



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
25000+ пакетов

**Направление
образования**

**20 лет на
рынке**

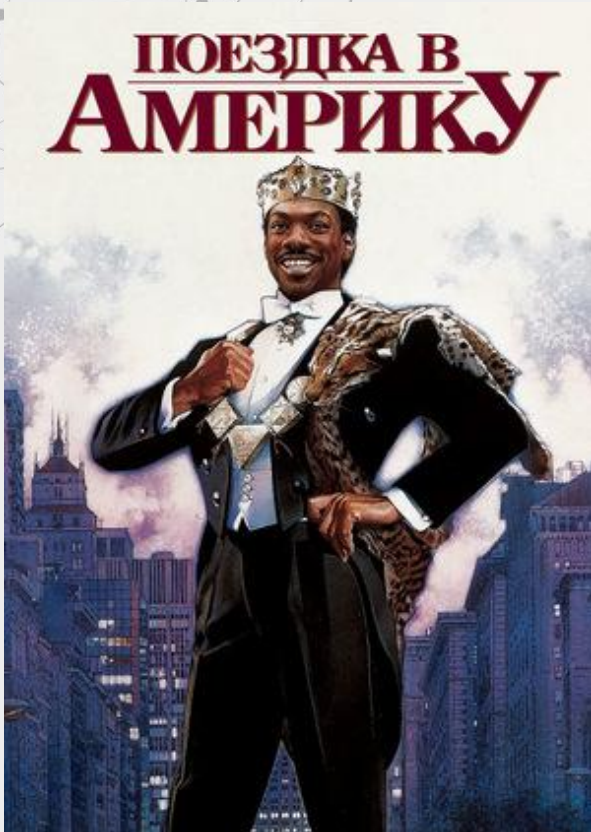
**125000+
заказчиков**

**800+ обученных
специалистов**

офисы в 4-х городах

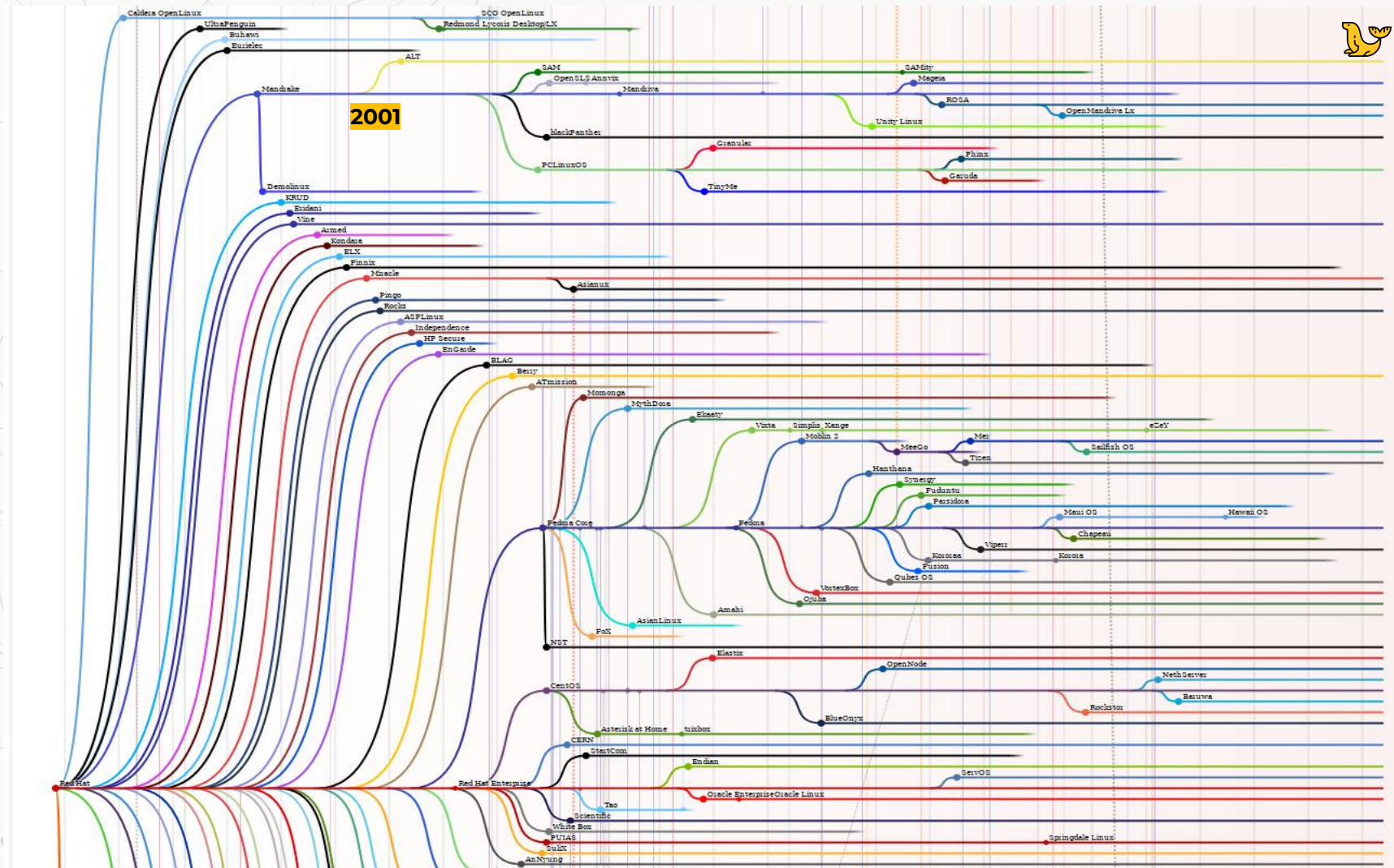


Он настоящий принц
и у него свои деньги



А мы короли : у нас свой диалект линукс !

ALT НА ГЕНЕАЛОГИЧЕСКОМ ДРЕВЕ LINUX



СВОБОДНОЕ ПО
Международная
разработка

Российский
репозиторий
«Сизиф» (Sisyphus)

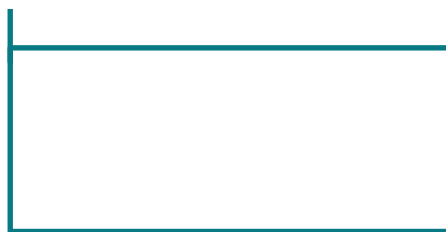
Продукты
«Базальт СПО»

- ФСТЭК
- ФСБ
- МО



Платформы
(стабильные ветки)
репозитория

Для различных
архитектур



Операционные
системы



Виртуализация



Образование

СОБСТВЕННАЯ ИНФРАСТРУКТУРА РАЗРАБОТКИ (Свидетельства Роспатента)



Репозиторий «Базальт»

