



ООО «БАЗАЛЬТ СПО»

**Сергей Перроте,
директор по работе
с корпоративными клиентами
ООО «Базальт СПО»,
sp@basealt.ru**

**ОС «Альт» - универсальный инструмент плавной
миграции с MS на Linux: AD + Samba DC**

**Своя платформа
сборки**

Свои инструменты
разработки
тестирования
обеспечения целостности

Свой репозиторий
100+ тыс пакетов

**ПО с открытым
исходным кодом**

**20+ лет на
рынке**

**200+ тыс
лицензий в год**

**800+ обученных
специалистов**

офисы в 4-х городах



Российские



- Эльбрус 4С/8С/8СВ
4/8/8 ядер VLIW
1,6 GHz (e2k) 28 нм



- «Байкал Т» тонкий клиент (MIPSEL)
- «Байкал М» полноценный ПК (ARM64)



- Mcom-02 (ARMH)



- PPC64LE

Зарубежные



- i586
- x86_64



- Kunpeng 920
48 ядер ARM64
2,4 GHz 7 нм



- Pi 3 /4
4 ядра (ARM64)



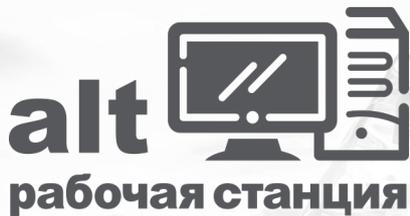
- RISC-V



- POWER

Семейство операционных систем «Альт»

Несертифицированная линейка :



Сертифицированная линейка :



«Альт СП»
Сервер



«Альт СП»
Рабочая Станция



Отечественные разработки в отечественной энергетике под управлением ОС Альт

В **РС-Сибирь** и **РС-Юг** завершена разработка и этап опытной эксплуатации:

* Отечественной многоуровневой автоматизированной системы управления технологическим процессом (АСУ ТП) на базе программного комплекса «КОТМИ» (компания «Децима») для решения задач EMS, OMS, DMS;

* Автоматизированной информационно-измерительной системы (АИИС) комплексного учёта энергоносителей (АИИС КУЭ) в виде ПО «Пирамида» (ГК «Системы и технологии»). При этом указанные системы работали в защищенном сегменте по криптоканалу на основе решений «ИВК Крипто» (АО ИВК).



Отечественные разработки в отечественной энергетике под управлением ОС Альт

ТЕХНИЧЕСКОЕ РЕШЕНИЕ ПРОЕКТА. ПАК МАРС



Серверы Эльбрус – ОС Альт
(сектор АСКУЭ)

Системы хранения данных BIZBLADE Sirius 3000 (базы данных) –
серверы Эльбрус – ОС Альт

Системы хранения данных BIZBLADE Sirius 8000
(архив) – серверы Эльбрус – ОС Альт

Серверы Эльбрус – ОС Альт
(сектор SCADA)

Коммутаторы системы хранения данных

Коммутаторы

Серверы ИВК КРИПТО (Эльбрус – ОС Альт)

Источники бесперебойного питания



BITBLAZE

ПАК МАРС

Программно-аппаратный комплекс
«Многофункциональная
аппаратно-независимая
ресурсоучетная система»



А теперь о самом главном



24.02.2022

Импортозамещение — это не просто и не быстро.

Главная проблема — прикладное ПО под Linux.

Нас ждет переходный период совместной эксплуатации систем под Windows и Linux не менее **4-5 лет.**

Фаза 1 : СРОЧНО импортозамещаться !!

Домен AD

Единая точка входа — сквозная аутентификация

Интеграция сервисов и оборудования

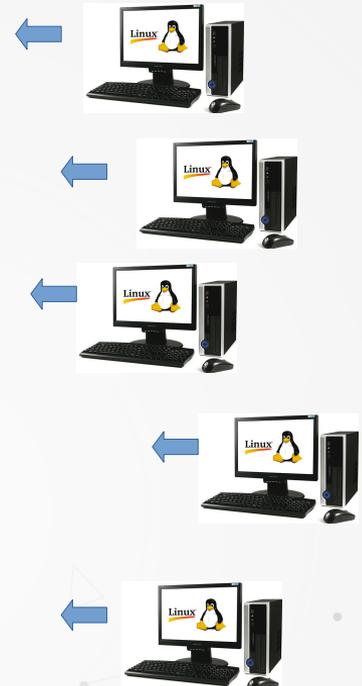
Управление конфигурациями и политиками

Поддержка связности узлов в сети предприятия

Удобный обмен файлами --> DFS

Организация удалённого доступа

Безопасность



**Как
администрировать
появившиеся машины
под ОС Линукс ?**

Чем заменить AD: FreeIPA vs SAMBA

Ключевое отличие :

