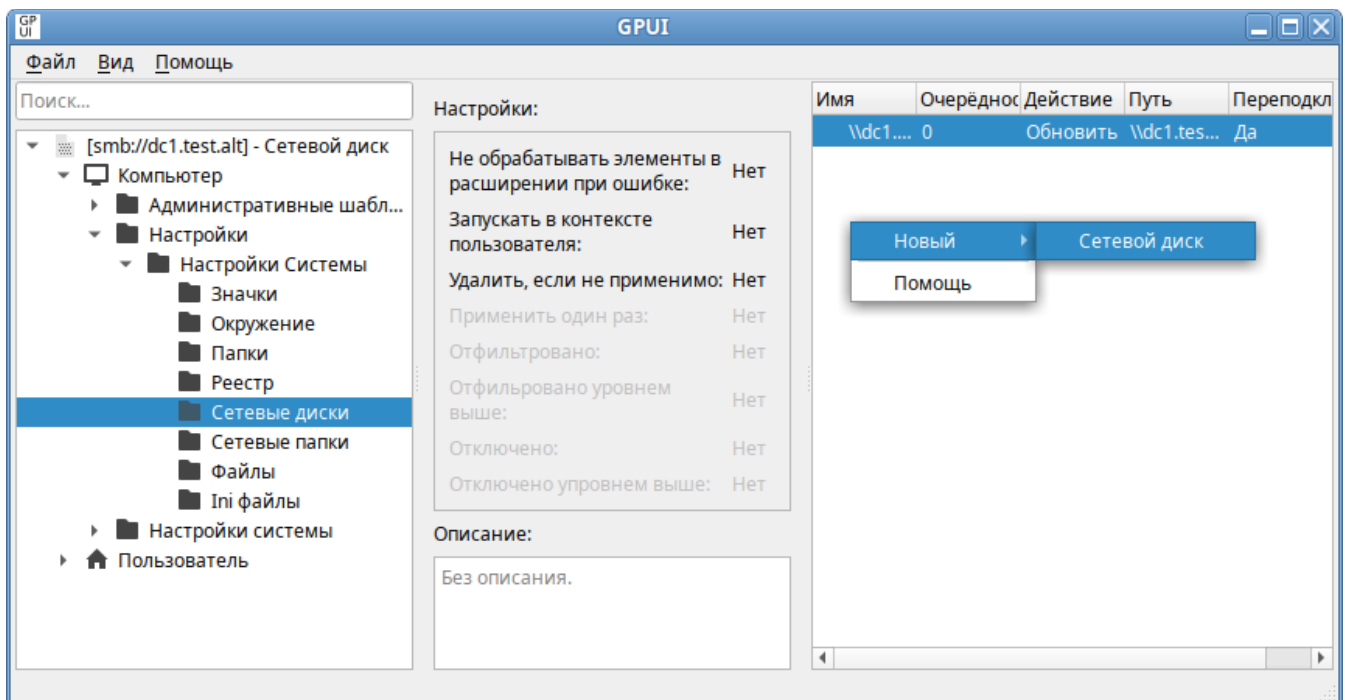


Рис. 218 – Создание новой политики «Сетевой диск»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 219).

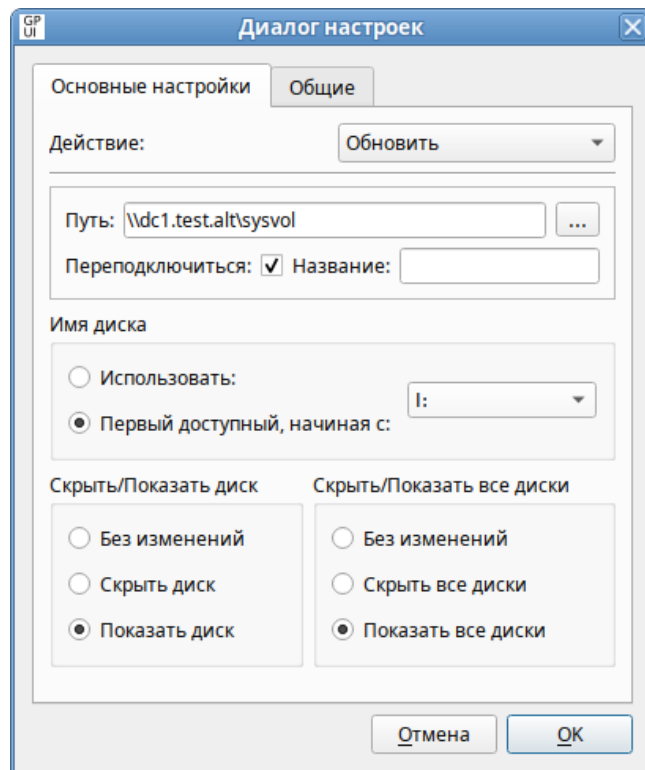


Рис. 219 – Настройки политики «Сетевой диск»

Опции доступные на вкладке «Основные настройки»:

- 1) «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 (жесткий диск, CD-Drive);
 - «Заменить» – удаление и повторное создание сетевого диска. Если диск до этого не был создан, то будет создан новый диск. Нельзя заменить локальный диск рабочей станции (жесткий 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);

- 2) «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;
- 3) «Переподключиться» – сохранять подключенный диск в настройках пользователя и повторно подключать его при каждом входе в систему;
- 4) «Название» – пользовательское имя для диска (можно оставить это поле пустым);

Примечание. Название должно представлять собой одно слово, состоящее только из латинских букв, цифр и символа подчеркивания, иначе монтирование не произойдет.

- 5) «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 определенную 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 определенной 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»;

б) 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. 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 СП будет отображаться только один диск (последний).

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. Недействующий ресурс по истечении таймаута (по умолчанию 120 секунд) будет отмонтирован, а каталог удален.

Политики подключения сетевых дисков относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 4.6.4.7).

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». Политики монтирования находятся в разделе «Пользователь» → «Административные шаблоны» → «Система ALT» → «Монтирование» (рис. 220).

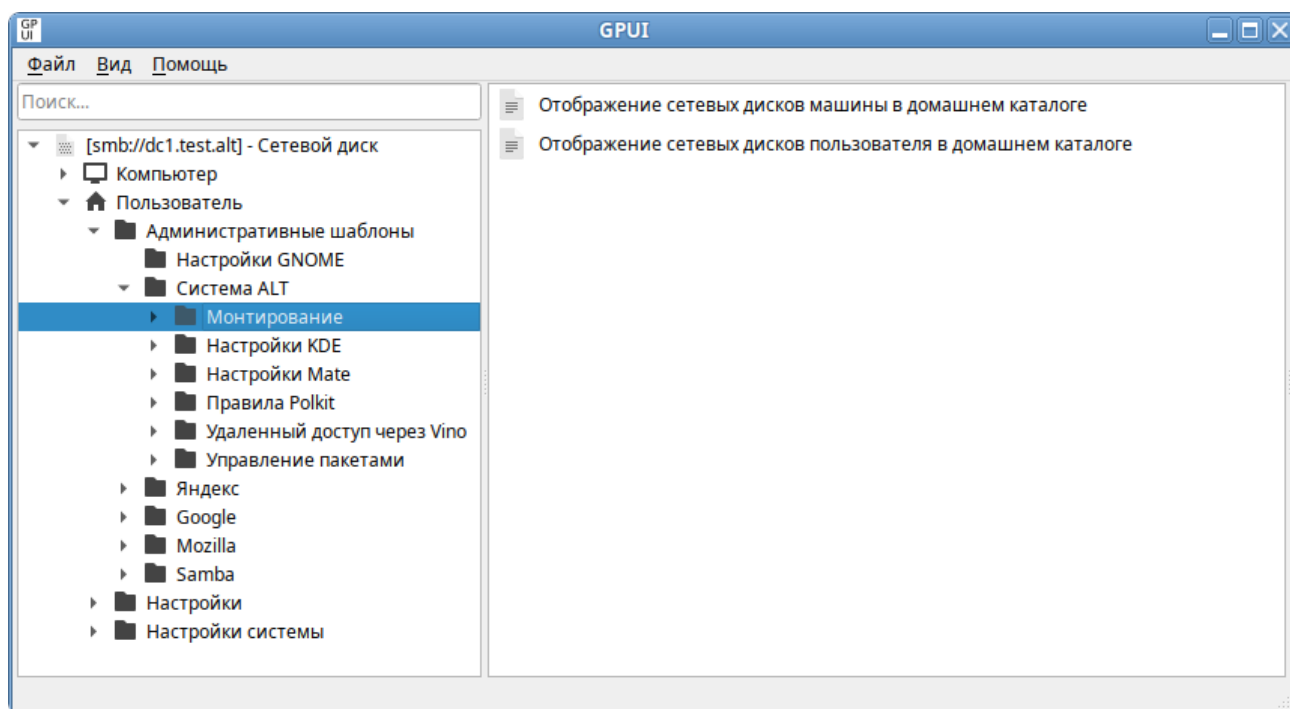


Рис. 220 – Раздел «Монтирование»

Для включения политики монтирования нужно щелкнуть на нужной политике, в открывшемся окне установить отметку в поле «Включено» и нажать кнопку «ОК» (рис. 221).

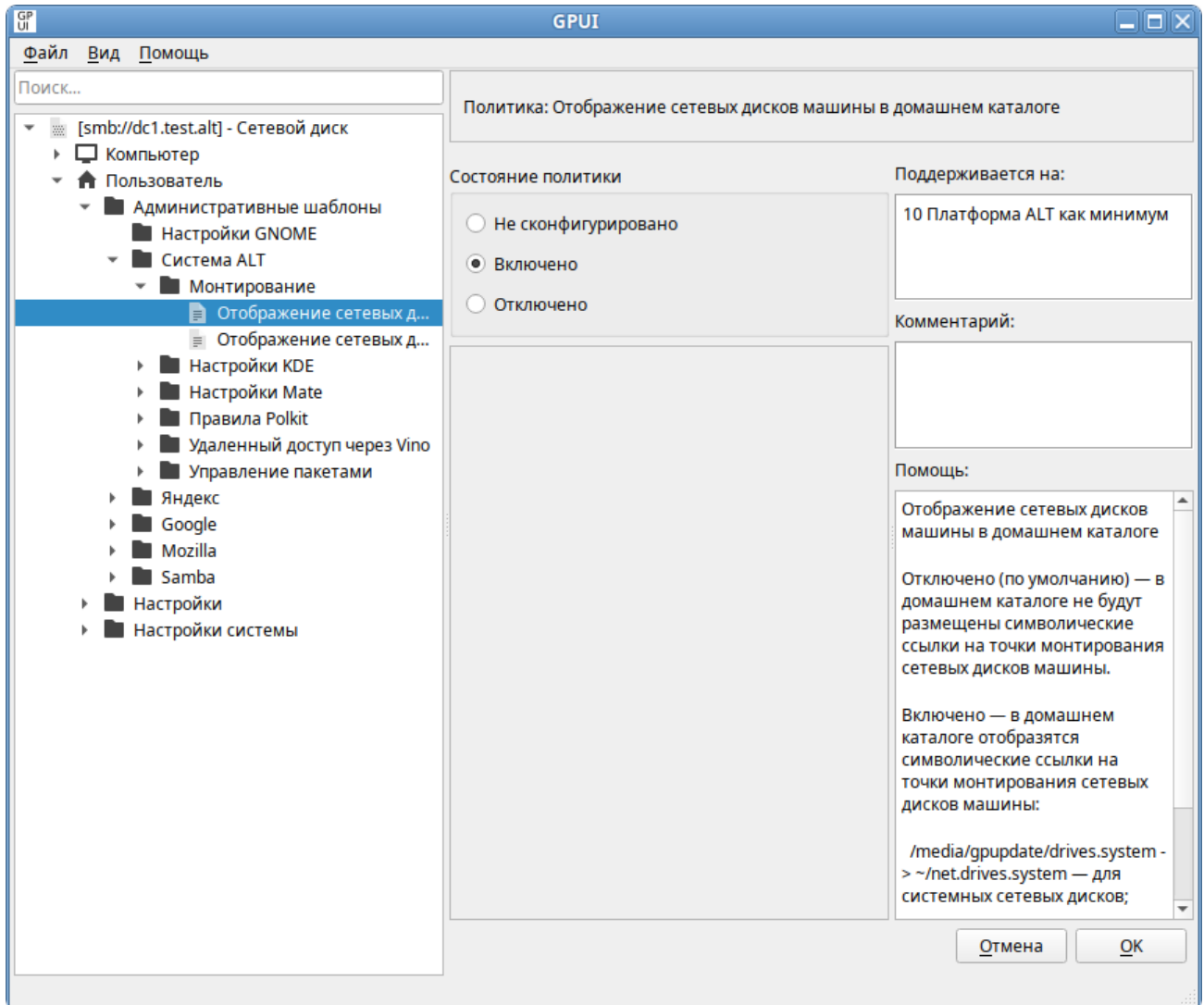


Рис. 221 – Включение политики монтирования

После обновления политик в сессии пользователя будет подключен сетевой диск, доступный из файлового менеджера и других программ (рис. 222, рис. 223).

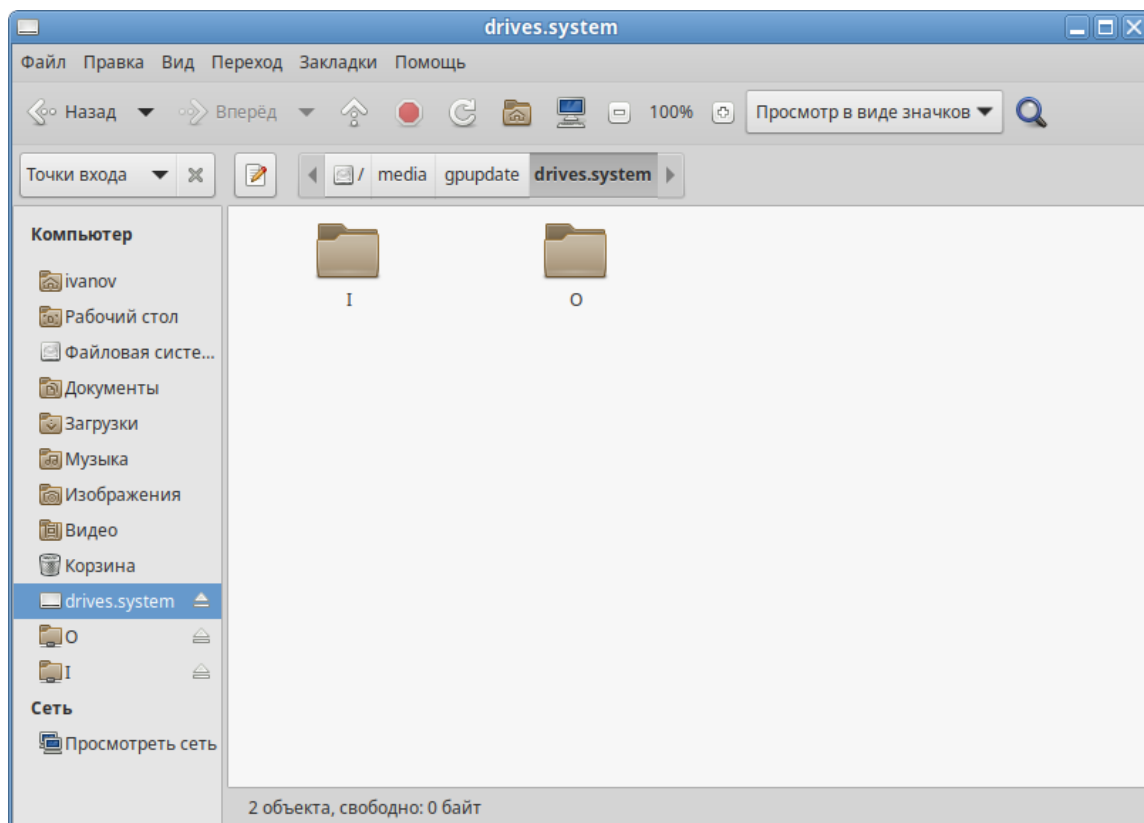


Рис. 222 – Сетевые диски в файловом менеджере Caja

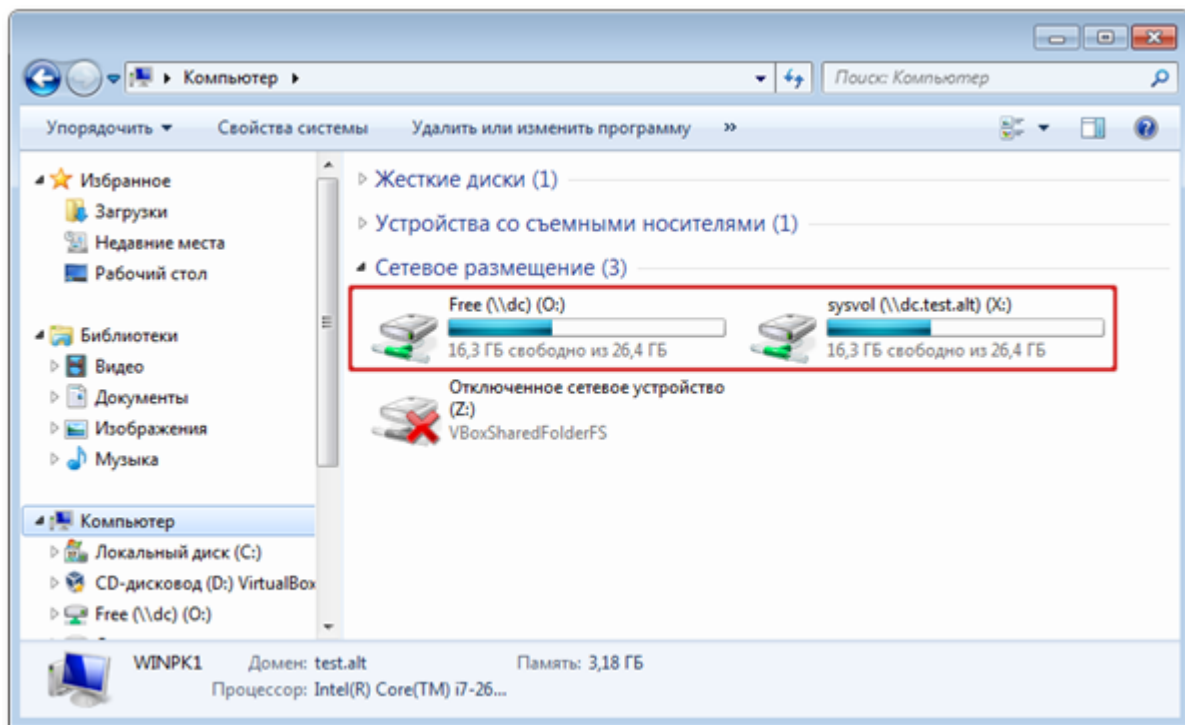


Рис. 223 – Сетевые диски в проводнике Windows

Если включены политики монтирования, 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.

Все настройки политики управления файлами 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:

```
<?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="//dc1.test.alt\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>
</Drives>
```

4.6.5.8. 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» (рис. 224).

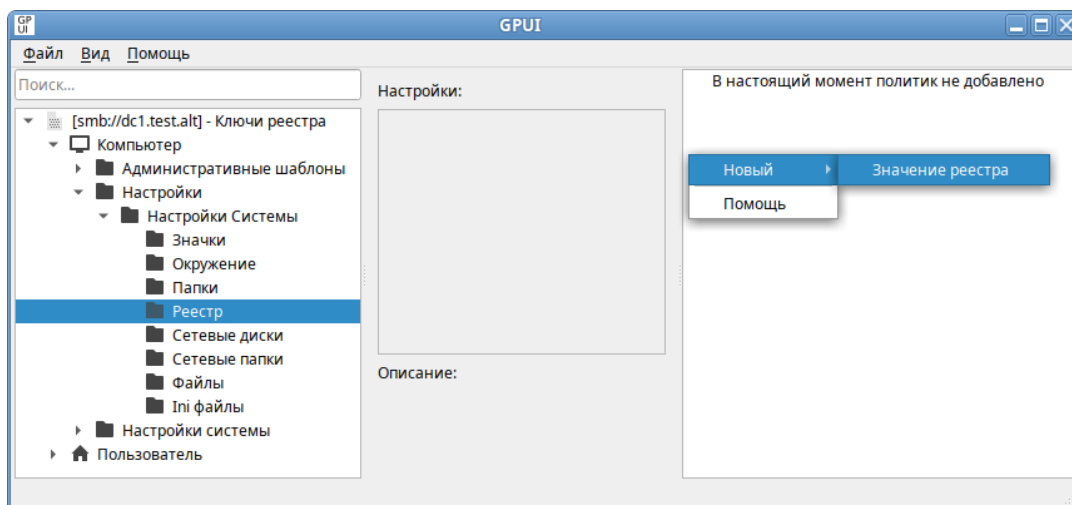


Рис. 224 – Создание политики «Значение реестра»

В диалоговом окне «Диалог настроек» задать настройки политики (рис. 225).

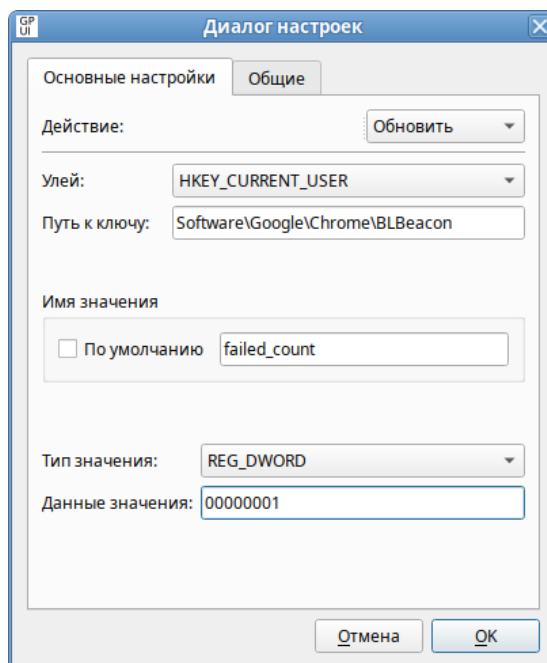


Рис. 225 – Настройки политики «Значение реестра»

Опции доступные на вкладке «Основные настройки»:

1) «Действие» – действие, которое будет выполняться для элемента реестра:

- «Создать» – создание нового значения или раздела, которое будет выполняться для элемента реестра;
- «Удалить» – удаление, которое будет выполняться для элемента реестра, 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;

2) «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;

- «HKKEY_LOCAL_MACHINE» –настройки, относящиеся к компьютеру (параметр по умолчанию для политики компьютера). Эти параметры применяются ко всем пользователям компьютера;
 - «HKKEY_USERS» –настройки для всех пользователей (параметр по умолчанию для политики пользователя). Эти параметры применяются к отдельным пользователям;
 - «HKKEY_CURRENT_CONFIG» – сведения о настройках оборудования (это псевдоним для HKKEY_LOCAL_MACHINE\System\CurrentControlSet\Hardware Profiles\Current).
- 3) «Путь к ключу» – путь к ключу. Не нужно указывать улей и вводить косую черту до или после пути. Это поле воспринимает переменные процесса настройки;
 - 4) «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;
 - 5) «Тип значения» – тип значения. Данный параметр доступен только при выбранном действии «Создать», «Заменить» или «Обновить», и введенном значении «Имя значения»;
 - 6) «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 файлами хранятся в файлах:

```
{GUID GPT}/Machine/Registry/Registry.xml
{GUID GPT}/User/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>
```

4.6.5.9. Указание прокси-сервера

С помощью групповых политик можно указать прокси-сервер.

Примечание. Если прокси-сервер был настроен в модуле «Прокси-сервер» ЦУС, предварительно нужно 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. п. 4.6.5.4).

Настройка политики для указания прокси-сервера – настроить групповую политику управления переменными окружения (рис. 226):

- в поле «Действие» выбрать пункт «Заменить»;
- в поле «Имя» указать имя переменной: HTTPS_PROXY;

- в поле «Значение» указать адрес и порт прокси-сервера, также при необходимости аутентификационные данные, в формате `http://username:password@address:port`

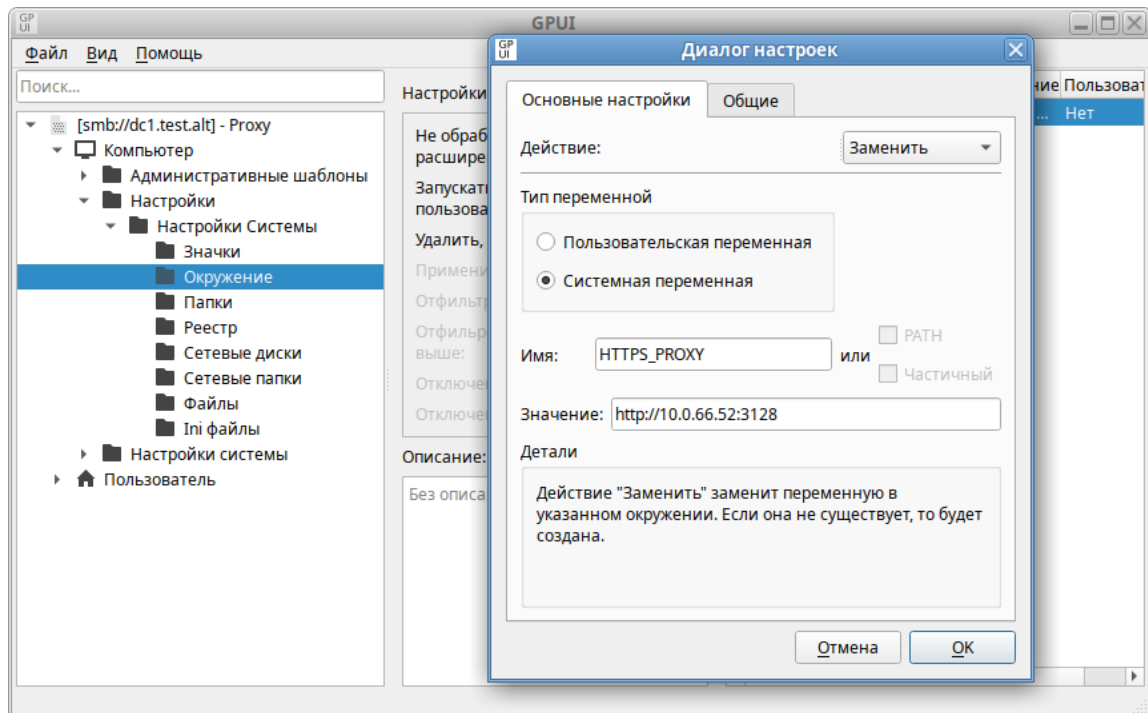


Рис. 226 – Настройка политики для указания прокси-сервера

Аналогичным способом создать настройки окружения для переменных HTTP_PROXY и FTP_PROXY (в поле «Имя» указывать соответственно HTTP_PROXY, FTP_PROXY).

Проверка применения политики:

- применить групповые политики на целевом компьютере, выполнив команду:

```
$ gpupdate
```

- повторно авторизоваться на целевом компьютере;

- 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
```

- запустить веб-браузер, убедиться, что сайты открываются через прокси-сервер.

4.6.5.10. 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. п. 4.6.5.2) и политика управления INI-файлами (см. п. 4.6.5.3).

Настройка политики задания периодичности запроса конфигураций:

1) настроить групповую политику создания каталога (рис. 227):

- в поле «Действие» выбрать пункт «Создать»;
- в поле «Путь» указать `/etc/systemd/system/gpupdate.timer.d`;

2) настроить групповую политику создания INI-файла (рис. 228):

- в поле «Действие» выбрать пункт «Обновить»;
- в поле «Путь» к файлу указать `/etc/systemd/system/gpupdate.timer.d/override.conf`;
- 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`.

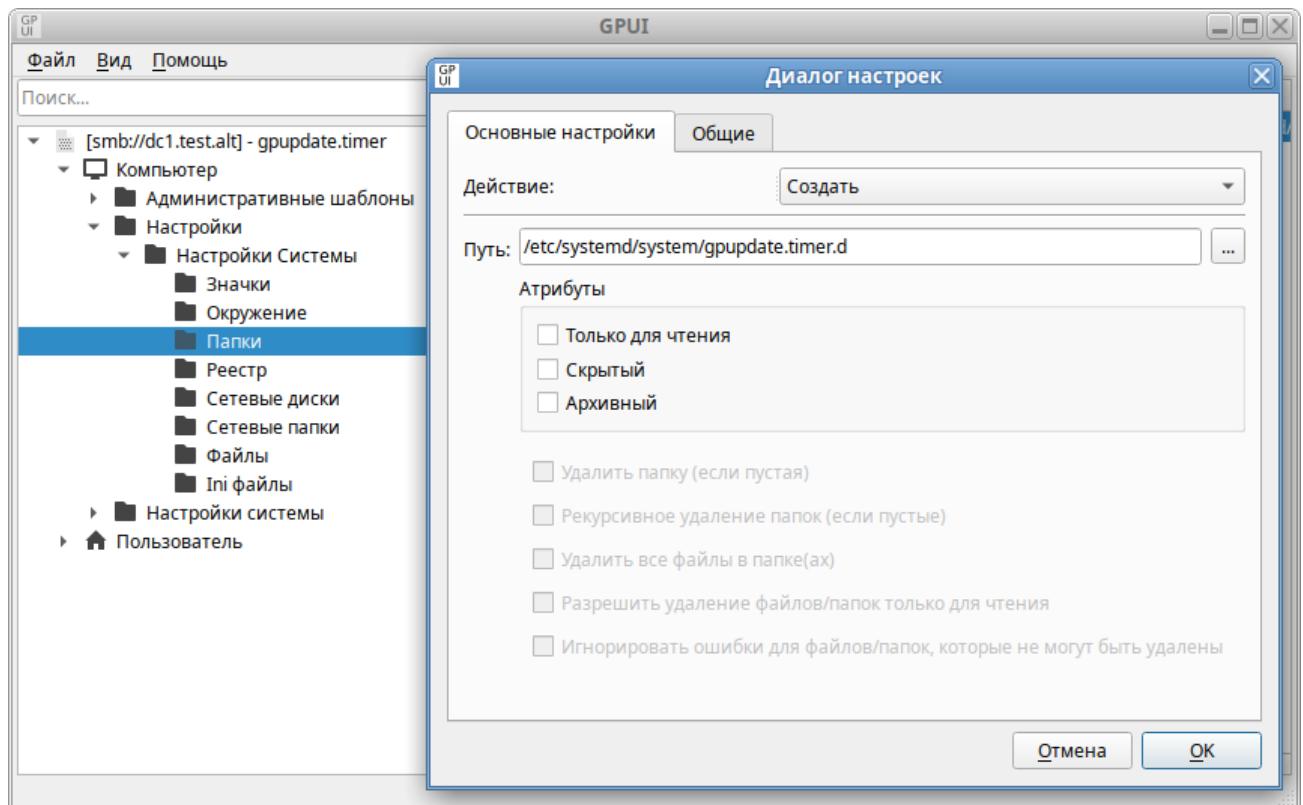


Рис. 227 – Создание каталога для настроек таймера

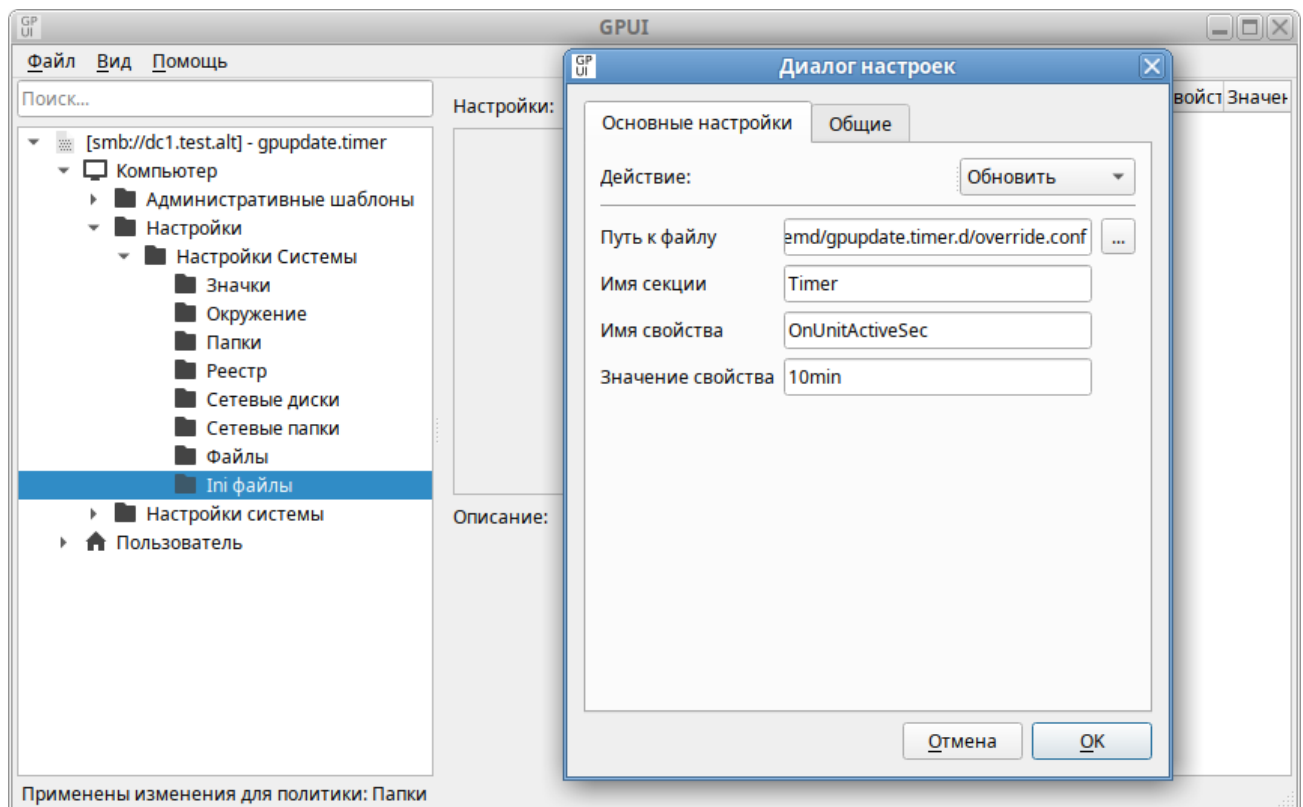


Рис. 228 – Настройка периодичности запроса конфигураций

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. 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`.

Примечание. Применить пользовательские настройки можно, выполнив команду:

```
$ systemctl --user daemon-reload
```

4.6.6. 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 иницируемыми событиями:

- 1) для машины:

- запуск компьютера (Startup);
- выключение компьютера/завершение работы (Shutdown);

- 2) 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 ALT, нужно 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.

4.6.6.1. 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». Щелкнуть левой кнопкой мыши на политике «Вход в систему» или «Выход из системы» (рис. 229).

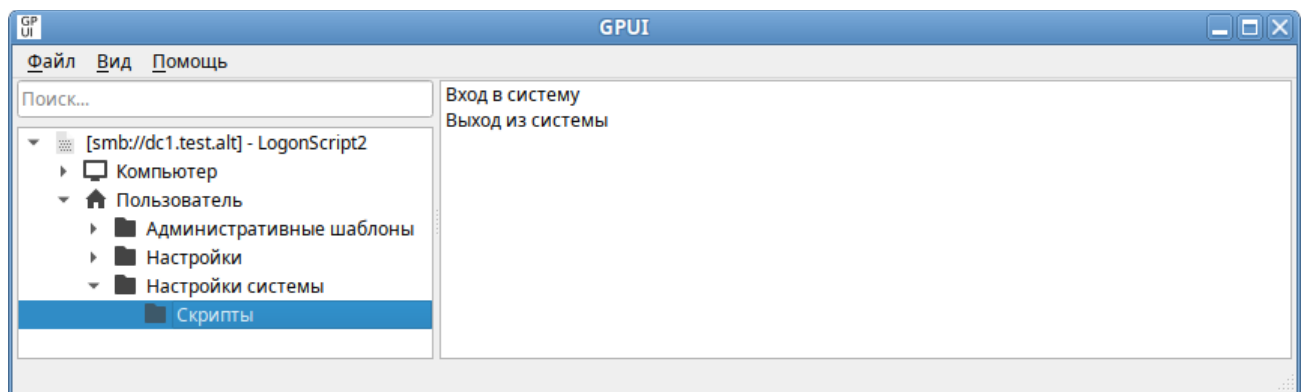


Рис. 229 – Политика «Вход в систему» или «Выход из системы»

В диалоговом окне свойств политики нажать кнопку «Добавить» (рис. 230).

В диалоговом окне «Добавить скрипт» в поле «Имя сценария» ввести путь к сценарию, в поле «Параметры сценария» ввести параметры аналогично вводу этих параметров в командной строке (рис. 231). Нажать кнопку «ОК».

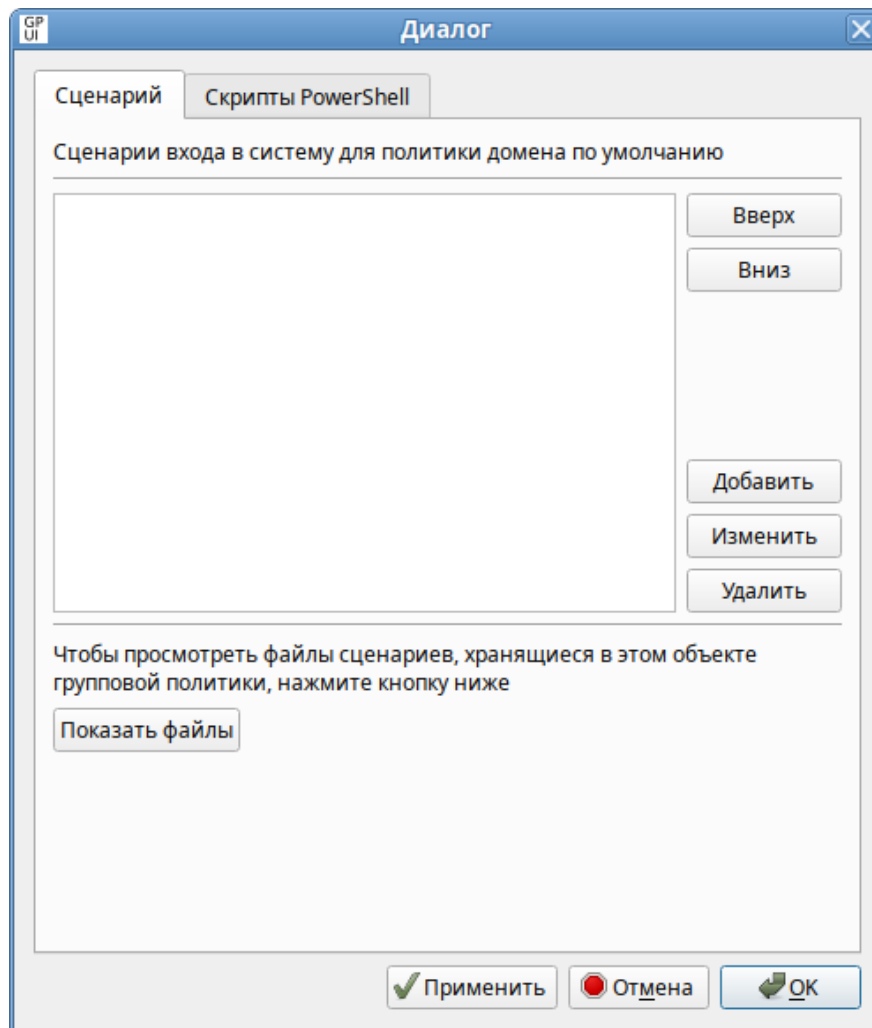


Рис. 230 – Диалоговое окно свойств политики «Вход в систему»

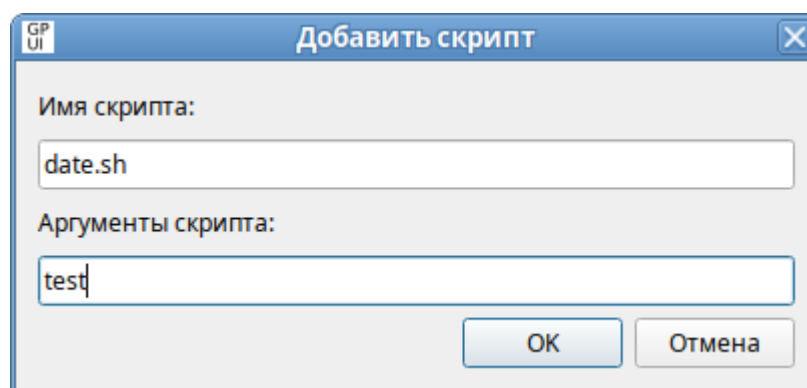


Рис. 231 – Пример добавления сценария для ОС Альт СП

П р и м е ч а н и е . Применение локальных скриптов реализовано в механизме `groupdate` версии 0.9.11. В версиях ниже скрипты для ОС Альт СП должны находиться в GPT настраиваемого объекта групповой политики.

В сценариях для ОС Windows можно указать локальный скрипт на компьютере клиента (рис. 232).

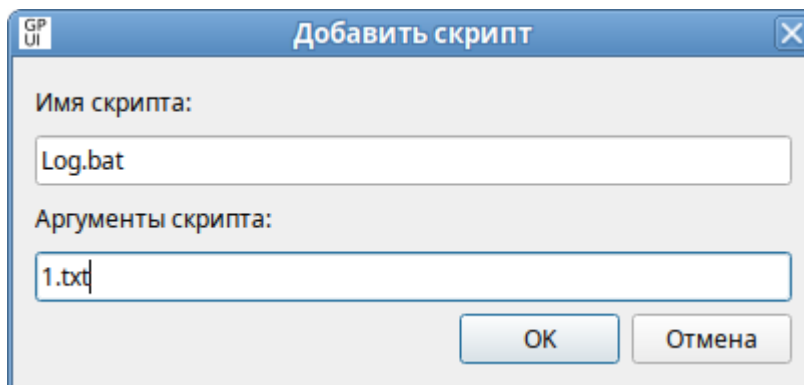


Рис. 232 – Пример добавления сценария для ОС Windows

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» (рис. 233).

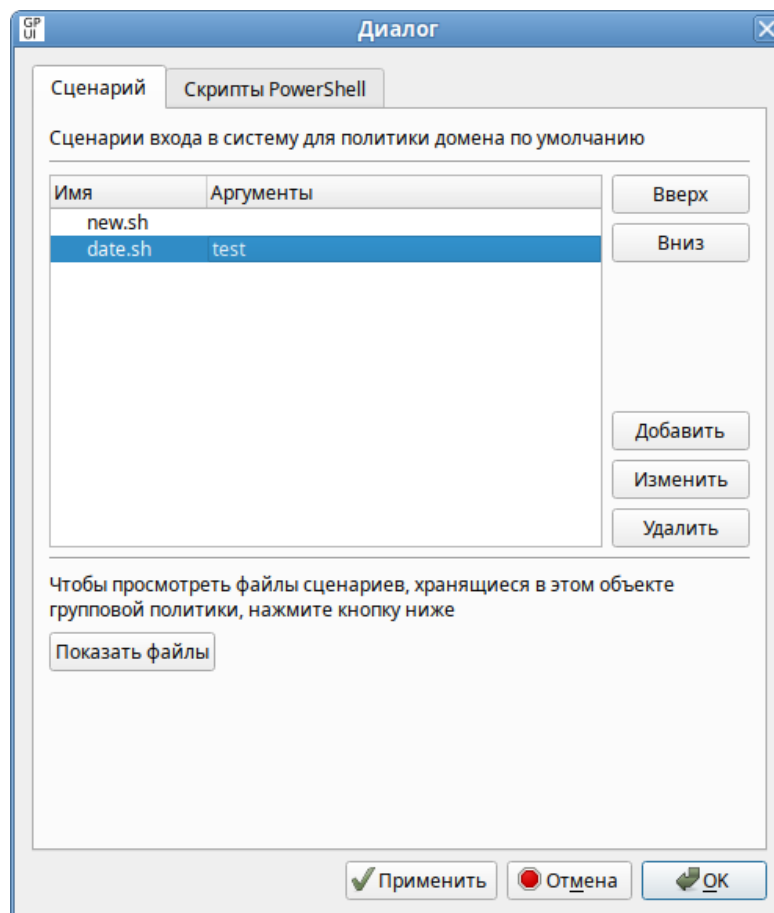


Рис. 233 – Список сценариев

Для того чтобы изменить параметры сценария, нужно 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.

4.6.6.2. 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». Щелкнуть левой кнопкой мыши на политике «Запуск» или «Завершение работы» (рис. 234).

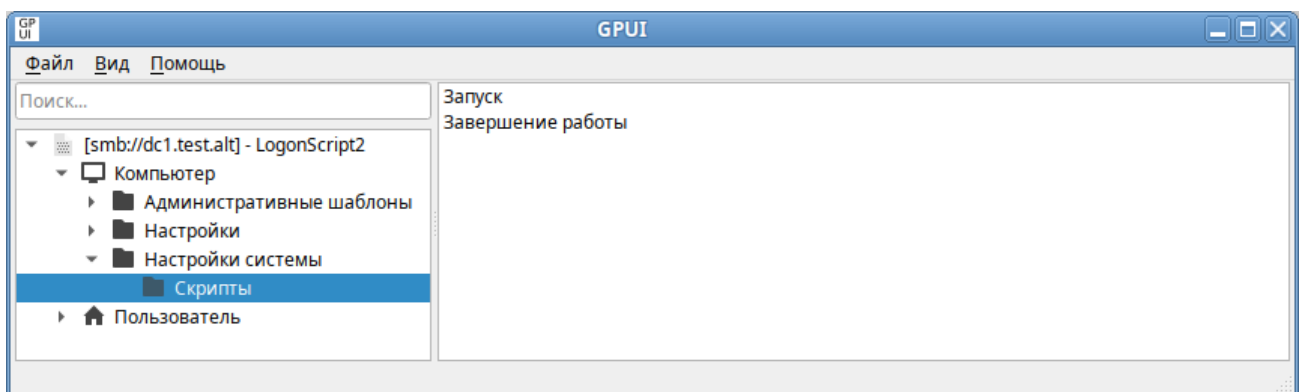


Рис. 234 – Сценарии для автозагрузки или завершения работы компьютера

В диалоговом окне свойств политики нажать кнопку «Добавить» (рис. 230).

В диалоговом окне «Добавить скрипт» в поле «Имя сценария» ввести путь к сценарию, в поле «Параметры сценария» ввести параметры аналогично вводу этих параметров в командной строке (рис. 231). Нажать кнопку «ОК».

Примечание. Применение локальных скриптов реализовано в механизме groupdate версии 0.9.11. В версиях ниже скрипты для ОС Альт СП должны находиться в GPT настраиваемого объекта групповой политики.

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, нужно 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.

4.6.6.3. Включение экспериментальных групповых политик

Политики управления logon-скриптами относятся к экспериментальным, поэтому на машинах с ОС Альт СП где они применяются должны быть включены экспериментальные групповые политики (подробнее см. п. 4.6.4.7).

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 GPOUpdate») (рис. 235).

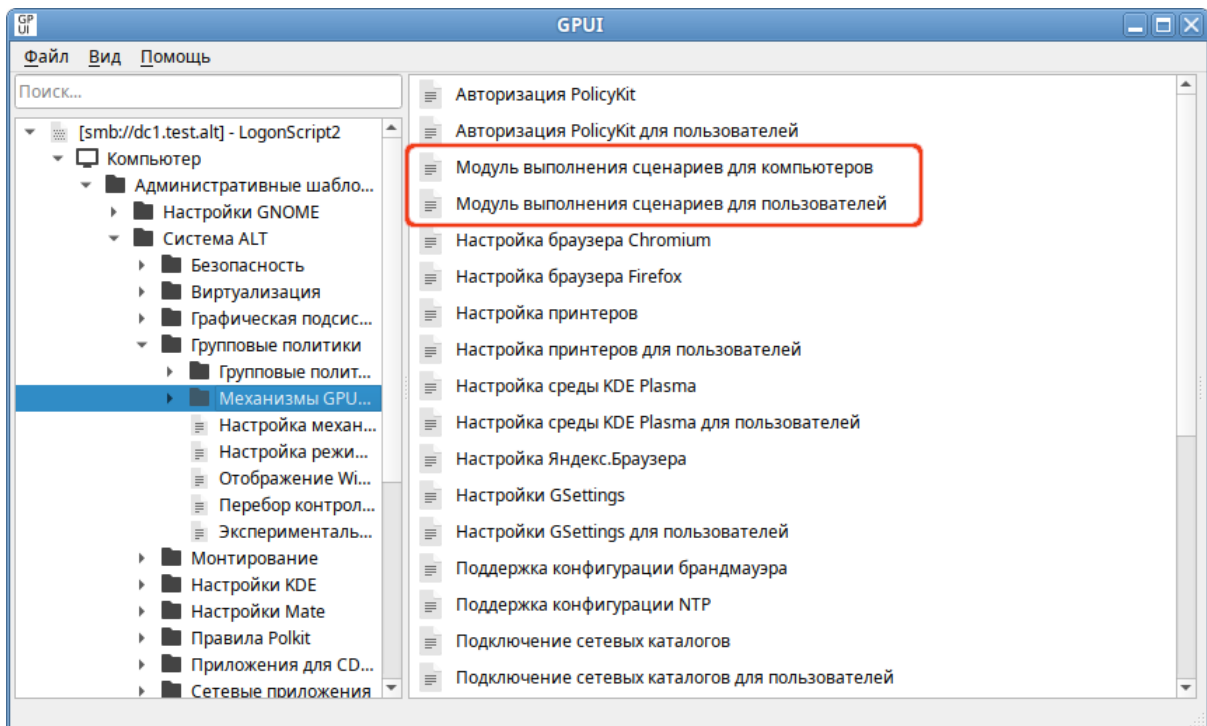


Рис. 235 – Механизмы GPOUpdate управления logon-скриптами

4.6.6.4. 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 входа и выхода пользователя хранятся в файле {GUID GPT}\User\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).

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).

4.7. Расширение возможностей ГП

4.7.1. 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.

4.7.1.1. Структура ADMX-файла

ADMX-файл состоит из семи разделов (рис. 236):

- 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 имен 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.

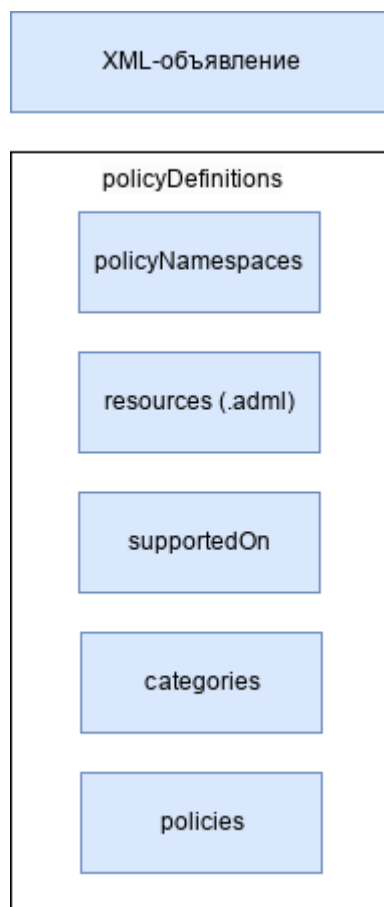


Рис. 236 – Структура ADMX-файла

XML-объявление не считается частью документа ADMX. Однако рекомендуется начинать файл ADMX с объявления 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="<MajorVersion.MinorVersion>"
schemaVersion="<MajorVersion.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 44.

Т а б л и ц а 44 – Атрибуты элемента policyDefinitions

Атрибут	Обязательный	Описание
xmlns:xsd	Нет	Обозначение элементов и типов данных, используемых в схеме пространства имен
xmlns:xsi	Нет	Обозначение пространства имен экземпляра XML-схемы, предоставленной в самом пространстве имен
revision	Да	Версия ADMX-файла, которая в большинстве случаев предназначена для отслеживания внесенных изменений. Синтаксис: revision="<MajorVersion.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 45.

Т а б л и ц а 45 – 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	Определяет требования для ресурсов определенного языка и минимальную необходимую версию связанного ADML-файла. Синтаксис: <resources minRequiredRevision="<MajorVersion.MinorVersion>" fallbackCulture="<language name>">/>

Окончание таблицы 45

Элемент	Обязательный	Описание
		где - <code>minRequiredRevision</code> – минимальный уровень версии соответствующего ADML-файла; <code>fallbackCulture</code> – язык, который будет использоваться, если ни в одном расположении не будет найден соответствующий ADML-файл. Если этот атрибут не указан будет использоваться английский язык
<code>supportedOn</code>	Нет	Определяет сопоставление ссылки на локализованные строки текста с ОС или приложениями, на которые влияют конкретные параметры политики. Синтаксис: <pre><supportedOn> <definitions> ... </definitions> </supportedOn></pre> Элементы <code>definitions</code> содержат информацию о поддерживаемой версии
<code>categories</code>	Нет	Содержит список категорий, в которых параметр политики текущего ADMX-файла будет отображаться в редакторе управления групповыми политиками. Синтаксис: <pre><categories> <category ... </category> </categories></pre> Элемент <code>category</code> указывает имя уникальной категории, которая будет отображаться в редакторе объектов групповой политики
<code>policies</code>	Нет	Содержит список определений параметров политики. Синтаксис: <pre><policies> <policy> ... </policy> </policies></pre> Дочерний элемент <code>policy</code> соответствует одному параметру групповой политики, отображаемому в редакторе объектов групповой политики. Элемент <code>policy</code> 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 46. Дочерние элементы `category` описаны в таблице 47.

Т а б л и ц а 46 – Атрибуты элемента `category`

Атрибут	Обязательный	Описание
<code>name</code>	Да	Имя, которое будет использоваться для конкретного поддерживаемого приложения и версии
<code>displayName</code>	Да	Ссылка на текстовую строку категории, расположенную в таблице строк ADML-файла
<code>explainText</code>	Нет	Текст объяснения или справки, связанный с конкретной категорией

Т а б л и ц а 47 – Дочерние элементы элемента `category`

Элемент	Обязательный	Описание
<code>parentCategory</code>	Да	Ссылка на родительскую категорию
<code>seeAlso</code>	Нет	Ссылка на другой элемент, который может быть связан с этим. Этот элемент не поддерживается и будет игнорироваться текущей ГП
<code>keywords</code>	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 valuenam>"
<parentCategory> ... </parentCategory>
<supportedOn> ... </supportedOn>
<enabledValue> ... </enabledValue>
<disabledValue> ... </disabledValue>
<enabledList> ... </enabledList>
<disabledList> ... </disabledList>
<elements> ... </elements>
</policy>
```

Атрибуты элемента `policy` описаны в таблице 48. Дочерние элементы `policy` описаны в таблице 49.

Т а б л и ц а 48 – Атрибуты элемента policy

Атрибут	Обязательный	Описание
name	Да	Уникальное имя элемента политики (строка без пробелов и специальных символов)
class	Да	Определяет, где в каком разделе редактора ГП будет размещен 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

Т а б л и ц а 49 – Дочерние элементы элемента 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: <enabledValue> <delete /> <decimal> ... </decimal> <string> ... </string> </enabledValue> где: - delete – удалить значение или ключ реестра; - decimal – десятичное беззнаковое число; - string – строка, ограниченная 255 символами
disabledValue	Нет	Значение, которое раздел реестра примет, если политика отключена. См. описание элемента enabledValue
enabledList	Нет	Набор значений и ключей реестра, представляющих включенное состояние элемента политики. Синтаксис: <enabledList defaultKey="<registry subkey>"> <item> ... </item> </enabledList> где: - атрибут defaultKey – подраздел реестра по умолчанию для всех элементов; - item – подраздел реестра со связанным значением

Окончание таблицы 49

Элемент	Обязательный	Описание
disabledList	Нет	Набор значений и ключей реестра, представляющих отключенное состояние элемента политики. См. описание элемента <code>enabledList</code>
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 50.

Т а б л и ц а 50 – Дочерние элементы `elements`

Элемент	Обязательный	Описание
boolean	Нет	Представляет логический элемент в политике. Синтаксис: <pre><boolean id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" <trueValue> ... </trueValue> <falseValue> ... </falseValue> <trueList> ... </trueList> <falseList> ... </falseList> </boolean></pre> где: - атрибут <code>id</code> – сопоставление с элементом (обязательный); - атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valueName</code> – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - <code>trueValue</code> – устанавливает значение на основе истинного условия; - <code>falseValue</code> – устанавливает значение на основе ложного условия; - <code>trueList</code> – устанавливает значения на основе истинного состояния; - <code>falseList</code> – устанавливает значения на основе ложного состояния.

Продолжение таблицы 50

Элемент	Обязательный	Описание
		Пример: <pre><boolean id="OrgXfceThunar_blocker" key="Software\BaseALT\Policies\PolkitLocks" valueName="org.xfce.thunar"> <trueValue> <decimal value="1" /> </trueValue> <falseValue> <decimal value="0" /> </falseValue> </boolean></pre> Для элемента boolean из ADMX-файла требуется элемент checkbox с соответствующим идентификатором в ADML-файле
decimal	Нет	Представляет числовой/десятичный элемент в политике. Число может быть определено для хранения в виде числового или строкового репрезентативного значения. Синтаксис: <pre><decimal id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" required="true false" minValue="<MinValue>" maxValue="<MaxValue>" storeAsText="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 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: <pre><decimal id="OrgMateSessionIdleDelay_setter" valueName="org.mate.session.idle-delay" minValue="1" maxValue="2147483647" /></pre> Для элемента decimal требуется элемент decimalTextBox с соответствующим идентификатором в ADML-файле

Продолжение таблицы 50

Элемент	Обязательный	Описание
text	Нет	Представляет текстовый элемент в политике. Синтаксис: <pre><text id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" required="true false" maxLength="<maxLength>" expandable="true false" soft="true false" / ></pre> где: - атрибут <code>id</code> – сопоставление с элементом (обязательный); - атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valueName</code> – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - атрибут <code>required</code> – требует ввести значение в поле параметра; - атрибут <code>maxLength</code> – максисмально допустимое количество символов; - атрибут <code>expandable</code> – если <code>true</code>, значение подраздела реестра будет создано как расширяемый строковый тип (<code>REG_EXPAND_SZ</code>) вместо строкового типа (<code>REG_SZ</code>); - атрибут <code>soft</code> – следует ли перезаписывать существующий подраздел. Пример: <pre><text id="OrgMateFilename_setter" valueName="org.mate.background.picture-filename" /></pre> Элемент <code>text</code> допускает строковые значения длиной до 1023 символов. - Для элемента <code>text</code> требуется соответствующий элемент <code>textBox</code> или <code>comboBox</code> с соответствующим идентификатором в ADML-файле
enum	Нет	Представляет элемент перечисления. Синтаксис: <pre><enum id="<ID>" clientExtension="<GUID>" key="<RegKey>" valueName="<Name>" required="true false"> <item> ... </item> </enum></pre> где: - атрибут <code>id</code> – сопоставление с элементом (обязательный); - атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом;

Продолжение таблицы 50

Элемент	Обязательный	Описание
		- атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valueName</code> – значение реестра, которое будет настроено для этого конкретного элемента политики (обязательный); - атрибут <code>required</code> – требует ввести значение в поле параметра; - <code>item</code> – представляет набор отображаемых имен с одним значением или набор значений подразделов реестра. Синтаксис элемента <code>item</code>: <pre><item displayName="\$ (string.<placeholder for text>)"> <item> ... </item> </item></pre> - где <code>displayName</code> – ссылка на отображаемую строку, расположенную в таблице строк ADML-файла. Пример: <pre><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></pre> Элемент <code>enum</code> обычно связан с элементом раскрывающегося списка в редакторе объектов групповой политики. Для элемента <code>enum</code> требуется элемент <code>dropdownList</code> с соответствующим идентификатором в ADML-файле
list	Нет	Представляет элемент списка в политике. Синтаксис: <pre><list id="<ID>" clientExtension="<GUID>" key="<RegKey>" valuePrefix="<Name>"> additive="true false" expandable="true false" explicitValue="true false" > </ list></pre> где: - атрибут <code>id</code> – сопоставление с элементом (обязательный);

Окончание таблицы 50

Элемент	Обязательный	Описание
		- атрибут <code>clientExtension</code> – клиентское расширение, которое будет обрабатывать на клиентском компьютере конкретные настройки, представленные элементом; - атрибут <code>key</code> – местоположение ключа реестра, под которым будет создан параметр реестра; - атрибут <code>valuePrefix</code> – префикс, добавляемый к увеличенному целому числу, создает подраздел реестра, используемый при настройке значений политики (обязательный); - атрибут <code>additive</code> – если для этого параметра указано значение <code>true</code>, существующие подразделы не удаляются, а значения, установленные в списке, добавляются к существующим подразделам; - атрибут <code>explicitValue</code> – если для этого параметра указано значение <code>true</code>, пользователь должен указать значение подраздела реестра и имя подраздела реестра. В списке отображаются два столбца: один для имени и один для данных; атрибут <code>expandable</code> – если <code>true</code>, значение подраздела реестра будет создано как расширяемый строковый тип (<code>REG_EXPAND_SZ</code>) вместо строкового типа (<code>REG_SZ</code>). Пример: <pre><list id="InstallPackagesList" key="Software\BaseALT\Policies\Packages\Install" additive="true"/></pre> Для элемента <code>list</code> требуется элемент <code>listBox</code> 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.

4.7.1.2. Структура ADML-файла

ADML-файл состоит из пяти разделов (рис. 237):

- 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` – элемент, который 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 флаги, 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.

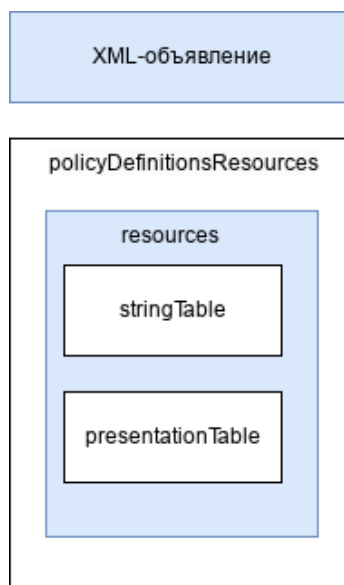


Рис. 237 – Структура ADML-файла

Синтаксис элемента `policyDefinitionResources`:

```
<policyDefinitionResources
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVersion.MinorVersion>"
schemaVersion="<MajorVersion.MinorVersion>"
xmlns="
http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinition
s" >
<displayName> ... </displayName>
<description> ... </description>
<annotation> ... </annotation>
<resources> ... </resources>
</policyDefinitionResources>
```

Дочерние элементы `policyDefinitionResources` описаны в таблице 51.

Атрибуты элемента `policyDefinitionResources` описаны в таблице 52.

Т а б л и ц а 51 – Доочерние элементы `policyDefinitionResources`

Элемент	Обязательный	Описание
<code>displayName</code>	Да	Название политики, содержащееся в ADML-файле
<code>description</code>	Нет	Описание параметров политики, содержащееся в ADML-файле
<code>annotation</code>	Да	Локализованный комментарий
<code>resources</code>	Нет	Содержит элементы <code>stringTable</code> и <code>presentationTable</code> для указанного языка.

Т а б л и ц а 52 – Атрибуты элемента `policyDefinitionResources`

Атрибут	Обязательный	Описание
<code>xmlns:xsd</code>	Нет	Обозначение элементов и типов данных, используемых в схеме пространства имен
<code>xmlns:xsi</code>	Нет	Обозначение пространства имен экземпляра XML-схемы, предоставленной в самом пространстве имен
<code>revision</code>	Да	Версия ADMX-файла. Синтаксис: <code>revision="<MajorVersion.MinorVersion>"</code> где <code>MajorVersion</code> и <code>MinorVersion</code> являются номерами версии, например, <code>revision="1.0"</code>
<code>schemaVersion</code>	Да	Указывает версию схемы, используемую средствами работы с ГП для определения того, поддерживается ли ими формат конкретных ADMX-файлов. Синтаксис этой команды идентичен синтаксису <code>revision</code>
<code>xmlns</code>	Нет	Пространство имен схемы ГП

Синтаксис элемента resources:

```
<resources>
<stringTable> ... </stringTable>
<presentationTable> ... </presentationTable>
</resources>
```

Дочерние элементы resources описаны в таблице 53.

Т а б л и ц а 53 – 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: <pre><stringTable> <string> ... </string> </stringTable></pre> 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, флаги, переключатели); подписи и текст подсказки для ввода параметров; а также значения по умолчанию и диапазон возможных значений для каждого параметра. Синтаксис: <pre><presentationTable> <presentation> ... </presentation> </presentationTable></pre> 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>
```

Атрибут элемента presentation описаны в таблице 54.

Дочерние элементы presentation описаны в таблице 55.

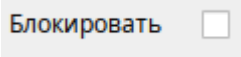
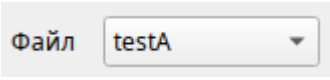
Т а б л и ц а 54 – Атрибут элемента presentation

Атрибут	Обязательный	Описание
id	Да	Указывает логическое имя при ссылке на информацию о представлении для определенного параметра политики

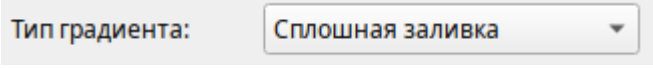
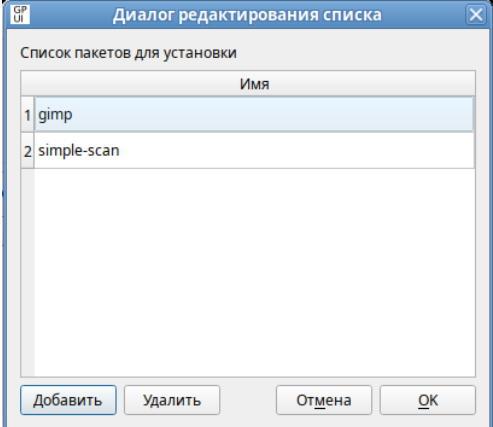
Т а б л и ц а 55 – Дочерние элементы resources

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. Синтаксис: <decimalTextBox refId="Sample_NumericTextLabel">Метка</decimalTextBo x> где: - атрибут refId – сопоставление с элементом. Пример: <decimalTextBox refId="OrgMateScreensaverLockDelay_setter"defaultVal ue="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> 

Продолжение таблицы 55

Элемент	Обязательный	Описание
checkBox	Нет	Элемент флага. Должен быть связан с элементом boolean, определенным в элементе elements. Синтаксис: <code><checkBox refId="<ID> defaultChecked="true false"> Label: </checkBox></code> где: - атрибут <code>refId</code> – сопоставление с элементом (обязательный); - атрибут <code>defaultChecked</code> – значение по умолчанию. Если не указано, атрибуту <code>defaultChecked</code> будет присвоено значение <code>false</code>. Пример: <code><checkBox refId="OrgXfceThunar_blocker"> Блокировать</checkBox></code> 
comboBox	Нет	Поле со списком со значениями по умолчанию или предлагаемыми записями. Должно быть связано с элементом text, определенным в элементе elements. Синтаксис: <code><comboBox refId="<ID> noSort="true false"> <label> ... </label> <default> ... </default> <suggestion> ... </suggestion> </comboBox></code> где: - атрибут <code>refId</code> – сопоставление с элементом (обязательный); - атрибут <code>noSort</code> – если <code>true</code>, отображать предлагаемые значения в определенном порядке элементов предложения; в противном случае отсортировать предлагаемые значения в алфавитном порядке. Если не указано, атрибуту <code>noSort</code> будет присвоено значение <code>false</code>; - <code>label</code> – подпись для параметра (обязательный); - <code>default</code> – строка, по умолчанию отображаемая в параметре; - <code>suggestion</code> – строка раскрывающегося списка. Пример: <code><comboBox refId="OrgMateFilename_setter"> <label>Файл</label> <default>None</default> <suggestion>testA</suggestion> <suggestion>testB</suggestion> <suggestion>testC</suggestion> </comboBox></code> 

Окончание таблицы 55

Элемент	Обязательный	Описание
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: <pre><listBox refId="ID">Описание:</listBox></pre> где: - атрибут refId – сопоставление с элементом. Пример: <pre><listBox refId="InstallPackagesList">Список пакетов для установки</listBox></pre> 

Дочерние элементы, указанные в элементе `presentation`, должны соответствовать элементам, определенным в элементе `elements` ADMX-файла.

4.7.2. 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 флага (`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 флага (`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 соответствовать 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 ее 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 выше 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.

4.7.3. 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.

Пример создания 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/PolicyD
efinitions">
<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/PolicyD
efinitions">
<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>
```

4.7.4. Разработка новой политики

Программа `grpupdate` состоит из ряда механизмов, позволяющих обращаться к настройкам ОС Альт СП. Механизмы обращаются к интерфейсам системы или отдельных приложений через API. Через систему механизмов `grpupdate` пользователю доступно создание собственных ГП так, чтобы не менять содержимое пакетов `adm` и `grpupdate`. 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 правяет 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.

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 ее описание на русском или английском языке;
- 4) проверить корректность кода в ADMX-файлах, открыв редактор групповых политик – GPUI в ОС Альт СП или RSAT в Windows;
- 5) загрузить собственный набор административных шаблонов групповых политик (admx) на контроллер домена в каталог Sysvol.

4.7.4.1. 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/PolicyDef
initions"
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/PolicyDef
initions"
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
 \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;
 - файл ru-RU/MySystemd.adml В каталог
 \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;
 - файл en-US/MySystemd.adml В каталог
 \\<DOMAIN>\sysvol\<DOMAIN>\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 ОС Альт СП (рис. 238) 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/).

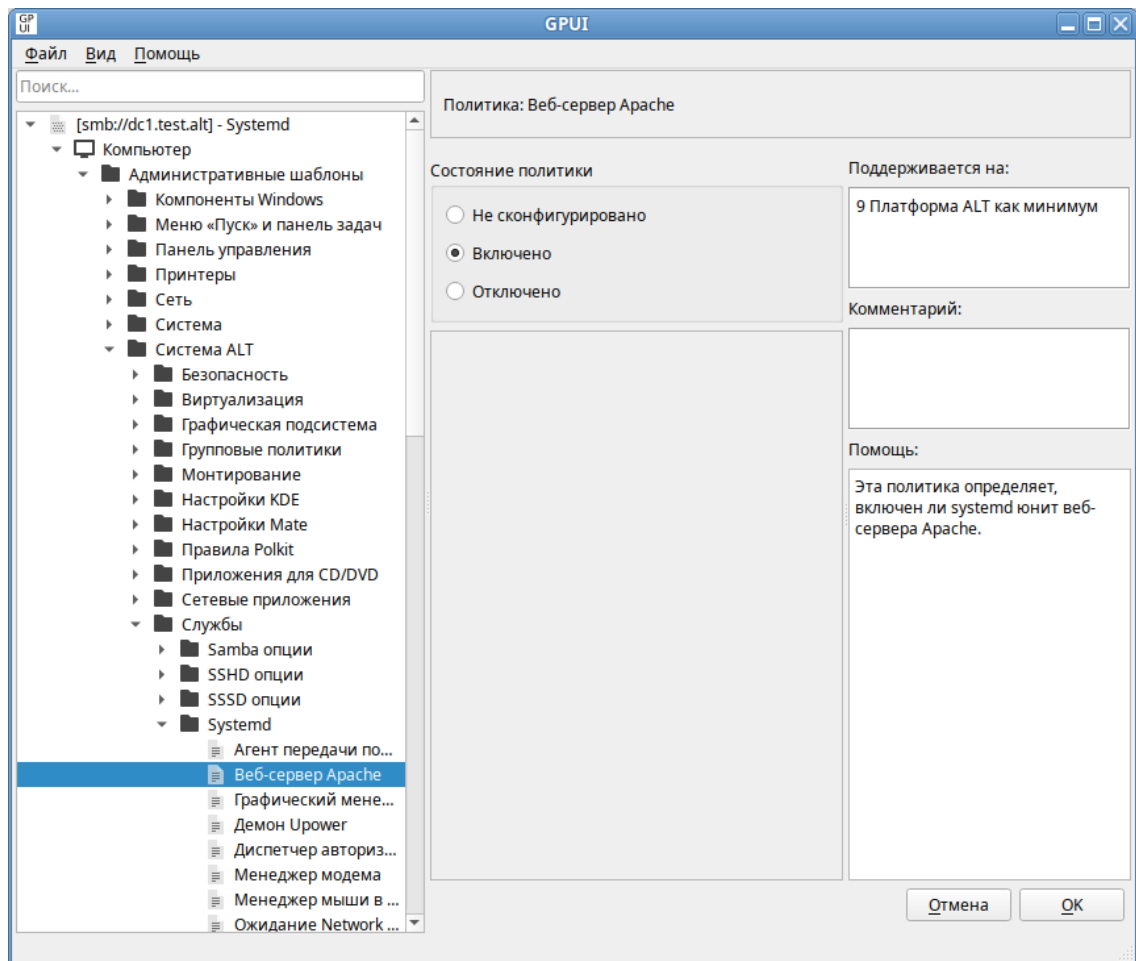


Рис. 238 – Проверка новой политики Systemd в GPUI

4.7.4.2. 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
```

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/PolicyDef
initions">
<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="$(string.ossec-send)"
explainText="$(string.ossec-send_help)"
key="Software\BaseALT\Policies\Control"
name="ossec-send" presentation="$(presentation.ossec-send)">
<parentCategory ref="system:ALT_Services"/>
<supportedOn ref="system:SUPPORTED_AltP9"/>
<elements>
<enum id="ossec-send_setter" required="true" valueName="ossec-send">
<item displayName="$(string.ossec-send_mail)">
<value>
<string>mail</string>
</value>
</item>
<item displayName="$(string.ossec-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/PolicyDef
initions"
revision="1.0" schemaVersion="1.0">
<displayName>Определения политик управления системными
компонентами</displayName>
<description>Этот файл содержит определения политик управления
системными компонентами.</description>
```

```

<resources>
<stringTable>
<string id="osec-send">Отчет подсистемы osec</string>
<string id="osec-send_help">Политика позволяет определить куда
отправлять ежедневный отчет:

```

Почта - отправлять отчет на почтовый ящик пользователя root

Журнал - записывать отчет 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 отчет:
</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/PolicyDef
initions"
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
	\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;		
- файл	ru-RU/MyControl.adml	В	каталог
	\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;		
- файл	en-US/MyControl.adml	В	каталог
	\\<DOMAIN>\sysvol\<DOMAIN>\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 ОС Альт СП (рис. 239) 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/).