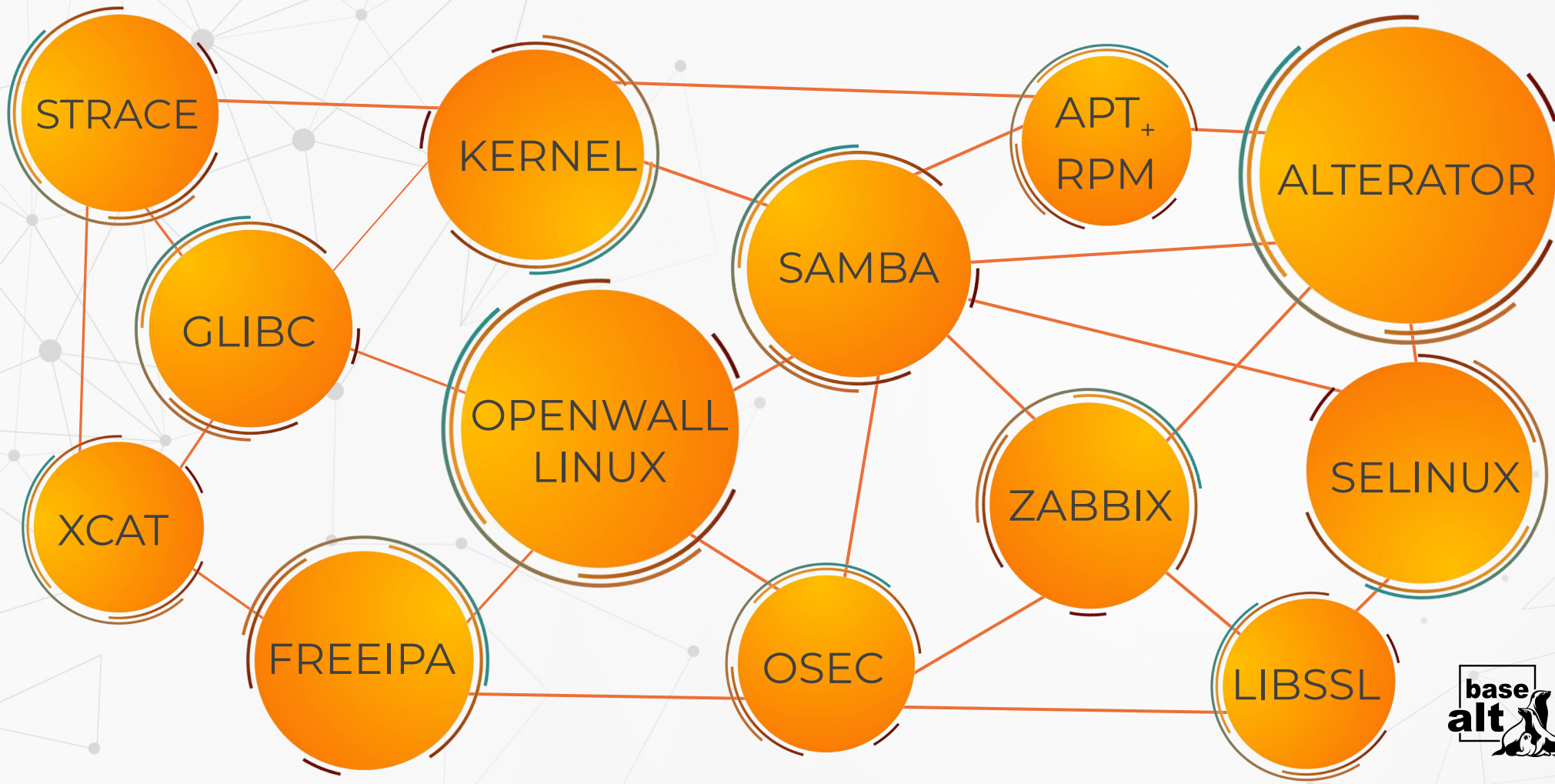


**Инструментарий
сборки**

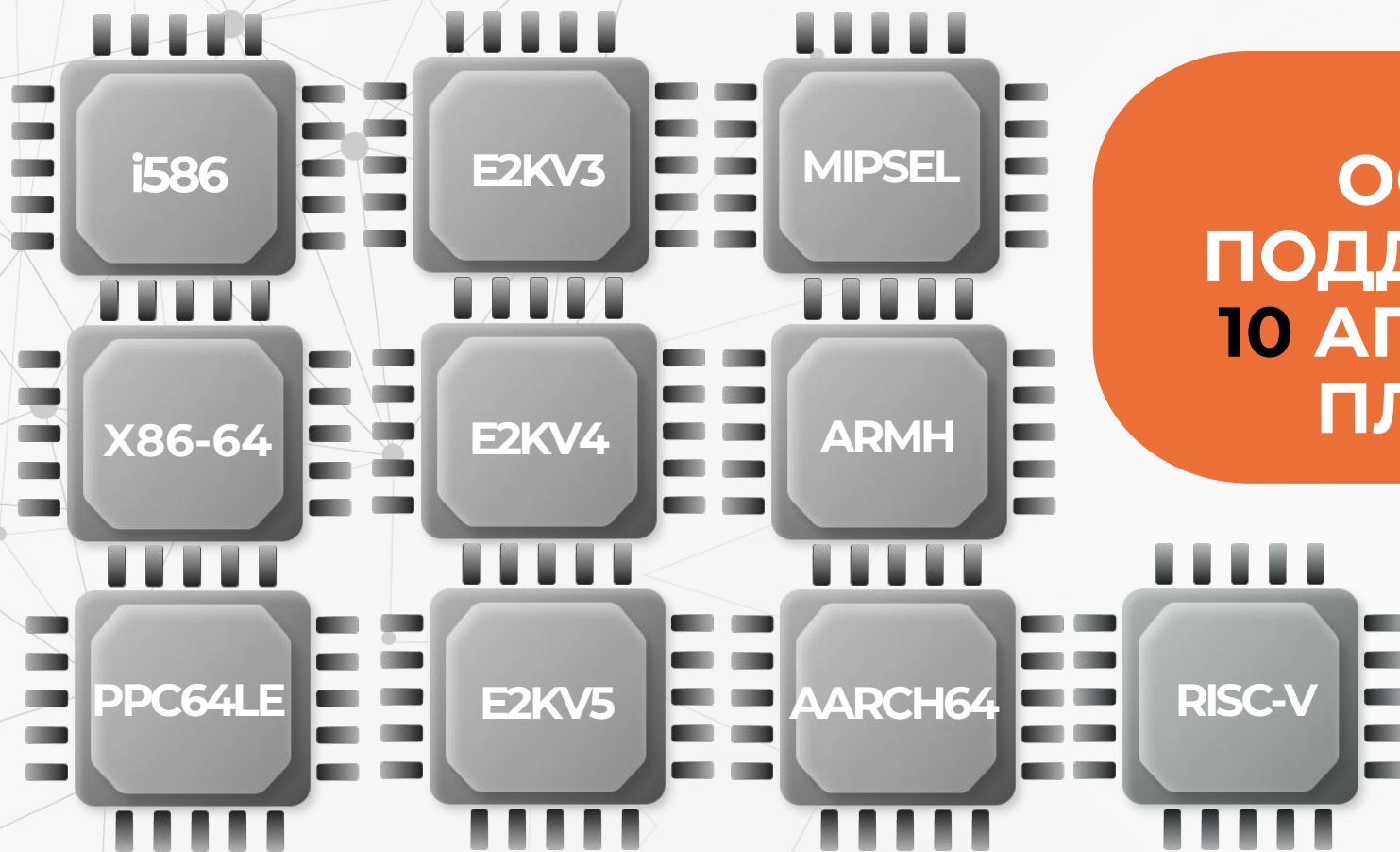


**Инфраструктура
разработки**

ВКЛАД «БАЗАЛЫТ СПО» В МЕЖДУНАРОДНЫЕ ПРОЕКТЫ РАЗРАБОТКИ СВОБОДНОГО ПО



ОС «АЛТ» ПОДДЕРЖИВАЕТ 10 АППАРАТНЫХ ПЛАТФОРМ



ОС «АЛТ»
ПОДДЕРЖИВАЕТ
10 АППАРАТНЫХ
ПЛАТФОРМ

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

ЛИНЕЙКИ ОС «АЛЬТ» В РАЗВИТИИ

Платформа 8

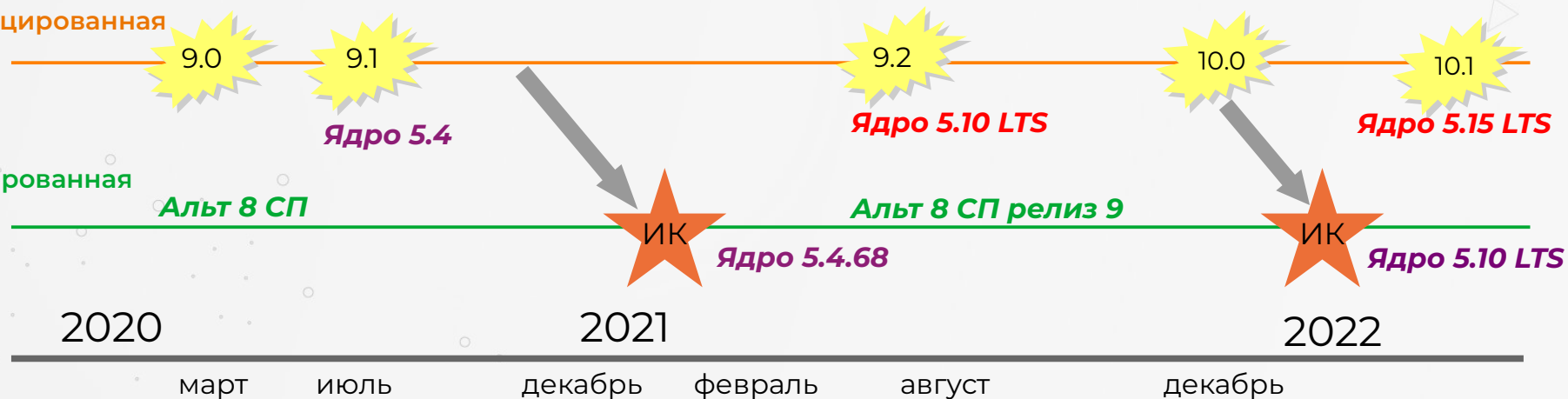
Поддержка до 2023 г

Платформа 9

Платформа 10

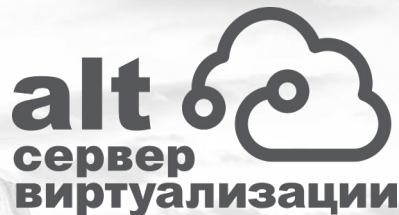
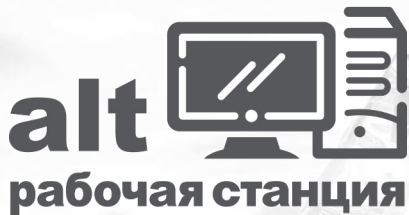
Несертифицированная
линейка

Сертифицированная
линейка

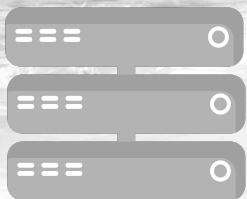


Семейство операционных систем «Альт»

Несертифицированная линейка:



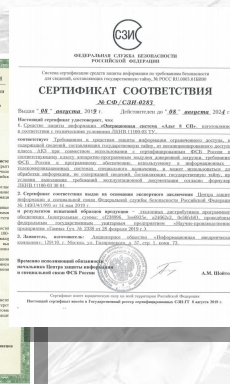
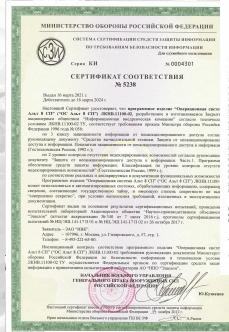
Сертифицированная линейка:



«Альт СП»
Сервер



«Альт СП»
Рабочая Станция



ОС «АЛТ РАБОЧАЯ СТАНЦИЯ»

Офисные редакторы,
Libreoffice, PDF, ЭЦП



Интернет: EMAIL,
IM, браузер



Мультимедия



Облачные сервисы групповой
работы NextCloud



Централизованное
управление ALTERATOR
с графическим интерфейсом



Векторная,
растровая графика,
3D, анимация



Архивные
файлы



Сканирование
и распознавание



ОС «АЛТ СЕРВЕР»

Доменная структура:
AD или Альт Сервер

Групповые политики

Сетевые службы DNS,
DHCP, HTTP(S), OpenVPN

Веб-сервер Apache,
NGINX

Почта и групповая
работа: SMTP, POP3,
IMAP, SOGo, CalDAV,
CarDAV, WebDAV,
FTP-сервер