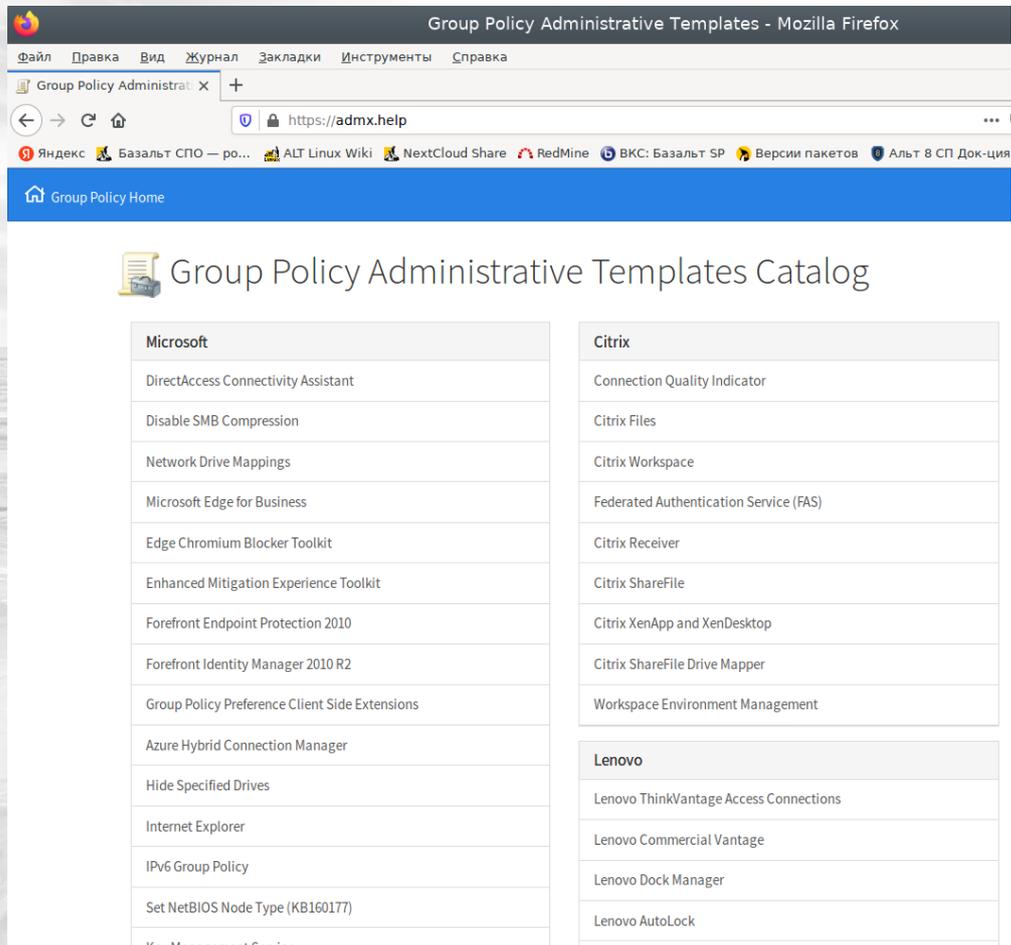
- **FreeIPA** умеет управлять только машинами под Linux. Часть задач решает через протокол smb (CIFS) ;
- **Samba** в чистом виде управляет только машинами под Windows ;
- Решение ОС «Альт» внутри проекта Samba дает **универсальный инструмент** для работы с **любым доменом**, позволяющий управлять как Linux-, так и Windows-машинами и пользователями.

- ОС «Альт» поддерживает 3 вида домена:
- Samba
 - FreeIPA
 - Alt-domain (LDAP + Kerberos)



Поддержка ГП MS AD в ОС «Альт» - как это работает:

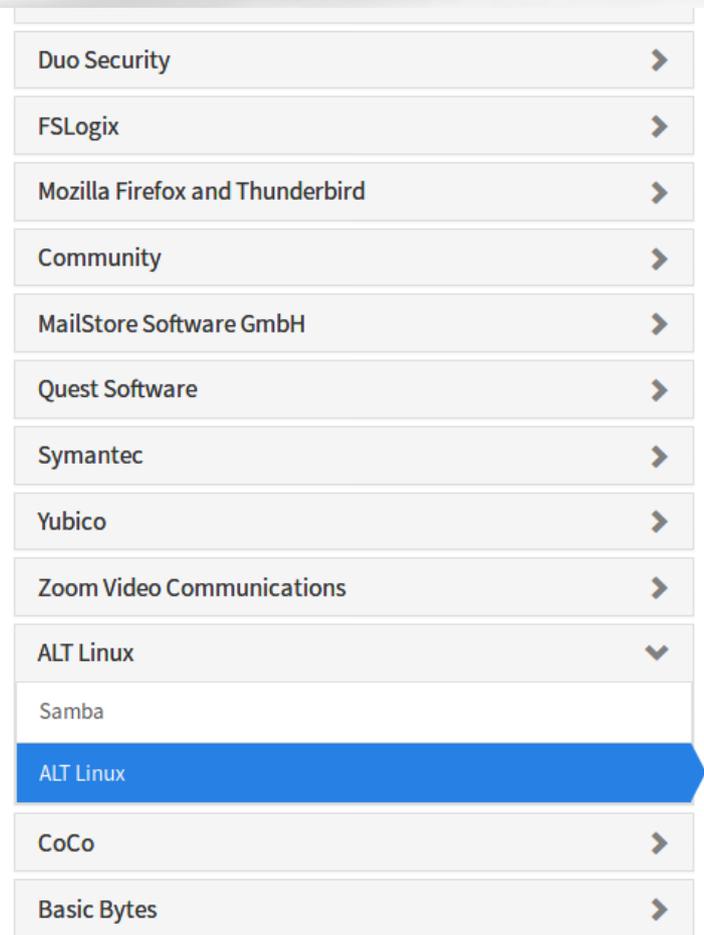
1. Ресурс <https://admx.help/>



The screenshot shows a Mozilla Firefox browser window displaying the Group Policy Administrative Templates Catalog. The browser's address bar shows the URL <https://admx.help>. The page title is "Group Policy Administrative Templates Catalog". The content is organized into two columns of templates, categorized by vendor:

| Microsoft | Citrix |
|--|--|
| DirectAccess Connectivity Assistant | Connection Quality Indicator |
| Disable SMB Compression | Citrix Files |
| Network Drive Mappings | Citrix Workspace |
| Microsoft Edge for Business | Federated Authentication Service (FAS) |
| Edge Chromium Blocker Toolkit | Citrix Receiver |
| Enhanced Mitigation Experience Toolkit | Citrix ShareFile |
| Forefront Endpoint Protection 2010 | Citrix XenApp and XenDesktop |
| Forefront Identity Manager 2010 R2 | Citrix ShareFile Drive Mapper |
| Group Policy Preference Client Side Extensions | Workspace Environment Management |
| Azure Hybrid Connection Manager | |
| Hide Specified Drives | Lenovo |
| Internet Explorer | Lenovo ThinkVantage Access Connections |
| IPv6 Group Policy | Lenovo Commercial Vantage |
| Set NetBIOS Node Type (KB160177) | Lenovo Dock Manager |
| Key Management Service | Lenovo AutoLock |

2. В списке слева найти раздел [ALT Linux](#) :



The screenshot shows a vertical sidebar menu with various software categories. The categories listed are:

- Duo Security
- FSLogix
- Mozilla Firefox and Thunderbird
- Community
- MailStore Software GmbH
- Quest Software
- Symantec
- Yubico
- Zoom Video Communications
- ALT Linux** (highlighted in blue)
- Samba
- CoCo
- Basic Bytes

ГП MS AD в ОС «Альт» - как это работает (ч.2) :

3. Скачать шаблоны ГП на Windows-машину администратора **RSAT**

The screenshot shows a web browser window with the URL `https://admx.help/?Category=ALTLinux&Language=ru-ru`. The page title is "Group Policy Home" and the language is set to "русский (Россия)".

On the left side, there is a list of vendors with expandable arrows:

- Microsoft
- Citrix
- Lenovo
- Google
- VMware
- Cjwdev
- Foxit Software Inc.
- Tracker Software
- Adobe
- Login Consultants Nederland B.V
- Bentley

The main content area is titled "ALT Linux" and describes it as an "Административный шаблон Active Directory для дистрибутивов BaseALT". A green button labeled "Скачать" is located in the top right corner.

Below the main title, there is a section titled "Административные шаблоны (компьютеры)" which contains a tree view of administrative templates:

- Система ALT
 - Безопасность
 - Выполнение команды `/usr/bin/chfn`
 - Выполнение программы `/usr/bin/chage`
 - Выполнение программы `/usr/bin/gpasswd`
 - Выполнение программы `/usr/bin/groupmets`
 - Запрос пароля `sudo` для пользователей группы «wheel»
 - Метод аутентификации
 - Передача родительской среды в `sudo`
 - Разрешение на использование `/usr/bin/chsh`
 - Разрешение на использование `/usr/sbin/hddtemp`
 - Разрешение на использование `consolehelper`
 - Разрешения для `/bin/su`



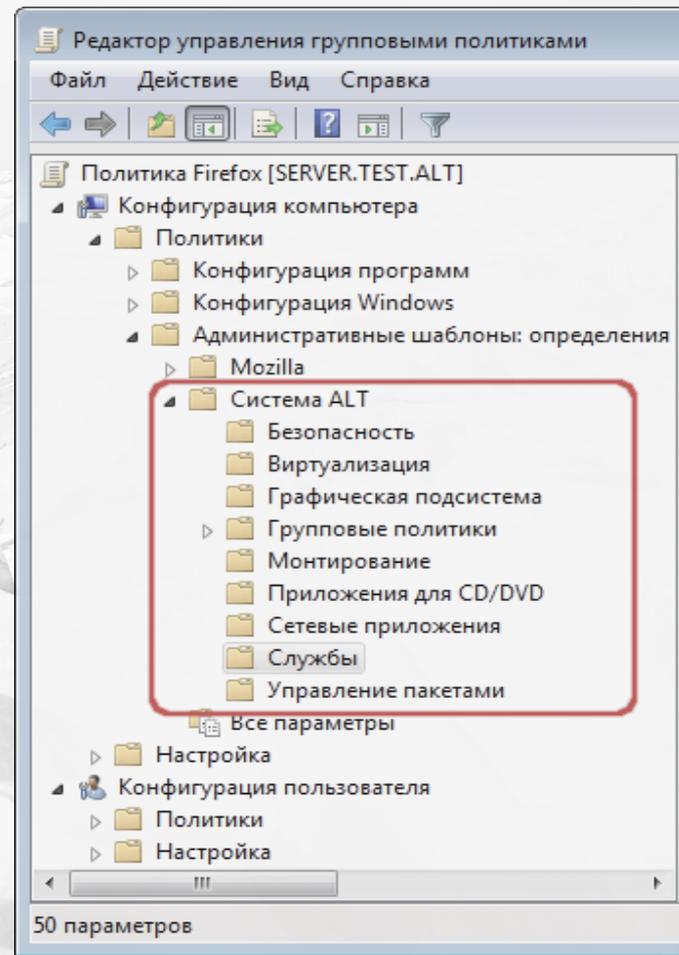
ГП MS AD в ОС «Альт» - как это работает (ч.3) :