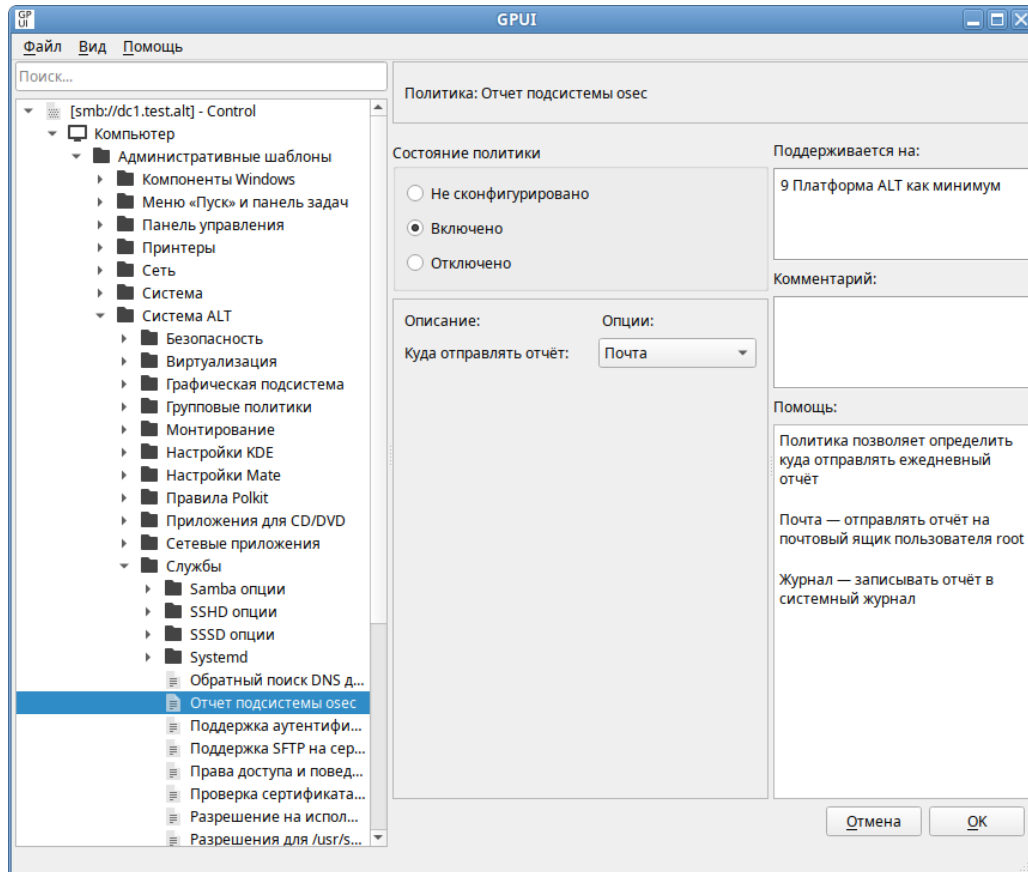


Рис. 239 – Проверка новой политики Control в GPUI

4.7.4.3. Пример для механизма Gsetting

Конфигурация DE Mate хранится в базе dconf, ключами которой управляет консольное приложение GSettings. Механизм gupdate 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-recursive
```

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/PolicyDef
initions">
<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/PolicyDef
  initions"
  revision="1.0" schemaVersion="1.0">
  <displayName>Определения списка настроек рабочего окружения
  МАТЕ</displayName>
  <description>Этот файл содержит определения настроек рабочего
  окружения МАТЕ.</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 ее
      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>
  </presentationTable>

```

```

</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</check
Box>
</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/PolicyDef
initions"
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</check
Box>

```

```
</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
  \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;
- файл ru-RU/MyGsettings.adml В каталог
  \\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;
- файл en-US/MyGsettings.adml В каталог
  \\<DOMAIN>\sysvol\<DOMAIN>\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 ОС Альт СП (рис. 240) 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/).

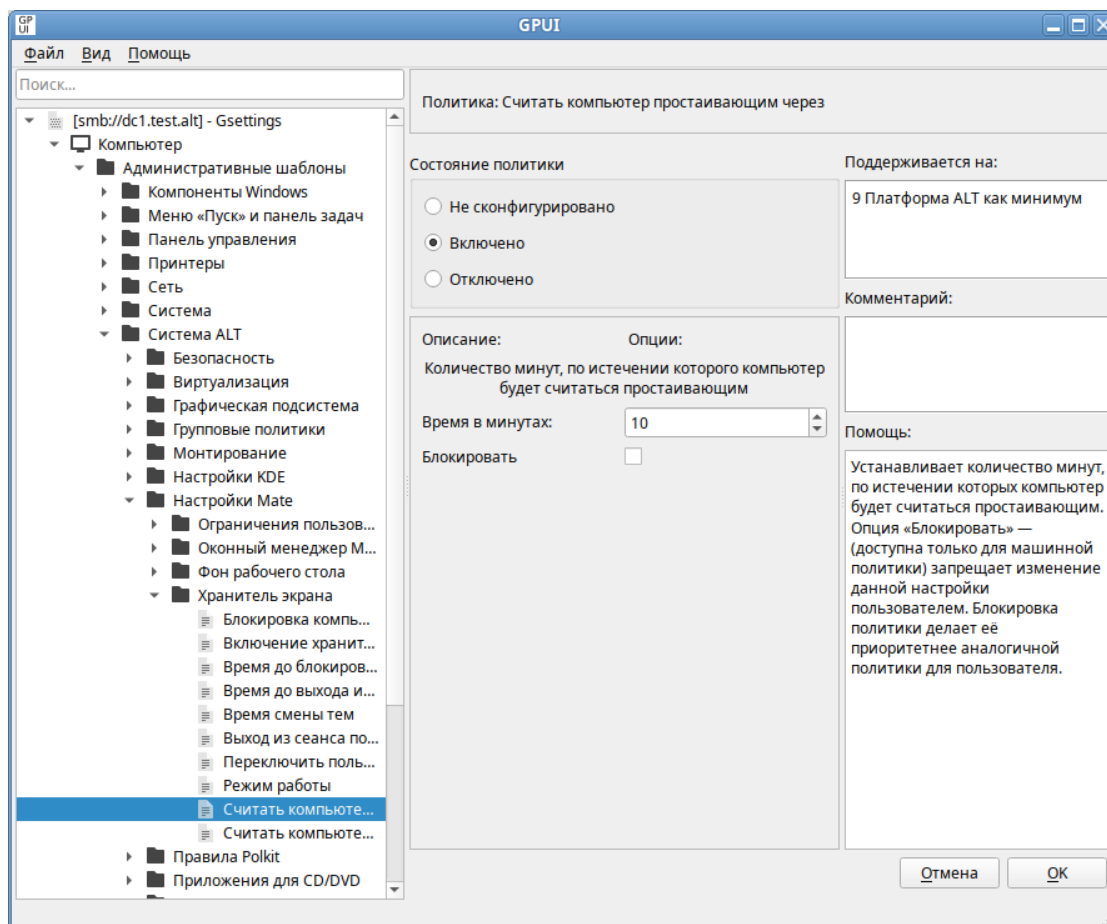


Рис. 240 – Проверка новой политики Gsetting в GPUI

4.7.4.4. 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 `gupdate` 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, определенных 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/PolicyDef
initions">
<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"
valuenam="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 ее 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/PolicyDef
initions"
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 GGUI.

В Windows RSAT:

- файл MyPolkit.admx в каталог

```
\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions;
```

- файл ru-RU/MyPolkit.adml в каталог

```
\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\ru-RU;
```

- файл en-US/MyPolkit.adml в каталог

```
\\<DOMAIN>\sysvol\<DOMAIN>\Policies\PolicyDefinitions\en-US.
```

Windows RSAT автоматически проверит корректность этих файлов.

В GGUI:

- 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 – GGUI в ОС Альт СП (рис. 241) 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/).

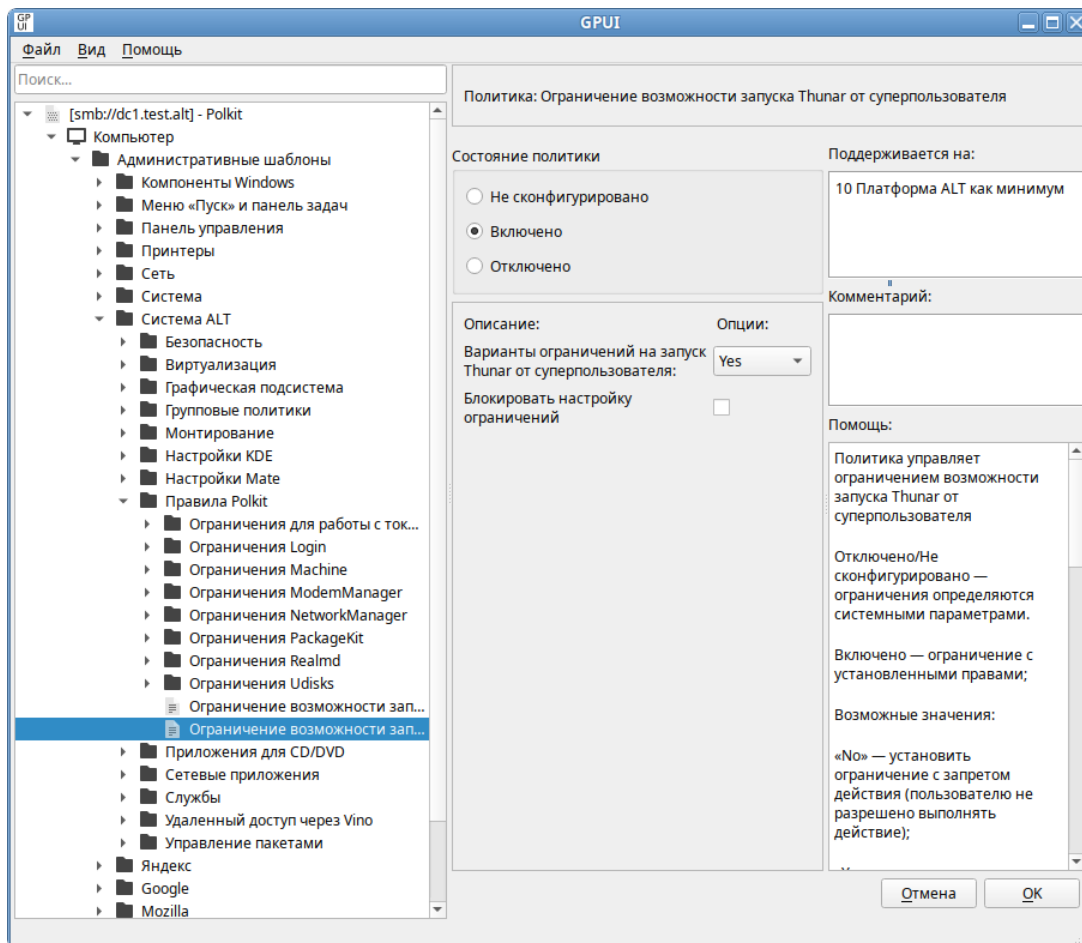


Рис. 241 – Проверка новой политики Polkit в GPUI

4.8. Решение проблем

Прежде чем разбираться, почему групповые политики не применяются, как ожидается, необходимо убедиться, что инфраструктура «Альт Домен» работает штатно. Работа групповых политик в домене зависит от корректности работы контроллеров домена и репликации между ними.

Не рекомендуется использовать сложную структуру групповых политик и создавать дополнительные политики без необходимости. Рекомендуется использовать единую схему наименования политик. Имя групповой политики должно давать однозначное понимание того, для чего она нужна.

4.8.1. Область действия и статус групповой политики

В каждой групповой политике 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. п. 4.8.4).

Если ГП настраивает только параметры пользователя или только параметры компьютера, неиспользуемый раздел можно отключить. Это снизит трафик ГП и позволит уменьшить время обработки групповой политики на клиентах.

Статус групповой политики можно проверить в ADMS в свойствах подразделения на вкладке «Групповая политика» (рис. 242).

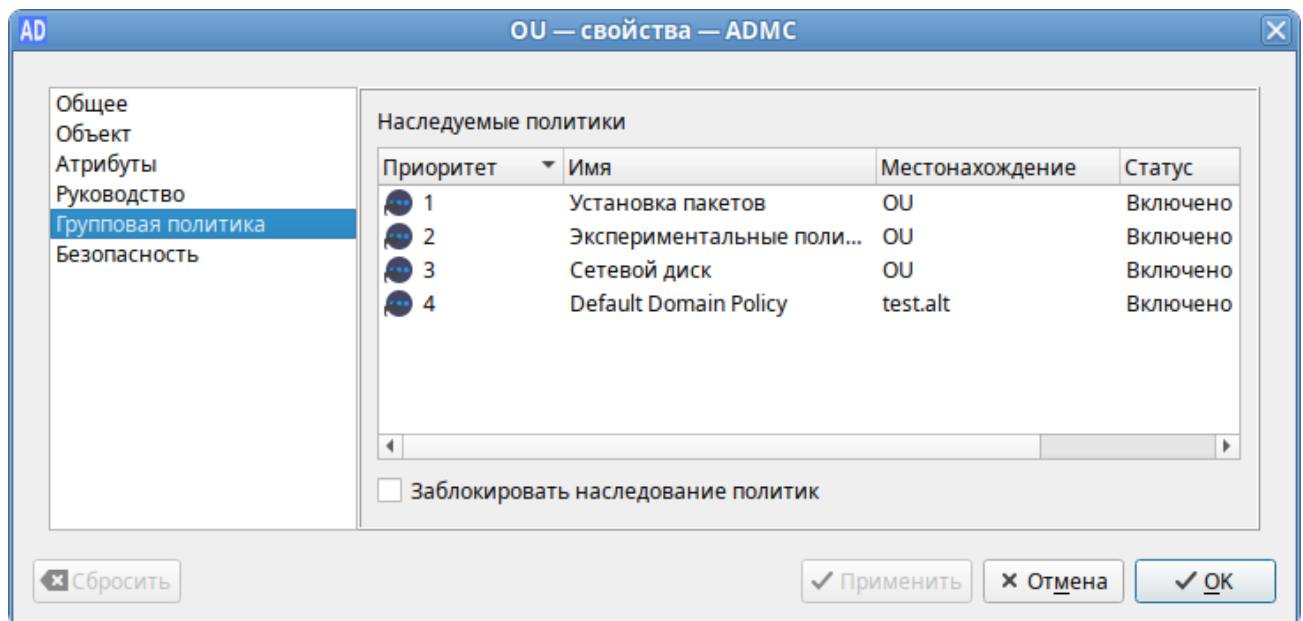


Рис. 242 – Статус групповых политик

Изменение статуса групповой политики возможно в свойствах на вкладке «Атрибуты» (рис. 243).

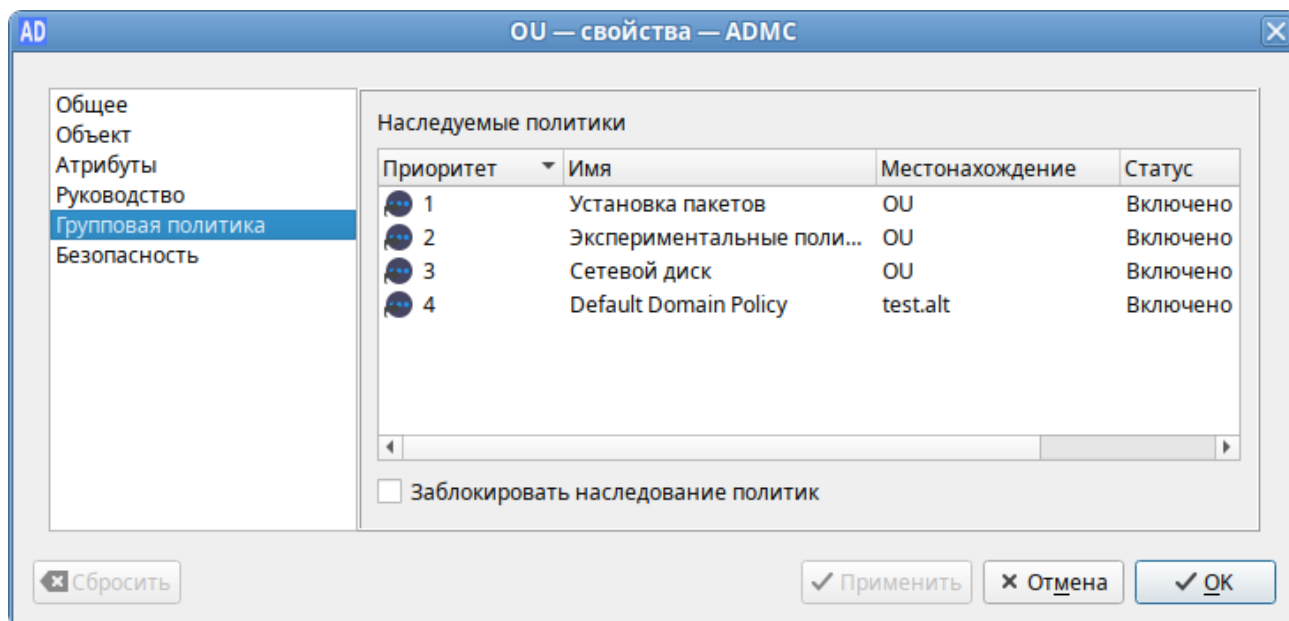


Рис. 243 – Атрибут «flags» в свойствах ГП

Состояние объекта групповой политики указывается в значении атрибута flags. Данный атрибут может принимать следующие значения:

- значение «0» – объект ГП включен (все настройки политики применяются к целевым объектам домена);
- значение «1» – отключен раздел «Конфигурация пользователя» (не применяются настройки пользовательских политик);
- значение «2» – отключен раздел «Конфигурация компьютера» (не применяются настройки из параметров ГП компьютера);
- значение «3» – объект ГП полностью отключен (все настройки политики не применяются).

4.8.2. 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 ADMS при выборе подразделения на вкладке «Наследуемые политики» (рис. 244).

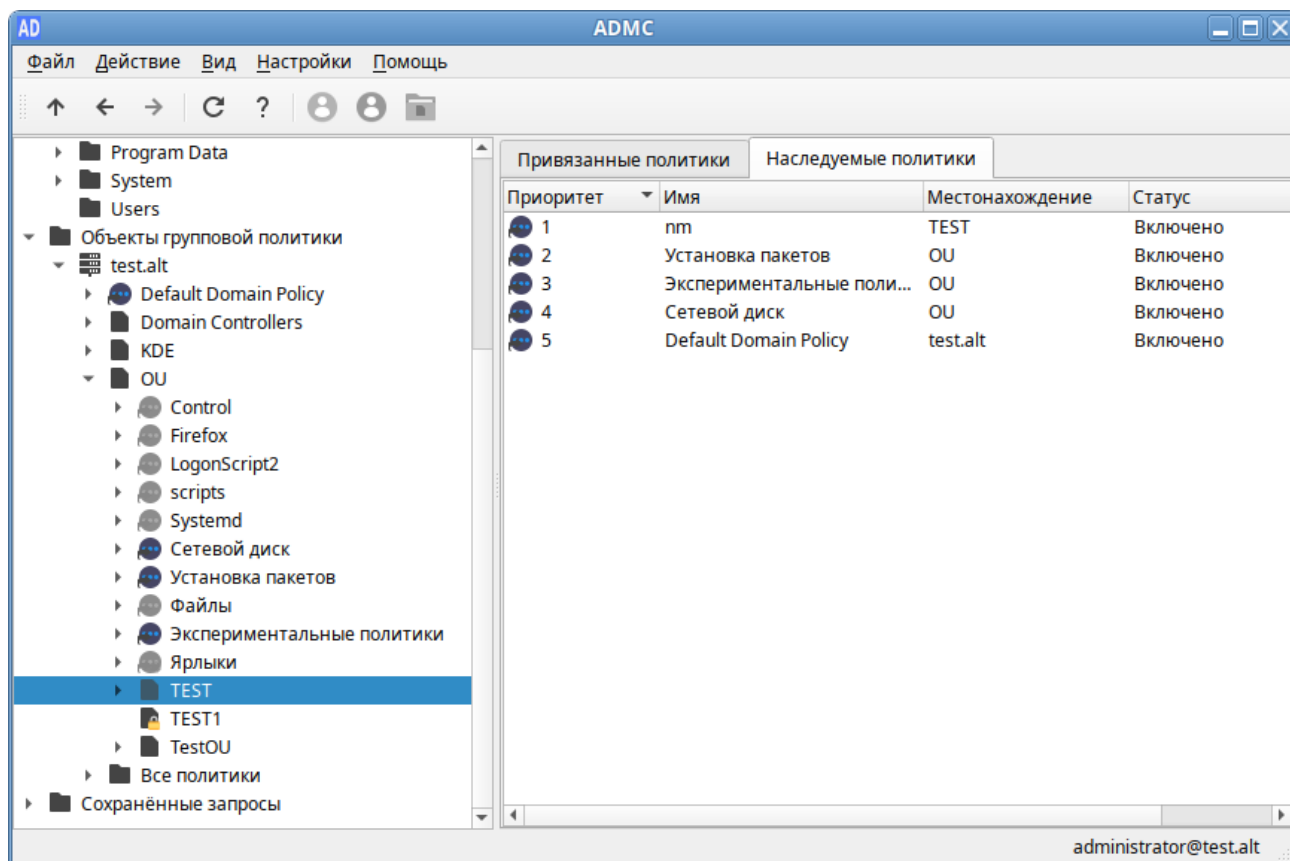


Рис. 244 – Политики подразделения без блокирования наследования

Также наследуемые политики можно увидеть на вкладке «Групповая политика» свойств подразделения (рис. 245).

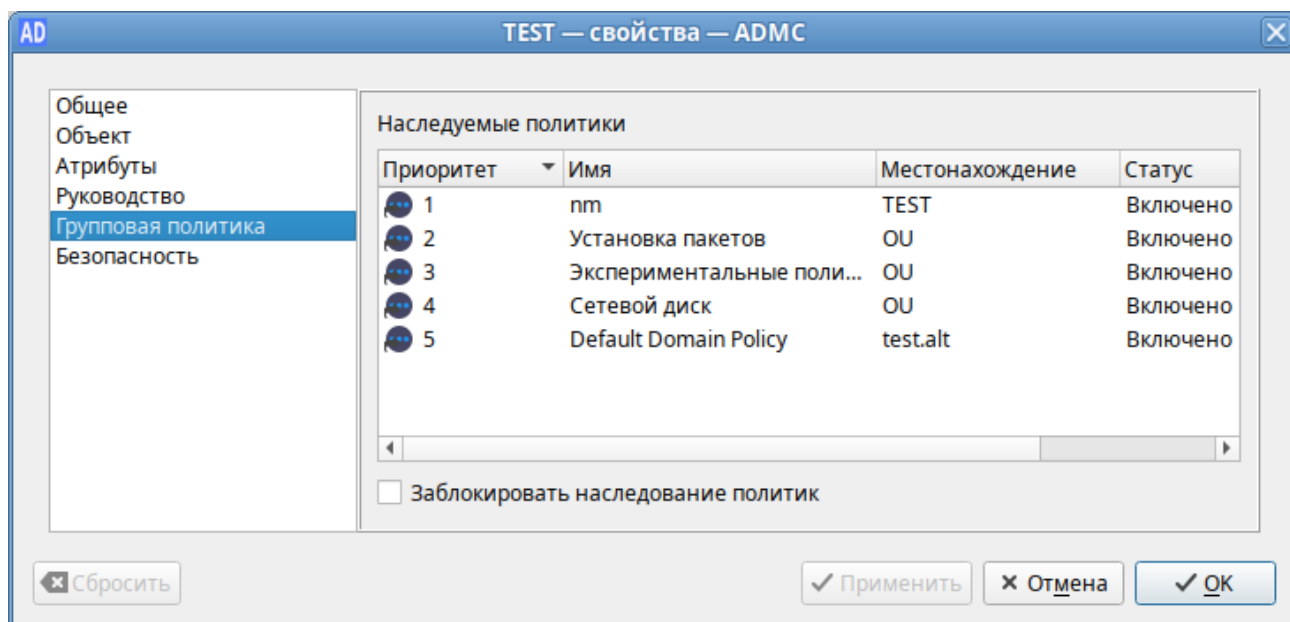


Рис. 245 – Вкладка «Групповая политика»

Каждый объект групповой политики можно настроить на блокирование наследования политик более высокого уровня (см. п. 4.5.12.3). 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 (рис. 246).

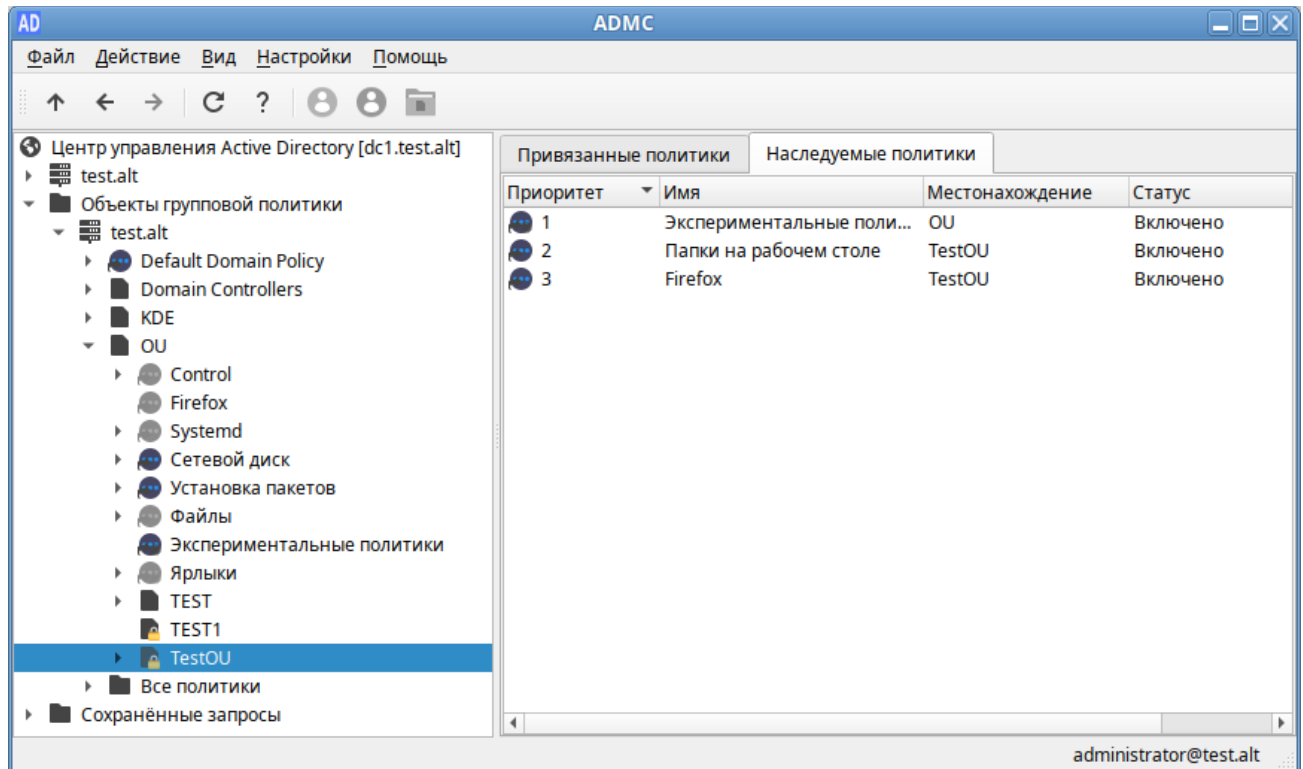


Рис. 246 – Политики подразделения с блокированием наследования

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».

4.8.3. 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 в наборе клиентских компонентов);

- объекты групповой политики, связанные с OU: сначала обрабатываются объекты групповой политики, связанные с OU, находящейся на самом высоком уровне в иерархии Active Directory, 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 «Альт Домен»).

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) (рис. 247).

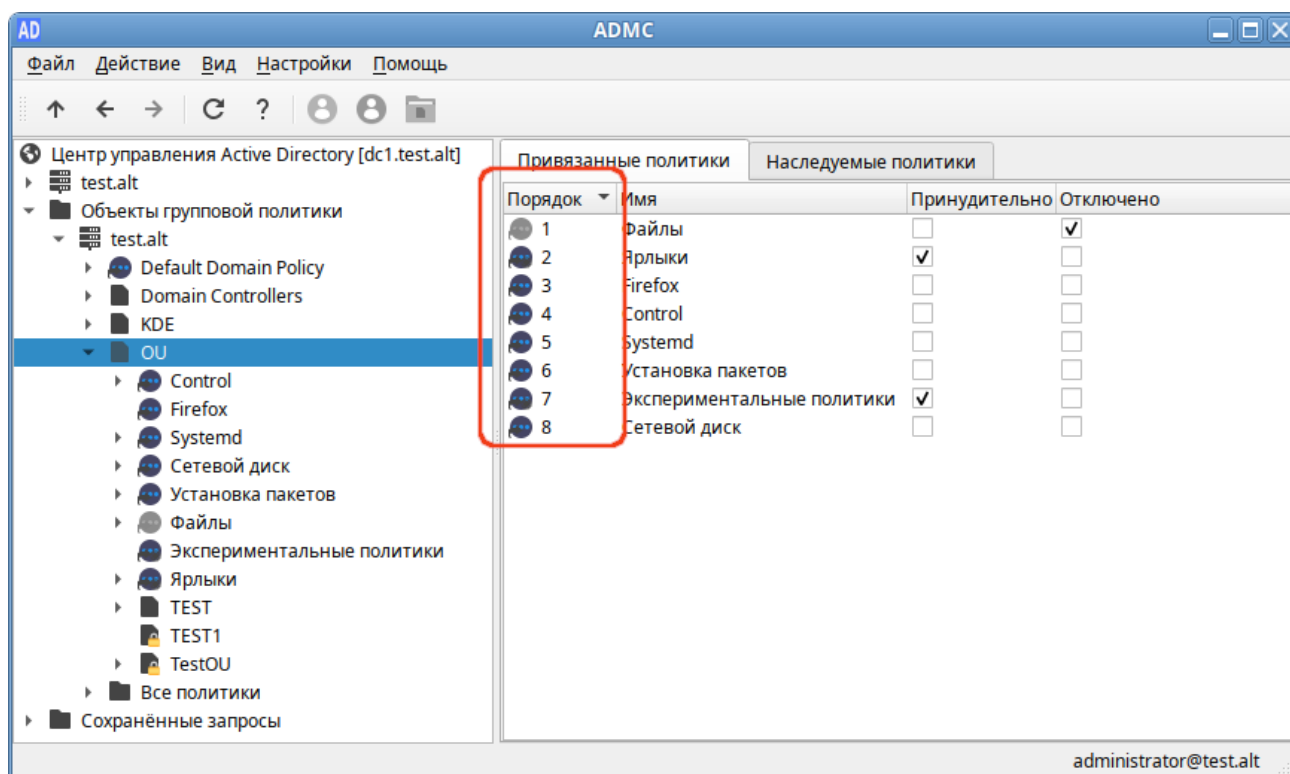


Рис. 247 – Порядок обработки групповых политик

При необходимости этот порядок можно изменить, выбрав в контекстном меню политики пункт «Переместить вверх» или «Переместить вниз» (рис. 248).

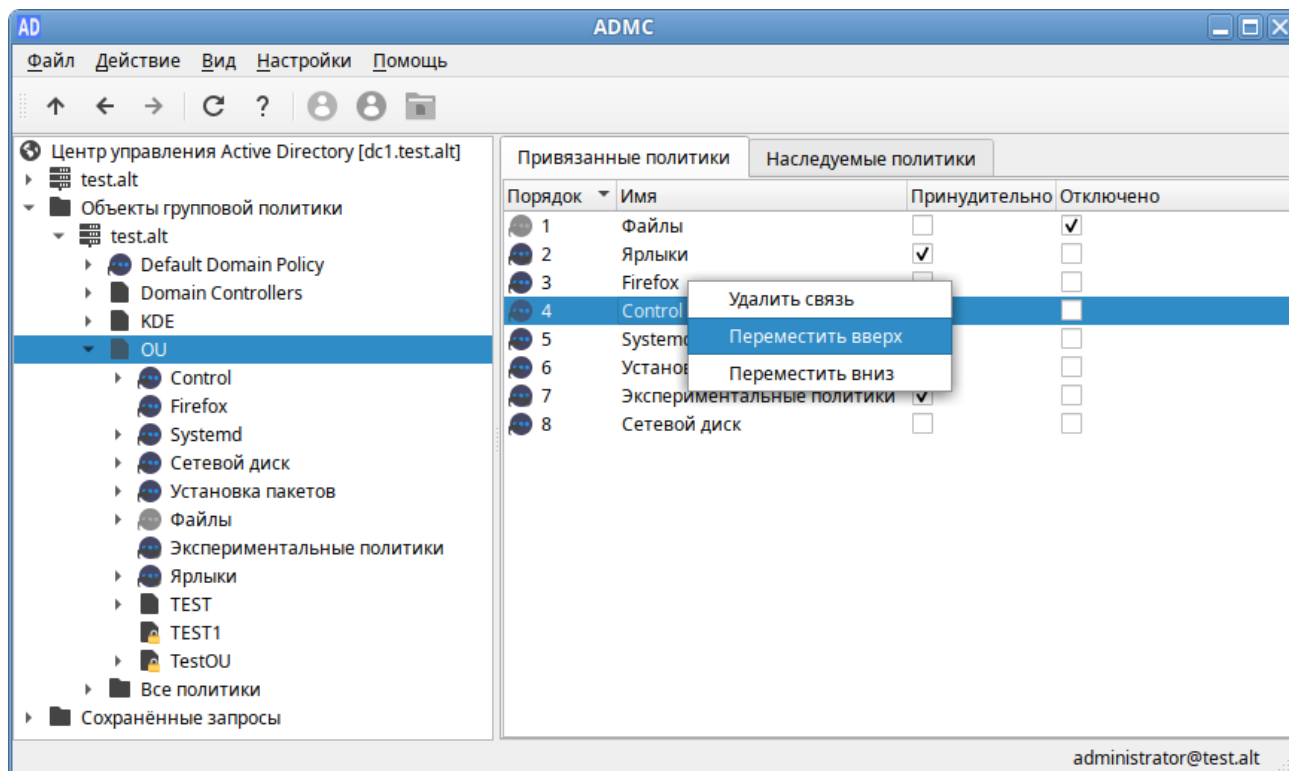


Рис. 248 – Изменение порядка обработки политики

При использовании параметра «Принудительно» у групповой политики выигрывает та политика, которая находится выше в иерархии домена, например, политика Default Domain Policy будет выигрывать у всех других групповых политик, если у нее активирован этот параметр.

У каждого объекта групповой политики, который привязан к организационному контейнеру домена 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 групповой политики не удаляется из иерархии. Активировать данную связь можно в любой момент.

4.8.4. 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 домене. В некоторых случаях может потребоваться применить к пользователям политику в зависимости от расположения объекта компьютера.

На компьютерах, расположенных в организационном подразделении (Organization Unit, 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 учетная 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 учетных записей пользователей и их локальные компьютеры, во втором – объекты серверов (рис. 249).

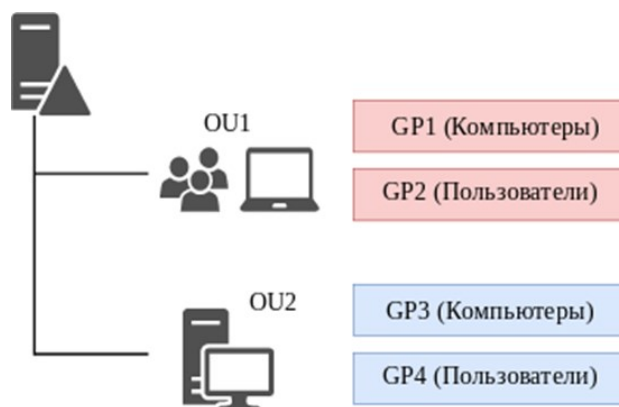


Рис. 249 – Схема деления домена

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. п. 4.8.4), 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.

4.8.5. Диагностика применения ГП на стороне клиента

Для диагностики применения групповых политик на стороне клиента используются утилиты gpoa (на машинах Альт), gpresult (на машинах Windows).

Для диагностики механизмов применения групповых политик на клиенте можно выполнить команды:

- 1) получить и применить настройки для текущей машины:

```
# gpoa --loglevel 0
```

- 2) получить и применить настройки для пользователя:

```
# gpoa --loglevel 0 <имя_пользователя>
```

4.8.6. Коды ошибок

Сообщения, сопутствующие кодам ошибок, могут изменяться (переводиться, исправляться), но сам код уникален для определенной части программы, что позволяет однозначно идентифицировать проблему (таблица 56).

Т а б л и ц а 56 – Коды ошибок и их описание

Код	Описание	Решение
E00001	Недостаточно прав для запуска программы <code>groupdate</code>	Необходимо повысить уровень привилегий. Может помочь запуск программы от имени администратора
E00002	Программа <code>groupdate</code> не будет запущена из-за предыдущих ошибок	
E00003	Ошибка работы бэкэнда, которая привела к досрочному прекращению обработки групповых политик. Этот код характеризует серьезные 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 <code>appliers</code> . С большой вероятностью может оказаться ошибкой в коде
E00005	Не получилось запустить <code>appliers</code> политик для обновления групповых политик компьютера	Проверить, что машина все еще в домене, демон <code>oddjobd</code> доступен через D-Bus и у пользователя достаточно прав для запуска ПО
E00006	Показать список доступных бэкэндов	Проверить, что машина все еще в домене, демон <code>oddjobd</code> 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 установку Samba на машине, убедиться, что машина введена в домен и домен доступен
E00008	Невозможно инициализировать бэкэнд <code>no-domain</code> для выполнения процедуры бутстрапа групповых политик	Возможно, было произведено вмешательство в локальную политику или произошел <code>misconfiguration</code> . Необходимо проверить целостность пакета <code>local-policy</code> и настройки домена в Alterator.
E00009	Произошла ошибка при попытке запуска <code>adp</code>	Необходимо обратиться к руководству по устранению неполадок проекта ADP
E00010	Произошел сбой при попытке получить имя домена Active Directory	Необходимо проверить работу доменной службы имен (DNS), а также доступность доменного LDAP. Для доступа к LDAP необходим работоспособный Kerberos, так что стоит проверить и его конфигурацию

Продолжение таблицы 56

Код	Описание	Решение
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	Запустить программу с правами администратора
E00014	Не прошла проверка наличия билета Kerberos. Билет Kerberos нужен для доступа к сервисам домена	Проверить конфигурацию Kerberos в файле /etc/krb5.conf. Попытаться получить билет Kerberos вручную
E00015	Запрос на получение имени домена Active Directory через LDAP не прошел	Проверить возможность получения Kerberos ticket для машины. Проверить работу DNS и возможность обратиться к доменному LDAP
E00016	Утилита wbinform не отдает SID для пользователя, для которого выполняется обновление групповых политик	Проверить целостность программы wbinform. 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. Также необходимо 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 groa для текущего пользователя	Следует удостовериться, что D-Bus работает корректно и демон oddjobd запущен.
E00022	Не был получен ответ от D-Bus при попытке запустить groa для машины	Необходимо удостовериться, что D-Bus работает корректно и демон oddjobd запущен

Продолжение таблицы 56

Код	Описание	Решение
E00023	Не был получен ответ от D-Bus при попытке запустить groa 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
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 подключенных 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)

Окончание таблицы 56

Код	Описание	Решение
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

4.8.7. Диагностика проблем при работе с политикой скриптов

На контроллере домена:

- 1) проверить работоспособность загружаемого скрипта в дистрибутиве ОС Альт СП;
- 2) убедиться, что кодировка файла со скриптом – UTF8, без BOM;
- 3) убедиться, что скрипт расположен в каталоге (GPT) применяемого объекта групповой политики (GPO);
- 4) убедиться, что включена групповая политика «Экспериментальные групповые политики» или политика «Управление logon-скриптами» (см. 4.6.6.3);
- 5) убедиться, что целевой компьютер, входит в подразделение (OU), к которому привязан объект групповой политики (GPO).

На компьютере пользователя:

- 1) проверить версию gpupdate (политики скриптов выполняются с релиза 0.9.11-alt1);
- 2) убедиться, что механизм применения политик (gpupdate) запущен:

```
# gpupdate-setup status
```

3) убедиться, что служба скриптов запущена:

```
# systemctl status gpupdate-scripts-run.service
```

4) проверить содержимое каталога и права для загруженных скриптов:

```
# ls -Rl /var/cache/gpupdate_scripts_cache/
```

5) проверить состояние службы запуска скриптов пользователя
(от пользователя):

```
$ systemctl --user status gpupdate-scripts-run-user.service
```

6) вывести журнал применения политик:

```
# gpoa --loglevel 0
```

5. ДОВЕРИТЕЛЬНЫЕ ОТНОШЕНИЯ (ТРАСТЫ)

Доверительные отношения (trusts) позволяют аутентифицироваться под пользователями не только текущего домена, но и доверенных.

5.1. Настройка доверия

5.1.1. Общие сведения

Доверительные отношения (рис. 250) 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.

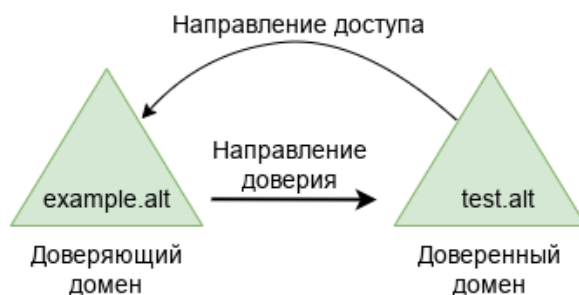


Рис. 250 – Схема доверительных отношений в рамках механизма аутентификации

Отношения доверия обеспечивают доступ к ресурсам в одном или двух направлениях:

- одностороннее доверие – 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 – 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) – связывает леса и все их домены (это двухсторонние или односторонние отношения доверия между разными лесами, всегда являющиеся транзитивными);
- внешнее доверие (External) – устанавливается между двумя доменами напрямую вне леса (для установки двухстороннего доверия нужно использовать два разнонаправленных доверия, которыми надо связать все требуемые пары доменов).

5.1.2. Особенности доверительных отношений в Samba

Поддерживается:

- доверие леса (это доверие может быть установленным между двумя Samba-доменами или Samba-доменом и Windows-доменом);
- внешние доверительные отношения между доменом AD и доменом в стиле NT;
- добавление пользователей и групп доверенного домена в группы доверяющего домена (при этом необходимо использовать SID пользователей и групп, имя пользователя или имя группы использовать невозможно);
- в RSAT можно увидеть foreignSecurityPrincipal для всех добавленных пользователей и групп из доверенного домена.

Особенности и ограничения:

- не применяются правила фильтрации SID;
- нельзя добавить пользователей и группы доверенного домена в доменные группы доверяющего домена по имени;

- для входа в доверенный домен через SSSD надо использовать тип связи External, а не Forest;
- обе стороны траста должны полностью доверять друг другу (администратор из домена А может управлять всеми объектами в домене Б и наоборот);
- не поддерживается выборочная аутентификация;
- нельзя создать доверительные отношения между доменами в одном дереве с одним и тем же пространством имен 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).

Для управления доверием можно использовать инструмент командной строки samba-tool (таблица 57).

Т а б л и ц а 57 – 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 (если --type=external по умолчанию yes, если --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	

Окончание таблицы 57

Команда	Описание	Примечание
domain trust validate <домен>	Проверить доверие к домену	Можно использовать следующие опции: --validate-location=LOCATION – проверить объект доверенного домена (local, both); -U USERNAME – имя пользователя

5.2. Настройка DNS

Перед настройкой доверия необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена.

5.2.1. Два домена Samba

Доменные имена, относящиеся к версии Samba, представлены в таблице 58.

Т а б л и ц а 58 – Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	192.168.0.132	ALT Server SP	4.19.7
EXAMPLE.ALT	s1.example.alt	192.168.0.172	ALT Server SP	4.19.7

5.2.1.1. Настройка переадресации DNS на DC с BIND9_DLZ

Если используется dns_backend BIND9_DLZ, 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 удаленный DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить 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
```

5.2.1.2. Настройка переадресации DNS на DC с SAMBA_INTERNAL

Если используется DC с `dns_backend 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`:

- отключить проверку DNSSEC, для этого в секцию `options` добавить параметр:

```
dnssec-validation no;
```

- в конец файла 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
```

5.2.1.3. 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
25.04.2023          15:38:17           26.04.2023          01:38:17
krbtgt/EXAMPLE.ALT@EXAMPLE.ALT
renew until 26.04.2023 15:38:14
```

- 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
25.04.2023          15:17:50           26.04.2023          01:17:50
krbtgt/TEST.ALT@TEST.ALT
renew until 26.04.2023 15:17:46
```

ВАЖНО

realm должен быть записан заглавными буквами.

5.2.2. Samba DC и Windows Server с AD

Исходные данные Samba DC и Windows Server с AD представлены в таблице 59.

Т а б л и ц а 59 – Исходные данные

Имя домена	Контроллер домена	IP-адрес	ОС контроллера домена	Версия Samba
TEST.ALT	dc1.test.alt	192.168.0.132	ALT Server SP	4.19.7
WIN.ALT	DC1.win.alt	192.168.0.190	Windows Server 2012	

5.2.2.1. 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 (рис. 251);
- 3) сохранить настройки.

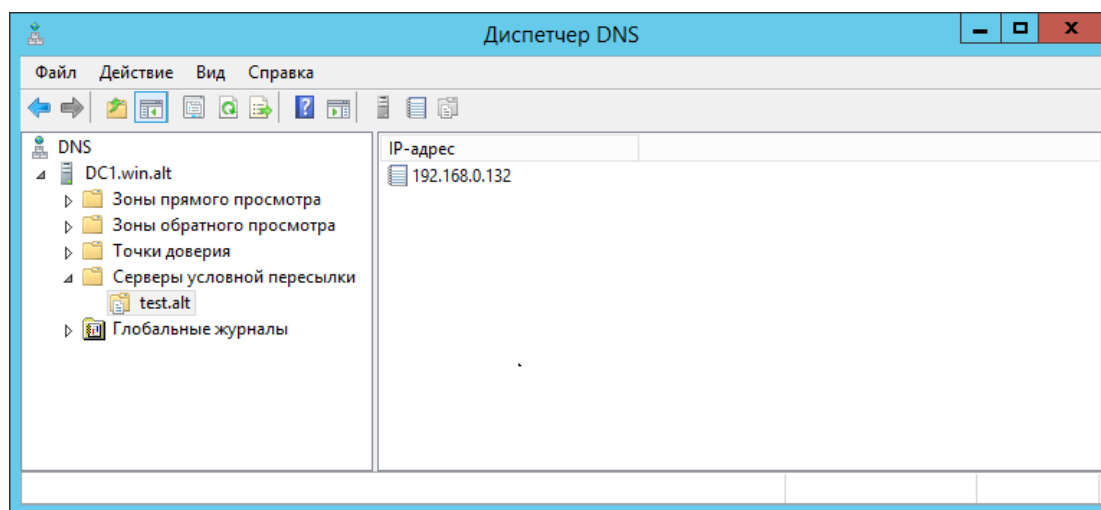


Рис. 251 – Окно «Диспетчер DNS»

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
```

5.2.2.2. Samba DC с BIND9_DLZ

Если используется `dns_backend 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 удаленный DNS-сервер не использует DNSSEC и включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить 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
```

5.2.2.3. Samba DC с SAMBA_INTERNAL

Если используется DC с `dns_backend 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 сервере bind9 отредактировать файл /etc/bind/options.conf:

- 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; };
};
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

5.2.2.4. 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
...
```

5.3. Создание двухстороннего транзитивного подключения

5.3.1. Два домена Samba

На контроллере домена dc1.test.alt:

```
# 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 sl.example.alt:

```
[root@sl ~]# 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] TD0[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 домена 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[\\sl.example.alt] CONNECTION[WERR_OK]
TRUST[WERR_OK] VERIFY_STATUS_RETURNED
OK: LocalRediscover: DC[\\sl.example.alt] CONNECTION[WERR_OK]
RemoteDC      Netbios[S1]           DNS[sl.example.alt]
ServerType[PDC,GC,LDAP,DS,KDC,TIMESERV,CLOSEST,WRITABLE,GOOD_TIME
SERV,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]
```


5.3.2. Samba DC и Windows Server с AD

Настройка на стороне Windows:

- 1) открыть «Диспетчер серверов», выбрать «Средства» → «Active Directory – домены и доверие» (рис. 252);

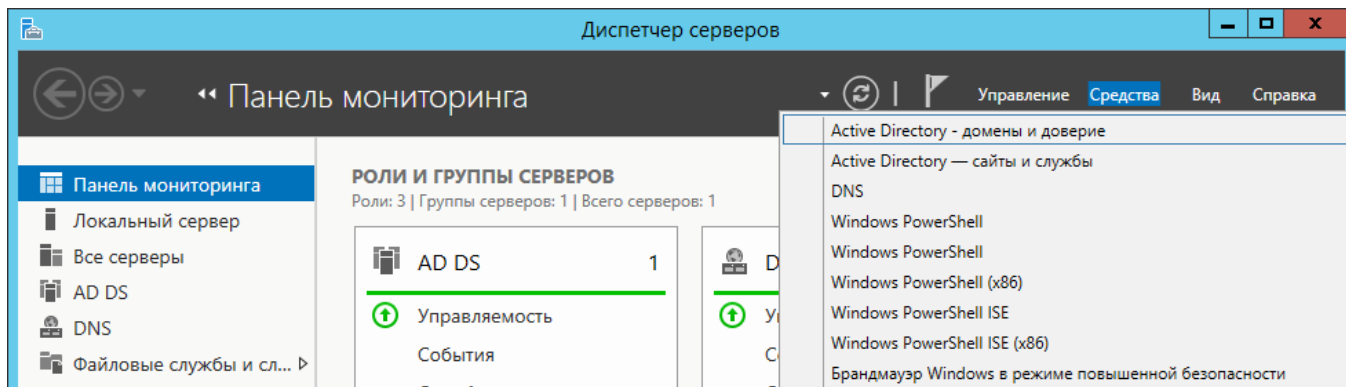


Рис. 252 – Окно «Диспетчер серверов»

- 2) в открывшемся окне в контекстном меню домена выбрать пункт «Свойства» (рис. 253);

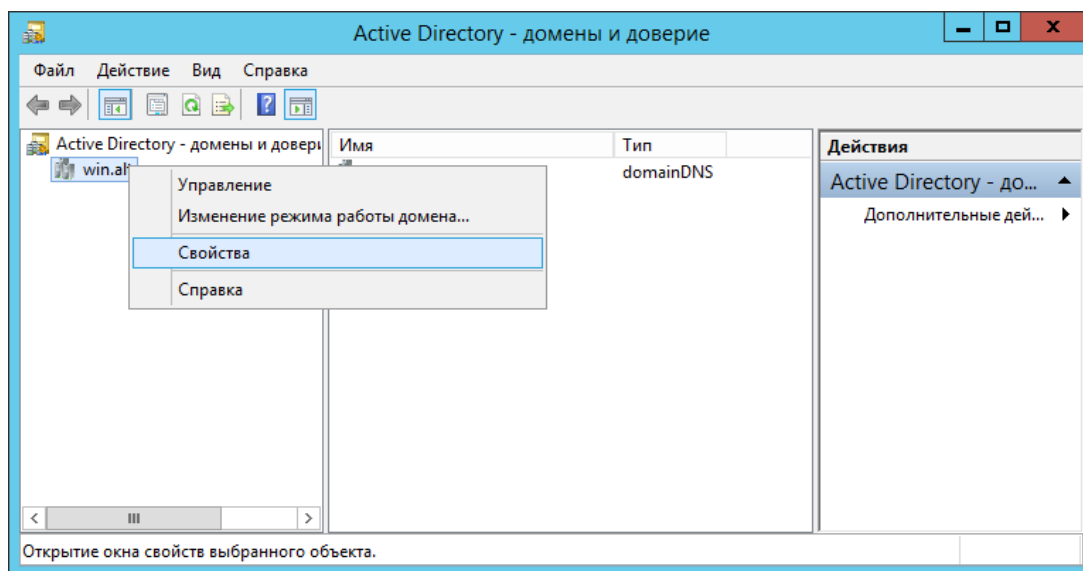


Рис. 253 – Окно «Active Directory – домены и доверие»

- 3) откроется окно свойств домена. Необходимо перейти во вкладку «Отношения доверия» и нажать кнопку «Создать отношение доверия...» (рис. 254);

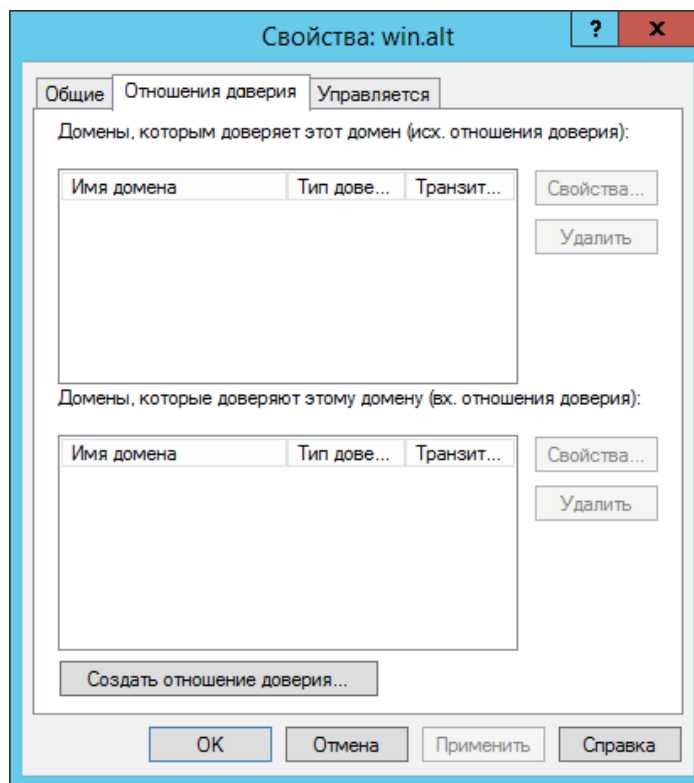


Рис. 254 – Окно свойств домена

4) будет запущен «Мастер создания отношения доверия» (рис. 255);

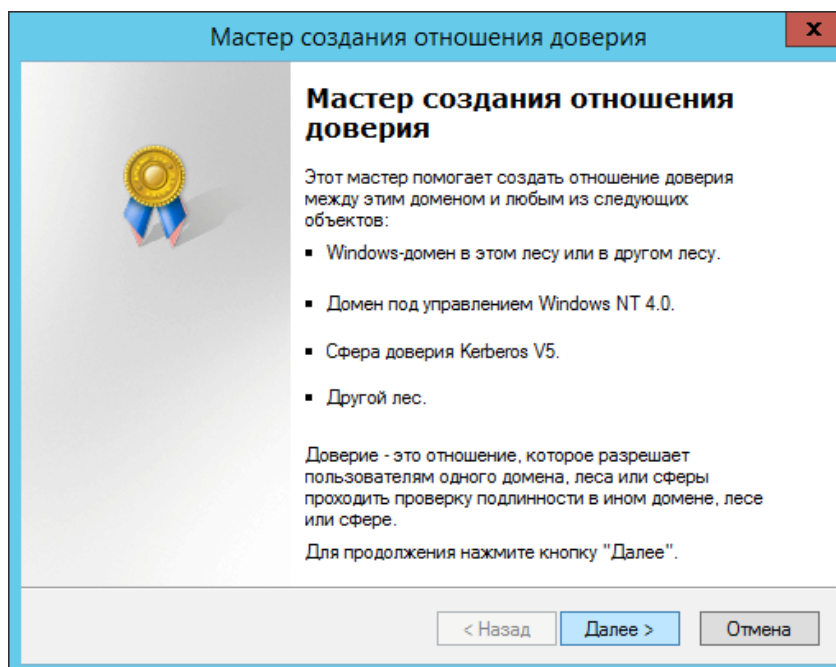


Рис. 255 – Окно «Мастер создания отношения доверия»

- 5) на втором шаге создания отношения доверия необходимо ввести имя домена Samba DC (в примере TEST.ALT) (рис. 256);

The screenshot shows a Windows XP-style window titled 'Мастер создания отношения доверия' (Master of creating trust relationship). The window has a blue title bar with a close button (X) in the top right corner. The main content area has a light blue header with the text 'Имя отношения доверия' (Trust relationship name) and a sub-header 'Вы можете создать отношение доверия с помощью NetBIOS- или DNS-имени.' (You can create a trust relationship using NetBIOS or DNS name). Below this, there is a text box for entering the name, with the example 'test.alt' entered. To the right of the text box is a gold medal icon with a blue ribbon. At the bottom of the window, there are three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel).

Рис. 256 – Окно ввода имени домена Samba DC

- 6) на следующем шаге следует выбрать тип доверия (рис. 257);

The screenshot shows the same 'Мастер создания отношения доверия' window, but at a different step. The header now says 'Тип доверия' (Type of trust relationship). The sub-header reads 'Этот домен является корневым доменом леса. Если указанный домен квалифицирован, можно создать доверие леса.' (This domain is the root domain of the forest. If the specified domain is qualified, you can create a forest trust). Below this, there is a text box for selecting the type of trust relationship. Two radio buttons are visible: 'Внешнее доверие' (External trust) and 'Доверие леса' (Forest trust). The 'Доверие леса' option is selected. To the right of the text box is a gold medal icon with a blue ribbon. At the bottom of the window, there are three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel).

Рис. 257 – Окно выбора типа доверия

7) далее выбирается направление доверия (рис. 258);

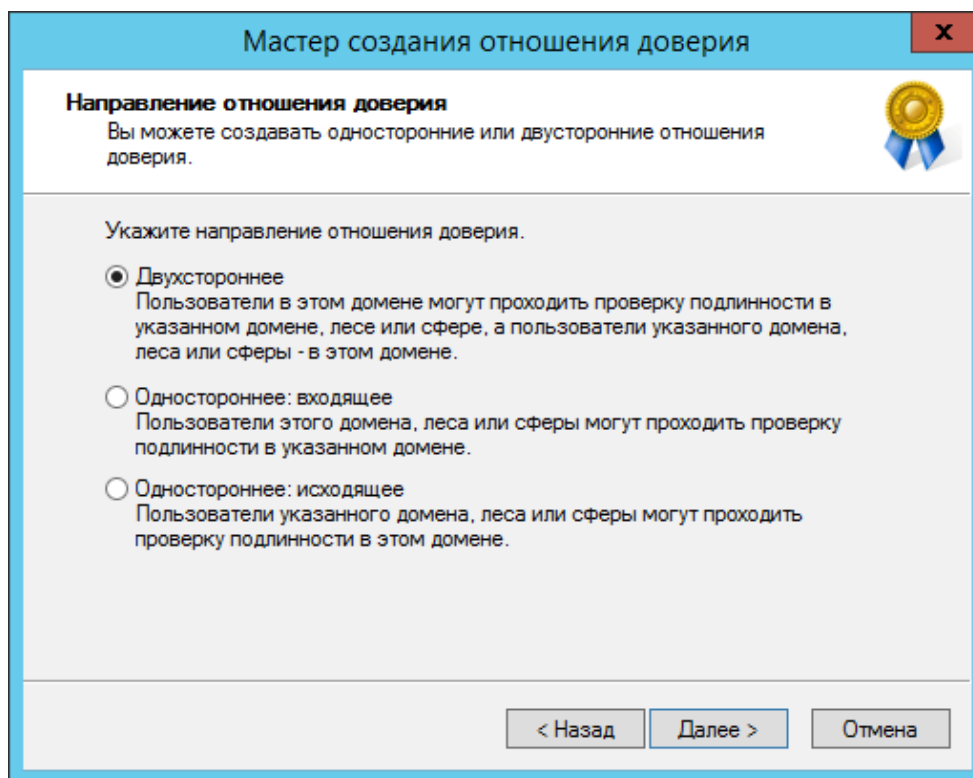


Рис. 258 – Окно выбора направления доверия

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» (рис. 259);

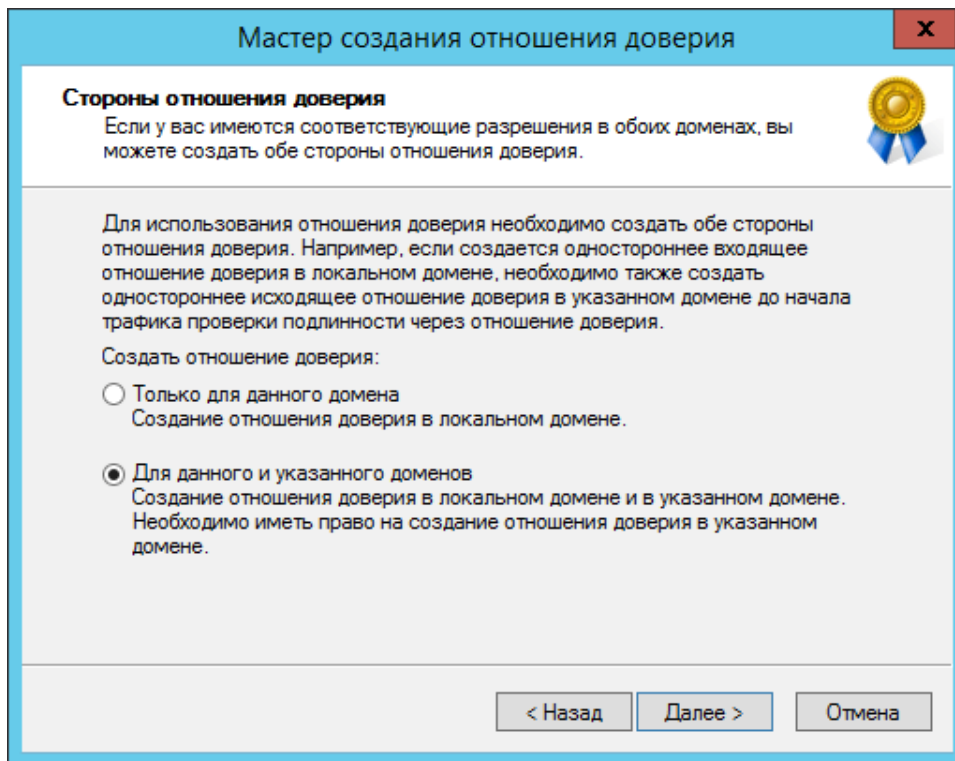


Рис. 259 – Стороны отношения доверия

Примечание. Если выбрать параметр «Только для данного домена» (рис. 260), необходимо задать «Пароль отношения доверия» (Trust Secret Key), который в дальнейшем будет использоваться при создании доверительного отношения на стороне Samba DC (рис. 261).

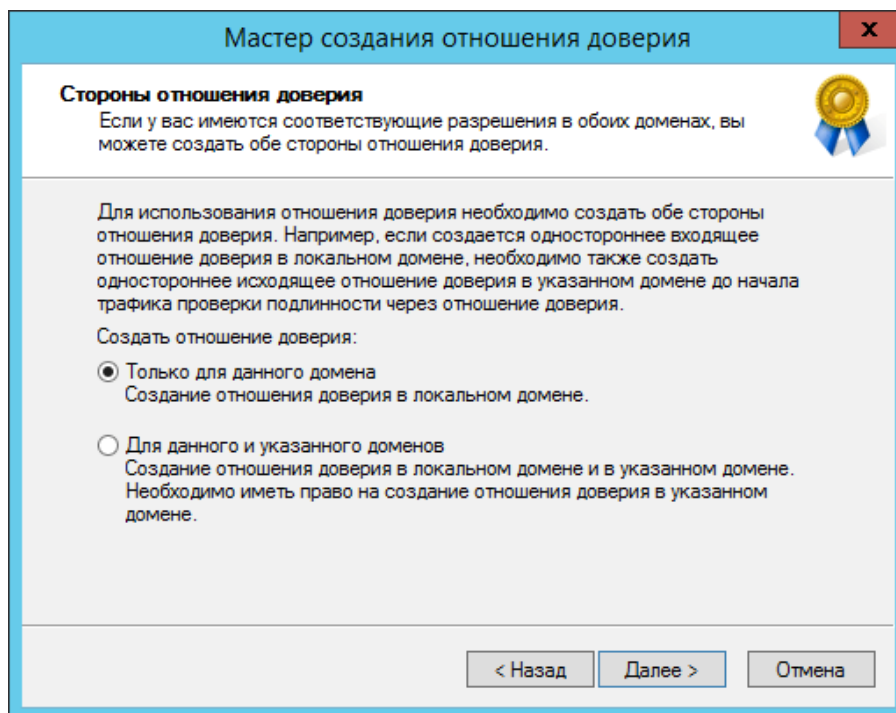


Рис. 260 – Стороны отношения доверия «Только для данного домена»

The screenshot shows a Windows XP-style window titled "Мастер создания отношения доверия" (Master of creating trust relationship). The window has a blue title bar with a close button (X) in the top right corner. Below the title bar, there is a header section with the title "Пароль отношения доверия" (Trust relationship password) and a gold medal icon. The main text explains that passwords are used by Active Directory controllers to confirm trust relationships. Below this, there are two text boxes: "Пароль отношения доверия:" (Trust relationship password:) and "Подтверждение пароля отношения доверия:" (Confirm trust relationship password:). Both boxes contain masked characters (dots). At the bottom of the window, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рис. 261 – Окно «Пароль отношения доверия»

- 9) на следующем этапе мастер свяжется с удаленным доменом (если он доступен), и запросит имя и пароль пользователя с правами установки доверительных отношений в домене (рис. 262);

The screenshot shows the same "Мастер создания отношения доверия" window, but at a different step. The header section now has the title "Имя и пароль пользователя" (User name and password) and a gold medal icon. The main text states that to create a trust relationship, administrative rights are needed. Below this, it says "Указанный домен: test.alt" (Specified domain: test.alt). Then, it asks to enter the name and password of a user with administrative rights. There are two input fields: "Пользователь:" (User:) with a dropdown menu showing "administrator" and a user icon, and "Пароль:" (Password:) with masked characters. At the bottom, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рис. 262 – Окно ввода имени пользователя и пароля

- 10) далее на шаге «Уровень проверки подлинности исходящего доверия – Локальный лес» следует выбрать «Проверка подлинности в лесу» (рис. 263);

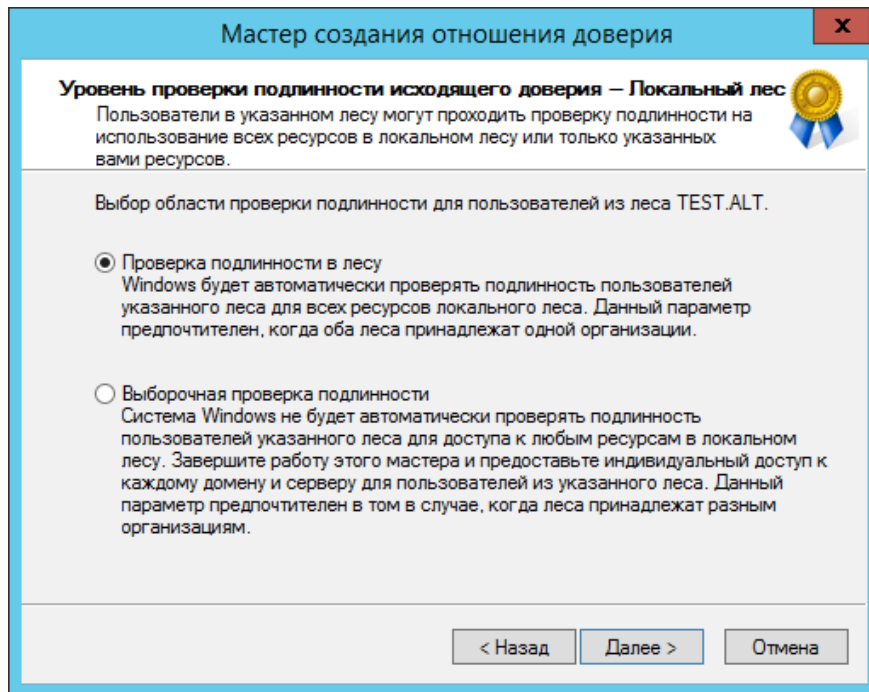


Рис. 263 – Окно выбора области проверки подлинности

- 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 (рис. 264);

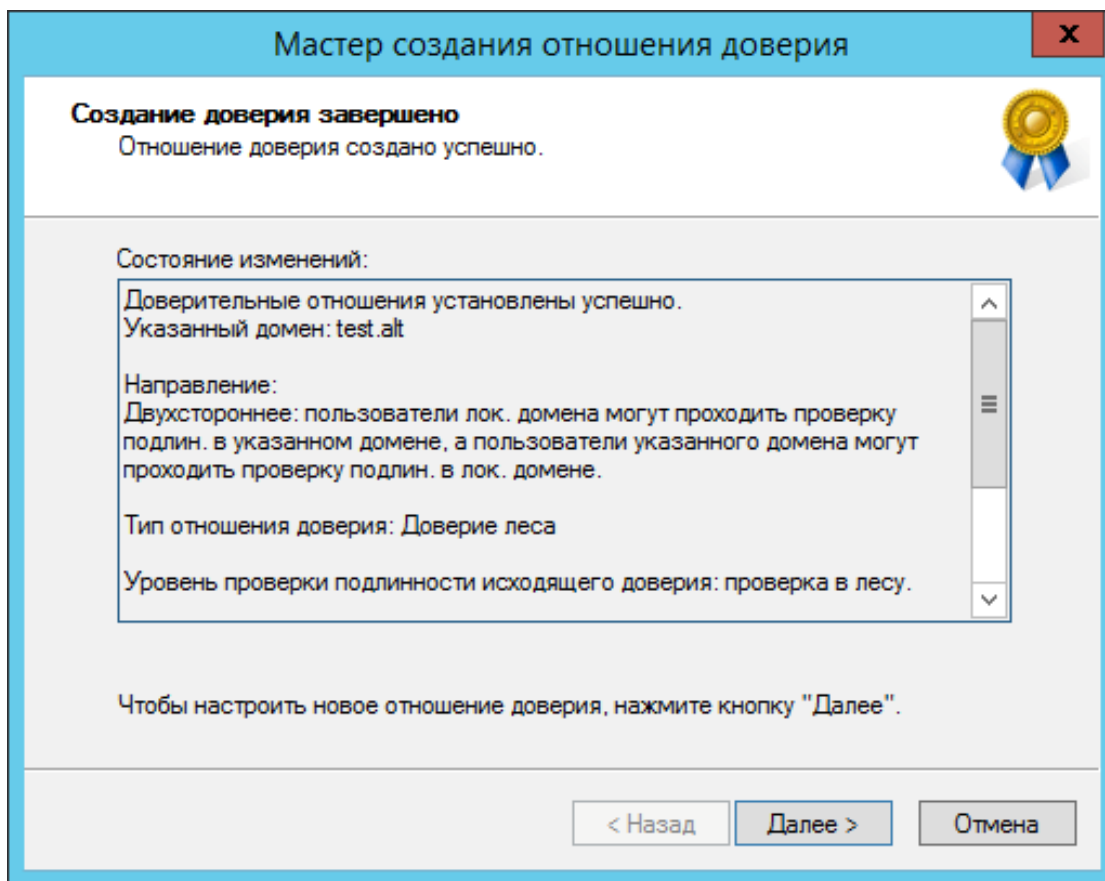


Рис. 264 – Окно «Создание доверия завершено»

- 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 доверия», так как на стороне Samba DC доверие еще не создавалось (рис. 265).

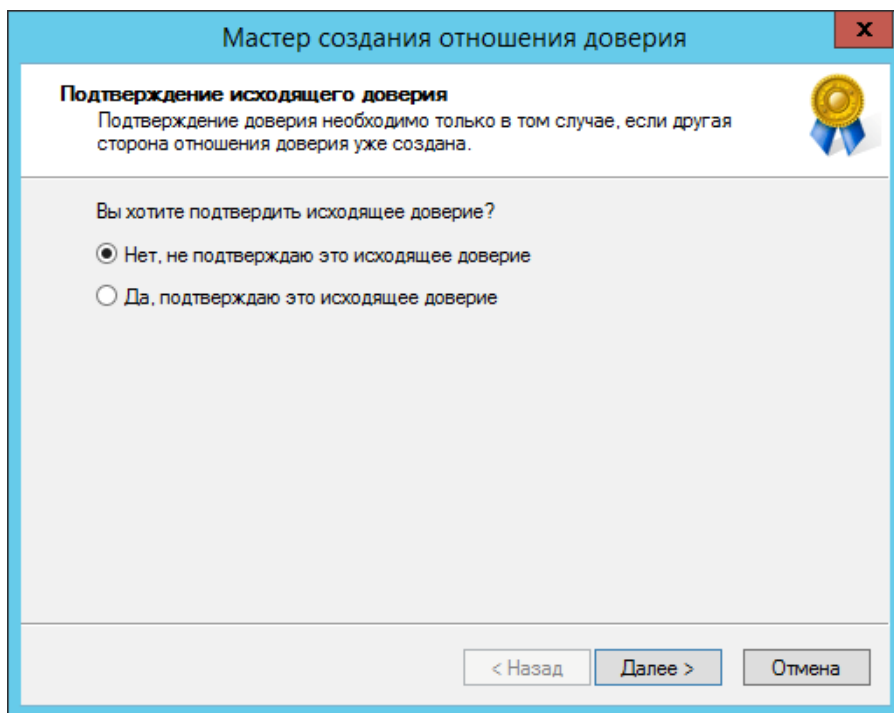


Рис. 265 – Окно подтверждения доверия

В результате будут получены двухсторонние доверительные отношения между доменами (рис. 266).

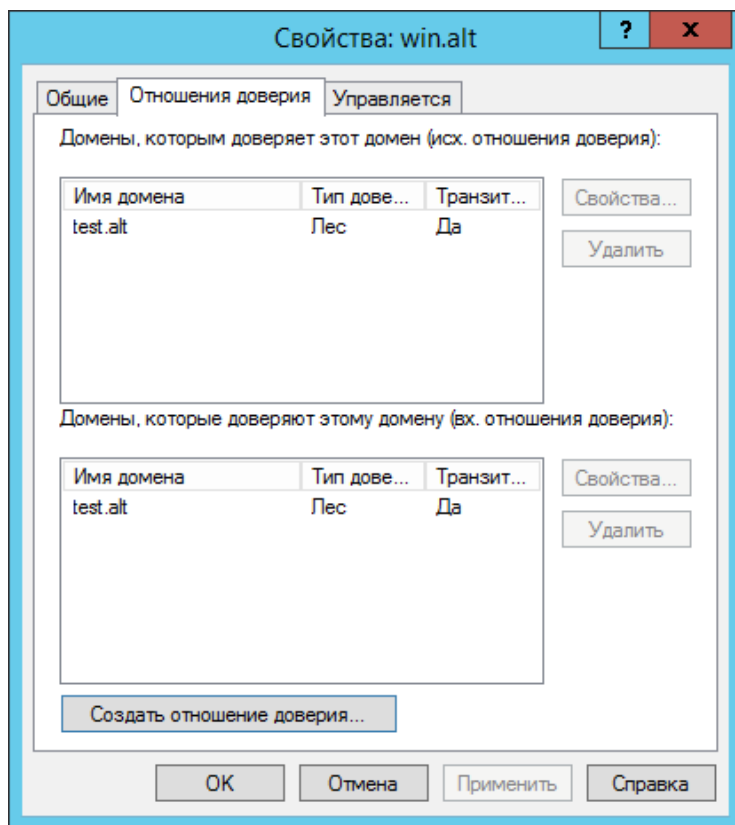


Рис. 266 – Окно установленных доверительных отношения между доменами

На стороне Samba DC для создания доверия необходимо выполнить команду:

```
# samba-tool domain trust create win.alt --type=forest \
--direction=both --create-location=both -Uadministrator@WIN
```

ВАЖНО

Для входа в доверенный домен через SSSD надо использовать тип связи external, а не forest.

При появлении запроса введите пароль администратора.

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_TIME
SERV,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[WERR_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, 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 домена 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_TIME
SERV,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]

```

5.4. Управление пользователями и группами

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.