Сервер ВКС
на базе Jitsi Meet

LXC, docker-ce, podman, kubernetes,
kvm+libvirt+qemu

СУБД (PostgreSQL,
MariaDB)

Сервер
мониторинга
Zabbix

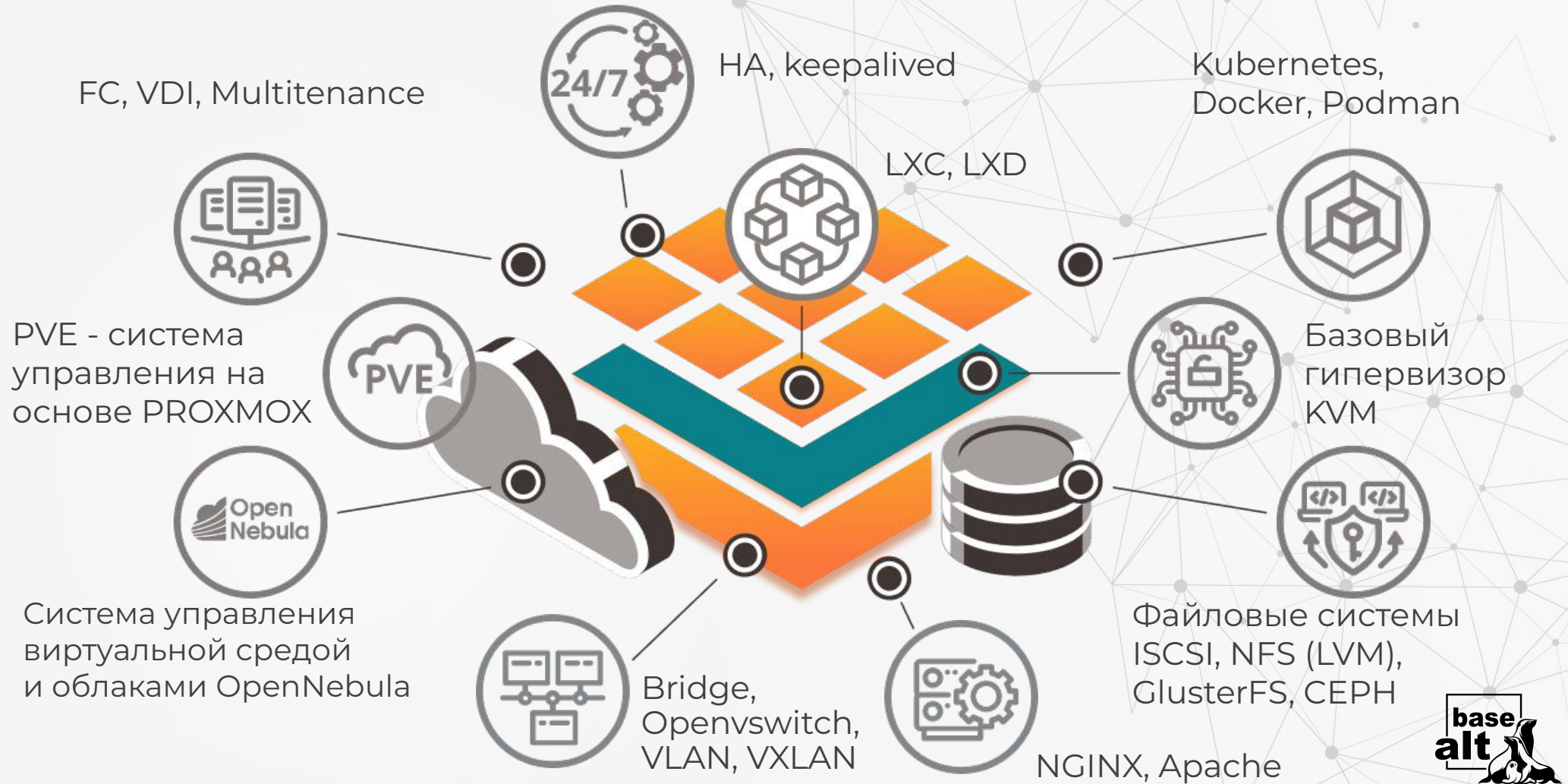
Резервное
копирование

Сервер печати

Средства создания репозитория
для централизованного
обновления



ОС «АЛТ СЕРВЕР ВИРТУАЛИЗАЦИИ»



9.2 НОВЫЕ ВОЗМОЖНОСТИ. «ГОРЫНЫЧ» ИЗ КОРОБКИ

Персональный компьютер коллективного пользования: до **6** рабочих мест на одном ПК. Стоимость одного рабочего места делится на **6**.

Кабель HDMI - 15 м max

Первое внедрение прошло в МФЦ г.Орла, где установлены комплексные и полностью отечественные АРМ на базе компьютеров с российскими процессорами «Эльбрус8С» и Baikal-M (BE-M1000).



А теперь о самом главном



24.02.2022

Исходное положение : работали, работаем и будем работать на импортном ПО



Фаза 1 : СРОЧНО импортозамещаться !!



Фаза 1 : СРОЧНО импортозамещаться !!

Домен AD

Единая точка входа — сквозная аутентификация

Интеграция сервисов и оборудования

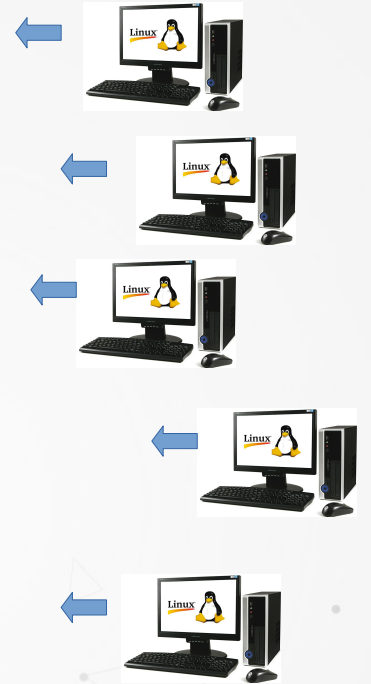
Управление конфигурациями и политиками

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

- **Поддержка связности узлов в сети предприятия**
 - Почта предприятия (Exchange) — SOGo/CommuniGate
 - DNS — решается сторонними проектами
 - DHCP — решается сторонними проектами
 - Внутренние сервисы (корпоративные порталы)
- **Сквозная аутентификация**
Предоставляется обоими проектами — FreeIPA и Samba
- **Управление конфигурацией**
Решается **только с помощью Samba**
- **Файлообмен**
Только с помощью Samba, даже в FreeIPA — через Samba: CIFS
- **Организация удалённого доступа**
Полноценно не решается ни одним из проектов

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



Чем заменить AD: FreeIPA vs SAMBA

Ключевое отличие :

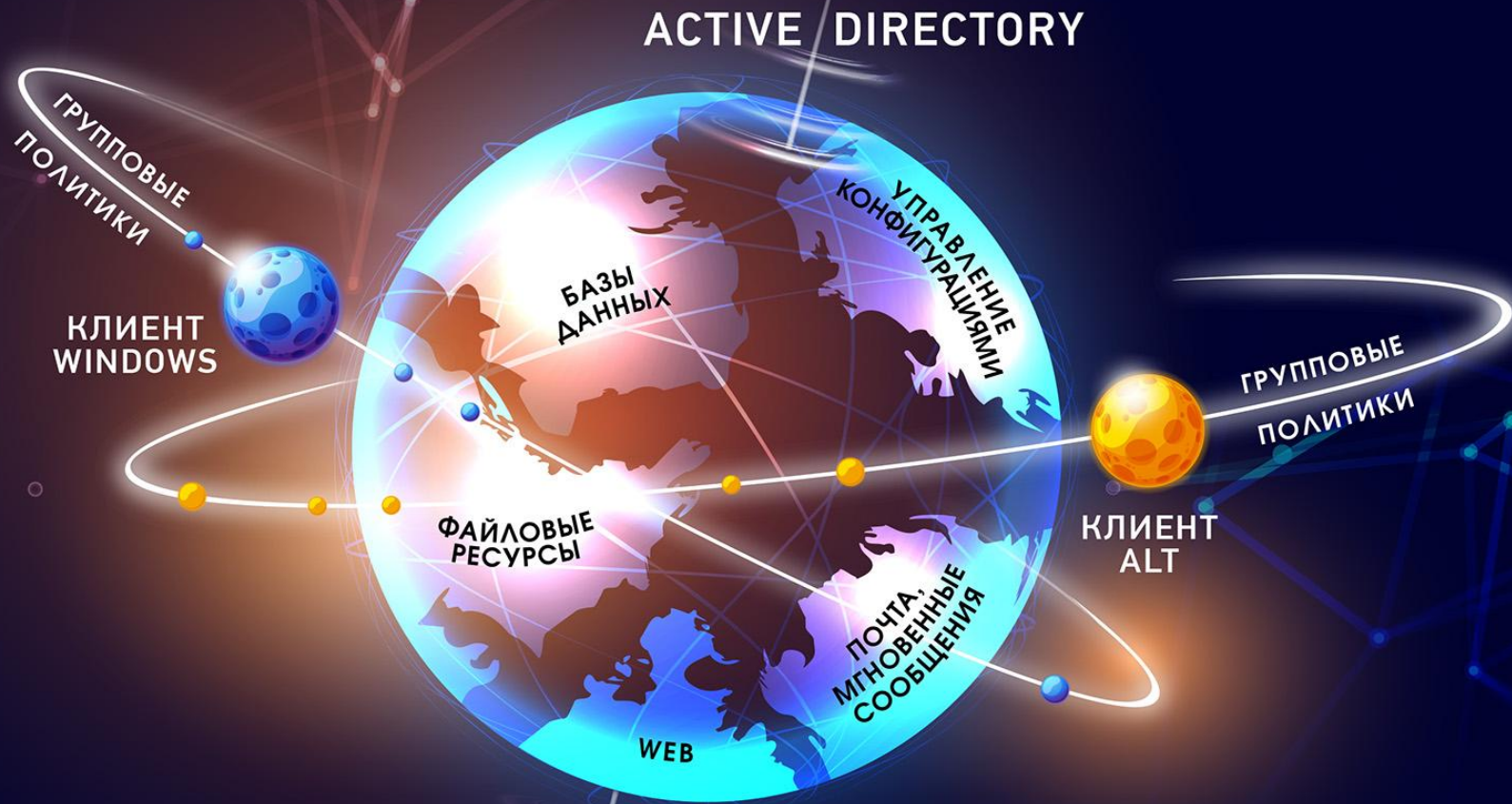
- **FreeIPA** управляет только машинами под Linux ;
- **Samba** в чистом виде управляет только машинами под Windows ;
- Решение ОС «Альт» внутри проекта Samba дает **универсальный инструмент** для работы с **любым доменом**, позволяющий управлять как Linux-, так и Windows-машинами и пользователями.