На сегодня реализовано
700+ политик

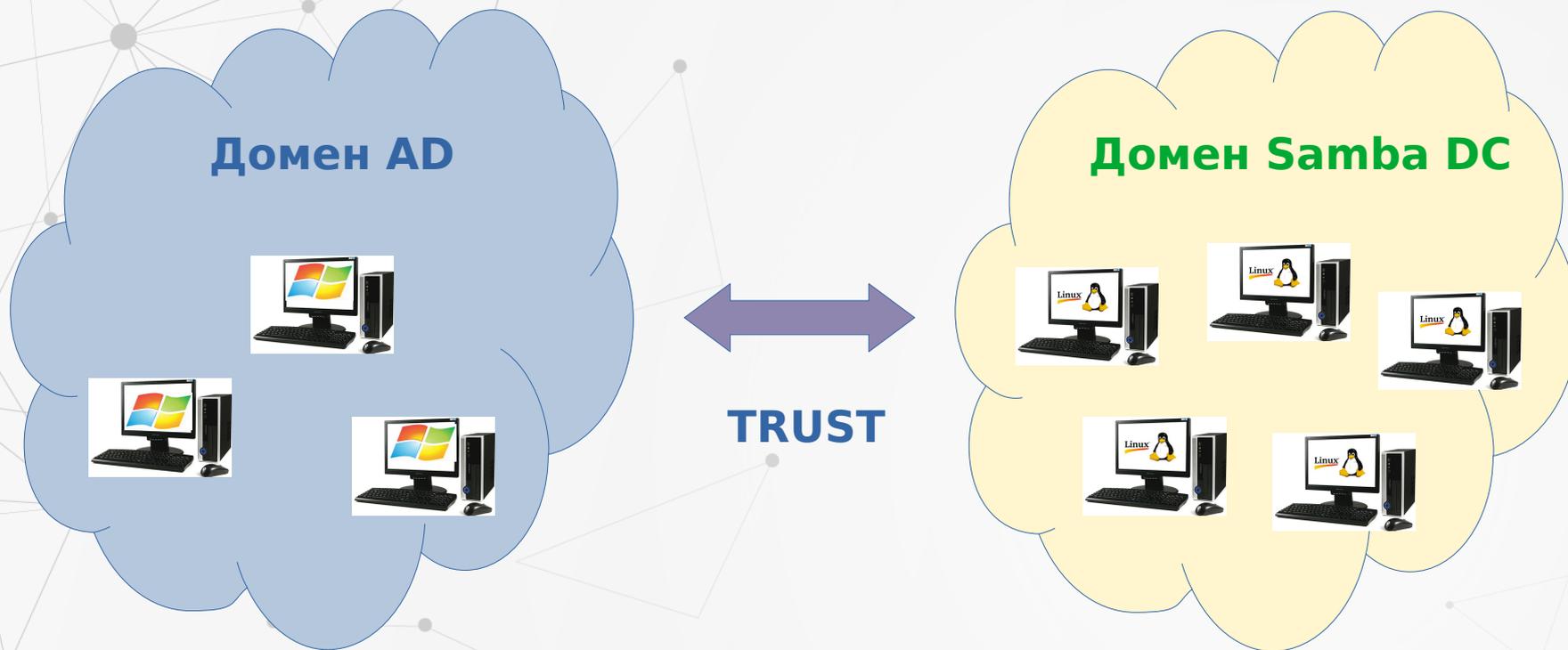
Управление политиками происходит через знакомую всем администраторам Windows оснастку RSAT (**Remote Server Administration Tool**).

Реализованные политики:

- подключение разделяемых ресурсов;
- ограничение доступа к носителям, включая мобильные устройства;
- управление службами;
- управление каталогами;
- управление ярлыками на рабочем столе;
- управление доступом к виртуальным машинам и виртуализации;
- установка и удаление пакетов*;
- управление внешним видом браузеров;
- управление оформлением рабочего стола
- и др.



Фаза 2 : Импортозамещение в разгаре



Численность парка ПК под Windows и под Linux примерно сровнялась.

ADMC - АЛЬТЕРНАТИВА RSAT и др.