5.4.1. 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:

- 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://sl -Uadministrator@EXAMPLE.ALT
Password for [administrator@EXAMPLE.ALT]:
dns-sl
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 примере команды выполняются на контроллере домена `dc1.test.alt`):

```
# wbinfo --all-domains
BUILTIN
TEST
EXAMPLE

# wbinfo --own-domain
TEST

# wbinfo --trusted-domains
BUILTIN
TEST
EXAMPLE

# 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
```

5.4.2. 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
```

5.4.3. Просмотр доверия в Windows

Модуль RSAT (см. п. 4.2.3) «Active Directory – домены и доверие» (Active Directory – Domain and Trusts) позволяет проверить состояние отношений доверия между доменами (рис. 267).

В модуле RSAT «Active Directory – пользователи и компьютеры» (Active Directory – Users and Computers) можно просмотреть список пользователей группы (рис. 268).

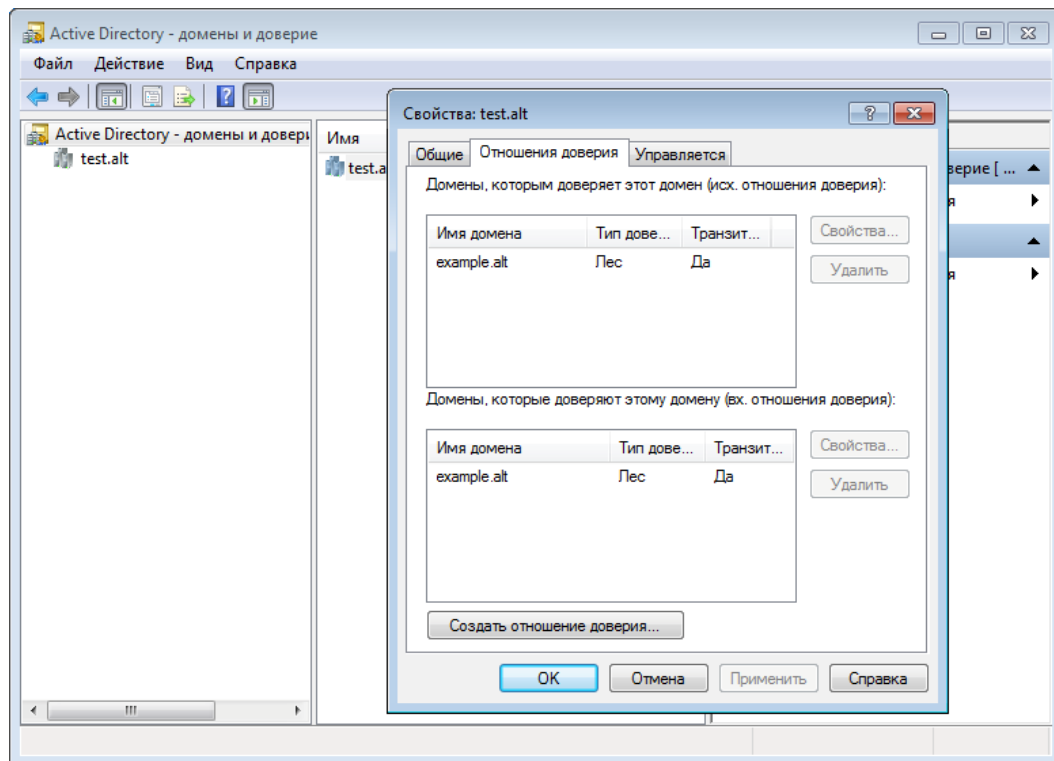


Рис. 267 – Модуль RSAT «Active Directory – домены и доверие»

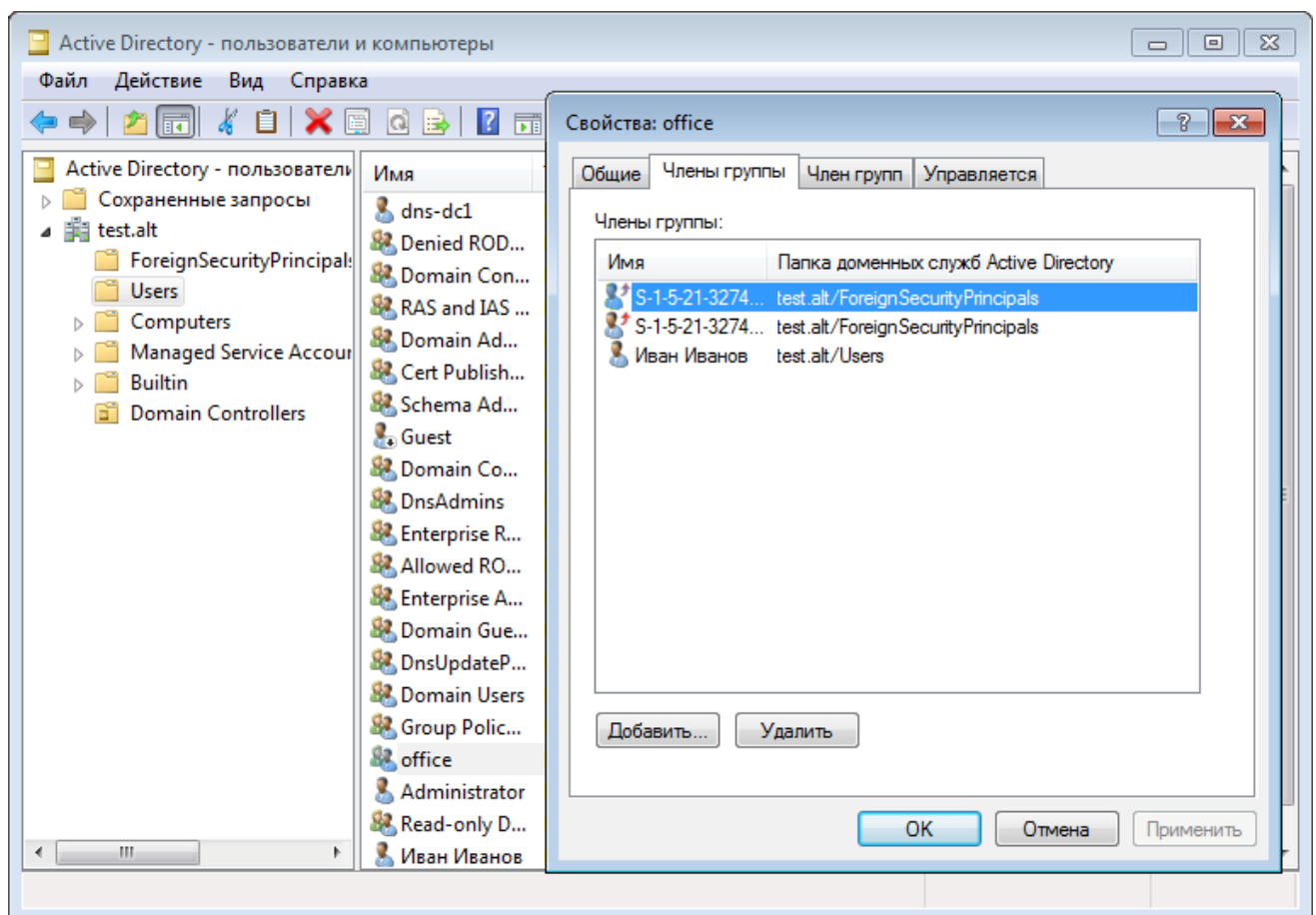


Рис. 268 – Модуль RSAT «Active Directory – пользователи и компьютеры»

5.5. Использование трастов на LINUX-клиентах

Если необходимо использовать пользователей из обоих доменов (установлены двухсторонние доверительные отношения с типом связи Лес), то рабочую станцию с ОС Альт СП следует вводить в домен через winbind (см. п. 3.3.3).

5.5.1. Настройка winbind

На машине, введенной в домен, необходимо в файле `smb.conf` установить ID-маппинг для обоих доменов (`backend = rid/tdb`).

Пример файла `smb.conf` на машине, введенной 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 = 10000-20000000
    idmap config * : backend = tdb

    idmap config EXAMPLE : backend = rid
    idmap config EXAMPLE : range = 10000-20000000
    idmap config TEST : backend = rid
    idmap config TEST : range = 10000-20000000
```

После перезапуска `smbd`, `nmbd`, `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
```

```
# 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)
```

Проверка с помощью getent:

```
# getent group TEST\\office
TEST\office*:11107:
```

```
# getent group EXAMPLE\\office2
office2*:11107:
```

```
# getent passwd TEST\\ivanov
TEST\ivanov*:11105:10513::/home/EXAMPLE.ALT/ivanov:/bin/bash
```

```
# getent passwd EXAMPLE\\kim
kim*:10000:10001:Олег Ким:/home/EXAMPLE.ALT/kim:/bin/bash
```

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.
```

Для авторизации в доверенном домене следует вводить учетные данные пользователя в формате DOMAIN\user.

5.5.2. Настройка SSSD

На машине, введенной в домен, необходимо в файл /etc/sss/sss.conf добавить доверенный домен:

```
[domain/EXAMPLE.ALT/TEST.ALT]
use_fully_qualified_names = false
```

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
```

5.6. Удаление доверия

5.6.1. 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
```

5.6.2. На стороне Windows Server с AD

Удаление доверия:

- 1) открыть «Диспетчер серверов», выбрать «Средства» → «Active Directory – домены и доверие» (рис. 269);

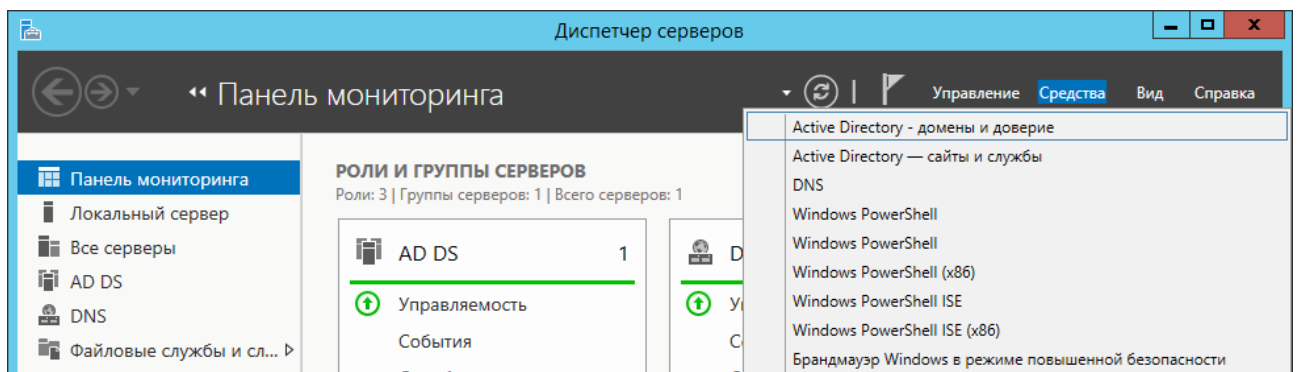


Рис. 269 – Окно «Диспетчер серверов»

- 2) в открывшемся окне в контекстном меню домена выбрать пункт «Свойства» (рис. 270);

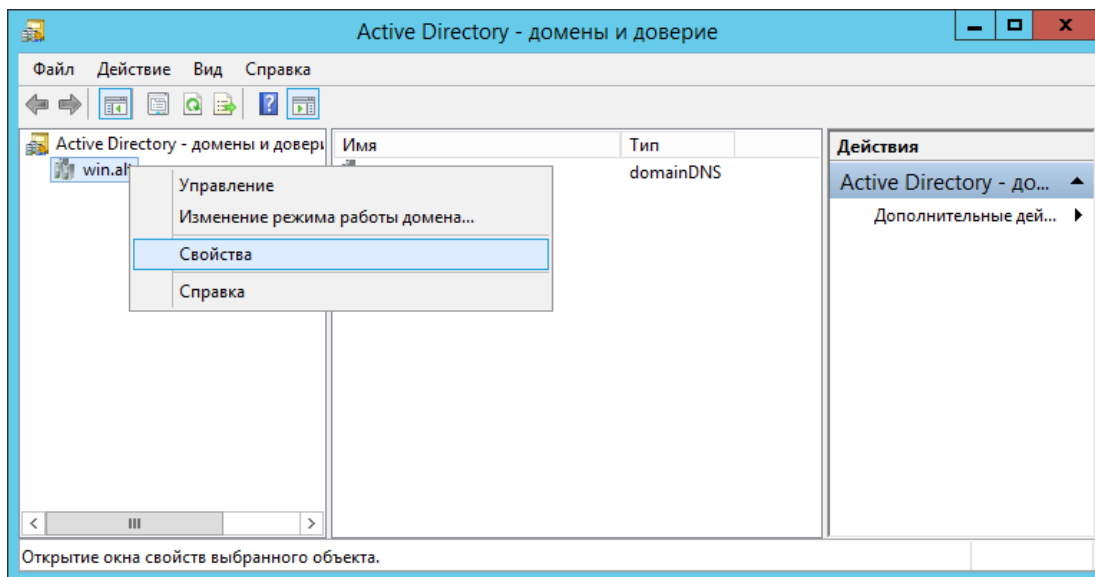


Рис. 270 – Окно «Active Directory – домены и доверие»

- 3) откроется окно свойств домена. Необходимо перейти во вкладку «Отношения доверия» и нажать кнопку «Создать отношение доверия...» (рис. 271);

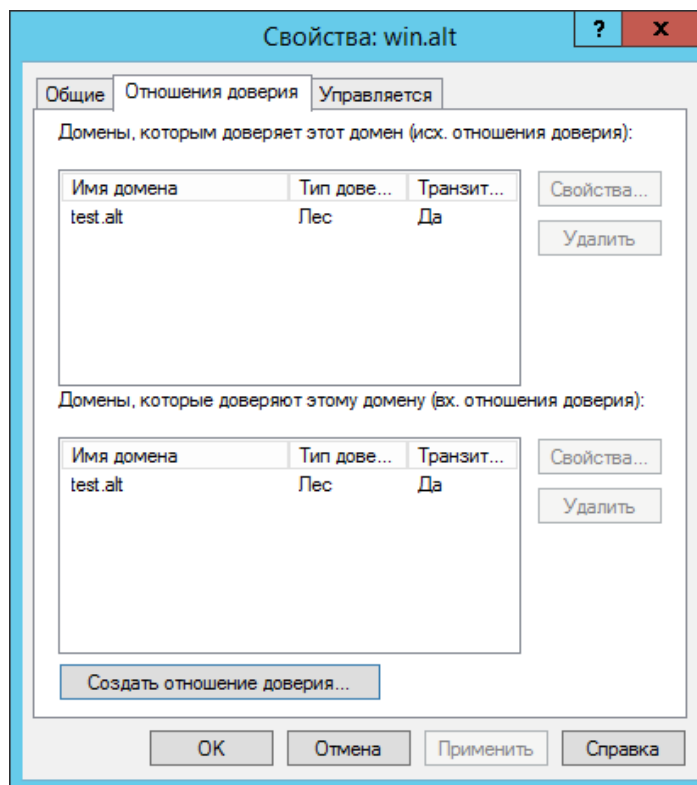


Рис. 271 – Вкладка «Отношения доверия»

- 4) 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»;
- 5) в открывшемся окне выбрать пункт, где нужно удалить доверие, и нажать кнопку «ОК» (рис. 272).

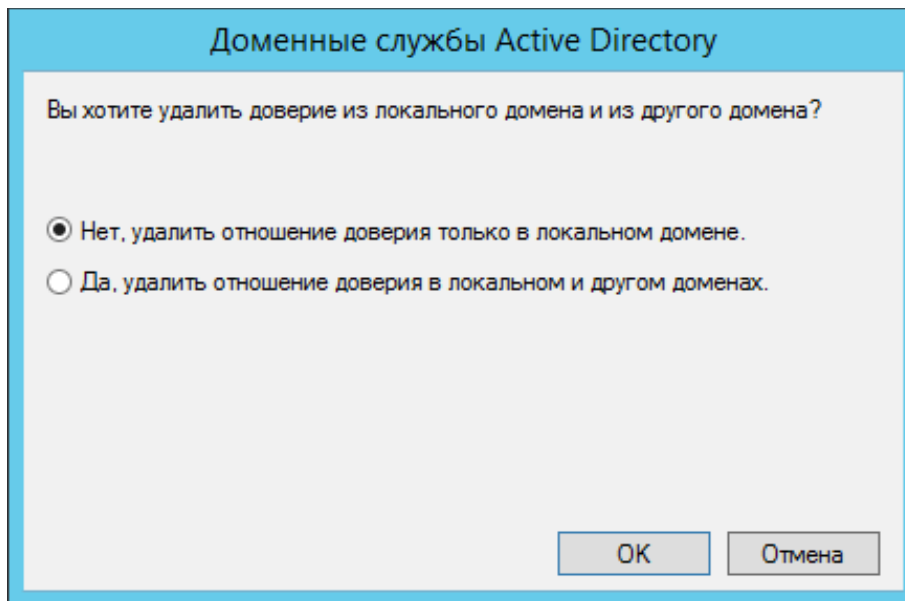


Рис. 272 – Окно выбора пункта удаления доверия

Если выбран параметр «Нет, удалить отношение доверия только в локальном домене», рекомендуется повторить эту процедуру для домена второй стороны.

Если выбран параметр «Да, удалить отношение доверия в локальном и другом доменах», необходимо ввести учетную запись и пароль администратора для домена второй стороны.

6. АДМИНИСТРИРОВАНИЕ ДОМЕНА

6.1. Управление пользователями и группами

6.1.1. В ADMS

Для управления пользователями и группами в «Альт Домен» можно использовать модуль удаленного управления базой данных конфигурации (ADMS). Подробнее см. п. 4.5.

6.1.2. Подкоманда user и group утилиты samba-tool

Для управления пользователями и группами в «Альт Домен» можно использовать инструмент командной строки samba-tool.

П р и м е ч а н и е . Для выполнения команд 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>`.

Команды управления пользователями представлены в таблице 60.

Т а б л и ц а 60 – Команды управления пользователями инструмента samba-tool

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; - --department – подразделение, к которому относится пользователь; - --description – информация о пользователе;

Продолжение таблицы 60

Команда	Описание	Примечание
		- --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)

Продолжение таблицы 60

Команда	Описание	Примечание
<code>user create <имя пользователя> [<пароль>] [опции]</code>	Создать нового пользователя	Команда доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду: <code>samba-tool user add</code>
<code>user delete <имя пользователя> [опции]</code>	Удалить существующего пользователя	При удалении учетной записи также удаляются все связанные с ней разрешения, права и членства в группах
<code>user disable (<имя пользователя> --filter <фильтр>) [опции]</code>	Отключить пользовательский аккаунт	Параметры вызова: - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене
<code>user edit <имя пользователя> [опции]</code>	Редактировать объект пользовательского аккаунта	В опции <code>--editor = <редактор></code> можно указать редактор (по умолчанию <code>vi</code>)
<code>user enable (<имя пользователя> --filter <фильтр>) [опции]</code>	Включить пользовательский аккаунт	Параметры вызова: - <code>--filter</code> – LDAP-фильтр для поиска объектов в домене
<code>user list [опции]</code>	Вывести список пользователей	По умолчанию выводятся <code>sAMAccountNames</code> пользователей. Можно использовать следующие опции: - <code>--full-dn</code> – показать различающиеся имена пользователей (CN) вместо <code>sAMAccountNames</code> ; - <code>-b BASE_DN --base-dn=BASE_DN</code> – вывести пользователей с указанным базовым DN; - <code>--hide-expired</code> – не выводить просроченные учетные записи пользователей; - <code>--hide-disabled</code> – не выводить отключенные учетные записи пользователей

Продолжение таблицы 60

Команда	Описание	Примечание
<code>user setprimarygroup <имя пользователя> <имя группы> [опции]</code>	Установить основную группу для учетной записи пользователя	
<code>user getgroups <имя пользователя> [опции]</code>	Вывести список групп, в которые входит учетная запись пользователя напрямую	Можно использовать следующие опции: - <code>--full-dn</code> – показать в списке вместо имен групп SAM (sAMAccountName) их полные уникальные имена (DN)
<code>user show <имя пользователя> [опции]</code>	Вывести пользовательский объект	В опции <code>--attributes=USER_ATTRS</code> можно указать, разделенный запятыми, список атрибутов, значения которых требуется отобразить. Для вывода скрытых атрибутов, их необходимо явно указать в параметре <code>--attributes</code>
<code>user move <имя пользователя> <контейнер> [опции]</code>	Переместить учетную 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 или без компонента domainDN.
<code>user password [опции]</code>	Изменить пароль, текущей учетной записи (пользователя, прошедшего аутентификацию)	Если пароль не передается в открытом виде в значении параметра <code>--newpassword</code> , пользователь получит запрос на ввод пароля в командной строке

Продолжение таблицы 60

Команда	Описание	Примечание
<pre>user rename <имя пользователя> [опции]</pre>	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. Можно использовать следующие опции: - --surname=SURNAME – новая фамилия; - --given-name=GIVEN_NAME – новое имя; - --initials=INITIALS – новые инициалы; - --force-new-cn=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=DISPLAY_NAME – новое отображаемое имя; - --mail-address=MAIL_ADDRESS – новая электронная почта; - --samaccountname=SAMACCOUNTNAME – новое имя для входа (sAMAccountName); - --upn=UPN – новое основное имя
<pre>user setexpiry (<имя пользователя> --filter <фильтр>) [опции]</pre>	Установить срок действия для учетной 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.

Продолжение таблицы 60

Команда	Описание	Примечание
		Параметры вызова: - --filter – LDAP-фильтр для поиска объектов в домене; - --days=DAYS – продолжительность периода в днях; - --noexpiry – период действия неограничен
user setpassword (<имя пользователя> --filter <фильтр>) [опции]	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. 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 учетную запись пользователя в домене	Параметры вызова: - --filter – LDAP-фильтр для поиска объектов в домене
user getpassword (<имя пользователя> --filter <фильтр>) [опции]	Получить атрибуты пароля учетной записи пользователя	Параметры вызова: - --filter – LDAP-фильтр для поиска объектов в домене;

Окончание таблицы 60

Команда	Описание	Примечание
		- <code>--attributes</code> – атрибуты (через запятую), которые требуется вывести или передать скрипту, заданному в параметре <code>--script</code>. В параметре могут передаваться любые атрибуты, заданные в схеме каталога, а также следующие виртуальные атрибуты: <code>virtualClearTextUTF16</code>, <code>virtualClearTextUTF8</code>, <code>virtualCryptSHA256</code>, <code>virtualCryptSHA512</code>, <code>virtualKerberosSalt</code>, <code>virtualSSHA</code>, <code>virtualSambaGPG</code>, <code>virtualDigest01..29</code>; - <code>--decrypt-samba-gpg</code> – дешифровать пароль SambaGPG (должен быть установлен пакет <code>python3-module-gpg</code>)
<code>user syncpasswords [--cache-ldb-initialize] [опции]</code>	Синхронизировать пароли всех учетных 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: <code>--cache-ldb-initialize</code> Для корректной инициализации кеша требуется передать список атрибутов в параметре <code>--attributes</code>

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 учетных 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 disable --filter=mail=k*
Enabled user 'mail=k*'
```

- изменить пароль пользователя `ivanov`:

```
# samba-tool user setpassword ivanov
```

- 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
```



Не следует допускать одинаковых имен для пользователя и компьютера, это может привести к коллизиям (например, такого пользователя нельзя добавить в группу). Если компьютер с таким именем заведен, удалить его можно командой:

```
pdbedit -x -m имя
```

Примечание. При удалении учетной записи также удаляются все связанные с ней 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.

Команды инструмента командной строки `samba-tool` для управления группами в «Альт Домен» приведены в таблице 61.

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 должна быть передана опция `--group-type=Distribution`.

Группы располагаются в подразделениях (OU). Область действия (scope) группы определяет место группы в дереве доменов.

Т а б л и ц а 61 – Команды управления группами инструмента samba-tool

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 NIS; --special – используется для создания группы безопасности с именем Protected Users

Продолжение таблицы 61

Команда	Описание	Примечание
<code>group create <имя группы> [опции]</code>	Создать новую группу	Доступна только в целях совместимости. Рекомендуется вместо этой команды использовать команду <code>samba-tool group add</code>
<code>group addmembers (<список участников> --member-dn=<member-dn>) [опции]</code>	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. Некоторые опции: - <code>--member-dn</code> – уникальное составное имя (DN) добавляемого в группу нового участника (значение опции <code>--object-types</code> игнорируется); - <code>--object-types</code> – список типов объектов (через запятую); указанные типы используются в качестве фильтра при выполнении поиска для указанных в команде участников; возможные значения: <code>user, group, computer, serviceaccount, contact, all</code>; значение по умолчанию – <code>user,group,computer</code>; - <code>--member-base</code> – базовое уникальное имя (DN) для поиска участников группы; значение по умолчанию – уникальное имя (DN) домена

Продолжение таблицы 61

Команда	Описание	Примечание
<code>group delete <имя группы> [опции]</code>	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
<code>group addunixattrs <имя группы> <gidnumber> [опции]</code>	Добавить атрибуты Unix/RFC 2307 для группы	Для использования этих атрибутов для сопоставления UID/GID в конфигурации (<code>smb.conf</code>) должен быть задан параметр <code>idmap_ldp:use rfc2307 = Yes</code>
<code>group edit <имя группы> [опции]</code>	Редактировать объект группы	В опции <code>--editor=<редактор></code> можно указать редактор (по умолчанию <code>vi</code>)
<code>group list [опции]</code>	Вывести список групп	По умолчанию выводится список имен учетных записей SAM (<code>sAMAccountName</code>). Можно использовать следующие опции: <code>--full-dn</code> – выводить уникальные имена (DN) вместо <code>sAMAccountNames</code>; <code>-b BASE_DN --base-dn=BASE_DN</code> – выводить в списке только группы с указанным базовым уникальным именем (DN)
<code>group listmembers <имя группы> [опции]</code>	Вывести список участников данной группы	По умолчанию выводятся <code>sAMAccountNames</code> участников. Если <code>sAMAccountName</code> недоступен, будет использоваться CN.

Продолжение таблицы 61

Команда	Описание	Примечание
		Можно использовать следующие опции: - <code>--full-dn</code> – показать различающиеся имена участников (CN) вместо <code>sAMAccountNames</code>; - <code>--hide-expired</code> – не выводить членов группы с истекшим сроком действия; - <code>--hide-disabled</code> – не выводить отключенных членов группы
<code>group move <имя группы> <контейнер> [опции]</code>	Переместить группу в указанную организационную единицу или контейнер	Имя организационной единицы или контейнера можно указать как полное DN или без компонента <code>domainDN</code>
<code>group stats [опции]</code>	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; - максимальное количество участников в группе; - медианное количество участников в группе; - распределение участников по группам с точки зрения количественного состава

Продолжение таблицы 61

Команда	Описание	Примечание
group show <имя группы> [опции]	Вывести группу и ее атрибуты	В опции --attributes=USER_ATTRS можно указать, разделенный запятыми, список атрибутов
group removemembers <имя группы> (<список участников> --member-dn=<member-dn>) [опции]	Удалить участника 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

Окончание таблицы 61

Команда	Описание	Примечание
group rename <имя группы> [опции]	Переименовать группу и изменить ее 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)

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool group add --help
```

Примеры:

- добавить группу:

```
# samba-tool group add office --description='Simple group'
Added group office
```

- добавить новую группу рассылки с указанием удаленного 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 определенные 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
```


6.2. Администрирование DNS

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.

6.2.1. 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 домена. Для ее 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 -Uadministrator
Password for [TEST\administrator]:
Zone 0.168.192.in-addr.arpa created successfully
```

6.2.2. Подкоманда dns утилиты samba-tool

Для администрирования службы доменных имен (DNS) в «Альт Домен» можно использовать подкоманду dns утилиты samba-tool.

Примечание. Для выполнения команд на удаленном компьютере можно использовать опцию -H или --URL= с указанием URI LDAP-сервера. Например:

```
$ samba-tool dns add 192.168.0.132 test.alt \
DC2 A 192.168.0.133 -H ldap://<DC> -Uadministrator
```

По умолчанию в качестве значения опции -H передается текущий узел в формате ldap://<имя узла>.

6.2.2.1. Работа с DNS-записями

Команды инструмента командной строки samba-tool для управления DNS-записями приведены в таблице 62.

Т а б л и ц а 62 – Команды управления DNS-записями инструмента samba-tool

Команда	Описание	Примечание
<pre>dns add <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SRV TXT> <данные></pre>	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 (см. ниже)
<pre>dns delete <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SRV TXT> <данные></pre>	Удалить DNS-запись	
<pre>dns edit <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SOA SRV TXT> <текущие-данные> <новые-данные></pre>	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; - 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

Окончание таблицы 62

Команда	Описание	Примечание
<code>dns cleanup <сервер> <имя узла> [опции]</code>	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
<code>dns query <сервер> <зона> <имя> <A AAAA PTR CNAME NS MX SOA SRV TXT ALL> [опции]</code>	Вывести информацию о DNS-записях	Можно использовать следующие опции: - <code>--authority</code> – поиск по записям полномочного DNS-сервера (значение по умолчанию); - <code>--cache</code> – поиск по записям в кеше; - <code>--glue</code> – поиск по связующим (glue) записям; - <code>--root</code> – поиск по корневым ссылкам DNS-сервера; - <code>--additional</code> – вывод списка дополнительных записей; - <code>--no-children</code> – исключение вывода дочерних записей; - <code>--only-children</code> – вывод только дочерних записей

Возможные типы записей:

- 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> <preference> – полное доменное имя (FQDN) и приоритет почтового сервера;

- SRV <FQDN> <port> <priority> <weight> – полное доменное имя (FQDN) сервера, на котором доступна определенная служба, порт для доступа к службе (port), приоритет (priority) и относительный вес (weight) 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
```

 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 -U administrator
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 successfully
```

- 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 successfully
```

- вывести все DNS-записи для указанной зоны:

```
$ samba-tool dns query dc1.test.alt 0.168.192.in-addr.arpa \
@ ALL -U administrator
```

6.2.2.2. Работа с DNS-зонами

Команды инструмента командной строки `samba-tool` для управления DNS-зонами приведены в таблице 63.

Т а б л и ц а 63 – Команды управления DNS-зонами инструмента `samba-tool`

Команда	Описание	Примечание
<code>dns zonecreate <сервер> <зона> [опции]</code>	Создать зону DNS	Дополнительно с помощью параметра <code>--client-version</code> можно указать версию DNS-клиента. Возможные значения: <code>w2k</code> , <code>dotnet</code> , <code>longhorn</code> (по умолчанию)
<code>dns zonedelate <сервер> <зона> [опции]</code>	Удалить зону DNS	
<code>dns zoneinfo <сервер> <зона> [опции]</code>	Вывести информацию о зоне DNS	
<code>dns zonelist <сервер> [опции]</code>	Вывести список зон DNS	Можно использовать следующие опции: - <code>--client-version</code> – версия DNS-клиента. Возможные значения: <code>w2k</code>, <code>dotnet</code>, <code>longhorn</code> (по умолчанию); - <code>--primary</code> – получение списка первичных зон DNS (по умолчанию); - <code>--secondary</code> – получение списка вторичных зон DNS; - <code>--cache</code> – получение списка зон DNS из кеша; - <code>--auto</code> – получение списка автоматически созданных зон DNS; - <code>--forward</code> – получение списка прямых зон DNS; - <code>--reverse</code> – получение списка обратных зон DNS; - <code>--ds</code> – получение списка зон DNS, интегрированных с доменом; - <code>--non-ds</code> – получение списка зон DNS без интеграции с доменом

Окончание таблицы 63

Команда	Описание	Примечание
dns zoneoptions <сервер> <зона> [опции]	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)

Примеры:

- создать обратную зону /24:

```
$ samba-tool dns zonecreate 192.168.0.132 \
0.168.192.in-addr.arpa -U administrator
Password for [TEST\administrator]:
Record added successfully
```

- вывести информацию об обратной зоне DNS:

```
$ samba-tool dns zoneinfo dc1.test.alt \
0.168.192.in-addr.arpa -U administrator
```

- включить очистку с большим интервалом обновления:

```
$ samba-tool dns zoneoptions dc1.test.alt \
test.alt --aging=1 --refreshinterval=306600
```

Примечание. Чтобы очистка работала, в файле `smb.conf` хотя бы на одном контроллере домена должен быть задан параметр `dns zone scavenging = yes`.

6.2.2.3. Получение информации о DNS-серверах

Команды инструмента командной строки `samba-tool` для получения информации о DNS-серверах приведены в таблице 64.

Т а б л и ц а 64 – Команды `samba-tool` для получения информации о DNS-серверах

Команда	Описание	Примечание
<code>dns serverinfo <сервер> [опции]</code>	Вывести информацию о DNS-сервере	Дополнительно с помощью параметра <code>--client-version</code> можно указать версию DNS-клиента. Возможные значения: <code>w2k</code> , <code>dotnet</code> , <code>longhorn</code> (по умолчанию)
<code>dns roothints <сервер> [<имя>] [опции]</code>	Вывести информацию о корневых серверах DNS	

Примеры:

- вывести информацию о DNS-сервере:

```
$ samba-tool dns serverinfo dcl.test.alt -U administrator
```

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 dcl.test.alt -U administrator
```

6.2.3. 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]
```


Опции команды `nsupdate` приведены в таблице 65.

Т а б л и ц а 65 – Опции команды `nsupdate`

Ключ	Описание
<code>-4</code>	Использовать только IPv4
<code>-6</code>	Использовать только IPv6
<code>-d</code>	Включить режим отладки
<code>-D</code>	Включить дополнительный режим отладки
<code>-i</code>	Принудительно включить интерактивный режим, даже если стандартный ввод не является терминалом
<code>-k keyfile</code>	Позволяет указать файл, содержащий ключ аутентификации TSIG. Файлы могут быть в двух форматах: один файл, содержащий оператор ключа <code>named.conf-format</code> , который может быть автоматически сгенерирован <code>ddns-confgen</code> ; или пара файлов, имена которых имеют формат <code>K{name}+.157.+{random}.key</code> и <code>K{name}+.157.+{random}.private</code> , которые могут быть сгенерированы <code>dnssec-keygen</code> . Параметр <code>-k</code> 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
<code>-l</code>	Установить режим локального хоста. Адрес сервера будет установлен на <code>localhost</code> (отключая сервер, чтобы адрес сервера не мог быть переопределен). Подключения к локальному серверу используют ключ TSIG, найденный в <code>/var/run/named/session.key</code> , который автоматически генерируется <code>named</code> , если какая-либо локальная первичная зона установила <code>update-policy</code> на <code>local</code> . Расположение этого файла ключа можно переопределить с помощью опции <code>-k</code>
<code>-L level</code>	Установить уровень отладки ведения журнала. Если 0, ведение журнала отключено
<code>-p port</code>	Установить порт для подключения к серверу имен. Значение по умолчанию – 53
<code>-P</code>	Вывести список частных типов записей ресурсов BIND, формат которых понимает <code>nsupdate</code>
<code>-r udpretries</code>	Установить количество повторных попыток UDP. Значение по умолчанию – 3. Если 0, выполняется только один запрос на обновление
<code>-t timeout</code>	Установить максимальное время, которое может занять запрос на обновление, прежде чем он будет прерван. Значение по умолчанию – 300 секунд. Если 0, тайм-аут отключен
<code>-T</code>	Вывести список стандартных типов записей ресурсов IANA, формат которых понимает <code>nsupdate</code> . <code>nsupdate</code> завершает работу после вывода списков. Параметр <code>-T</code> можно комбинировать с параметром <code>-P</code> . Другие типы можно ввести с помощью <code>TYPEXXXXXX</code> , где XXXXXX – это десятичное значение типа без начальных нулей. Rdata, если они присутствуют, анализируются с использованием формата <code>UNKNOWN rdata (<обратная косая черта> <хеш> <пробел> <длина> <пробел> <шестнадцатеричная строка>)</code>
<code>-u udptimeout</code>	Задать интервал повтора UDP. Значение по умолчанию – 3 секунды. Если равно 0, интервал вычисляется из интервала тайм-аута и количества повторов UDP

Окончание таблицы 65

Ключ	Описание
-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	Задаёт 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. 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 (таблица 66) 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.