ОС «Альт»
поддерживает
3 вида домена:

- Samba
- FreeIPA
- Alt-domain
(LDAP + Kerberos)



Выбор ОС «АЛТ»: Samba + ГРУППОВЫЕ ПОЛИТИКИ

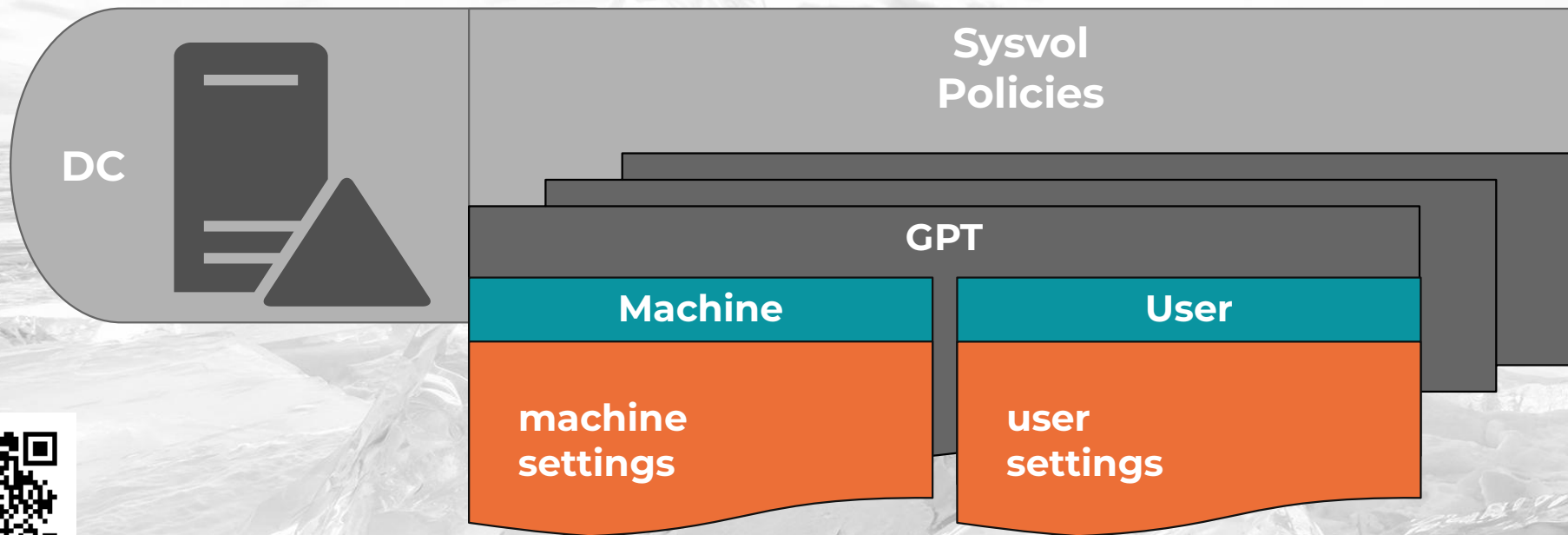


Групповые политики работают в рамках домена, где их создают сисадмины.
ГП применяются к компьютерам и/или к пользователям.

Групповые политики в ОС «Альт»

ГП в ОС «Альт» — это комплексное решение, которое включает :

- * хранение политик и шаблонов в каталоге **Sysvol** на контроллере домена ;
- * инструменты управления политиками ;
- * механизмы применения настроек для компьютеров и пользователей.

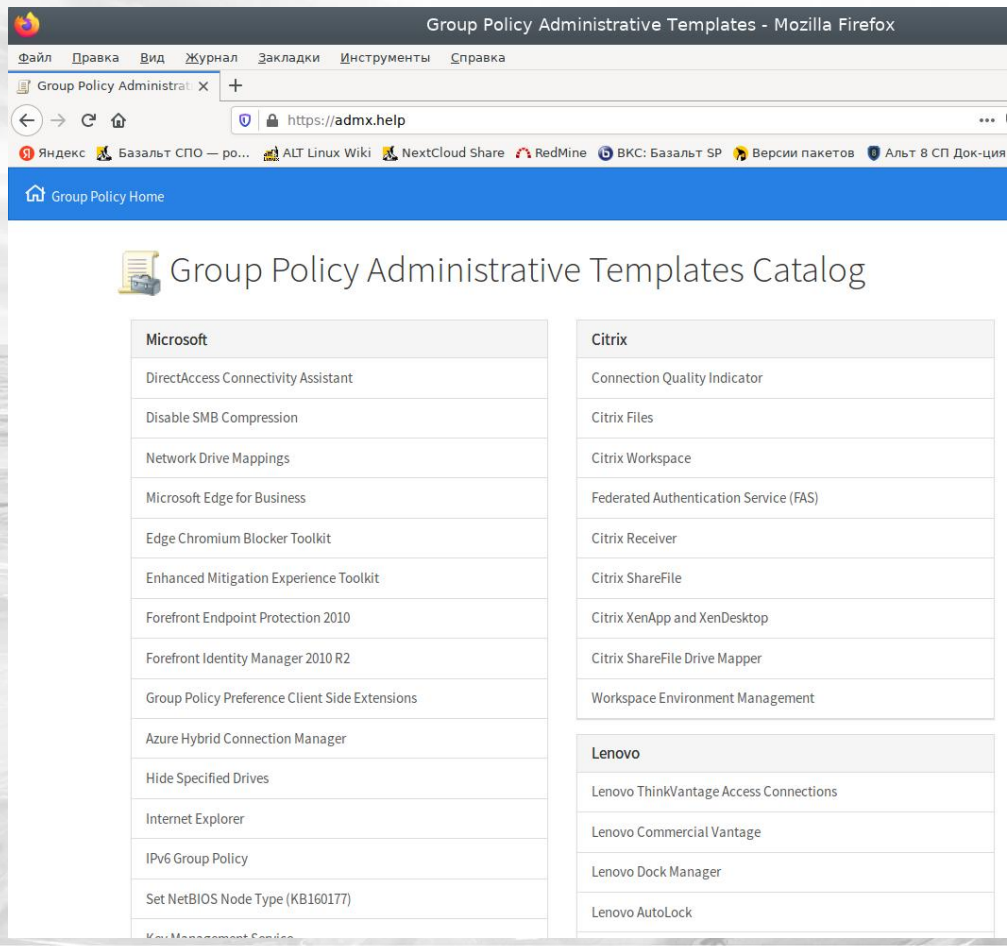


[Подробнее про групповые политики](#)

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

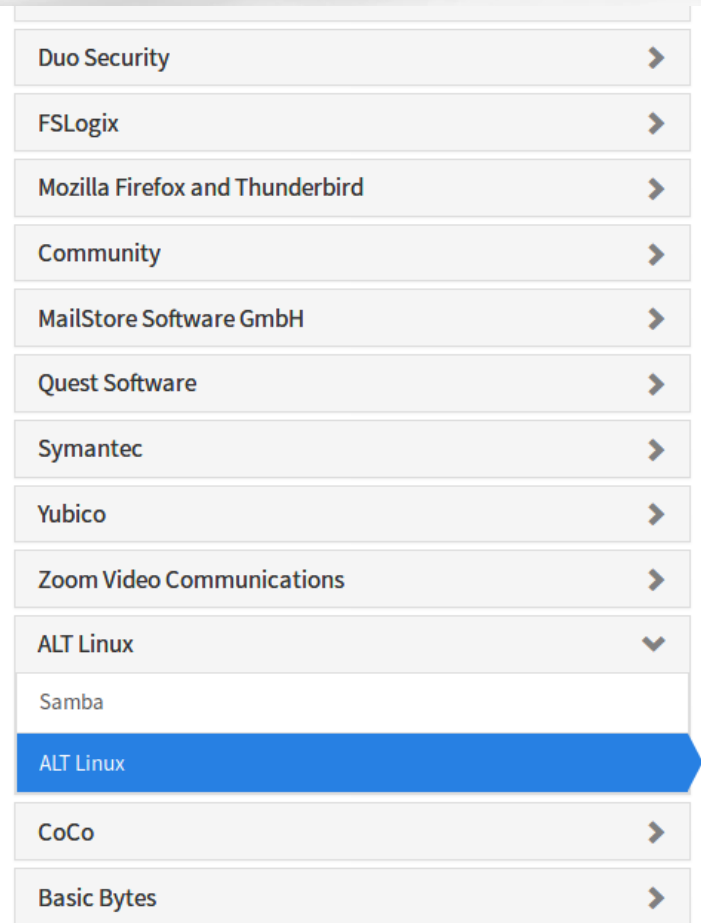
1. Ресурс <https://admx.help/>

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



The screenshot shows a web browser window with the title "Group Policy Administrative Templates - Mozilla Firefox". The address bar displays "https://admx.help". The page content is titled "Group Policy Administrative Templates Catalog" and is organized into two columns of categories. The left column includes "Microsoft" and "Azure Hybrid Connection Manager". The right column includes "Citrix" and "Lenovo".