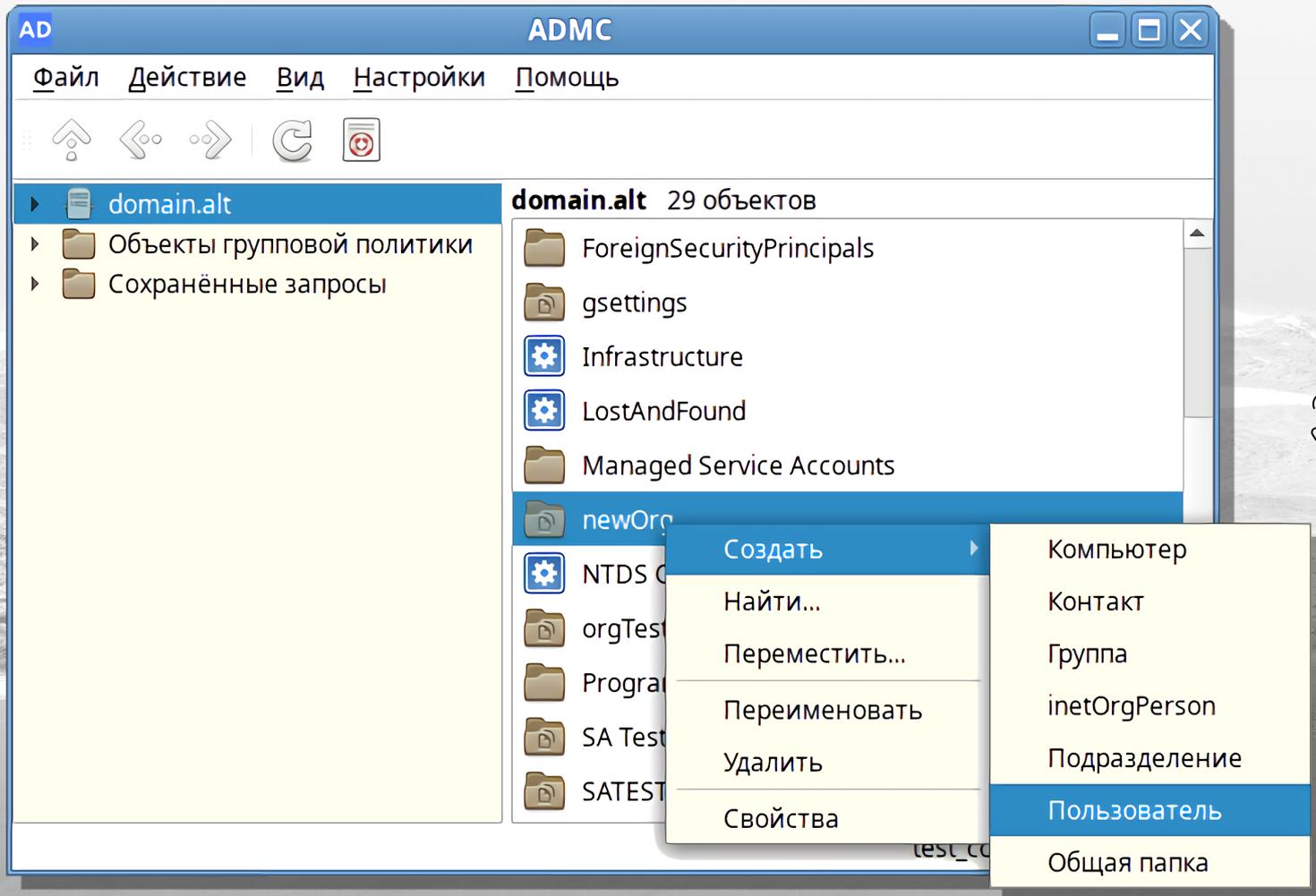
- ✓ Простой графический инструмент для работы с доменом AD/Samba
- ✓ Переосмысливает пользовательский опыт работы с RSAT

Впервые — в релизе 9.2.
Проект развития групповых политик и графического инструмента управления продолжится совместно с мейнстримом проекта **Samba**

The screenshot displays the ADCM (Active Directory Management Console) interface. The left pane shows a tree view of the domain structure, with 'Users' selected. The right pane shows a list of users and groups with columns for Name, Object class, and Description. The 'sin4 Details' dialog is open, showing the 'General' tab for the user 'sinnew'. The dialog includes fields for Logon Name, Account disabled, Password expiration settings, and Account expiration date.