Т а б л и ц а 66 – Форматы команд и их значения

Команда	Описание
<code>server servername port</code>	Отправить все динамические запросы на обновление на сервер имен <code>servername</code> . Если не указано ни одного оператора сервера, <code>nsupdate</code> отправляет обновления на основной сервер правильной зоны. Поле <code>MNAME</code> записи <code>SOA</code> этой зоны определяет основной сервер для этой зоны. <code>port</code> – это номер порта на <code>servername</code> , куда отправляются динамические запросы на обновление. Если номер порта не указан, используется номер порта <code>DNS</code> по умолчанию 53. Примечание. Эта команда не действует, если используется <code>GSS-TSIG</code>
<code>local address port</code>	Отправить все динамические запросы на обновление, используя локальный адрес. Если локальный оператор не указан, <code>nsupdate</code> отправляет обновления, используя адрес и порт, выбранные системой. <code>port</code> также может использоваться для принудительного поступления запросов с определенного порта. Если номер порта не указан, система назначает его
<code>zone zonename</code>	Указывает, что все обновления должны быть сделаны в зоне <code>zonename</code> . Если оператор <code>zone</code> не указан, <code>nsupdate</code> пытается определить правильную зону для обновления на основе остальной части ввода
<code>class classname</code>	Указывает класс по умолчанию. Если класс не указан, класс по умолчанию – <code>IN</code>
<code>ttl seconds</code>	Указывает время жизни по умолчанию в секундах для добавляемых записей. Значение <code>none</code> очищает <code>TTL</code> по умолчанию
<code>key hmac:keyname secret</code>	Указывает, что все обновления должны быть подписаны <code>TSIG</code> с использованием пары <code>keyname-secret</code> . Если указан <code>hmac</code> , он устанавливает используемый алгоритм подписи. Значение по умолчанию – <code>hmac-md5</code> ; если <code>MD5</code> отключен, то по умолчанию используется <code>hmac-sha256</code> . Команда <code>key</code> переопределяет любой ключ, указанный в командной строке с помощью <code>-y</code> или <code>-k</code>
<code>gsstsig</code>	Эта команда использует <code>GSS-TSIG</code> для подписи обновлений. Это эквивалентно указанию <code>-g</code> в командной строке
<code>oldgsstsig</code>	Эта команда использует версию <code>GSS-TSIG</code> для Windows 2000 для подписи обновлений. Это эквивалентно указанию <code>-o</code> в командной строке
<code>realm [realm_name]</code>	При использовании <code>GSS-TSIG</code> эта команда указывает использование <code>realm_name</code> вместо <code>realm</code> по умолчанию в <code>krb5.conf</code> . Если <code>realm</code> не указан, сохраненная <code>realm</code> очищается
<code>check-names [yes_or_no]</code>	Включить или выключить обработку <code>check-names</code> для добавляемых записей. <code>Check-names</code> не влияет на предварительные условия или удаляемые записи. По умолчанию обработка <code>check-names</code> включена. Если обработка <code>check-names</code> завершается неудачей, запись не добавляется в сообщение <code>UPDATE</code>

Окончание таблицы 66

Команда	Описание
<code>prereq nxdomain domain-name</code>	Эта команда требует, чтобы не существовало ни одной записи ресурса любого типа с именем <code>domain-name</code>
<code>prereq yxdomain domain-name</code>	Эта команда требует, чтобы существовал <code>domain-name</code> (как минимум одна запись ресурса любого типа)
<code>prereq nxrrset domain-name class type</code>	Эта команда требует, чтобы не существовало ни одной записи ресурса указанного типа, класса и <code>domain-name</code> . Если <code>class</code> не указан, предполагается IN (Интернет)
<code>prereq yxrrset domain-name class type</code>	Для этой команды требуется, чтобы существовала запись ресурса указанного типа, класса и доменного имени. Если <code>class</code> не указан, предполагается IN (Интернет)
<code>prereq yxrrset domain-name class type data</code>	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
<code>update delete domain-name ttl class type data</code>	Удалить все записи ресурсов с именем <code>domain-name</code> . Если указаны <code>type</code> и <code>data</code> , удаляются только соответствующие записи ресурсов. Если <code>class</code> не указан, предполагается класс Internet. TTL игнорируется и допускается только для совместимости
<code>update add domain-name ttl class type data</code>	Добавить новую запись ресурса с указанным <code>ttl</code> , <code>class</code> и <code>data</code>
<code>show</code>	Отобразить текущее сообщение, содержащее все предварительные условия и обновления, указанные с момента последней отправки
<code>send</code>	Отправить текущее сообщение (эквивалентно вводу пустой строки)
<code>answer</code>	Отобразить ответ
<code>debug</code>	Включить отладку
<code>version</code>	Вывести номер версии
<code>help</code>	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 'MACHINE$'
```

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.

6.2.4. 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. п. 4.2.3).

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...» (рис. 273). 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» (рис. 274) и нажать кнопку «OK».

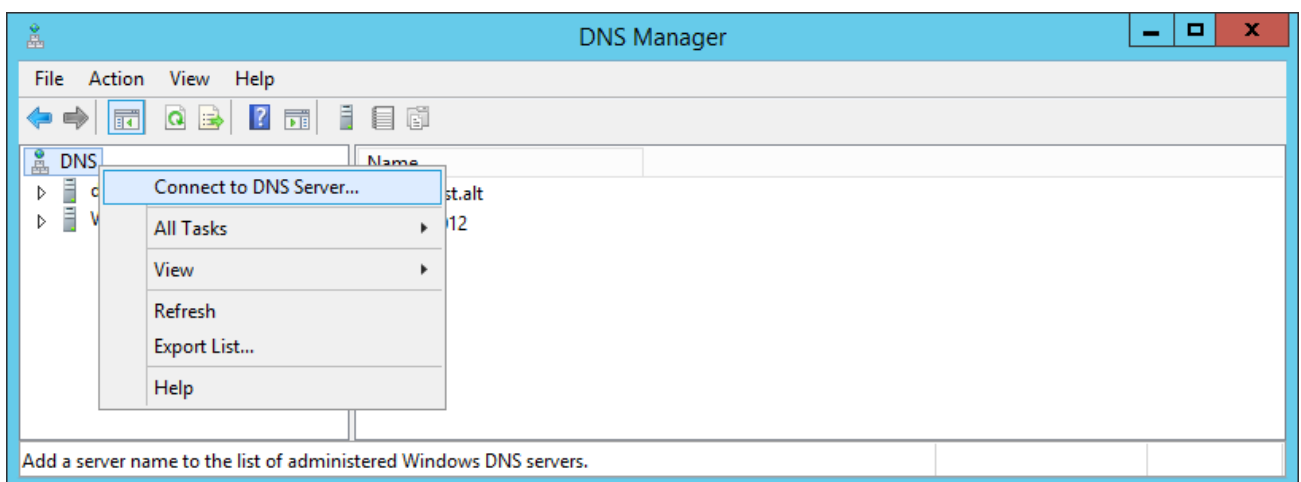


Рис. 273 – Подключение к DNS-серверу



Рис. 274 – Адрес DNS-сервера

6.2.4.1. 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 (рис. 275);
- 3) заполнить поля и сохранить запись, нажав кнопку «Add Host» (рис. 276).

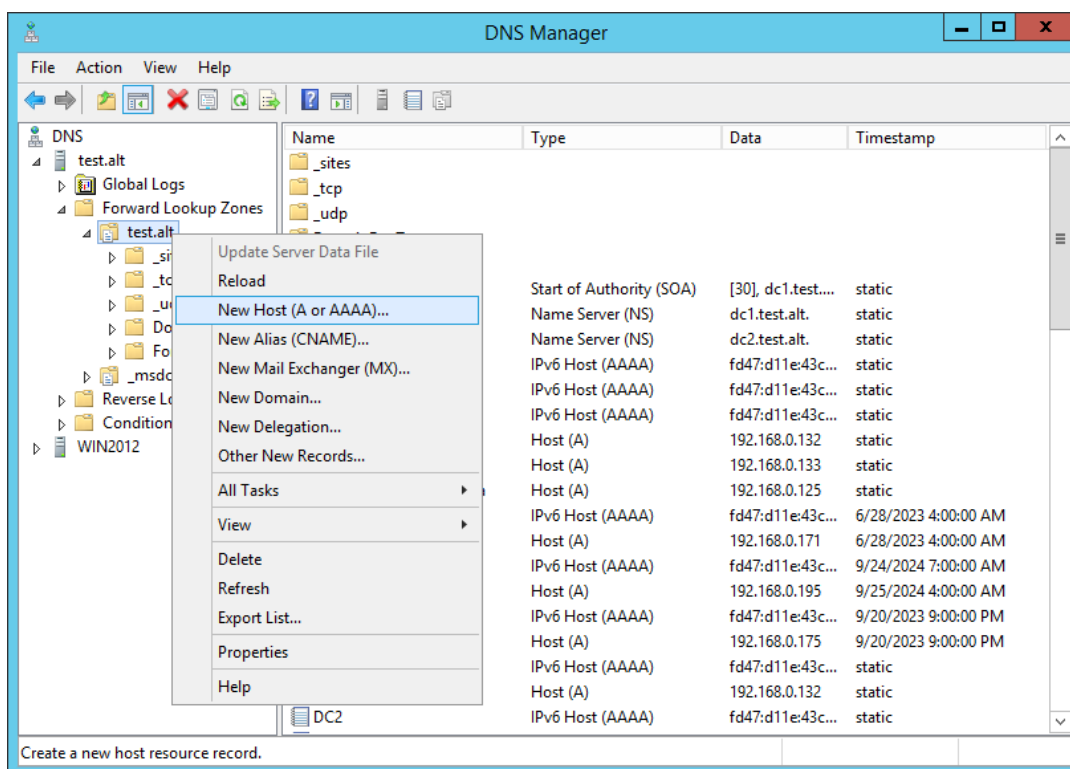


Рис. 275 – Добавление DNS-записи

Рис. 276 – Новая А-запись

Для обновления существующей записи необходимо:

- 1) перейти в зону, содержащую запись, которую нужно изменить;
- 2) в контекстном меню записи выбрать пункт «Properties» (рис. 277);
- 3) отредактировать запись и сохранить изменения, нажав кнопку «Apply» (рис. 278).

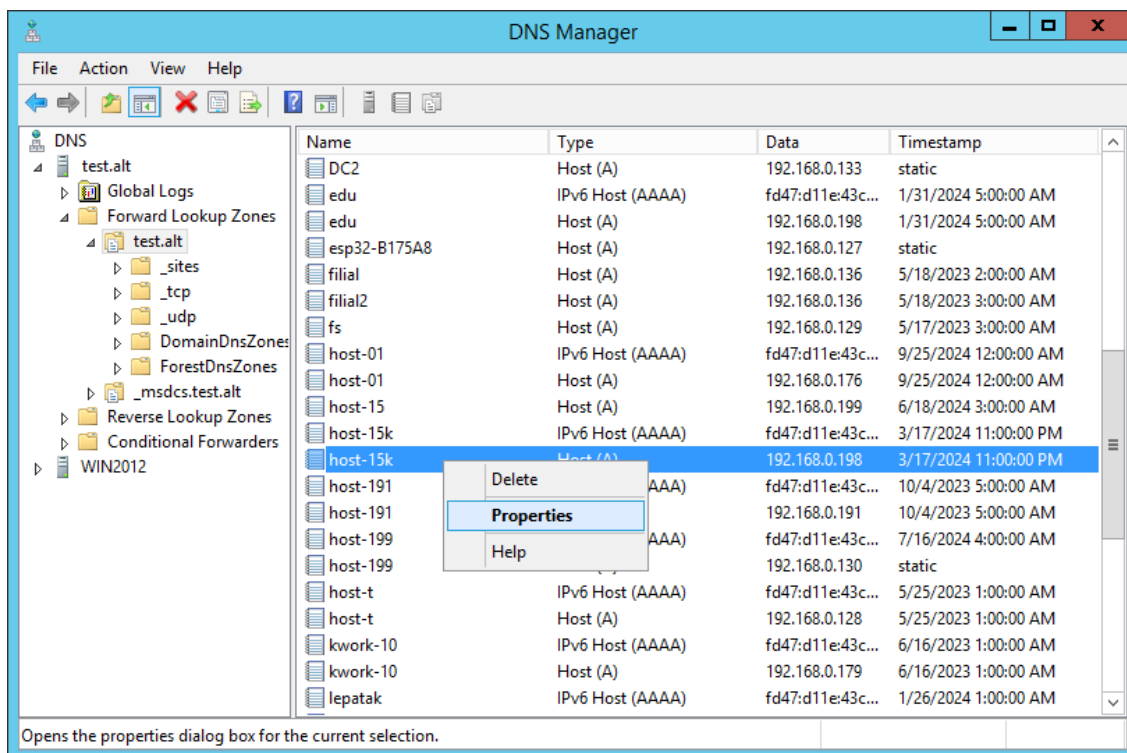


Рис. 277 – Изменение DNS-записи

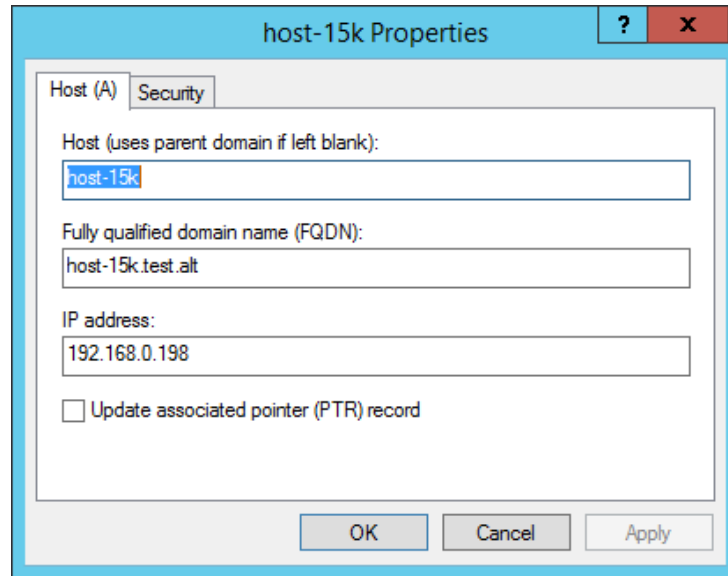


Рис. 278 – Параметры DNS-записи

Для удаления записи необходимо:

- 1) перейти в зону, содержащую запись, которую нужно удалить;
- 2) в контекстном меню записи выбрать пункт «Delete» (рис. 279).

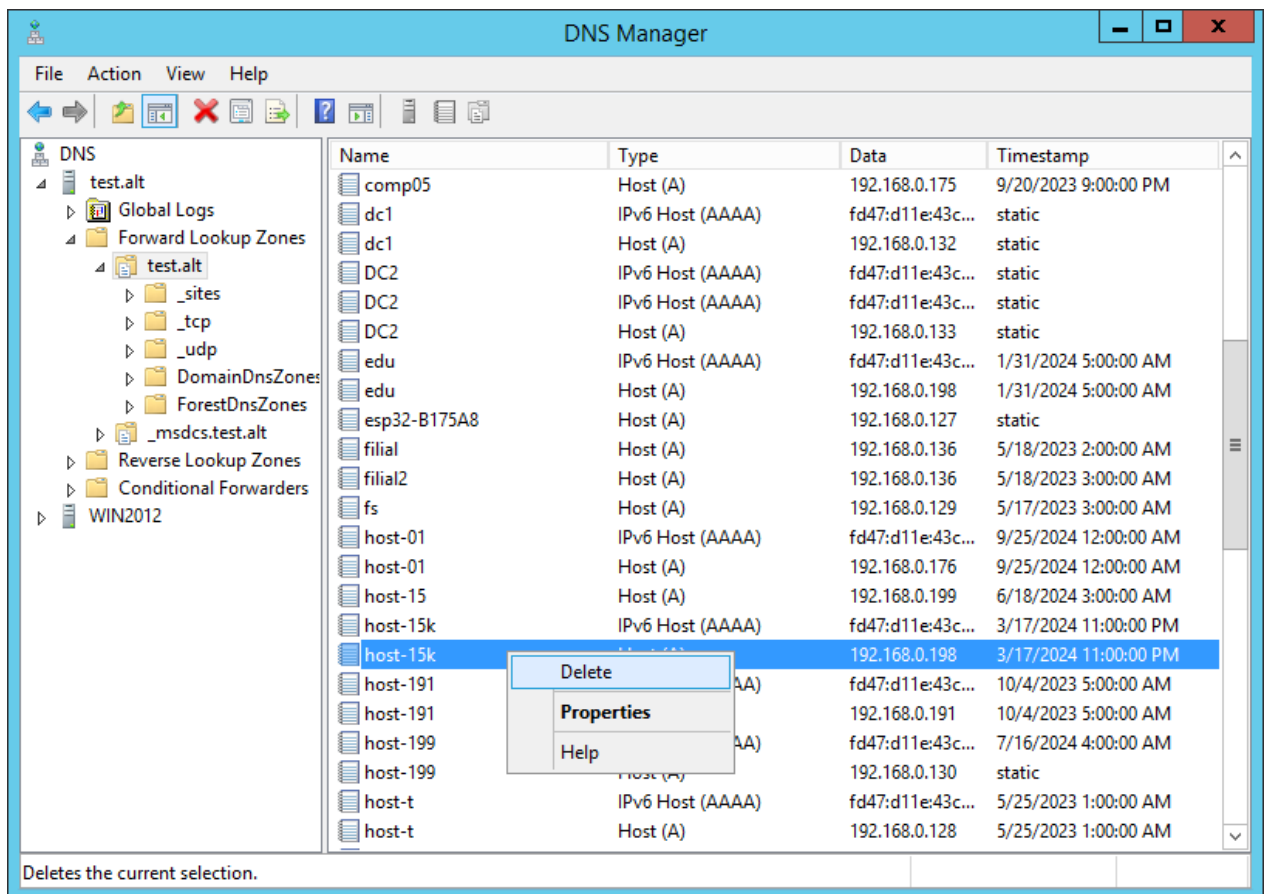


Рис. 279 – Удаление DNS-записи

6.2.4.2. 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...» (рис. 280);
- 2) на втором шаге мастера создания новой зоны выбрать «Primary zone» и установить отметку в пункте «Store the zone in Active Directory» (рис 281);
- 3) на следующем шаге мастера указать область репликации зоны (рис. 282);
- 4) указать имя зоны обратного просмотра (рис. 283);
- 5) включить динамическое обновление (рис. 284);
- 6) завершить работу мастера.

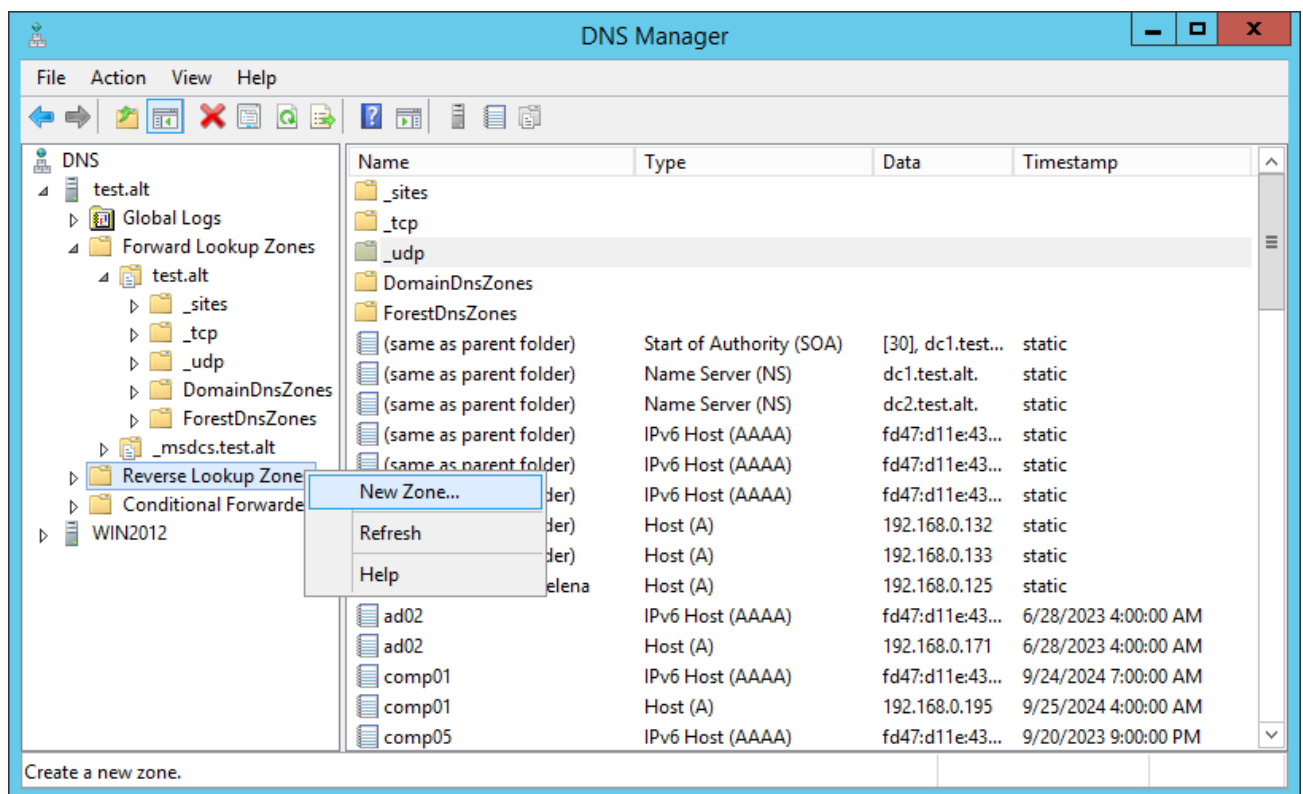
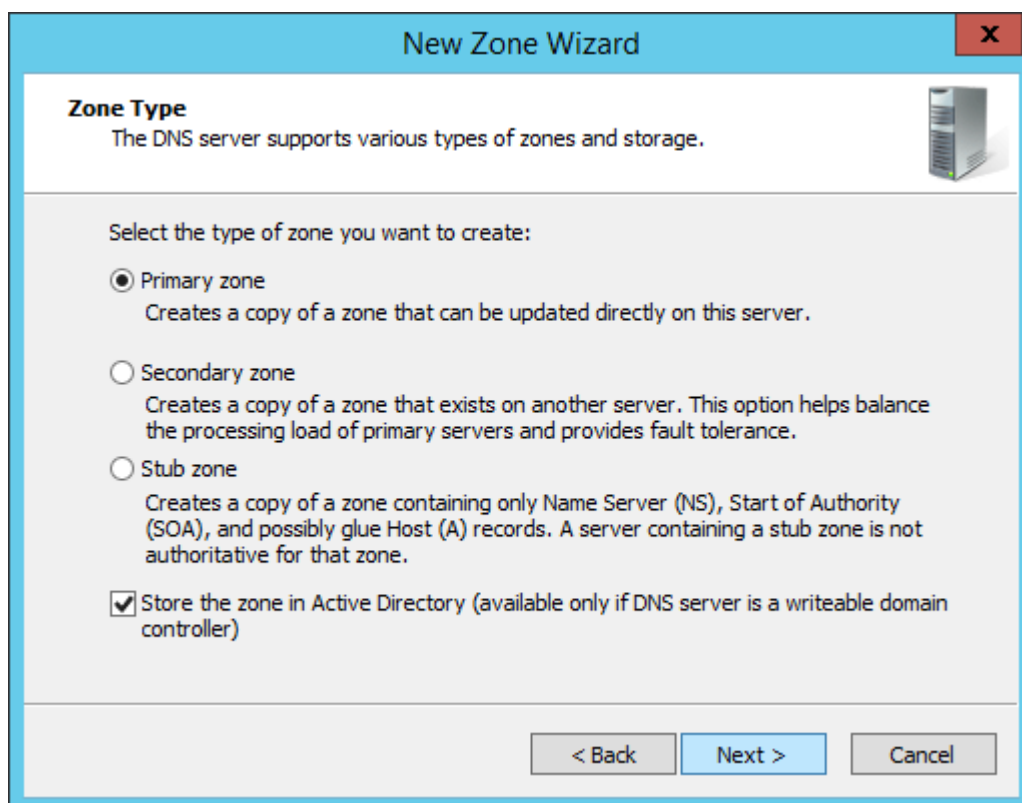


Рис. 280 – Добавление зоны обратного просмотра



The screenshot shows the 'New Zone Wizard' window with the title bar 'New Zone Wizard' and a close button. The main heading is 'Zone Type' with a subtext 'The DNS server supports various types of zones and storage.' and a server icon. Below this, it says 'Select the type of zone you want to create:'. There are four radio button options: 'Primary zone' (selected), 'Secondary zone', 'Stub zone', and a checked checkbox 'Store the zone in Active Directory (available only if DNS server is a writeable domain controller)'. Each option has a brief description. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

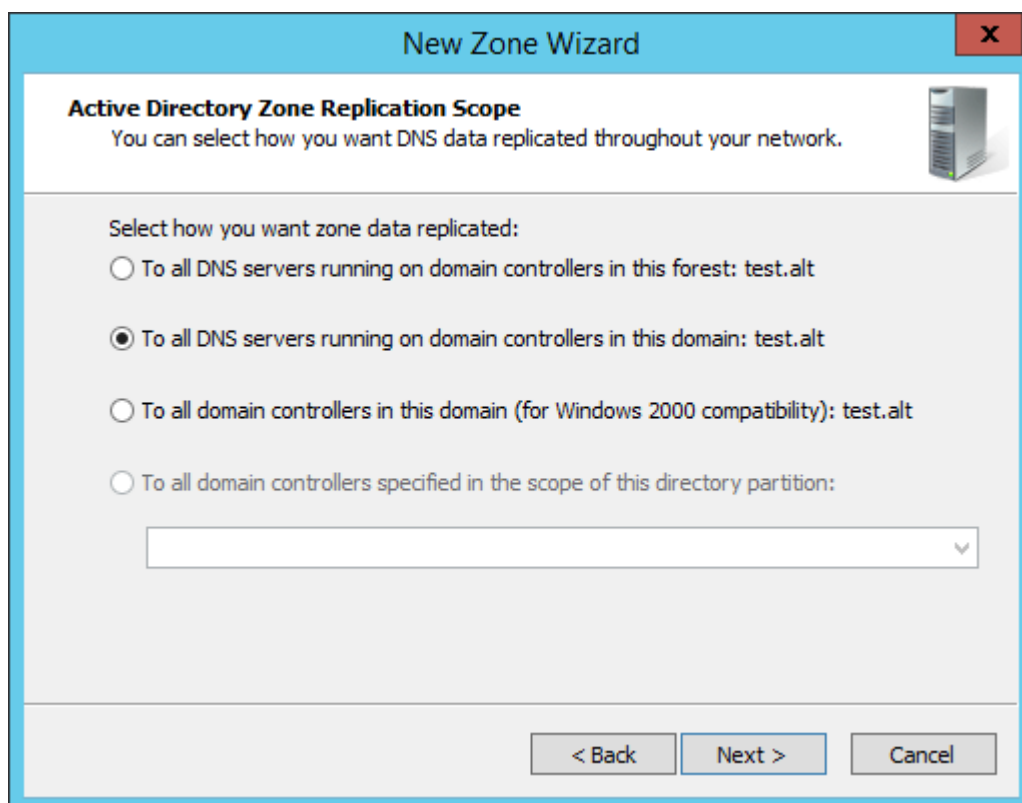
Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

- ☒ **Primary zone**
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
- ☒ **Store the zone in Active Directory** (available only if DNS server is a writeable domain controller)

< Back Next > Cancel

Рис. 281 – Выбор типа зоны



The screenshot shows the 'New Zone Wizard' window with the title bar 'New Zone Wizard' and a close button. The main heading is 'Active Directory Zone Replication Scope' with a subtext 'You can select how you want DNS data replicated throughout your network.' and a server icon. Below this, it says 'Select how you want zone data replicated:'. There are four radio button options, each followed by a domain name 'test.alt': 'To all DNS servers running on domain controllers in this forest:', 'To all DNS servers running on domain controllers in this domain:' (selected), 'To all domain controllers in this domain (for Windows 2000 compatibility):', and 'To all domain controllers specified in the scope of this directory partition:'. The last option has a text box with a dropdown arrow below it. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

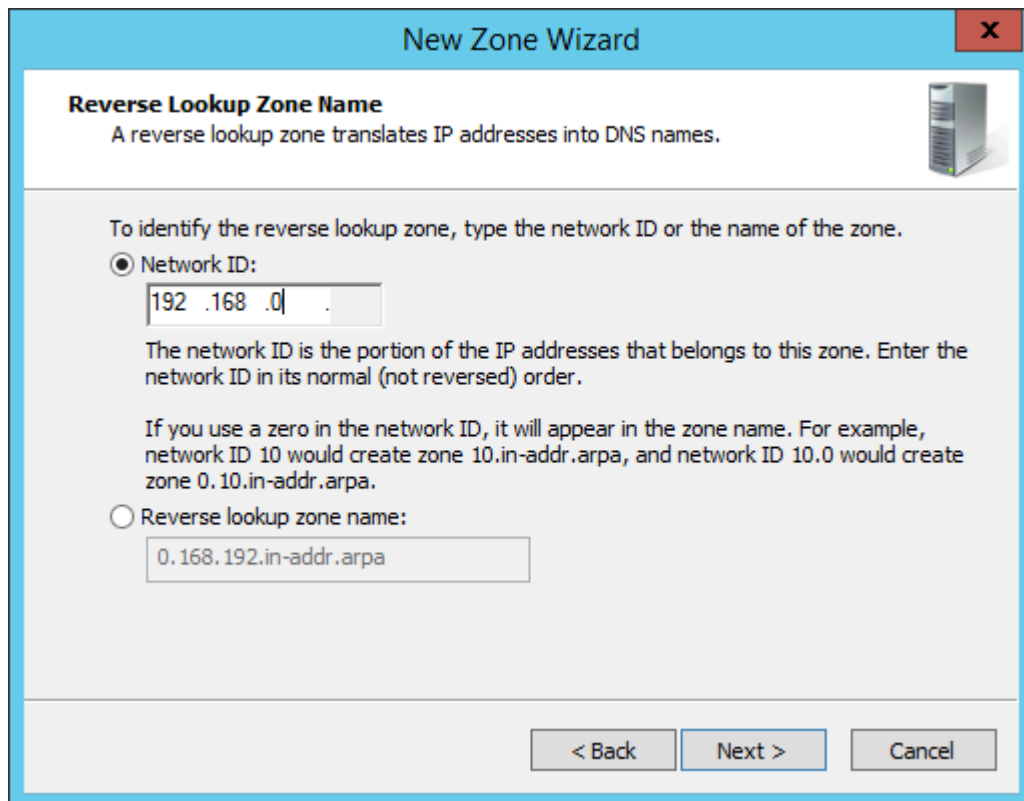
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

- ☐ To all DNS servers running on domain controllers in this forest: test.alt
- ☒ To all DNS servers running on domain controllers in this domain: test.alt
- ☐ To all domain controllers in this domain (for Windows 2000 compatibility): test.alt
- ☐ To all domain controllers specified in the scope of this directory partition:

< Back Next > Cancel

Рис. 282 – Область репликации зоны



New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:
[192 .168 .0] .

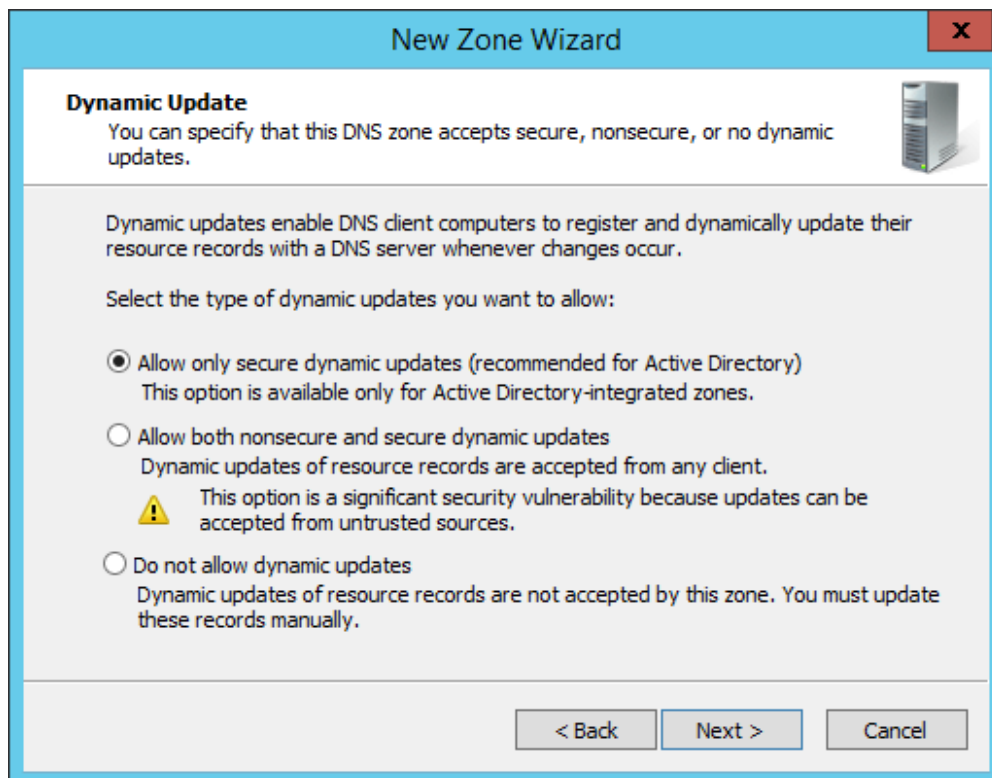
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:
[0.168.192.in-addr.arpa]

< Back Next > Cancel

Рис. 283 – Имя зоны обратного просмотра



New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

☒ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

Рис. 284 – Динамическое обновление

Новая зона будет активна сразу, без перезапуска Samba или BIND.

Для удаления зоны следует в контекстном меню зоны выбрать пункт «Delete» (рис. 285).

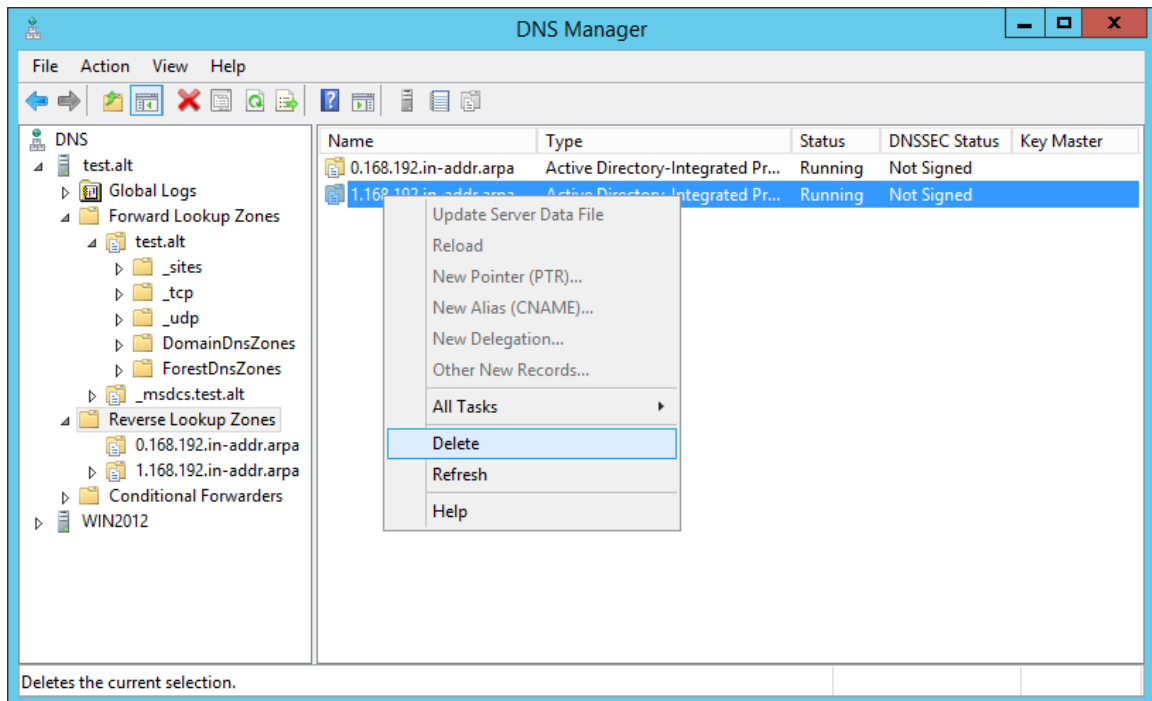


Рис. 285 – Удаление зоны

6.2.5. 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 доменом 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.

6.2.5.1. На стороне клиента

6.2.5.1.1. SSSD

Включить обновление IP-адресов службой sssd можно несколькими способами:

- отредактировав файл `/etc/sss/sss.conf`;
- в модуле ЦУС «Аутентификация» (пакет `alterator-auth`);
- применением `control`;
- групповыми политиками.

6.2.5.1.1.1. Настройка через файл `/etc/sss/sss.conf`

В файл конфигурации службы SSSD (`/etc/sss/sss.conf`) в секцию с параметрами домена можно добавить опции, приведенные в таблице 67.

Т а б л и ц а 67 – Параметры настройки автоматического обновления DNS

Параметр	Описание	Значение по умолчанию
<code>dyndns_update</code>	Позволяет включить или отключить автоматическое обновление DNS-записей (защищенных с помощью GSS-TSIG) IP-адресом клиента через SSSD. Соответственно, администратору домена требуется только разрешить защищенные обновления для зоны DNS. Для обновления будет использован IP-адрес LDAP-соединения AD, если с помощью параметра <code>dyndns_iface</code> не указано иное	<code>true</code>
<code>dyndns_ttl</code>	Значение TTL, которое применяется при обновлении DNS-записи клиента. Если <code>dyndns_update</code> имеет значение <code>false</code> , этот параметр не имеет никакого эффекта. Если администратором установлено значение TTL на стороне сервера, оно будет переопределено этим параметром	3600 (секунд)
<code>dyndns_iface</code>	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 <code>dyndns_update</code> имеет значение <code>false</code> , этот параметр не имеет никакого эффекта.	IP-адреса интерфейса, который используется для подключения LDAP AD

Продолжение таблицы 67

Параметр	Описание	Значение по умолчанию
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_force_tcp	Должна ли утилита nsupdate по умолчанию использовать TCP для обмена данными с сервером DNS	false (разрешить nsupdate выбрать протокол)
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_auth	Следует ли утилите nsupdate использовать проверку подлинности GSS-TSIG для защищенных обновлений сервера DNS. Незащищенные отправления можно отправлять, установив этот параметр в значение none	GSS-TSIG
dyndns_auth_ptr	Следует ли утилите nsupdate использовать проверку подлинности GSS-TSIG для защищенных обновлений PTR сервера DNS. Незащищенные отправления можно отправлять, установив этот параметр в значение none	То же, что и dyndns_auth
dyndns_server	Сервер DNS, который следует использовать для выполнения обновления DNS. В большинстве конфигураций рекомендуется не устанавливать значение для этого параметра.	none (разрешить nsupdate выбрать сервер)

Окончание таблицы 67

Параметр	Описание	Значение по умолчанию
	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 определенных 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

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 - 0, и 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
```

6.2.5.1.1.2. Настройка через ЦУС

Некоторые настройки автоматического обновления DNS для SSSD можно настроить в модуле ЦУС «Аутентификация». Подробнее см. п. 1.1.1.

6.2.5.1.1.3. При помощи механизма control

Список control, используемых для настройки автоматического обновления DNS для SSSD, представлен в таблице 68.

Т а б л и ц а 68 – control для настройки автоматического обновления DNS для SSSD

control	Опция в файле /etc/sssds/sssds.conf	Описание
sssds-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. Доступные режимы: - INTERVAL – задать интервал; - disabled – значение по умолчанию (86400); - unknown
sssds-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 – значение по умолчанию (3600); - unknown
sssds-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

Окончание таблицы 68

control	Опция в файле /etc/sss/sss.conf	Описание
sss-dyndns-update-ptr	dyndns_update_ptr	Определяет будет ли обновляться клиентская PTR-запись 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; - default – настройка автоматического обновления DNS-записи обратной зоны задана по умолчанию в пакете; - unknown

Список всех возможных настроек автоматического обновления DNS для SSSD с помощью control можно получить, выполнив команду:

```
# control | grep sss-dyndns
sss-dyndns-refresh-interval unknown      (disabled INTERVAL)
sss-dyndns-ttl unknown                  (disabled TTL)
sss-dyndns-update unknown                (disabled enabled default)
sss-dyndns-update-ptr unknown            (disabled enabled default)
```

Например, чтобы SSSD автоматически обновлял на сервере DNS AD IP-адрес клиента, необходимо включить control sss-dyndns-update:

```
# control sss-dyndns-update enabled
```

и перезапустить службу SSSD:

```
# systemctl restart sssd
```

Проверка:

```
# control sss-dyndns-update
enabled
```

6.2.5.1.1.4. 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. п. 4.6.4.2.