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

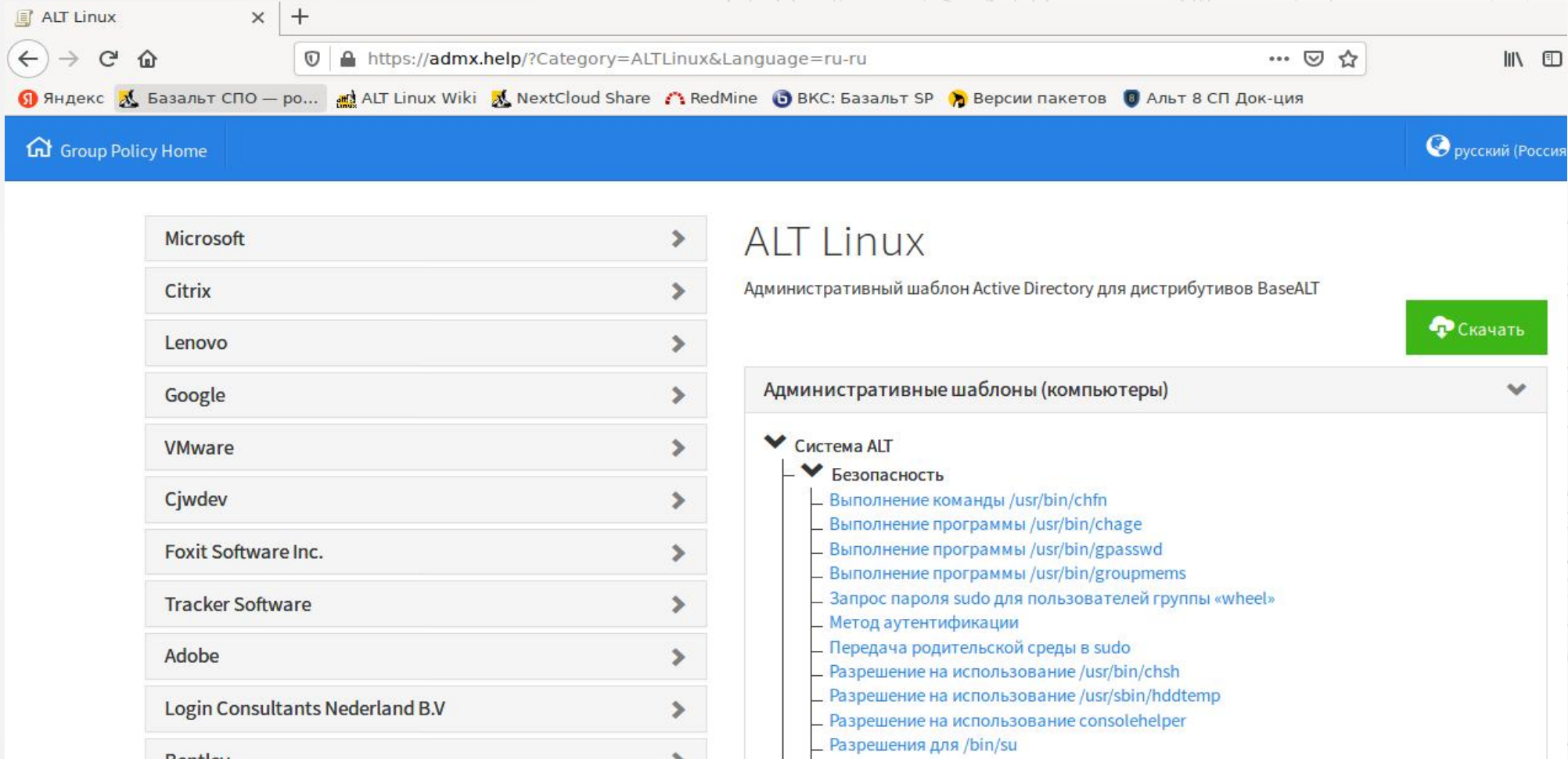


The screenshot shows a vertical navigation menu with several items, each with a right-pointing arrow. The item "ALT Linux" is highlighted with a blue background and a white arrow pointing right.

- Duo Security
- FSLogix
- Mozilla Firefox and Thunderbird
- Community
- MailStore Software GmbH
- Quest Software
- Symantec
- Yubico
- Zoom Video Communications
- ALT Linux**
- 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)". The main content area is titled "ALT Linux" and describes it as an "Административный шаблон Active Directory для дистрибутивов BaseALT". A green "Скачать" button is visible. On the left, there is a list of manufacturers: Microsoft, Citrix, Lenovo, Google, VMware, Cjwdev, Foxit Software Inc., Tracker Software, Adobe, Login Consultants Nederland B.V., and Bentley. On the right, a tree view shows "Административные шаблоны (компьютеры)" expanded to "Система ALT", which is further expanded to "Безопасность". Under "Безопасность", several administrative templates are listed, including "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", and "Разрешения для /bin/su".

ALT Linux

Административный шаблон Active Directory для дистрибутивов BaseALT

Скачать

Административные шаблоны (компьютеры)

- 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



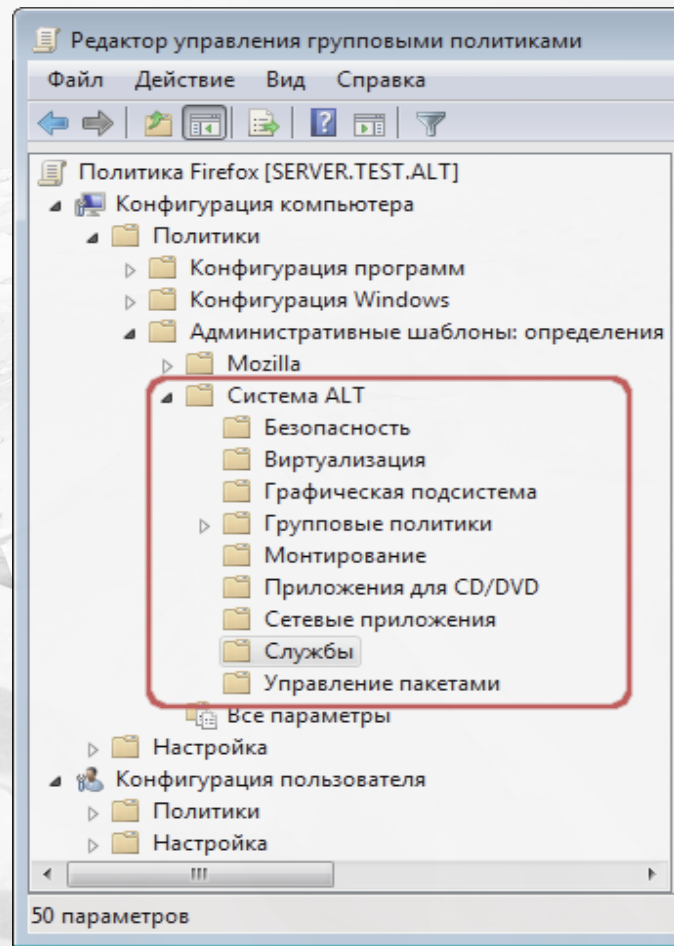
ГП MS AD в ОС «Альт» - как это работает (ч.3) :

На сегодня реализовано
150+ политик

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

Реализованные политики:

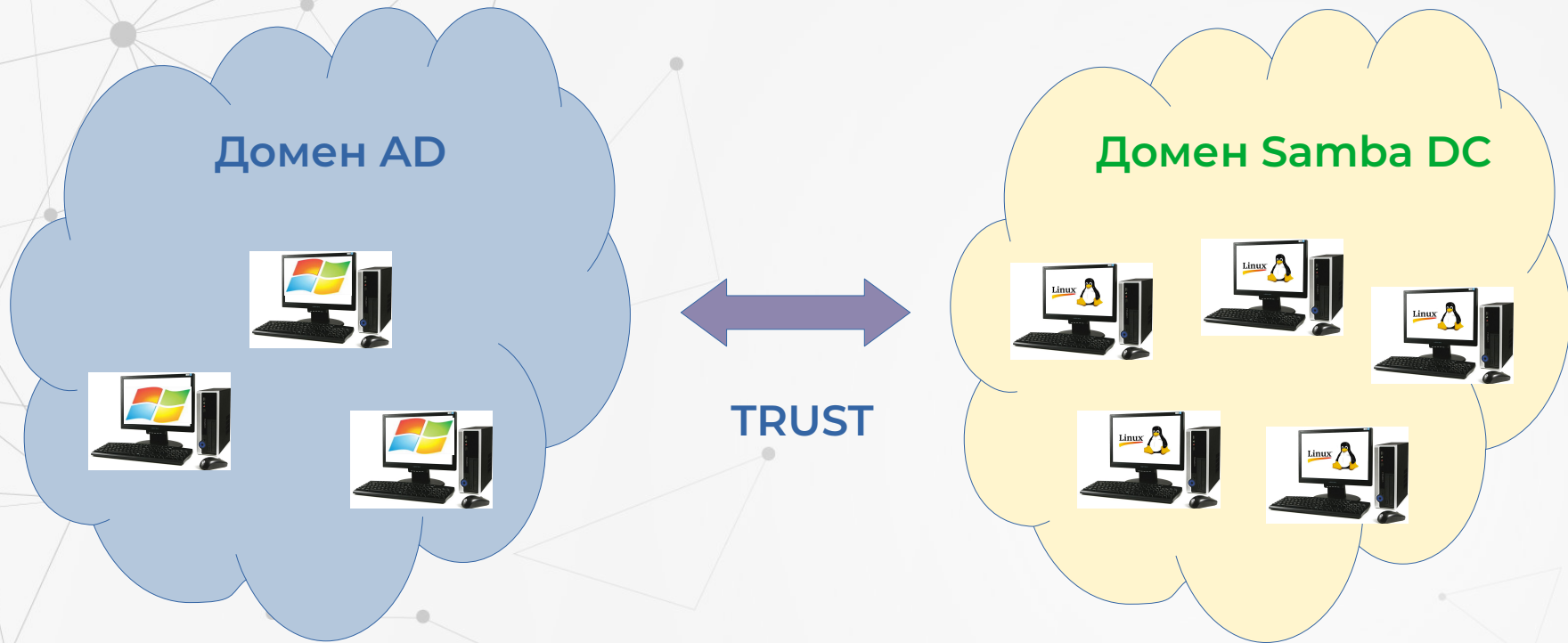
- подключение разделяемых ресурсов;
- ограничение доступа к носителям, включая мобильные устройства;
- управление службами;
- управление каталогами;
- управление ярлыками на рабочем столе;
- управление доступом к виртуальным машинам и виртуализации;
- установка и удаление пакетов*;
- управление внешним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



Фаза 2 : Импортзамещение в разгаре



Фаза 2 : Импортзамещение в разгаре



Численность парка ПК под Windows и под Linux примерно сравнялась.