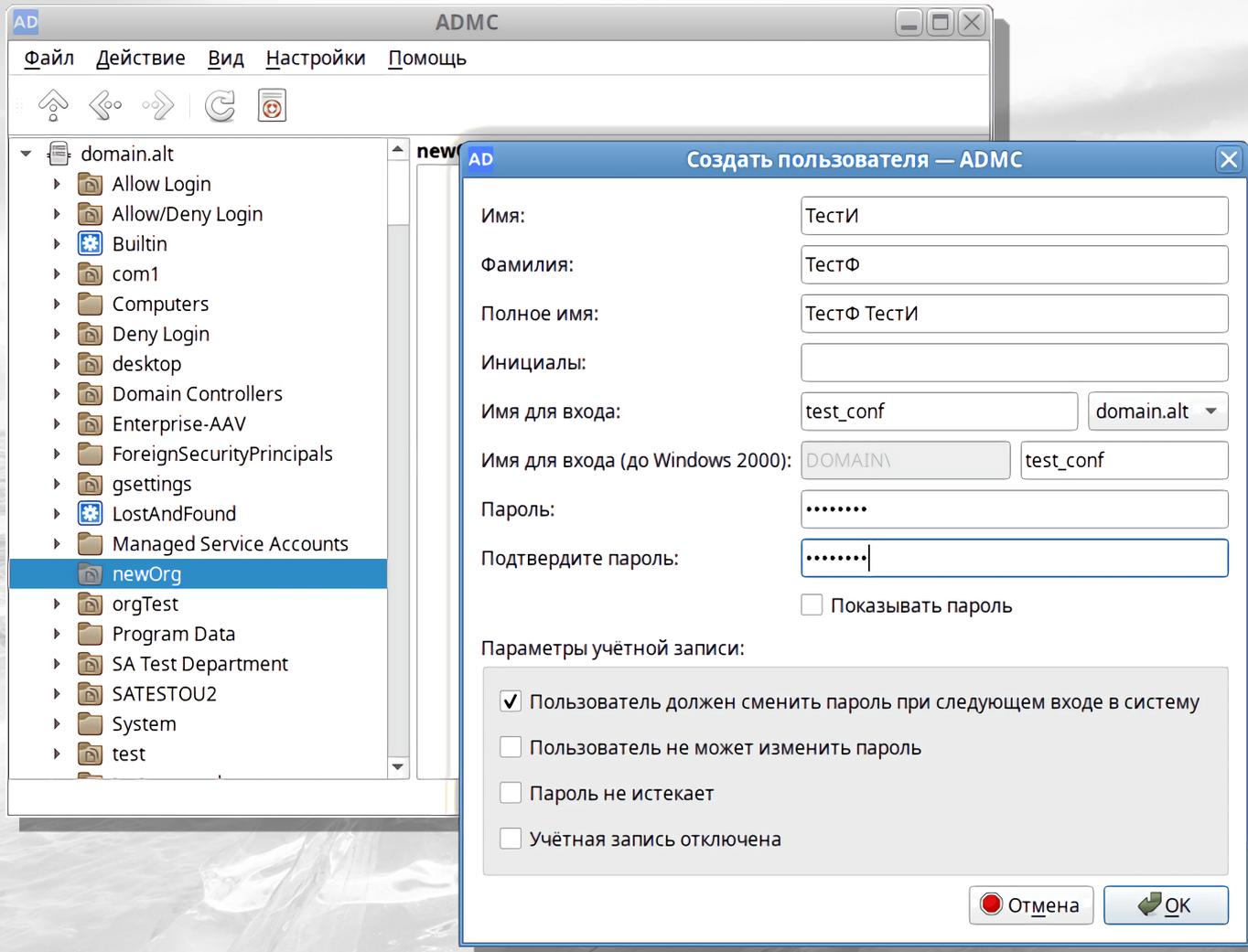
| Name | Object class | Description |
|----------------------------------|--------------|--|
| Administrator | User | Built-in account for administering the c... |
| Allowed RODC Password Repli... | Group | Members in this group can have their pa... |
| Cert Publishers | Group | Members of this group are permitted to... |
| Denied RODC Password Repl... | Group | Members in this group cannot have thei... |
| DnsAdmins | Group | DNS Administrators Group |
| DnsUpdateProxy | Group | DNS clients who are permitted to perfo... |
| Domain Admins | Group | Designated administrators of the domain |
| Domain Computers | Group | All workstations and servers joined to t... |
| Domain Controllers | Group | All domain controllers in the domain |
| Domain Guests | Group | All domain guests |
| Domain Users | Group | All domain users |
| Enterprise Admins | Group | Designated administrators of the enter... |
| Enterprise Read-only Domain C... | Group | Members of this group are Read-Only D... |
| Policy Creator Owners | Group | Members in this group can modify grou... |
| ... | User | Built-in account for guest access to the ... |
| ... | Group | Servers in this group can access remote ... |
| ... | Group | Members of this group are Read-Only D... |
| ... | Group | Designated administrators of the schema |
| ... | User | test descr |
| ... | User | test |
| ... | Group | ... |
| ... | User | Key Distribution Center Service Account |
| ... | Group | ... |
| ... | Group | ... |
| ... | User | test lastname |
| ... | User | test last |
| ... | User | xd3sd |
| ... | User | test new |
| ... | User | test new v34 |
| ... | Group | test new grp |
| ... | User | test new yendy |

ADMC. Создание пользователя



[Подробнее о ADMC](#)

ADMS. Внесение данных пользователя



The image shows a screenshot of the ADMS (Active Directory Management Service) console. The main window displays a tree view of the domain structure, with 'newOrg' selected. A dialog box titled 'Создать пользователя — ADMS' is open, allowing the creation of a new user. The dialog contains the following fields and options:

- Имя:** Тести
- Фамилия:** ТестФ
- Полное имя:** ТестФ Тести
- Инициалы:** (empty)
- Имя для входа:** test_conf (domain: domain.alt)
- Имя для входа (до Windows 2000):** DOMAIN test_conf
- Пароль:** (masked with dots)
- Подтвердите пароль:** (masked with dots)
- 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

Buttons at the bottom: Отмена (Cancel), OK.



ADMS. Просмотр свойств пользователя

ADMS. Просмотр свойств пользователя

ТестФ Тести — свойства — ADMS

Общее
Объект
Атрибуты
Адрес
Организация
Телефоны
Учётная запись
Группы
Делегирование
Безопасность