6.2.5.1.2. Samba Winbind

Samba Winbind не поддерживает возможность динамического обновления DNS-записей. Для обхода этой проблемы была 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
```

Активировать и запустить таймер, который в свою очередь запускает сервис:

```
# systemctl enable --now winbind-dnsupdate.timer
```

Основным функционалом утилиты `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]
```

Опции команды `winbind-dnsupdate` приведены в таблице 69. При запуске без параметров скрипт обновляет A запись.

Т а б л и ц а 69 – Опции команды `winbind-dnsupdate`

Ключ	Описание
<code>-h, --help</code>	Вывести справку о команде
<code>-v, --version</code>	Вывести версию
<code>-a, --all</code>	Включить обновление всех записей
<code>-6, --update-ipv6</code>	Включить обновление IPv6 (AAAA) записей
<code>-d, --daemon</code>	Отправлять логи в <code>journald</code>
<code>-t, --ttl <time></code>	Задать TTL («время жизни», указывает, как долго настройки DNS должны храниться в кеше, прежде чем они будут автоматически обновлены)
<code>--allow-ipv4-ptr-update</code>	Включить обновление обратной DNS-записи IPv4 (A) PTR
<code>--allow-ipv6-ptr-update</code>	Включить обновление обратной DNS-записи IPv6 (AAAA) PTR

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)
OnUnitActiveSec=120min установит новое значение (120min).
```

- 3) сохранить внесенные 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 создается 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.

6.2.5.1.3. 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.

6.2.6. Обновление IP-адресов вручную

Для обновления IP-адресов вручную существует несколько способов:

- с помощью команды `samba-tool` (см. п. 6.2.2);
- с помощью утилиты `nsupdate` (см. п. 6.2.3);
- оснастка DNS в RSAT (см. п. 6.2.4).

6.3. Администрирование сайтов и подсетей

Для администрирования сайтов и подсетей в «Альт Домен» можно использовать подкоманду `sites` утилиты `samba-tool`.

Примечание. Для выполнения команд 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>`.

Команды инструмента командной строки `samba-tool` для управления сайтами приведены в таблице 70.

Команды инструмента командной строки `samba-tool` для управления подсетями приведены в таблице 71.

Т а б л и ц а 70 – Команды управления сайтами инструмента `samba-tool`

Команда	Описание	Примечание
<code>sites create <сайт> [опции]</code>	Добавить новый сайт	В качестве аргумента (сайт) ожидается общее имя (CN) сайта. После создания сайта в него могут быть добавлены контроллеры домена, например, путем передачи имени сайта в параметре <code>--site=SITE</code> при выполнении операции присоединения (см. п. 2.2)
<code>sites list [опции]</code>	Вывести список сайтов	Подкоманда поддерживает два формата представления информации о сайтах: - без дополнительных параметров – список общих имен (CN) сайтов; - с параметром <code>--json</code> – вывод подробной информации о каждом сайте в формате JSON
<code>sites remove <сайт> [опции]</code>	Удалить сайт	В качестве аргумента (сайт) ожидается общее имя (CN) сайта
<code>sites subnet <подкоманда></code>	Подкоманды управления подсетью	См. таблицу 71
<code>sites view <сайт> [опции]</code>	Вывести информацию об отдельном сайте	В качестве аргумента (сайт) ожидается общее имя (CN) сайта. Подкоманда выводит тот же набор атрибутов сайта, что и подкоманда <code>samba-tool sites list --json</code>

Т а б л и ц а 71 – Команды управления подсетями инструмента samba-tool

Команда	Описание	Примечание
<code>sites subnet create</code> <подсеть> <сайт> [опции]	Создать новую подсеть	Параметры вызова: - подсеть – IP-адрес и маска подсети; - сайт – сайт, за которым будет закреплена подсеть
<code>sites subnet list</code> <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 <code>--json</code> – вывод подробной информации о каждой подсети в формате JSON
<code>sites subnet remove</code> <подсеть> [опции]	Удалить подсеть	В качестве аргумента (подсеть) ожидается общее имя (CN) существующей подсети
<code>sites subnet set-site</code> <подсеть> <сайт> [опции]	Закрепить подсеть за сайтом	Параметры вызова: - подсеть – IP-адрес и маска подсети; - сайт – сайт, за которым будет закреплена подсеть
<code>sites subnet view</code> <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 <code>samba-tool subnet list --json</code>

Полный список параметров каждой команды можно увидеть в справке, например:

```
# samba-tool sites list -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
```


6.4. Управление парольными политиками

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.

6.4.1. 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, что учетная запись пользователя заблокирована после нескольких неудачных попыток входа в систему можно, если `badPwdCount` достиг своего порога и для пользователя существует параметр `lockoutTime`:

```
# samba-tool user show ivanov
...
badPwdCount: 3
badPasswordTime: 133287267974607690
lockoutTime: 133287267974607690
...
```

Чтобы разблокировать пользователя, необходимо отредактировать объект учетной записи пользователя, установив для атрибута `lockoutTime` значение 0:

```
# samba-tool user edit ivanov
Modified User 'ivanov' successfully

# samba-tool user show ivanov
...
badPasswordTime: 133287277878749270
lockoutTime: 0
...
```

Разблокировать пользователя также можно в модуле удаленного управления базой данных конфигурации (ADMC) (подробнее см. п. 4.5) (рис. 286).

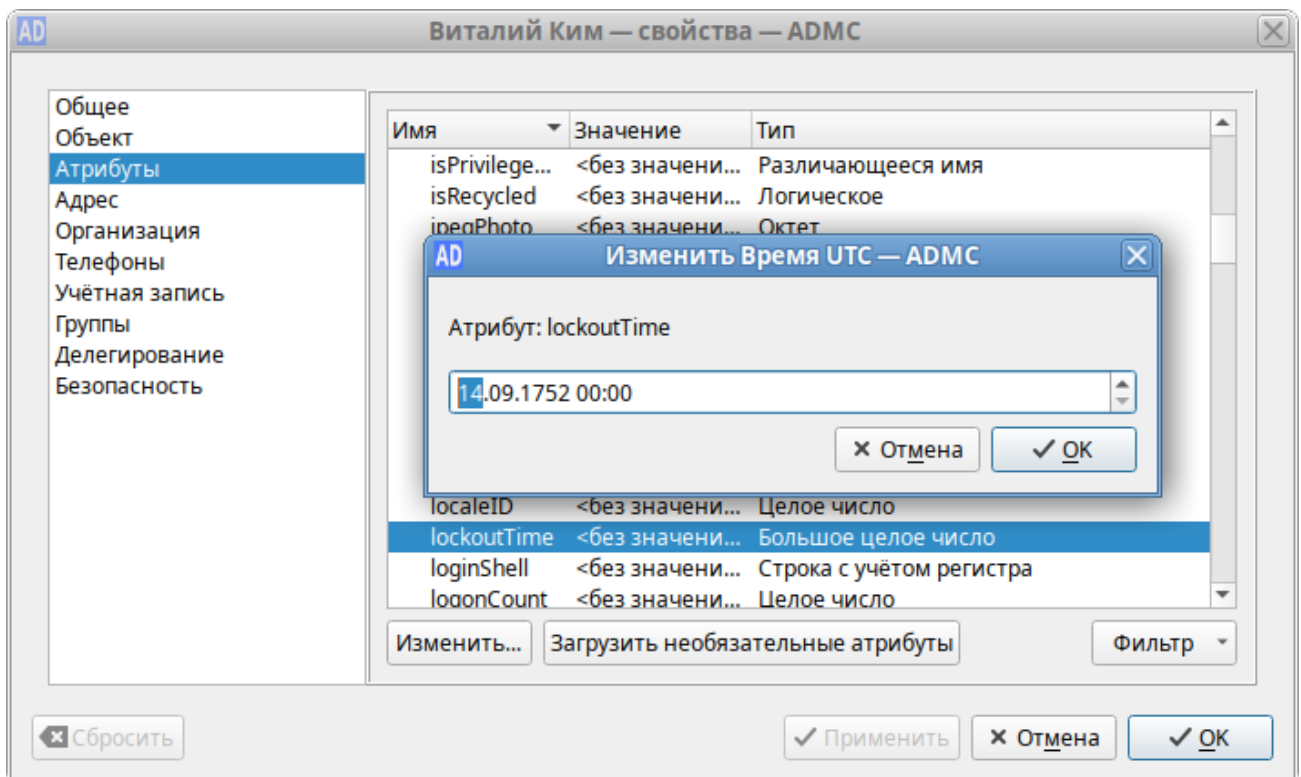


Рис. 286 – Окно модуля удаленного управления конфигурации (ADMC)

6.4.2. 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 определенных 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 (заданный с помощью параметра precedence). 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.

6.4.2.1. В ADMC

Для управления объектами настроек паролей можно использовать модуль удаленного управления базой данных конфигурации (ADMC). Подробнее см. п. 4.5.10.

6.4.2.2. 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`.

6.5. Резервное копирование и восстановление домена

6.5.1. 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. п. 6.5.2).

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 – выполняется клонирование работающей базы данных DC. По функциональности это похоже на присоединение нового контроллера домена к сети;
- offline (локальный) – резервные копии Samba создаются в том виде, в котором они появляются на диске. Сюда входят метаданные репликации, локальные для контроллера домена, которые не включаются в online резервные копии. Резервную копию также можно создать, когда контроллер домена находится в автономном режиме (т. е. процесс samba фактически не запущен);
- rename (локальный) – создается 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 DC с информацией о домене. Чтобы восстановить последующие контроллеры домена, необходимо присоединить новые контроллеры домена к восстановленному контроллеру домена.

6.5.1.1. Создание резервной копии в режиме онлайн/офлайн режимах

Схема создания резервной копии и восстановления из нее в онлайн/офлайн режимах представлена на рис. 287.

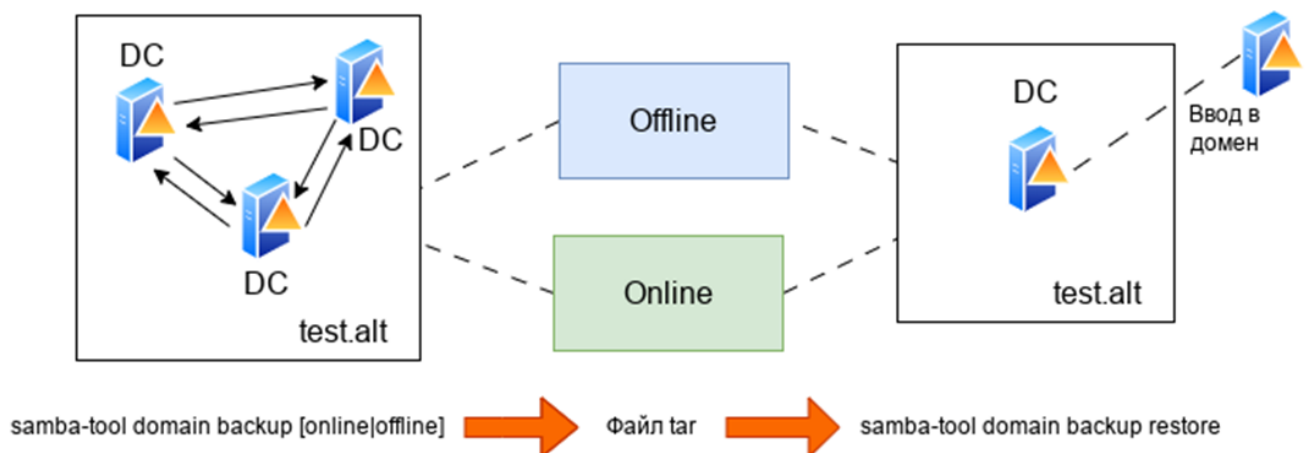


Рис. 287 – Схема создания резервной копии

6.5.1.1.1. 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 удаленно на другом компьютере. При удаленном запуске можно 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).

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...
```

6.5.1.1.2. 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 этот 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.
```

6.5.1.1.3. 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 службу каталогов 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 контроллер 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 первичной настройке домена «Альт Домен», но резервная копия содержит все объекты базы данных, добавленные 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 «Альт Домен».

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 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 параметр --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.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.
```

6.5.1.2. Переименованная резервная копия

Процедура создания резервной копии и восстановления из нее в режиме переименования показана на рис. 288.

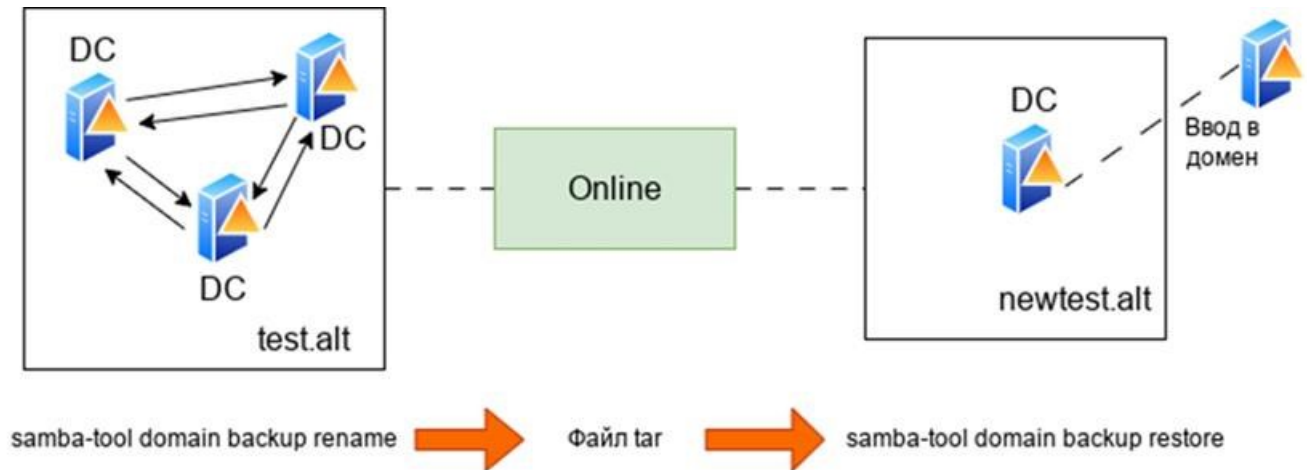


Рис. 288 – Схема создания резервной копии в режиме переименования

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, с одной стороны, обеспечить работоспособность ключевых сетевых сервисов службы каталогов, а с другой – иметь возможность детально исследовать причины возникновения проблем в существующем домене.

Создание резервной копии в режиме переименования может применяться для:

- 1) 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);

- 2) 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.

П р и м е ч а н и е . 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).

П р и м е ч а н и е . 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:

1) создание переименованной резервной копии домена:

`samba-tool domain backup rename` делает клон работающей базы данных DC, в процессе клонирования переименовывает домен и создает файл резервной копии;

2) восстановление резервной копии домена:

`samba-tool domain backup restore` берет файл резервной копии и заполняет файлы, необходимые для запуска нового контроллера.

6.5.1.2.1. 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.



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 учетных 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 подключен 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=dcl --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 запускалась на рабочем контроллере домена, необходимо скопировать сгенерированный файл резервной копии на узел, который будет использоваться в качестве нового контроллера домена.

6.5.1.2.2. 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 из переименованной резервной копии:

```
# samba-tool domain backup restore --backup-file=<tar-file> \
--targetdir=<output-dir> --newservername=<DC-name>
```

где:

- `tar-file` – файл резервной копии;
- `output-dir` – каталог, куда будут восстановлены все файлы службы каталогов (`smb.conf`, `sam.ldb` и т. п.);

- DC-name – новый контроллер домена.

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.tar.bz2
```

Примечания:

1. 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/`).

2. Новый контроллер домена не может использовать то же имя сервера, что и контроллер домена в исходной сети.

6.5.1.2.3. Сброс пароля

Во время резервного копирования/восстановления пароль для учетной 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» учетные записи пользователей/машин, либо «командовать» некоторыми учетными записями, скопированными из рабочего домена. Для учетных записей, скопированных из рабочего домена, не будут установлены пароли, поэтому на этом этапе также можно сбросить пароли для выбранных учетных записей. Или можно сделать это позже, когда служба каталогов действительно запустится на новом контроллере домена.

6.5.1.2.4. Запуск Samba

Перед запуском службы каталогов на новом контроллере домена, необходимо 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 него 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 `samba` могут быть зарегистрированы ошибки DNS. Это связано с тем, что `samba_dnupdate` 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
```

6.5.1.2.5. 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.

6.5.1.3. 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:

- 1) выполнить восстановление из файла резервной копии на временный контроллер домена и запустить службу каталогов;
- 2) повторно, по одному, присоединить исходные контроллеры домена к временному контроллеру домена (во время присоединения можно повторно использовать одно и то же имя сервера и место установки по умолчанию);
- 3) после присоединения всех исходных 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.

Пример разворачивания домена (SAMBA_INTERNAL) из резервной копии:

1) подготовить узел:

- установить пакет task-samba-dc:

```
# 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.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 каталог /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. п. 2.1.4.7):

```
# 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 4.19.7)
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.

```

6.5.1.4. Отладочная информация

Если команда резервного копирования или восстановления завершится с ошибкой, то они могут оставить после себя временный каталог (указанный в параметре `--targetdir`). Необходимо удалить этот каталог перед повторным запуском команды восстановления.

Создание резервной копии:

- 1) 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;
- 2) для резервных копий, выполненных в онлайн-режиме или в режиме переименования, следует проверить правильность используемых учетных данных и сведений о сервере. Например:

```
# ldbsearch -H ldap://<server> -UAdministrator
```
- 3) чтобы узнать больше информации о причине сбоя можно увеличить уровень журналирования. Например, добавить в команду параметр `--debug=3`;
- 4) работа команд для выполнения 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 удастся, 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;

- 5) инструменты резервного копирования не работают напрямую с контроллером домена Windows (в основном простое резервное копирование файлов sysvol не удастся из-за блокировки службы DFSR). Если используется смешанный домен контроллера домена, следует создать резервную копию контроллера домена Samba, а не контроллера домена Windows. Если у вас домен Windows, можно на время резервного копирования на контроллере домена остановить службу DFSR «Репликация DFS».

Восстановление из резервной копии:

- 1) команду восстановления необходимо запускать от имени пользователя root;
- 2) имя, указанное в параметре --newservername, не должно существовать в исходном домене. В противном случае будет получена ошибка вида:

```
Adding CN=NEWDC,OU=Domain Controllers,DC=test,DC=alt
ERROR(lldb): 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)
```

- 3) 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 для переименованных резервных копий).

6.5.2. 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, путем удаления всей информации о нем. 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 \
-Uadministrator@TEST.ALT --realm=test.alt
```

- запустить samba и обновить dns:

```
# systemctl enable --now samba
# samba_dnsupdate --use-samba-tool -verbose
```

Примечание. На других контроллерах домена в выводе команды `samba-tool drs showrepl` в секции неисправного КД 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.

6.6. Роли 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).

6.6.1. 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.

6.6.1.1. Эмулятор PDC

Владелец роли эмулятора PDC отвечает за следующие задачи в домене:

- 1) 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;
- 2) изменения паролей, внесенные другими контроллерами домена в домене, реплицируются преимущественно в эмулятор PDC. В случае недоступности эмулятора PDC информация об изменении пароля все равно распространится по домену, просто произойдет это несколько медленнее;
- 3) выполняет все функции, предоставляемые PDC в стиле NT4;
- 4) 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 учетной записи сразу после неудачной попытки, о ней уведомляется эмулятор PDC и сбрасывает счетчик неудачных попыток в ноль;
- 5) 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;
- 6) 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.
```

6.6.1.2. 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, учетные 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. Также пока хозяин RID домена находится в автономном режиме невозможно присоединиться к дополнительным контроллерам домена.

6.6.1.3. Хозяин схемы

Контроллер домена, обладающий ролью хозяина схемы, является единственным в лесу «Альт Домен», 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.

6.6.1.4. 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.

6.6.1.5. Хозяин инфраструктуры

Контроллер домена, которому принадлежит роль хозяина инфраструктуры, отвечающий 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.

6.6.1.6. Хозяин зоны DNS домена

Контроллер домена, которому принадлежит роль хозяина зоны DNS домена, отвечает за координацию добавления или удаления любых зон DNS, интегрированных в «Альт Домен», на контроллерах домена с DNS-серверами, на которых размещен домен.

На каждый домен приходится один хозяин зоны DNS-домена.

6.6.1.7. 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.

6.6.2. 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 возвращен в сеть, можно использовать принудительную передачу (захватить роль на оставшемся контроллере домена). Если старый контроллер домена будет снова подключен к сети, это вызовет конфликты и приведет к неконсистентному домену (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 удаленного управления базой данных конфигурации (ADMC).

6.6.2.1. ADCMC

См. п. 4.5.14.

6.6.2.2. Инструмент `samba-tool`

6.6.2.2.1. 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
```

6.6.2.2.2. 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=<поль>
```

Список возможных ролей:

- rid – хозяин RID;
- pdc – эмулятор PDC;
- infrastructure – хозяин инфраструктуры;
- schema – хозяин схемы;
- naming – хозяин именования доменов;
- domaindns – хозяин зоны DNS домена;
- forestdns – хозяин зоны DNS домена;
- 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

```

6.6.2.2.3. 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 (например, 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;
- pdc – эмулятор PDC;
- infrastructure – хозяин инфраструктуры;
- schema – хозяин схемы;
- naming – хозяин именования доменов;
- domaindns – хозяин зоны DNS домена;
- forestdns – хозяин зоны DNS домена;
- all – все роли.

Примечания:

1. Если роль была передана принудительно, старый контроллер домена больше никогда не должен подключаться к сети.

2. При передаче ролей `domaindns` и `forestdns` необходимо предоставить аутентификацию.

3. 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 «еще более принудительную передачу»:

```
# samba-tool fsmo seize --force --role=naming
```

6.7. Репликация

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

В Samba все, 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 п. 6.7.3.

6.7.1. Настройка репликации

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

⚠ Указание аутентифицирующей информации (имени пользователя и пароля) обязательно!

Начиная с версии `samba 3.5` топология репликации выстраивается автоматически.

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. п. 6.7.2):

```
# 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.

6.7.2. Проверка статуса репликации

6.7.2.1. 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
```

JKHB.11102-01 89 01

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

JKHB.11102-01 89 01

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 : dcl.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 должен быть приведен список всех контроллеров домена, чьи КСС установили соглашения о репликации с текущим контроллером домена. В случае, когда контроллер домена 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.

6.7.2.2. 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.

6.7.3. Двухнаправленная репликация SysVol

Каталог Sysvol присутствует на всех контроллерах домена и используется для хранения logon 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:

- двухнаправленная репликация SysVol на основе Rsync/Unison (только Samba DC);
- двухнаправленная 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` 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).

6.7.3.1. 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 присоединен 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.

Примечание. Предварительно должно быть настроено беспарольное межсерверное взаимодействие (подробнее, см. п. 6.17).

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, поэтому при повторной его работе будет использоваться ранее созданное подключение по ssh, для этого:

```
# mkdir ~/.ssh/ctl
# cat < < EOF > ~/.ssh/ctl/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

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
copyprogrestart = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace --compress
copyquoterem = true
copymax = 1

# 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
```

Примечание. 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 на DC1 и DC2 в `/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/.inison/default.prf` в другой файл, например:
`/root/.inison/sync_dc2.prf`;
- 2) в файле `/root/.inison/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
...
```

6.7.3.2. 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 присоединен 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. п. 6.17).

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 удаленном сервере
TARGET_SYNC_DIR="ssh://root@DC2:22//var/lib/samba/sysvol"
# ssh ключ root
SSH_RSA_PRIVATE_KEY="/root/.ssh/id_ed25519"
# Удаленные хосты которые osync пингует перед стартом
REMOTE_3RD_PARTY_HOSTS=""
# Сохранять xattr
PRESERVE_ACL=yes
# Сохранять xattr
PRESERVE_XATTR=yes
# Сохранять резервную копию удаленных 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
```

Примечание. 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 удаленных 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 * * * * root /usr/local/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 * * * * root /usr/local/bin/osync.sh /etc/osync/sync.conf --silent
*/5 * * * * root /usr/local/bin/osync.sh /etc/osync/sync_dc3.conf --silent
...
```

6.7.3.3. 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» (PDC Emulator), 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 FSMO «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 все прошло успешно, создать ежедневное задание `cron`:

```
#Sync 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
```

6.8. Настройка Samba для привязки к определенным 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
```

Примечания:

1. В параметре `interfaces` вместо имен интерфейсов можно указывать IP-адреса.

2. Некоторые утилиты подключаются к петлевому IP-адресу, если имя хоста не указано. Поэтому всегда нужно указывать Samba прослушивать петлевые (lo) устройства.

6.9. Создание keytab-файла

6.9.1. 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 учетной записи, которая будет использоваться для входа. К учетной 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 DNS-имя или objectGUID объекта службы каталогов, DNS-имя домена (если сервис реализует определенную службу на уровне всего домена), DNS-имя записи SRV или MX.

П р и м е ч а н и е . 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. п. 6.10.1):
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 принcipала 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.

6.9.2. Создание SPN и генерация keytab с помощью samba-tool

Добавить имена SPN для пользователя можно с помощью команды samba-tool:

```
samba-tool spn add host/fdqn@KerberosRealm <sAMAccount name>
```

В качестве аргументов передаются значение SPN и имя учетной записи SAM (значение атрибута sAMAccountName).

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 ADMS изменить для пользователя webauth значение параметра userPrincipalName на значение servicePrincipalName + REALM (в данном примере нужно поменять webauth на HTTP/test.alt@TEST.ALT рис. 289).

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).

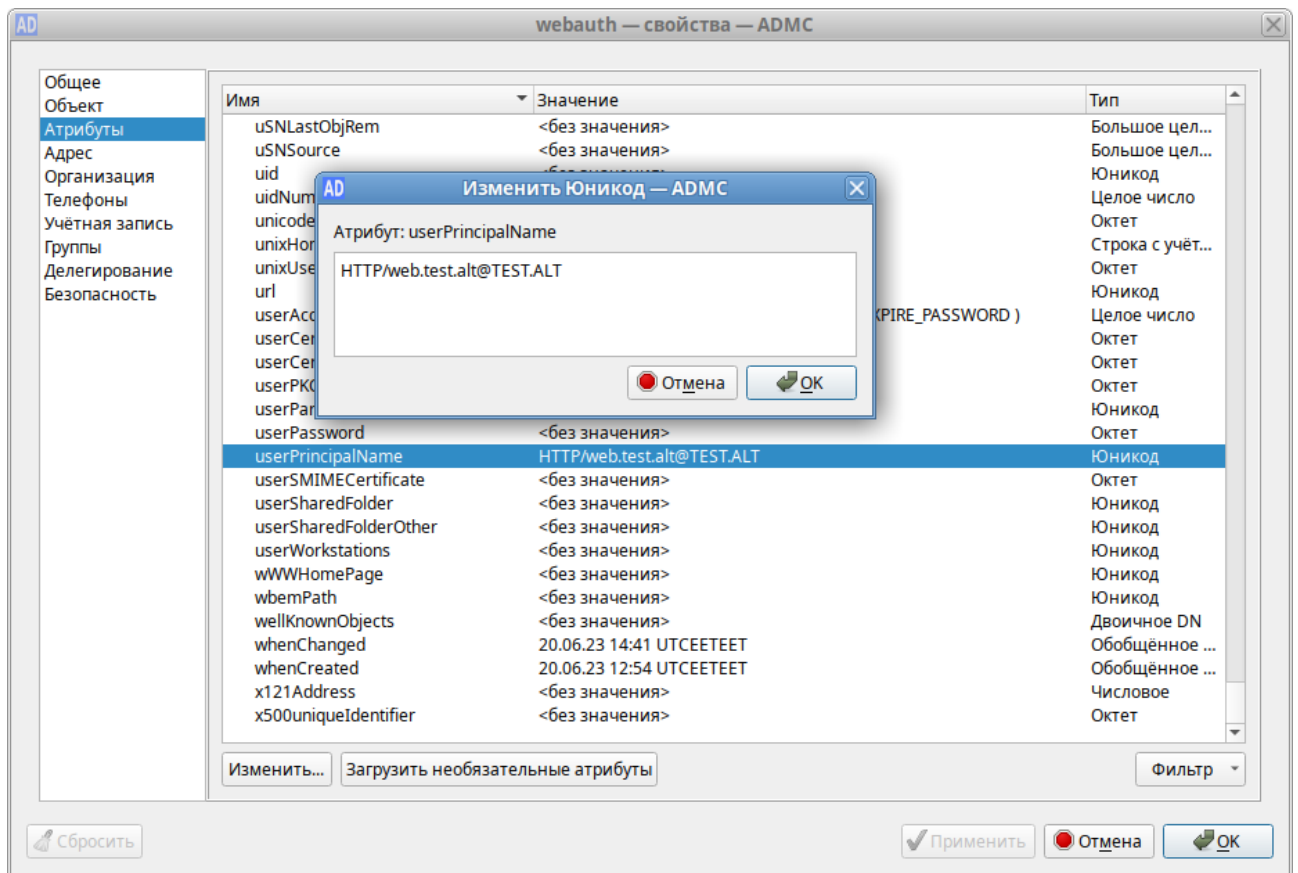


Рис. 289 – Изменение параметра userPrincipalName в ADMC

6.10. Аутентификация других сервисов в домене

6.10.1. 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.

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. DNS, предоставленный во время настройки, поставляется только с рабочей прямой зоной (и только прямой записью для DC, поэтому понадобится добавить прямую запись для веб-сервера, в качестве веб-сервера используется не DC).

Если в качестве веб-сервера используется не DC, следует добавить А-запись для веб-сервера:

```
$ samba-tool dns add dc1 test.alt web A 192.168.0.150 -Uadministrator
Password for [TEST\administrator]:
Record added successfully
```

6.10.1.1. Создание keytab-файла

Нужно настроить SPN (имена участников-служб) для имени сервера, на которое разрешается любой веб-сайт. Если виртуальный хостинг не используется, веб-адрес и имя машины будут одинаковыми. Для создания SPN на контроллере домена выполнить команды:

```
# samba-tool user create --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 /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
```

6.10.1.2. Настройка Apache2

Для настройки Apache2 необходимо выполнить следующие действия:

- 1) 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
```

- 2) 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>
```

3) добавить файл login.html в корень веб-сервера, например:

```
# echo '<html><body><h1>It works!</h1></body></html>' \
> /var/www/html/login.html
```

4) перезапустить Apache:

```
# systemctl restart httpd2
```

6.10.1.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу

http://<полное_доменное_имя_веб-сервера>.

На рабочей станции, введенной 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 прочитывать 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 прочитывать 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/2.4.62 (Unix) mod_auth_gssapi/1.6.3 OpenSSL/1.1.1u</span>
</address>
</body>
</html>

```

Содержимое страницы не доступно.

6.10.2. Настройка аутентификации Kerberos для веб-сервера Nginx

В этом подразделе показано, как обеспечить прозрачную авторизацию пользователей домена на веб-сайте, размещенном на веб-сервере Nginx.

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.

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
где dc1.test.alt – имя контроллера домена.

```

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 -Uadministrator

```

6.10.2.1. 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 create --random-password nginxauth
# samba-tool user setexpiry nginxauth
# 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
```

6.10.2.2. 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 /etc/nginx. Установить права на файл keytab:

```
# chmod 644 /etc/nginx/nginx.keytab
```

Nginx должен иметь права на чтение файла keytab, 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 учетные 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 включенной 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 в параметре `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>$

```

6.10.2.3. Проверка аутентификации

Тестовый сайт должен быть доступен по адресу

`http://<полное_доменное_имя_веб-сервера>.`

На рабочей станции, введенной 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.

6.10.3. Настройка веб-браузеров для SSO

Предварительно необходимо ввести компьютер в домен (см. п. 3) и убедиться, что доменный пользователь получает билет Kerberos.

Для работы SSO в веб-браузерах необходимо произвести некоторые настройки.

6.10.3.1. 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 (рис. 290);
- 5) 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`.

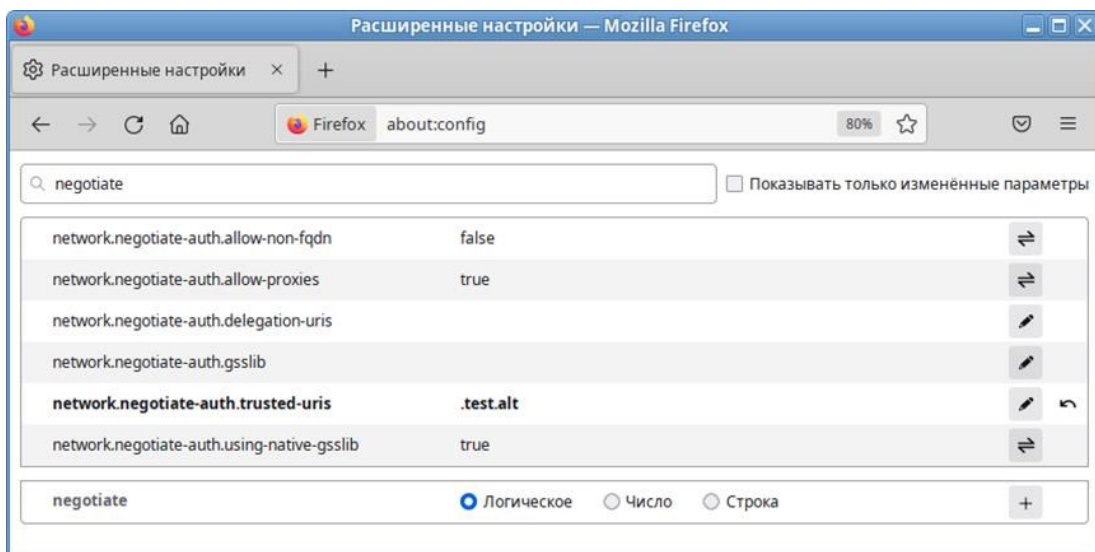


Рис. 290 – Ограниченный список параметров конфигурации

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 (см. п. 4.6.4.10):

- 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).

6.10.3.2. 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 веб-браузер. Результат применения параметров политики для Chromium можно проверить, указав в адресной строке URL: `chrome://policy`.

Этот параметр может быть распространен через групповые политики для Chromium (см. п. 4.6.4.9): политика «Список разрешенных серверов для аутентификации» и «Список разрешенных серверов для делегирования прав по протоколу Kerberos».

Примечание. Для проверки работы аутентификации без изменения настроек веб-браузера можно запустить веб-браузер из командной строки, выполнив команду:

```
$ chromium-browser --auth-server-whitelist="*.test.alt"
```

6.10.3.3. 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 веб-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» (см. п. 1.1.1.1): политики «Разрешить аутентификацию на серверах из списка» и «Разрешить делегирование прав по протоколу Kerberos на серверах».

6.11. Distributed File System

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.

6.11.1. 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 отсчет пространства имен (рис. 291). В зависимости от типа корень доступен по адресу `\\ServerName\RootName` (Stand-alone) или `\\DomainName\RootName` (Domain-based).

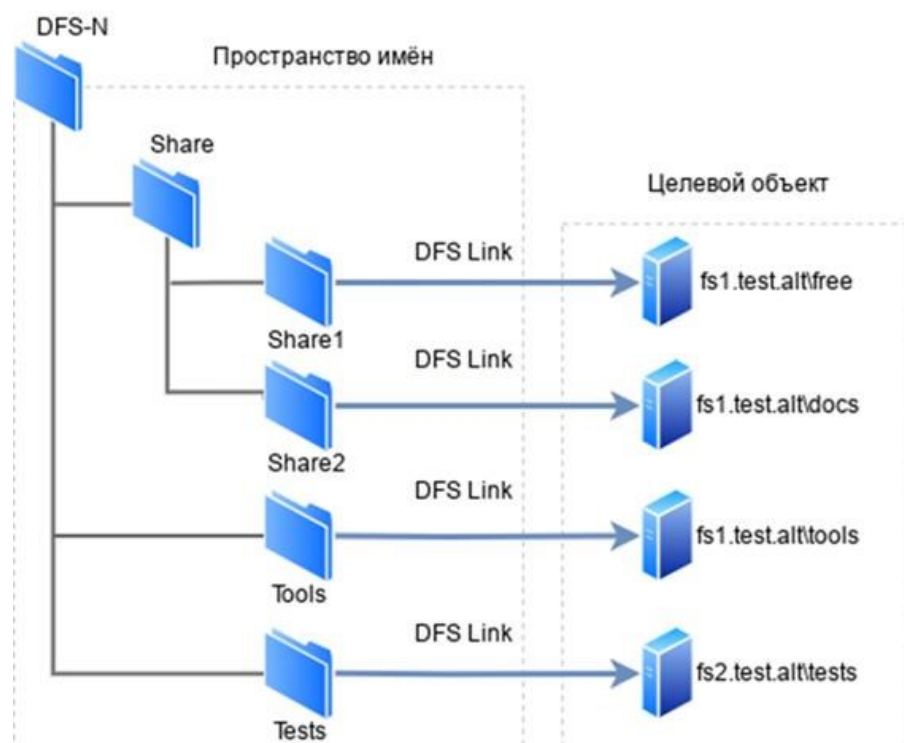


Рис. 291 – Структура дерева

Каталог – ссылка в пространстве имен DFS, указывающая на целевой объект. Каталог 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.

6.11.2. 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 `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 имен необходимо выполнить следующие действия:

- 1) создать каталог, в котором будут настроены ссылки DFS на другие серверы в сети (в примере `/media/dfsroot`):

```
# mkdir /media/dfsroot
```

- 2) в файле `/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
```

- 3) 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
```

- 4) перезапустить samba:

```
# systemctl restart samba
```

- 5) 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>` (рис. 292).

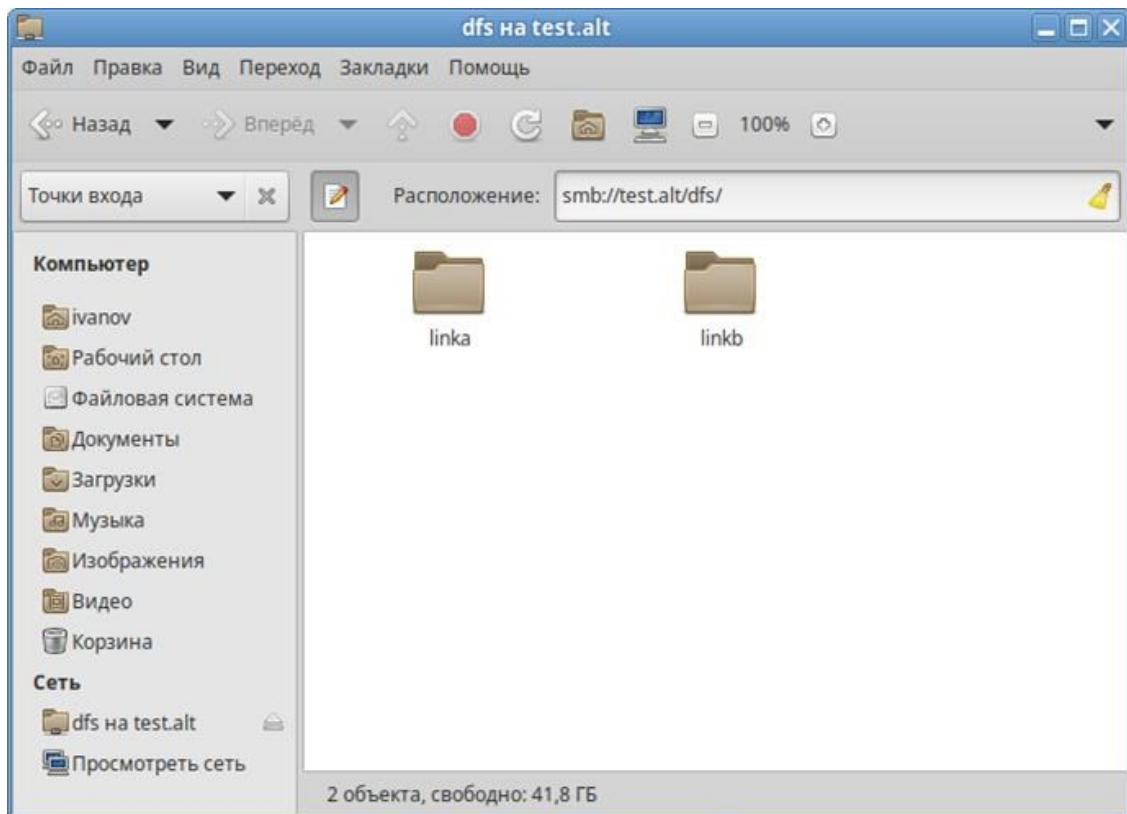


Рис. 292 – Подключение к пространству

6.12. Настройка SSSD

6.12.1. Журналирование SSSD

6.12.1.1. Файлы журналов SSSD

Каждая служба SSSD записывает логи в свой собственный файл журнала в каталоге `/var/log/sss/`. Например, для машины в домене `test.alt`, файлы журналов SSSD могут выглядеть следующим образом:

```
# ls -l /var/log/sss/
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
```

где:

- `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 ее запроса непосредственно из AD;
- `sssd_pam.log` – файл журнала для ответчика Pluggable Authentication Module (PAM);
- `sssd_ssh.log` – файл журнала для процесса ответчика SSH.

6.12.1.2. Уровни журналирования SSSD

Уровни журналирования SSSD представлены в таблице 72.

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, серьезных ошибок и для данных функций, следует использовать значение 0x0270.

Т а б л и ц а 72 – Уровни журналирования SSSD

Уровень	Описание
0 (0x0010)	Фатальные ошибки. Ошибки, которые не позволяют запустить службу SSSD или вызывает завершение работы сервиса
1 (0x0020)	Критические ошибки. Ошибки, которые не завершают работу службы SSSD, но означает, что как минимум одна из основных функций не работает должным образом
2 (0x0040)	Серьезные 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 2-го 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 еще более низкого уровня. Практически никогда не требуется

6.12.1.3. Настройка уровня журналирования 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 `<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
```

6.12.1.4. Настройка уровня журналирования 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`.