ADMC – АЛЬТЕРНАТИВА RSAT и др.

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

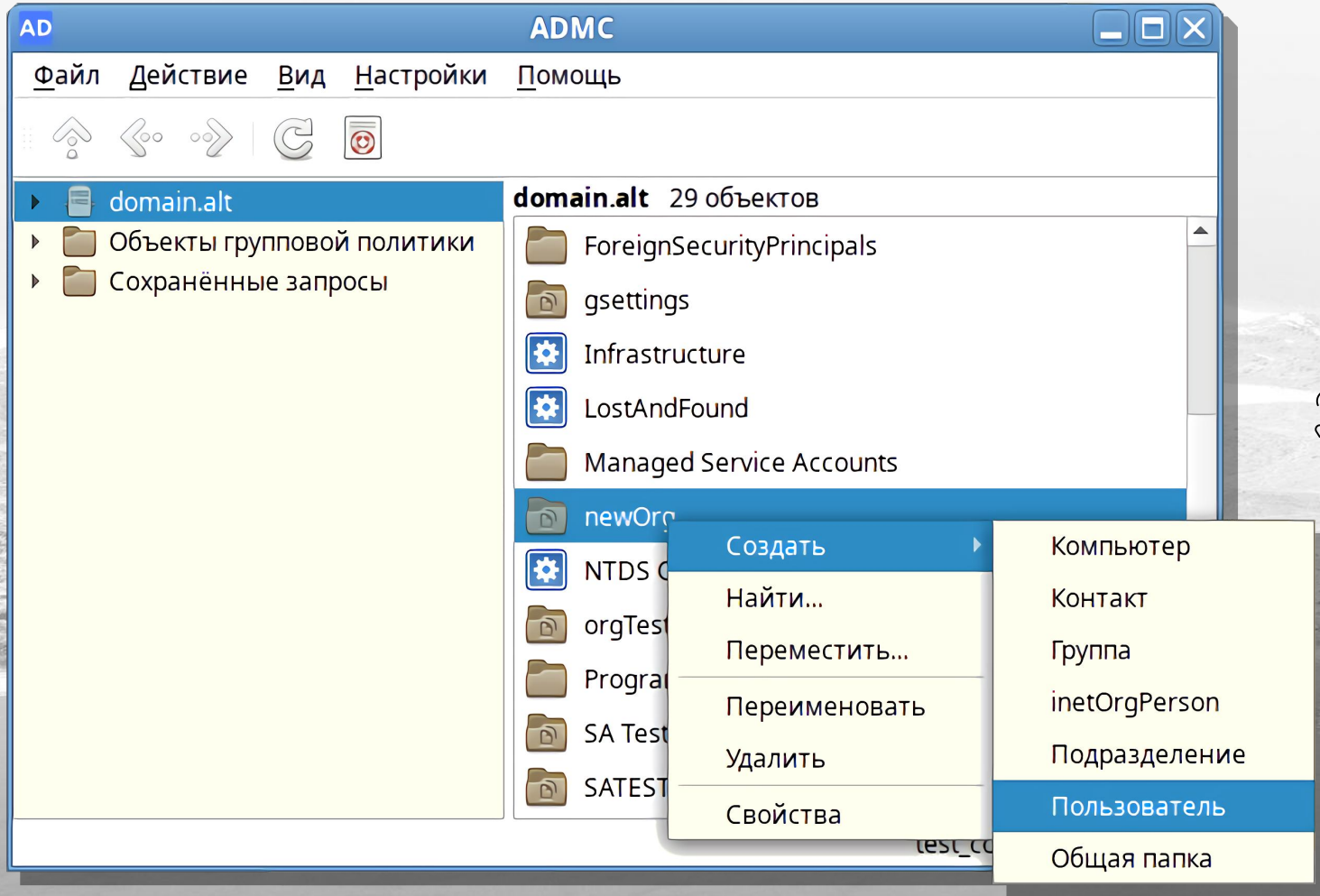
Впервые — в релизе 9.2.
Проект развития групповых политик и графического инструмента управления продолжится совместно с мейнстримом проекта **Samba**

The screenshot displays the ADCM interface. On the left, a tree view shows the 'domain' folder expanded to 'Users'. On the right, a table lists domain objects:

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	User	Built-in account for guest access to the ...
Read-only IAS Servers	Group	Servers in this group can access remote ...
Read-only Domain Controllers	Group	Members of this group are Read-Only D...
Schema Admins	Group	Designated administrators of the schema
test descr	User	test descr
Key Distribution Center Service Account	User	Key Distribution Center Service Account
xd3sd	User	xd3sd
testnew	User	
testnv34	User	
tuesd	Group	
xendy	User	

Below the table, the 'sin4 Details' dialog is open for the user 'xd3sd'. It shows the 'General' tab with fields for Logon Name (sinnew), Account disabled, User must change password on next logon, Don't expire password, Store password using reversible encryption, Smartcard is required for interactive logon, Account is sensitive and cannot be delegated, and Don't require Kerberos preauthentication. The account expires section is set to 'Never'. Buttons for 'Unlock account', 'Edit', 'Apply', and 'Cancel' are visible.

ADMC. Создание пользователя



The screenshot shows the ADMC (Active Directory Management Console) interface. The main window displays the hierarchy of the domain **domain.alt**, which contains 29 objects. The left pane shows the domain structure, including "Объекты групповой политики" and "Сохранённые запросы". The right pane lists objects such as "ForeignSecurityPrincipals", "gsettings", "Infrastructure", "LostAndFound", "Managed Service Accounts", "newOrg", "NTDS", "orgTest", "Program", "SA Test", and "SATEST". A context menu is open over the "newOrg" object, with the "Создать" (Create) option selected. The "Создать" menu is expanded, showing options: "Компьютер", "Контакт", "Группа", "inetOrgPerson", "Подразделение", "Пользователь" (highlighted), and "Общая папка".



[Подробнее о ADMC](#)

ADMC. Внесение данных пользователя

ADMC

Файл Действие Вид Настройки Помощь

domain.alt

- Allow Login
- Allow/Deny Login
- Builtin
- com1
- Computers
- Deny Login
- desktop
- Domain Controllers
- Enterprise-AAV
- ForeignSecurityPrincipals
- gsettings
- LostAndFound
- Managed Service Accounts
- newOrg**
- orgTest
- Program Data
- SA Test Department
- SATESTOU2
- System
- test

Создать пользователя — ADMC

Имя: Тести

Фамилия: ТестФ

Полное имя: ТестФ Тести

Инициалы:

Имя для входа: test_conf domain.alt

Имя для входа (до Windows 2000): DOMAIN test_conf

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



ADMS. Просмотр свойств пользователя

ADMS. Просмотр свойств пользователя

ТестФ Тести — свойства — ADMS

Общее
Объект
Атрибуты
Адрес
Организация
Телефоны
Учётная запись
Группы
Делегирование
Безопасность