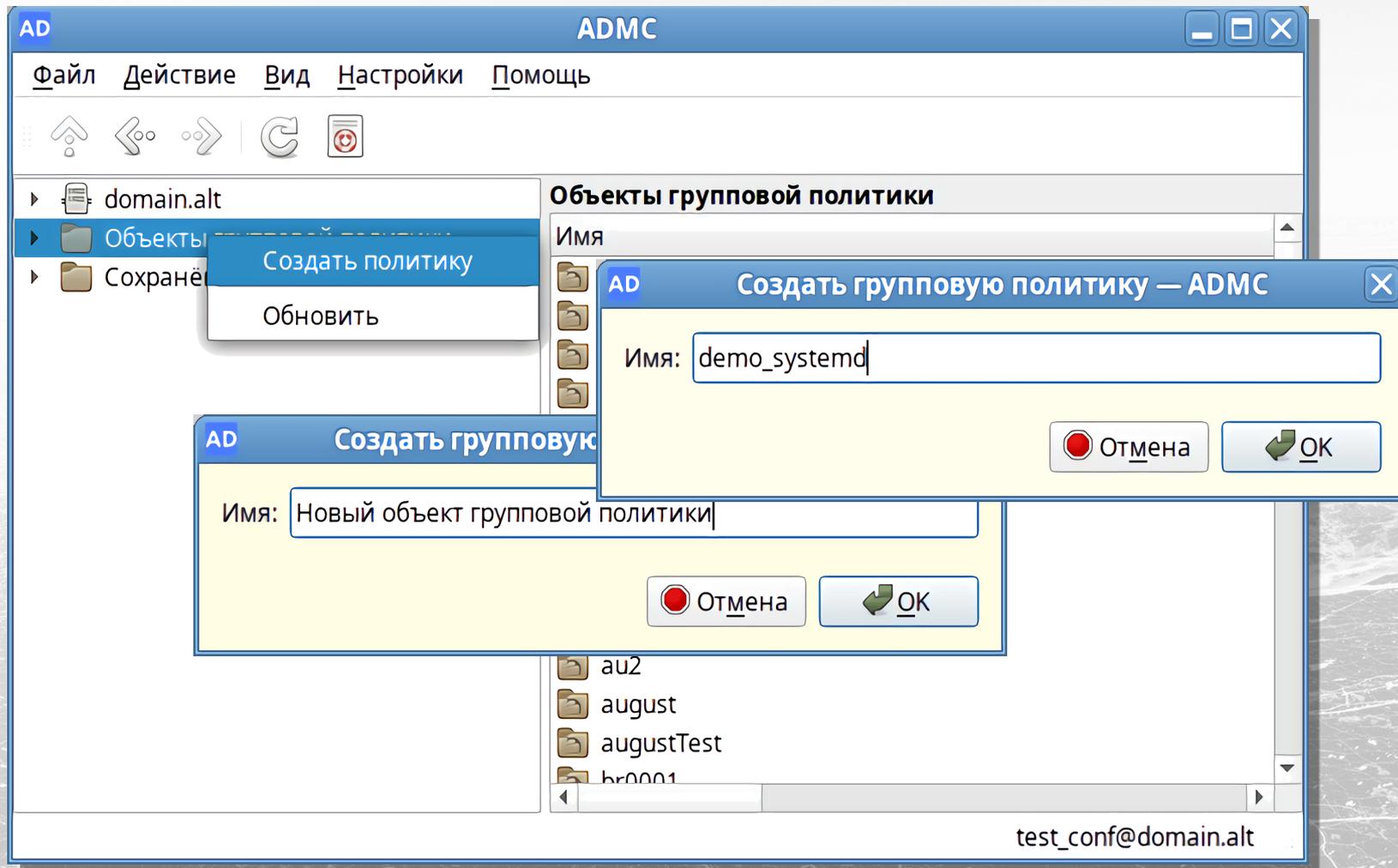
| Имя | Значение | Тип |
|-----------------|-----------------|-----------------------|
| USNIntersite | <без значени... | Целое число |
| aCSPolicyN... | <без значени... | Юникод |
| accountExp... | (никогда) | Большое целое число |
| accountNa... | <без значени... | Юникод |
| adminCount | <без значени... | Целое число |
| adminDesc... | <без значени... | Юникод |
| adminDispl... | <без значени... | Юникод |
| allowedAttr... | <без значени... | Идентификатор объекта |
| allowedAttr... | <без значени... | Идентификатор объекта |
| allowedChil... | <без значени... | Идентификатор объекта |
| allowedChil... | <без значени... | Идентификатор объекта |
| altSecurityI... | <без значени... | Юникод |
| assistant | <без значени... | Различающееся имя |
| attributeCe... | <без значени... | Октет |
| audio | <без значени... | Октет |
| badPasswo... | (никогда) | Большое целое число |
| badPwdCo... | 0 | Целое число |
| bridgehead... | <без значени... | Различающееся имя |
| businessCa... | <без значени... | Юникод |
| c | <без значени... | Юникод |
| canonicalN... | <без значени... | Юникод |
| carLicense | <без значени... | Юникод |
| cn | ТестФ Тести | Юникод |
| co | <без значени... | Юникод |
| codePage | 0 | Целое число |
| comment | <без значени... | Юникод |
| company | <без значени... | Юникод |