6.12.2. Настройки SSSD в ЦУС

Настройки SSSD в ЦУС представлены на рис. 293 и таблице 73.

Т а б л и ц а 73 – Настройки SSSD в ЦУС

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
Правила применения групповых политик	ad_gpo_access_control	Определяет в каком режиме будет осуществляться контроль доступа в SSSD основанный на групповых политиках AD (GPO)	enforced (принудительный режим) – правила управления доступом в SSSD основанные на GPO выполняются, ведется логирование. permissived (разрешающий режим) – правила управления доступом в SSSD основанные на GPO не выполняются, ведется 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 основанное на GPO сброшена на значение по умолчанию в пакете
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)	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,

Продолжение таблицы 73

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
			если шаблоны групповых политик не доступны. default (по умолчанию) – настройка игнорирования политик, при недоступности шаблонов групповых политик сброшена на значение по умолчанию
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)	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
Кешировать учетные данные	cache-credentials	Определяет, будут ли учетные данные удаленных пользователей сохраняться в локальном кеше SSSD	enabled (включить) – сохранение в локальном кэше SSSD учетных данных пользователей включено. disabled (отключить) – сохранение в локальном кэше SSSD учетных данных пользователей отключено. default (по умолчанию) – настройка сохранения в локальном кеше SSSD учетных данных пользователей сброшена на значение по умолчанию

Продолжение таблицы 73

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
Привилегии запуска SSSD	control sss-drop-privileges	Позволяет сбросить права службы SSSD, чтобы избежать работы от имени суперпользователя (root)	privileged (привилегированный) – служба SSSD запущена от имени привилегированного суперпользователя (root). unprivileged (непривилегированный) – служба SSSD запущена от имени непривилегированного пользователя (_sss). 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 является применимым только в том случае, если для dyndns_update установлено значение true.	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, это не имеет никакого эффекта	enabled (включить) – задать TTL. disabled (отключить) – установить значение по умолчанию (3600) unknown

Окончание таблицы 73

Настройка	Опция в файле /etc/sss/sss.conf	Описание	Режимы
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	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
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 dyndns_update имеет значение true.	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

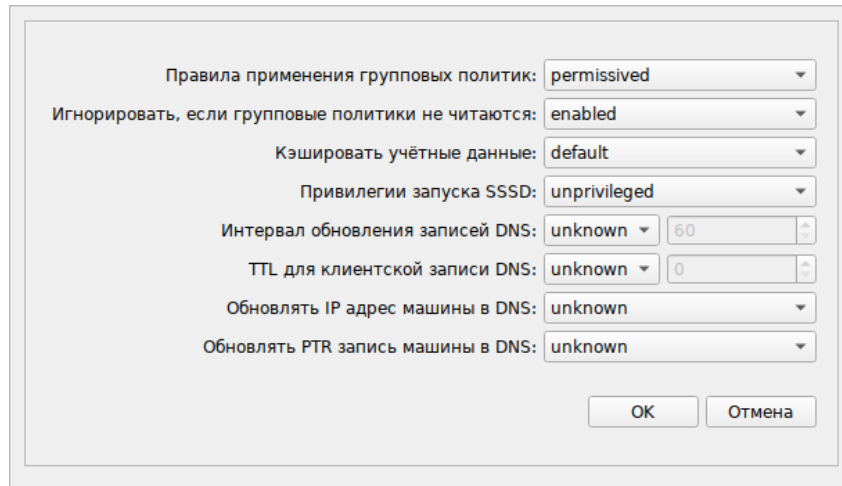


Рис. 293 – Настройки SSSD в ЦУС

6.12.3. Включение автономной аутентификации

По умолчанию SSSD не кэширует 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 кэширование учетных данных, установив параметр `cache_credentials` в значение `true` в файле `/etc/sss/sss.conf`.

Чтобы пользователи могли пройти аутентификацию, даже когда провайдер идентификации недоступен, можно включить кэширование учетных данных, установив параметр `cache_credentials` в значение `true` в разделе домена.

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
```

- отключить кеширование учетных данных:

```
# control sssd-cache-credentials disabled
```

Данные настройки можно применить с помощью механизма групповых политик `control`. Подробнее см. п. 4.6.4.2.

6.13. Монтирование общих ресурсов samba

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

6.13.1. Подключение с использованием gio

Примечание. Способ актуален для дистрибутивов, использующих gio.

Недостаток этого способа – необходимо открыть ресурс в файловом менеджере (Caja, Rmanfm). Однако можно открывать любые ресурсы на любых серверах, входящие в домен.

Процедура монтирования общих ресурсов с использованием gio:

- установить необходимые пакеты (дистрибутив ОС Альт СП Рабочая станция):

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

- включить пользователя в группу fuse:

```
# gpasswd -a <пользователь> fuse
```

- разрешить для всех доступ к fuse под root:

```
# control fusermount public
```


- войти под доменным пользователем;
- открыть ресурс в файловом менеджере (например, по адресу `smb://server/sysvol`). Ресурс 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 путем `/var/run/uid_пользователя/gvfs`.

6.13.2. 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`

Примечание. 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:

- а) `uid="10000-2000200000"` – диапазон присваиваемых для доменных пользователей UID (подходит для Winbind и для SSSD);
- б) `server="dc1.test.alt"` – имя сервера с ресурсом;
- в) `path="sysvol"` – имя файлового ресурса;
- г) `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`.

⚠ В параметре `server` необходимо указывать настоящее имя сервера, а не имя домена.

⚠ 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 также можно проверить доступность ресурса с помощью `smbclient`, например: `smbclient -L dc1.test.alt -U ivanov -m SMB2`

6.13.3. Подключение с использованием Autofs

При этом способе заданный ресурс подключается автоматически при каждом обращении пользователя и отключается после определенного времени бездействия (определяется конфигурацией Autofs).

Принцип работы:

- задается 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*`. Основным шаблоном 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.

П р и м е ч а н и е . 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
```

где:

- `/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 в диспетчере файлов (рис. 294) или в командной строке, например:

```
$ ls /mnt/samba/<имя_хоста>
```

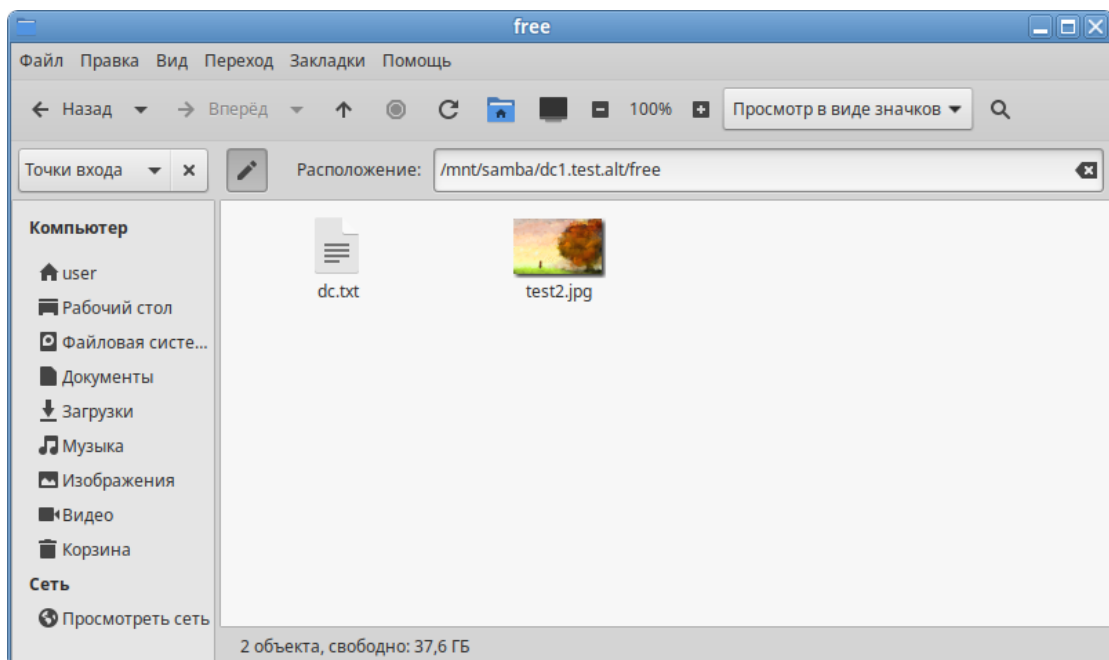


Рис. 294 – Диспетчер файлов

6.14. Журналирование в Samba

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 находятся в каталоге `/var/log/samba/`.

6.14.1. 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 `logging`, который задается в разделе `[global]` файла `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 Мбайт).
- 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
```

6.14.2. Настройка файлов журнала

Параметр `log file` в разделе `[global]` файла `smb.conf` позволяет переопределить файл журнала Samba.

Параметр `log file` использует стандартные подстановки, что позволяет 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]` `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 `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 Мбайт:

```
max log size = 1000
```

П р и м е ч а н и е . В процессе ротации Samba перезаписывает архивированный ранее файл.

6.14.3. Уровни журналирования

Установить уровень журналирования для Samba можно, используя параметр `log level` в разделе `[global]` файла `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.

Доступны следующие классы отладки:

- all;
- tdb;

- printdrivers;
- lanman;
- smb;
- rpc_parse;
- rpc_srv;
- rpc_cli;
- passdb;
- sam;
- auth;
- winbind;
- vfs;
- idmap;
- quota;
- acls;
- locking;
- msdfs;
- dmapi;
- registry;
- scavenger;
- dns;
- ldb;
- tevent;
- auth_audit;
- auth_json_audit;
- kerberos;
- drs_repl;
- smb2;
- smb2_credits;
- dsdb_audit;

- dsdb_json_audit;
- dsdb_password_audit;
- dsdb_password_json_audit;
- dsdb_transaction_audit;
- dsdb_transaction_json_audit;
- dsdb_group_audit;
- dsdb_group_json_audit.

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 входили в другой файл, а не в файл журнала, можно добавить @ПАТН к классу.

П р и м е ч а н и е . Получить дополнительную информацию и список классов отладки можно на справочной странице smb.conf(5) (man smb.conf).

6.14.3.1. Установка уровня журналирования в файле smb.conf

Примеры использования параметра log level для настройки уровня журналирования:

- установить уровень журнала для всех классов отладки на 3:
log level = 3

- установить общий уровень журнала на 3 и для классов passdb и auth на 5:

```
log level = 3 passdb:5 auth:5
```

- установить уровень журнала для класса winbind на 1 и писать логи в файл /var/log/winbind.log:

```
log level = 3 winbind:1@/var/log/winbind.log
```

6.14.3.2. Установка уровня журналирования при выполнении команд

Команды Samba используют уровень журналирования, установленный в параметре `log level` в файле `smb.conf`. Это значение можно переопределить, используя следующую опцию для всех команд Samba:

```
-d DEBUGLEVEL, --debuglevel=DEBUGLEVEL
```

Например:

```
$ net usershare add Share2 /tmp/share2 -d 5  
# samba-tool group add testgroup12 -d dsdb_audit:10
```

6.14.4. 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 на 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.

6.14.4.1. Регистрация событий аутентификации и авторизации

Samba поддерживает протоколирование успешных событий и неуспешных событий аутентификации, а также успешных событий авторизации.

Примечания:

1. Аутентификация происходит, когда Samba проверяет комбинацию имени пользователя и пароля.
2. 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 контроллере домена, 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;

- 3) 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` – стандартный формат журнала;
- `auth_json_audit` – формат JSON.

Для классов `auth_audit` и `auth_audit_json` 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":
    "5bd240f7cc4delb5", "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}}
```

6.14.4.2. 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 логирования:

- 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 логирования:

- 5 – успешные события изменения и сброса пароля.

Для регистрации не успешных 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` доступны следующие уровни логирования:

- 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 изменений 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 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.

6.14.5. 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 трех 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": 2023-04-13T11:48:45.902942+0200,
  "type": одно из значений "Authentication", "Authorization", "dsdbChange",
        "dsdbTransaction", "passwordChange", "replicatedUpdate",
        "groupChange",
  type: { data }
}
```

Примечание. Некоторые атрибуты могут присутствовать в журнале, 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», а другие поля сетевого входа будут иметь аналогичные пустые значения.

6.14.5.1. Общие атрибуты

В таблице 74 приведено описание атрибутов, которые присутствуют при регистрации любого события.

Т а б л и ц а 74 – 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

6.14.5.2. Атрибуты событий аутентификации (Authentication)

В таблице 75 приведен набор атрибутов, который используется для регистрации событий аутентификации.

Т а б л и ц а 75 – Аутентификация

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 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 отличаться от учетной записи, предоставленной клиентом)
becameDomain	Имя домена, в который произведен вход
becameSid	Идентификатор безопасности (SID) аутентифицированной учетной записи
clientAccount	Имя учетной 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
localAddress	Адрес сервера и используемый порт

Продолжение таблицы 75

Атрибут	Значение
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 – NetworkCleartext с использованием нехешированных паролей, то есть вход выполняется по сети, при этом пароль передается в пакет подтверждения подлинности в нехешированной форме (NetworkCleartext)
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) учетной 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 здесь «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;

Окончание таблицы 75

Атрибут	Значение
	- 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); - 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 74 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 }}
```

6.14.5.3. Атрибуты событий авторизации (Authorization)

В таблице 76 приведен набор атрибутов, который используется для регистрации успешных событий авторизации.

Т а б л и ц а 76 – Успешные события авторизации

Атрибут	Значение
account	Имя авторизуемой учетной записи
accountFlags	Битовое поле атрибутов учетной записи
authType	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 канала (например, «SMB», «TLS», «SEAL», «NONE»)
version	См. описание в таблице 74 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
  }
}
```

```
{
  "timestamp": "2024-05-29T15:37:54.370408+0200",
  "type": "KDC Authorization",
  "KDC Authorization": {
    "version": {
      "major": 1,
      "minor": 0
    },
    "status": "NT_STATUS_OK",
    "localAddress": null,
    "remoteAddress": "ipv6:fd47:d11e:43c1:0:a00:27ff:fe9d:4de0:38254",
    "serviceDescription": "cifs/dc1.local@TEST.ALT",
    "authType": "TGS-REQ with Ticket-Granting Ticket",
    "domain": "TEST",
    "account": "ivanov",
    "sid": "S-1-5-21-578923263-1107570656-1287136478-1103",
    "logonServer": "DC1",
    "authTime": "2024-05-29T15:37:54.366830+0200",
    "serverPolicyAccessCheck": null
  }
}
```

```
{
  "timestamp": "2024-05-29T14:39:06.431833+0200",
  "type": "KDC Authorization",
  "KDC Authorization": {
    "version": {
      "major": 1,
      "minor": 0
    },
    "status": "NT_STATUS_OK",
    "localAddress": null,
    "remoteAddress": "ipv4:192.168.0.135:55142",
    "serviceDescription": "WORK135$@TEST.ALT",
    "authType": "TGS-REQ with Ticket-Granting Ticket",
    "domain": "TEST",
    "account": "ivanov",
    "sid": "S-1-5-21-578923263-1107570656-1287136478-1103",
    "logonServer": "DC1",
    "authTime": "2024-05-29T14:39:06.429012+0200",
    "serverPolicyAccessCheck": null
  }
}
```

6.14.5.4. Атрибуты событий, связанных с изменениями в базе данных (dsdbChange)

События dsdbChange регистрируются, когда клиент вызывает существенные изменения в базе данных (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 77 приведен набор атрибутов, который используется для регистрации событий, связанных с внесением значимых изменений в базу данных службы каталогов.

Т а б л и ц а 77 – События dsdbChange

Атрибут	Значение
attribute	Список изменяемых атрибутов
dn	Уникальное составное имя (DN) изменяемого объекта
operation	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»;

Окончание таблицы 77

Атрибут	Значение
	- «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
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)
userSid	Идентификатор безопасности (SID) пользователя, инициировавшего операцию
version	См. описание в таблице 74 Текущая версия: {"major": 1, "minor": 0}

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": "2024-05-29T15:20:19.635275"}
        ]
      }
    ]
  }
}
```

описывает изменение, выполненное этим LDIF:

```
dn: @SAMBA_DSDB
changetype: modify
add: backupDate
backupDate: 2024-05-29T15:20:19.635275
```

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 } ] } } } }
```

6.14.5.5. 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 78 приведен набор атрибутов, связанных с транзакциями (dsdbTransaction).

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 } }
```

Т а б л и ц а 78 – 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 74 Текущая версия: {"major": 1, "minor": 0}

6.14.5.6. Атрибуты событий, связанных с изменением пароля (passwordChange)

PasswordChange – это особый вид dsdbChange.

В таблице 79 приведен набор атрибутов, который используется для регистрации событий, связанных с изменением пароля (passwordChange).

Т а б л и ц а 79 – События, связанные с изменением пароля (passwordChange)

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 74 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" }
```

6.14.5.7. Атрибуты событий, связанных с изменением группы (groupChange)

Событие groupChange указывает на изменение DSDB, которое добавляет или удаляет пользователя из группы.

В таблице 80 приведен набор атрибутов, который используется для регистрации событий, связанных с изменением группы (groupChange).

Т а б л и ц а 80 – Атрибуты событий, связанных с изменением группы (groupChange)

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

Окончание таблицы 80

Атрибут	Значение
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 74 Текущая версия: { "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" }}
```

6.15. Усиление безопасности DC

6.15.1. 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
```

6.15.2. 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 smb.conf:

```
[global]
disable netbios = yes
smb ports = 445
```

6.15.3. 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 smb.conf:

```
[global]
printcap name = /dev/null
load printers = no
disable spoolss = yes
printing = bsd
```

6.15.4. 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 smb.conf:

```
[global]
ntlm auth = mschapv2-and-ntlmv2-only
```

6.15.5. Генерация дополнительных хешей паролей

Чтобы разрешить передачу хешей в другую базу аутентификации, можно указать «Альт Домен» генерировать дополнительные хеши, когда пользователь меняет свой пароль. Для этого следует добавить в секцию [global] файла smb.conf строку:

```
[global]
password hash userPassword schemes = CryptSHA256 CryptSHA512
```

6.15.6. 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 веб-браузерах WPAD, в частности в веб-браузерах Internet Explorer.

Даже если конфигурации wpad и isatap не используются, все 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
```

6.15.7. 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 smb.conf строку:

```
[global]
rpc server dynamic port range = 50000-55000
```

Примечание. Если используется фаервол, то его нужно будет перенастроить.

6.15.8. Аудит запросов к каталогам SYSVOL и NetLogon

Для возможности аудита запросов к каталогам SYSVOL и NetLogon следует добавить в файл `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
```

6.15.9. Отправка логов аудита в rsyslog

6.15.9.1. Настройка rsyslog

Установить пакет `rsyslog-classic`:

```
# apt-get install rsyslog-classic
```

На стороне отправителя сообщений (клиента) создать файл `/etc/rsyslog.d/all.conf`, в котором прописать протокол (`@@` – TCP, `@` – UDP) и адрес доставки сообщений:

```
*.* @@192.168.0.111:514
```

На стороне приемника сообщений (сервера) 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")
```

И создать свой шаблон для логов `/etc/rsyslog.d/myrules.conf`:

```
$template remote-incoming-logs, "/var/log/%HOSTNAME/%PROGRAMNAME.log"
*. * ?remote-incoming-logs
```

6.15.9.2. rsyslog на том же хосте

В секцию `[global]` файла `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="dcl.test.alt" port="514" protocol="tcp"
action.resumeRetryCount="100"
queue.type="LinkedList" queue.size="10000")
}
```

6.15.9.3. rsyslog на вышестоящем хосте

В секцию `[global]` файла `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
```

6.16. Инструменты командной строки

Основные инструменты командной строки для управления доменом представлены в таблице 81.

Т а б л и ц а 81 – Основные инструменты

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 – <code>/etc/samba/smb.conf</code>

6.16.1. Команда `samba-tool`

Основные команды утилиты `samba-tool` приведены в таблице 82.

Т а б л и ц а 82 – Основные команды `samba-tool`

Команда	Описание
<code>computer</code>	Управление учетными записями компьютеров
<code>contact</code>	Управление контактами
<code>dbcheck</code>	Проверка локальной базы данных домена на наличие ошибок
<code>delegation</code>	Управление делегированием
<code>dns</code>	Управление параметрами доменной службы DNS
<code>domain</code>	Управление параметрами домена
<code>drs</code>	Управление службой репликации каталогов (Directory Replication Services, DRS)
<code>dsacl</code>	Управление групповыми политиками
<code>forest</code>	Управление ролями (Flexible Single Master Operations, FSMO)
<code>fsmo</code>	Управление конфигурацией леса
<code>gpo</code>	Управление списками контроля доступа DS
<code>group</code>	Управление группами
<code>ldapcmp</code>	Сравнение двух баз данных ldap
<code>ntacl</code>	Вывод списка процессов
<code>processes</code>	Управление списками контроля доступа ACL
<code>ou</code>	Управление организационными подразделениями (OU)
<code>rodc</code>	Управление контроллером домена (Read-Only Domain Controller, RODC)
<code>schema</code>	Управление и запрос схемы
<code>sites</code>	Управление сайтами
<code>spn</code>	Управление службой принципалов (Service Principal Name, SPN)
<code>testparm</code>	Проверка конфигурационного файла на корректность синтаксиса
<code>time</code>	Получение показаний текущего времени сервера
<code>user</code>	Управление пользователями
<code>visualize</code>	Графическое представление состояния сети Samba

Получить дополнительную информацию можно на справочной странице `samba-tool (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
```

ЛКНВ.11102-01 89 01

```

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-F5FFFAA1010FD}
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
```

6.16.2. Команда wbinfo

Команда `wbinfo` создает запросы и возвращает информацию к (от) демона `winbindd`.

Параметры команды `wbinfo` представлены в таблице 83.

Т а б л и ц а 83 – Параметры команды wbinfo

Параметр	Описание	Пример
-a --authenticate username %password	Попытаться аутентифицировать пользователя через winbindd 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: Enter ivanov's new password:
--dc-info <домен>	Вывести текущий контроллер домена для домена	\$ wbinfo --dc-info TEST dc1.test.alt (192.168.0.132)

Продолжение таблицы 83

Параметр	Описание	Пример
--domain <домен>	Определяет домен, в котором будут выполняться любые указанные операции	
-D --domain-info <домен>	Показать информацию об указанном домене	<pre>\$ wbinfo -D TEST Name : TEST Alt_Name : test.alt SID : S-1-5-21-578923263-1107570656-1287136478 Active Directory : Yes Native : Yes Primary : Yes</pre>
--dsgetdcname <домен>	Найти DC для домена	<pre>\$ 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</pre>
--gid-info <gid>	Получить информацию о группе по gid	<pre>\$ wbinfo --gid-info 10000 domain admins:*:10000:</pre>
--group-info <группа>	Получить информацию о группе по имени группы	<pre>\$ wbinfo --group-info "TEST\\domain admins" domain admins:*:10000:</pre>
-g --domain-groups	Вывести список доменных групп	<pre>\$ wbinfo -g ... TEST\domain admins TEST\domain users TEST\domain guests TEST\domain computers ...</pre>

Продолжение таблицы 83

Параметр	Описание	Пример
--get-auth-user	Эта функция была перенесена в утилиту net	
--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	\$ 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 кэша учетных данных Kerberos, используемый для аутентификации	
--lanman	Использовать криптографию Lanman для аутентификации пользователей	
--logoff	Выйти из системы	

Продолжение таблицы 83

Параметр	Описание	Пример
--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	\$ 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	\$ wbinfo --online-status BUILTIN : active connection TEST : active connection

Продолжение таблицы 83

Параметр	Описание	Пример
--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	\$ 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>	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

Продолжение таблицы 83

Параметр	Описание	Пример
--separator	Вывести активный разделитель winbind	\$ wbinfo --separator \\
--sequence	Команда устарела, вместо нее следует использовать параметр --online-status	
--set-auth-user <имя_пользователя>%<пароль>	Эта функция была перенесена в утилиту net	
--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
--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

Продолжение таблицы 83

Параметр	Описание	Пример
-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
--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

Окончание таблицы 83

Параметр	Описание	Пример
-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	\$ wbinfo -Y S-1-5-21-578923263-1107570656-1287136478-513 10001

6.16.3. Команда 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.

Основные подкоманды команды net ads представлены в таблице 84.

Т а б л и ц а 84 – Основные подкоманды 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: Чт, 08 июн 2023 11:48:01 EET
KDC server: 192.168.0.132
Server time offset: -171
Last machine account password change: Вт, 16 мая 2023 09:26:46 EET
```

Получение информации об учетной записи компьютера:

```
# net ads status -U administrator
```

6.16.4. Команда `adcli`

`adcli` — инструмент для выполнения действий в домене Active Directory.

Основные команды `adcli` представлены в таблице 85.

Т а б л и ц а 85 – Основные команды `adcli`

Команда	Описание
<code>info домен</code>	Вывести информацию о домене
<code>join домен</code>	Присоединить данную машину к домену (создает учетную запись компьютера в домене и настраивает <code>keytab</code> для этой машины. Не настраивает службу аутентификации, например, <code>sssd</code>).
<code>update</code>	Обновляет пароль учетной записи компьютера на контроллере домена для локальной машины, записывает новые ключи в <code>keytab</code> и удаляет старые ключи
<code>testjoin</code>	Проверить, действителен ли пароль учетной записи компьютера
<code>create-user [--domain=домен] пользователь</code>	Создать учетную запись пользователя
<code>delete-user [--domain=домен] пользователь</code>	Удалить учетную запись пользователя
<code>passwd-user [--domain=домен] пользователь</code>	Установить (повторно) пароль пользователя
<code>create-group [--domain=домен] группа</code>	Создать группу
<code>delete-group [--domain=домен] группа</code>	Удалить группу
<code>add-member [--domain=домен] группа пользователь</code> или компьютер...	Добавить пользователей в группу

Окончание таблицы 85

Команда	Описание
<code>remove-member</code> <code>[--domain=домен] группа пользователь...</code>	Удалить пользователей из группы
<code>preset-computer [--domain=домен] компьютер...</code>	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).
<code>reset-computer [--domain=домен] компьютер</code>	Сбросить учетную запись компьютера (если соответствующая машина присоединена к домену, ее членство будет нарушено).
<code>delete-computer [--domain=домен] компьютер</code>	Удалить учетную запись компьютера
<code>show-computer [--domain=домен] компьютер</code>	Показать атрибуты учетной записи компьютера, хранящиеся в AD
<code>create-msa</code> <code>[--domain=домен]</code>	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`.

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
```

6.16.5. Утилита 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.

Если утилита ldapsearch найдет одну или несколько записей, то значения указанных атрибутов этих записей будут переданы в стандартный поток вывода. Если атрибуты не указаны, то возвращаются все атрибуты.

Результаты поиска отображаются в виде расширенной версии LDIF. Формат вывода контролируется с помощью параметра -L.

Параметры команды ldapsearch представлены в таблице 86.

Т а б л и ц а 86 – Параметры команды ldapsearch

Параметр	Описание
Параметры поиска	
-a {never always search find}	Задаёт 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);

Продолжение таблицы 86

Параметр	Описание
	- [!]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]	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}	Задаёт 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

Продолжение таблицы 86

Параметр	Описание
-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 подключении к каталогу LDAP. При SASL-подключениях сервер будет игнорировать это значение
-e [!] <i>ext</i> [= <i>extparam</i>]	Указывает общие расширения. Знак «!» обозначает критичность расширения. Общие расширения: - [!]<i>assert</i>=<<i>filter</i>> (RFC 4528; фильтр RFC 4515) - [!]<i>authzid</i>=<<i>authzid</i>> (RFC 4370; "dn:<dn>" или "u:<user>") - [!]<i>chaining</i>[=<<i>resolveBehavior</i>>[/<<i>continuationBehavior</i>>]] - [!]<i>manageDSAit</i> (RFC 3296) - [!]<i>noop</i> - <i>ppolicy</i> - [!]<i>postread</i>[=<<i>attrs</i>>] (RFC 4527; разделенный запятыми список атрибутов) - [!]<i>preread</i>[=<<i>attrs</i>>] (RFC 4527; разделенный запятыми список атрибутов) - [!]<i>relax</i>

Продолжение таблицы 86

Параметр	Описание
	- [!]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	Использовать тихий режим SASL. Запросы не выводятся никогда
-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)

Окончание таблицы 86

Параметр	Описание
-x	Использовать простую аутентификацию
-X authzid	Идентификатор авторизации SASL («dn:<dn>» или «u:<user>»)
-y file	Считать пароль из файла file. В качестве пароля используется все 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)

6.16.5.1. Фильтр

Фильтр должен быть указан в строковом формате фильтров. 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.

Примеры LDAP-фильтров представлены в таблице 87.

Т а б л и ц а 87 – 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	(&(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))

Окончание таблицы 87

Запрос	LDAP фильтр
Пользователи с ограниченным сроком действия учетной записи	(&(sAMAccountType=805306368)(accountExpires>=1)(accountExpires<=9223372036854775806))
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 учета вложенности)	(memberOf=CN=Sales,CN=Users,DC=test,DC=alt)
Все члены группы Sales (с учетом 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)

6.16.5.2. 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`, то будут выводиться только имена атрибутов.

Примечания:

1. 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

2. 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'
```

6.16.5.3. 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)
#
```

6.16.6. Команда `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 информации:

- состоянии домена;
- аутентификации пользователя;
- доступа пользователей к клиентам определенного домена;
- информация о кэшированном содержимом.

С помощью утилиты `sssctl` можно:

- управлять кэшем SSSD;
- управлять журналами;
- проверить конфигурационные файлы.

Основные команды `sssctl` представлены в таблице 88.

Т а б л и ц а 88 — Основные команды `sssctl`

Команда	Описание
Статус SSSD	
<code>domain-list</code>	Вывести список доступных доменов
<code>domain-status</code> домен	Вывести информацию о домене
<code>user-checks</code> пользователь	Вывести информацию о пользователе и проверить аутентификацию
<code>access-report</code> домен	Создание отчета о правилах управления доступом для домена, которые применяются к клиентскому компьютеру (работает только для домена FreeIPA)

Окончание таблицы 88

Команда	Описание
Информация о кэшированном содержимом	
user-show пользователь	Информация о кэше пользователя
group-show группа	Информация о кэше группы
netgroup-show группа	Информация о кэше 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 кэшированного содержимого
cache-upgrade	Выполнить обновление кеша
cache-expire	Сделать недействительными кэшированные 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
cert-show сертификат	Вывести информацию о сертификате
cert-map сертификат	Показать пользователей, привязанных к сертификату

Получить дополнительную информацию можно на справочной странице `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 кэше пользователя:

```
# sssctl user-show kim
Name: kim
Cache entry creation date: 12/28/22 13:39:46
Cache entry last update time: 06/19/23 09:55:29
Cache entry expiration time: Expired
Initgroups expiration time: Expired
Cached in InfoPipe: No
```

Проверить информацию о пользователе и его учетной записи:

```
# sssctl user-checks kim
user: kim
action: acct
service: system-auth
SSSD nss user lookup result:
- user name: kim
- user id: 1187401107
- group id: 1187400513
- gecos: Олег Ким
- home directory: /home/TEST.ALT/kim
- shell: /bin/bash
SSSD InfoPipe user lookup result:
- name: kim
- uidNumber: 1187401107
- gidNumber: 1187400513
- gecos: Олег Ким
- homeDirectory: not set
- loginShell: not set
testing pam_acct_mgmt
pam_acct_mgmt: Success
PAM Environment:
- no env -
```

6.16.7. Команда 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:tcipip = no
rpc_daemon:spoolssd = embedded
rpc_server:spoolss = embedded
rpc_server:winreg = embedded
rpc_server:ntsvcs = embedded
rpc_server:eventlog = embedded
rpc_server:svrsvc = 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

```

6.17. Конфигурационные файлы

/etc/samba/smb.conf – файл конфигурации Samba.

/etc/krb5.conf – файл конфигурации Kerberos.

6.17.1. Файл sssd.conf

/etc/sss/sss.conf – файл конфигурации SSSD.

Для работы с Active Directory в SSSD имеется специальный AD-провайдер sssd-ad.

Минимальный конфигурационный файл (/etc/sss/sss.conf) для sssd-ad:

```

[sss]
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 `man sssd.conf`.

6.17.2. Файл `resolv.conf`

`/etc/resolv.conf` – файл конфигурации резолвера (механизма преобразования имен хостов в адреса IP).

Файл конфигурации резолвера (resolver) содержит информацию, которая считывается функциями разрешения имен 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 имен. Файл настройки считается надежным 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 имен 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:

1) `nameserver` (IP-адрес сервера имен)

Интернет-адрес сервера имен, 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 имен, 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 имен на локальном компьютере. Используемый алгоритм заключается в том, чтобы попробовать обратиться к первому указанному серверу имен, 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;

2) `options`

Позволяют изменять некоторые внутренние переменные функций определения имен. Синтаксис:

`options параметр ...`

где параметр может иметь следующие значения:

- `attempts:n`

Задаёт количество попыток, которое преобразователь предпримет, отправляя запрос на свои серверы имен, 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);

- `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`, 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`, а не `gethostbyname`;

- `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);

- `ndots:n`

Задаёт минимальное количество точек, которые должны обязательно присутствовать в имени, переданном функции `res_query` (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 и 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 подчеркивания (`_`), не-ASCII или управляющие символы;

- no-reload (начиная с glibc 2.16)

Задаёт значение `RES_NORELOAD` в `_res.options`. Эта опция отключает автоматическую перезагрузку изменённого 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 имен. Без этой опции распознаватель всегда будет запрашивать первый сервер имен в списке и использовать последующий сервер имен только в случае сбоя первого. Эта опция позволяет распределить нагрузку между разными серверами имен;

- `single-request-reopen` (начиная с `glibc 2.9`)

Задаёт `RES_SNGLKUPREOP` в `_res.options`. Для разрешения имен 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 счёт некоторого замедления процесса разрешения имени);

- `timeout:n`

Задаёт промежуток времени, который функции определения имен будут ждать ответа от удаленного сервера имен перед тем как повторить запрос другому серверу имен.

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 и 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`)

Задает 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`; локальным доменным именем считается все, 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 имен, 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` выше, 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`. 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. Она настраивается как посредник между программами-поставщиками и программами-потребителями этой информации.

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 удастся, 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`.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ	– виртуальная машина;
ГП	– групповая политика;
ОЗУ	– оперативное запоминающее устройство;
ОС	– операционная система;
ПИ	– программное изделие;
ПО	– программное обеспечение;
ЦУС	– центр управления системой.

[illegible][illegible]