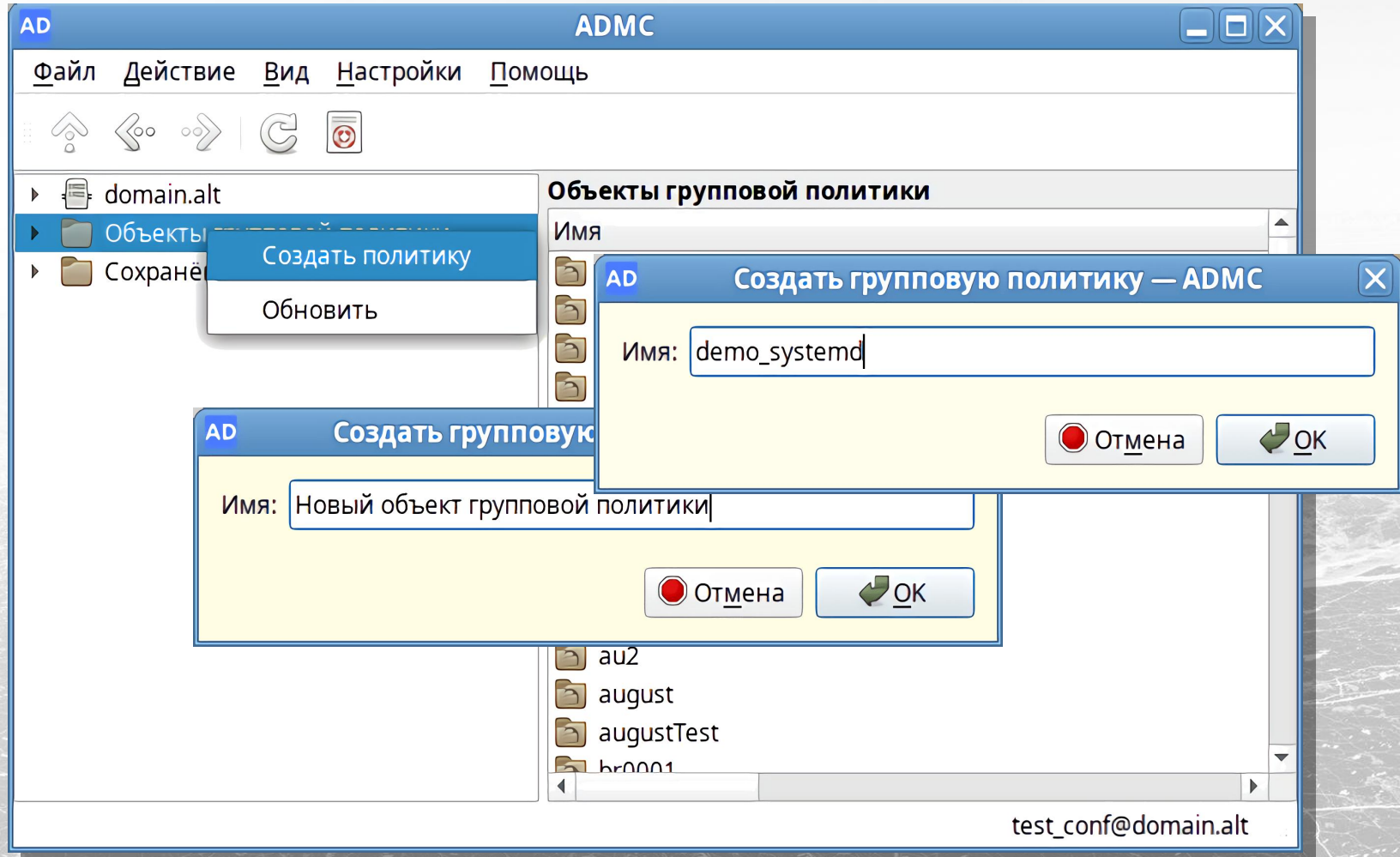
Имя	Значение	Тип
USNIntersite	<без значени...	Целое число
aCSPolicyN...	<без значени...	Юникод
accountExp...	(никогда)	Большое целое число
accountNa...	<без значени...	Юникод
adminCount	<без значени...	Целое число
adminDesc...	<без значени...	Юникод
adminDispl...	<без значени...	Юникод
allowedAttr...	<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

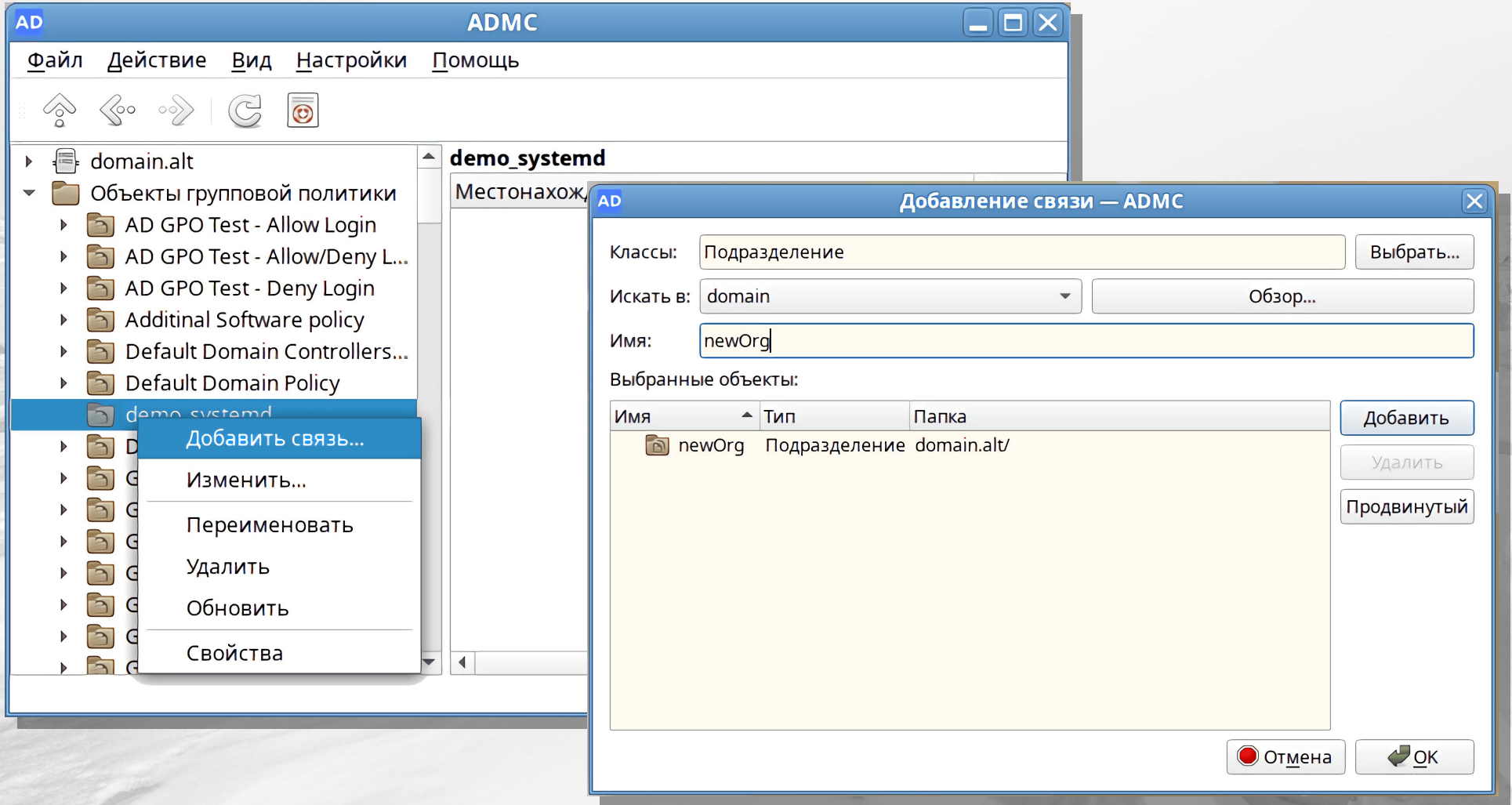
Сбросить Применить Отмена OK



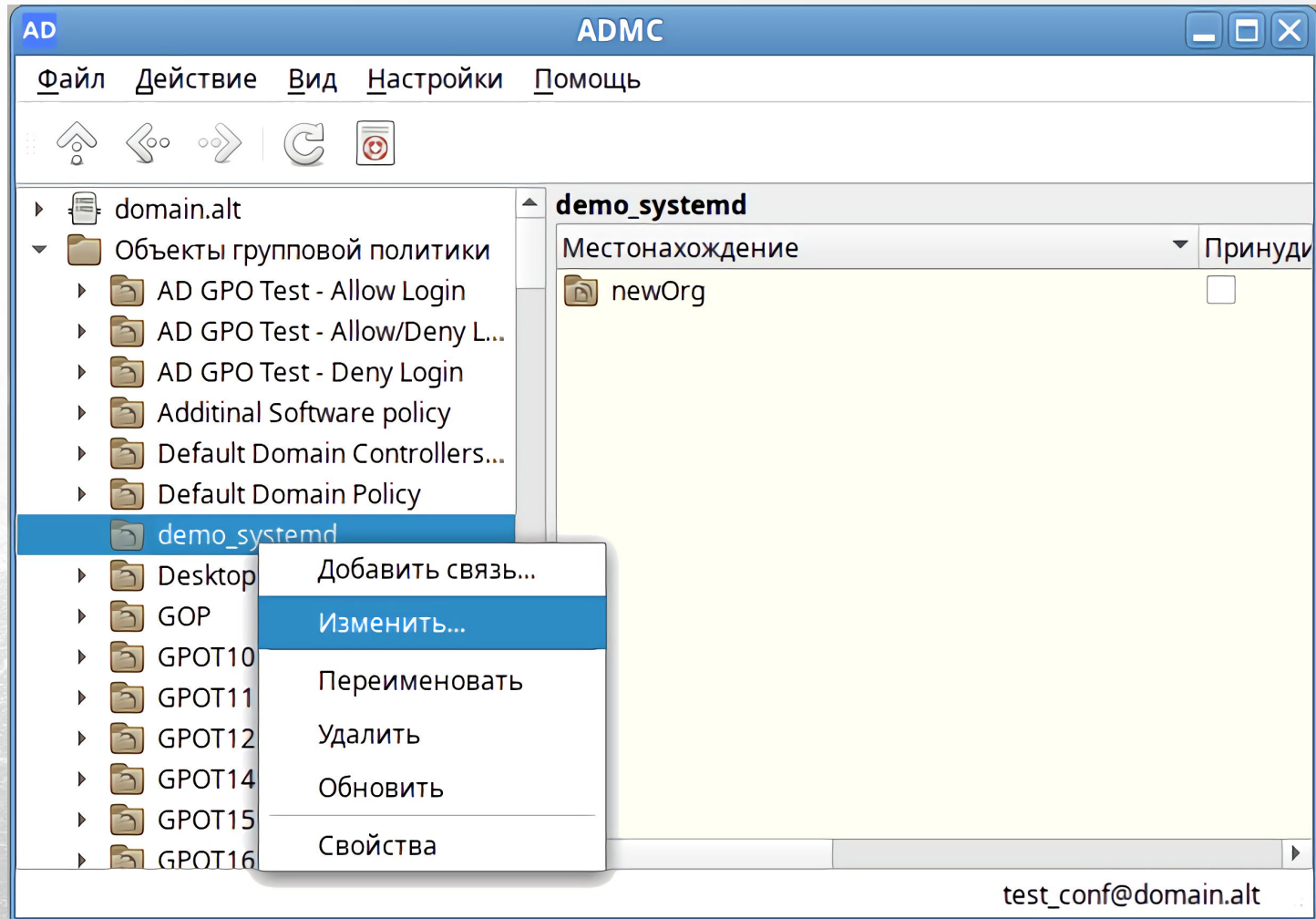
ADMS. Создание политики



ADMC. Создание политики. Добавление связи



ADMS. Создание политики. Изменение



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:

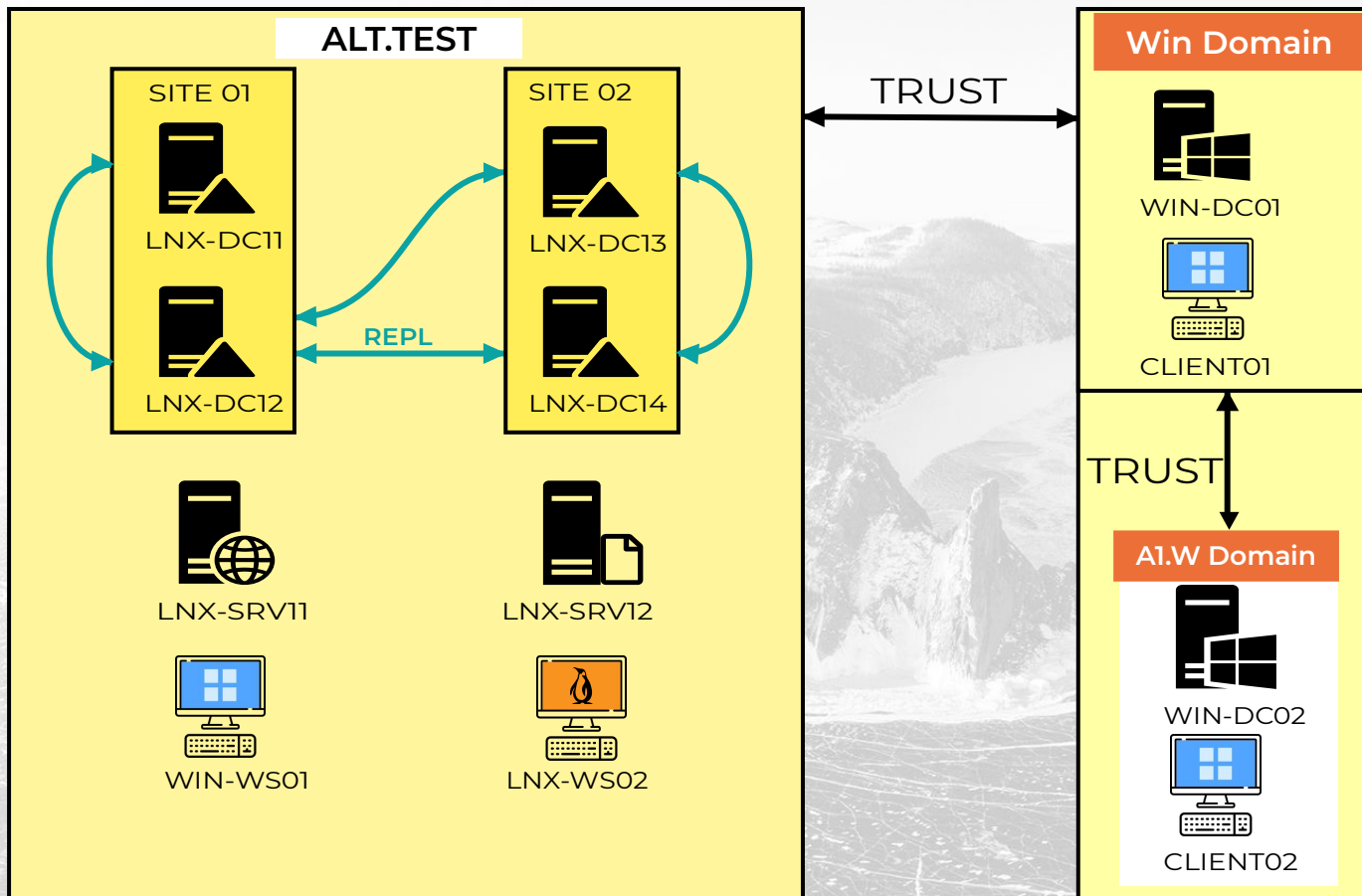
Пароль:

Включить групповые политики

OK

Отмена

Пример тестового стенда для реальной смешанной доменной инфраструктуры



**Фаза 3 : Импортзамещение состоялось.
Вы достигли совершенства, но вам все еще есть, куда расти.**



Подходы к миграции доменной инфраструктуры

Миграция — это замена операционных систем клиентов и серверов под управлением операционных систем семейства ОС Windows на базе инфраструктуры Microsoft Active Directory на аналогичные по функциональным возможностям свободные операционные системы и инфраструктурные решения.

1. Плавный перевод инфраструктуры на Samba Active Directory.
Клиенты — Windows и Linux.
2. Постепенная «миграция» на любое, аналогичное по функциональным возможностям инфраструктурное решение, например, FreeIPA. Клиенты — только Linux.

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.

Плавная миграция. Ограничения

- Только SambaDC.
- Риски простоя и сложности реализации.
 - ♦ Только 2012r2 со схемой леса 2008r2.
 - ♦ Особенность первичной репликации.
 - ♦ Ограничения в поддержке репликации объектов из расширенной схемы (Exchange, Sharepoint, ...).
 - ♦ Отсутствие поддержки полноценного леса.
- Преимущество — бесшовный сценарий



ОСОБЕННОСТИ ЛИЦЕНЗИРОВАНИЯ ОС «АЛЬТ»

- ✓ У всех ОС лицензии разрешают бесплатное использование ПО физическими лицами, ограничение — юридические лица
- ✓ Виды лицензий: бессрочные или годовые подписки
- ✓ Лицензия приобретается на каждую установку на оборудование (компьютер, терминал) или в виртуальную среду
- ✓ Исходные коды предоставляются на все свободные программы, входящие в дистрибутив, в течение 3-х лет с момента приобретения
- ✓ Лицензии для тестирования выдаются бесплатно на срок 3-6 месяцев

Техническая поддержка дистрибутива включена в лицензию на весь срок жизни продукта, но не менее чем на 3 года с момента покупки



ОСОБЕННОСТИ ЛИЦЕНЗИРОВАНИЯ ОС «АЛЬТ»

Лицензия на сервер:

- ✓ Неограниченное количество подключенных клиентов
- ✓ Неограниченное количество процессоров/ядер и т. п.

Лицензия на виртуальную рабочую станцию

- ✓ Неограниченное количество одновременно работающих пользователей
- ✓ Нет ограничения по используемым ресурсам (процессор/ядро, ОЗУ и т.п.)

Лицензия на Сервер Виртуализации:

- ✓ Лицензируется физическая или виртуальная нода
- ✓ Неограниченное количество запущенных виртуальных машин
- ✓ Нет ограничения по используемым ресурсам (процессор/ядро, ОЗУ и т.п.)



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА ОС «АЛЪТ» НА ВСЕЙ ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

- ✓ **Поддержка продукта** входит в стоимость лицензии и включает регулярный выпуск обновлений по безопасности и исправление ошибок в дистрибутивах. Поддержка предоставляется в течение всего срока жизни дистрибутива. Срок поддержки продукта составляет не менее 5 лет с даты выпуска и не менее 3 лет с даты последней продажи.
- ✓ **Поддержка пользователей** включает поддержку эксплуатации продукта. Предоставляется ИТ-подразделению заказчика или иной структуре, которая занимается поддержкой конечных пользователей. Предусмотрено несколько уровней поддержки с соответствующими SLA по объему поддержки, способам приема заявок и скорости реагирования. При необходимости могут быть предоставлены специальные условия, например, удаленное управление, а также прием на поддержку готового решения заказчика.

1 и 2 уровни поддержки обеспечивают авторизованные партнеры «Базальт СПО»

3 (вендорский) уровень поддержки предоставляет разработчик – компания «Базальт СПО»

С вопросами по работе технической поддержки дистрибутивов «Альт» обращайтесь по электронной почте: sales@basealt.ru

НАША ЛИНЕЙКА КУРСОВ В УЧЕБНЫХ ЦЕНТРАХ

подробнее о курсах:

www.basealt.ru/courses/training



ОБУЧАЮЩИЕ КУРСЫ

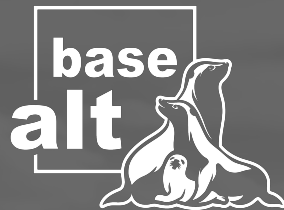
- | | |
|-------------------|---|
| ALTADM1 | «Администрирование ОС Альт. Часть 1» |
| ALTADM2 | «Администрирование ОС Альт. Часть 2» |
| ALTSHELL | «Автоматизация (shell-скрипты) в ОС Альт» |
| ALTVIRT | «Виртуализация в ОС Альт» |
| ALTSERV | «Инфраструктурные службы ОС Альт» |
| ALTUSERPRO | «Профессиональный пользователь ОС Альт» |



ОБУЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

- Авторские курсы по дистрибутивам «Альт»
- Портал дистанционного обучения
- kurs.basealt.ru
- Ролики на **YOUTUBE**-канале «Базальт СПО»
- Литература по СПО:
 - ♦ books.altlinux.org
 - ♦ docs.altlinux.org
 - ♦ altlinux.org





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”