Изменить... Фильтр

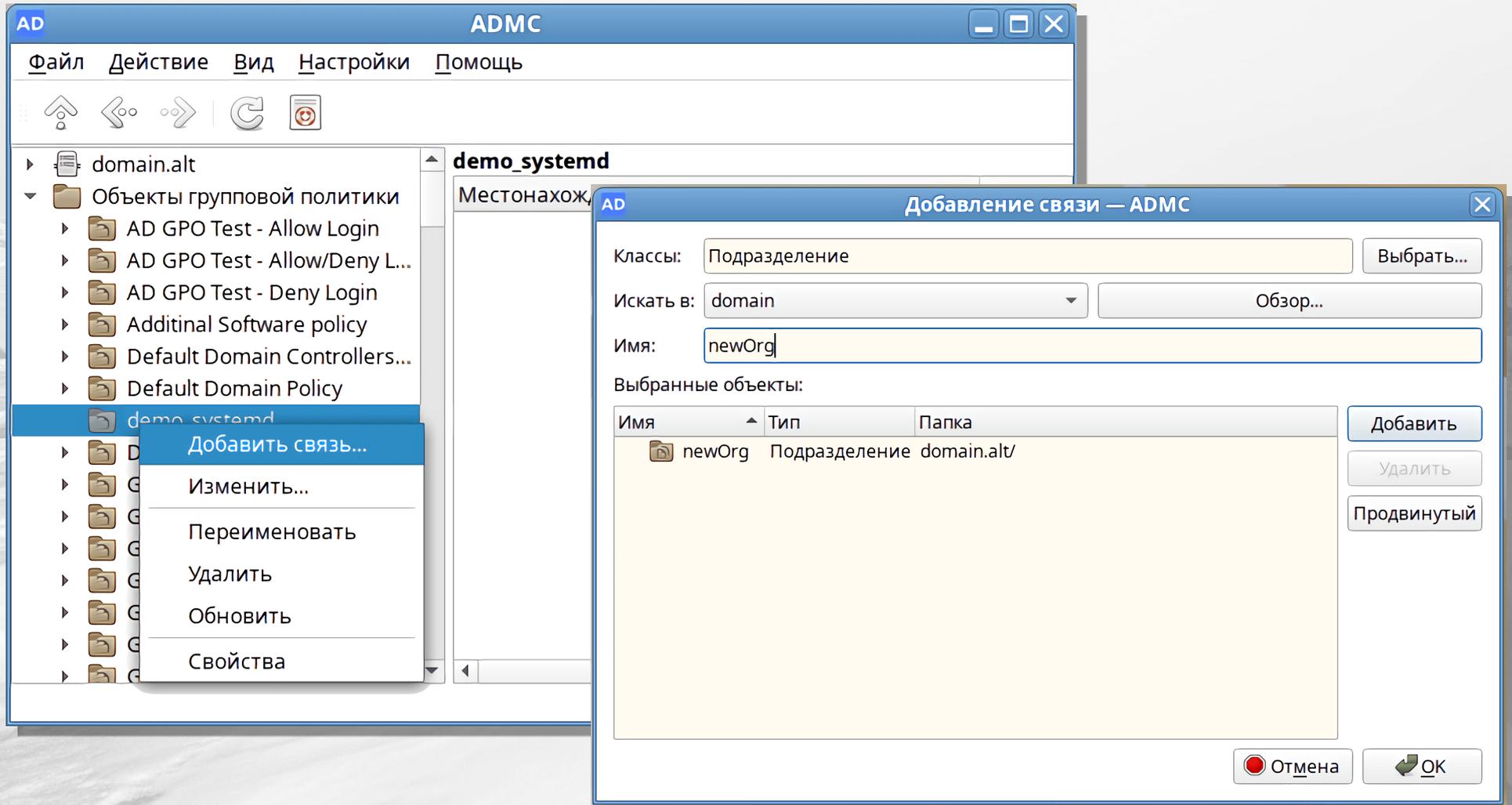
Сбросить Применить Отмена OK



ADMC. Создание политики



ADMS. Создание политики. Добавление связи.



Групповые политики. Включение.

Центр управления системой (от суперпользователя)

↑ Главная ★ Режим эксперта ✕ Выход ? Справка

Локальная база пользователей

Домен ALT Linux или Astra Linux Directory
Домен:

Кэшировать аутентификацию при недоступности сервера домена

Домен Active Directory
Домен:
Рабочая группа:
Имя компьютера:

Домен FreeIPA
Домен:
Имя компьютера:

Внимание!
Изменение домена заработает только после перезагрузки компьютера

Введите пароль для учётной записи с правами подключения к домену.

Имя пользователя:

Пароль:



Включить групповые политики

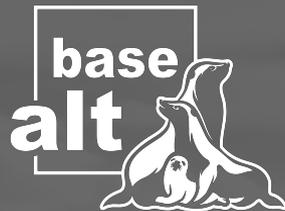
OK

Отмена

Плавная миграция: MS AD → Samba DC

Данный сценарий предполагает следующий алгоритм действий:

- Вывод из эксплуатации и замену сопутствующих инфраструктурных служб, работающих только с MS AD (MS Exchange, Sharepoint и д.р.);
- Перенос сопутствующих системных служб, не относящихся непосредственно к доменной инфраструктуре (DHCP-серверов, центров сертификации и т.п.), с Windows-серверов на Linux сервера;
- Временный, прозрачный для клиентов, перевод инфраструктуры в гибридное состояние через установку контроллеров домена на базе Samba в текущую инфраструктуру (в текущий домен);
- Миграцию всех системных (FSMO и иных) ролей с контроллеров домена на базе MS AD на контроллеры домена на базе Samba;
- Штатное отключение всех контроллеров на базе MS AD.



Контакты

Тел.: +7 (495) 123-47-99

basealt.ru

E-mail:

sales@basealt.ru

оптовые продажи:

sales@basealt.ru

Офисы:

Москва,
ул. Бутырская, д. 75

Санкт-Петербург,
Коломяжский пр-т, 27,
БЦ «Содружество», 3
этаж

Саратов,
ул. Октябрьская 44,
корпус А, офис № 3

Обнинск,
ул. Королёва, д. 4Б, БЦ
“Британика”