



ALD^{Pro}

РОССИЙСКАЯ СЛУЖБА КАТАЛОГА
КОРПОРАТИВНОГО КЛАССА

ALD^{pro}
3.0

Что такое служба каталога?

Служба каталога - это единая централизованная система управления пользователями, компьютерами и сетевыми ресурсами организации, представленная как единый каталог.

Поэтому принято называть её службой каталога, подчеркивая уникальность и целостность структуры.

ALD Pro — это инструмент экономии порядка



Служба каталога - **это инструмент экономии и порядка**

ALD Pro — это инструмент экономии порядка

Служба каталога - **это инструмент экономии и порядка**



Экономии трудозатрат и времени
администраторов и сотрудников
информационной безопасности

ALD Pro — это инструмент экономии порядка

Служба каталога - **это инструмент экономии и порядка**



Экономии трудозатрат и времени
администраторов и сотрудников
информационной безопасности



Порядок и централизация
управления пользователями,
их правами и доступом

Служба каталога - **это инструмент экономии и порядка**



Экономии трудозатрат и времени администраторов и сотрудников информационной безопасности

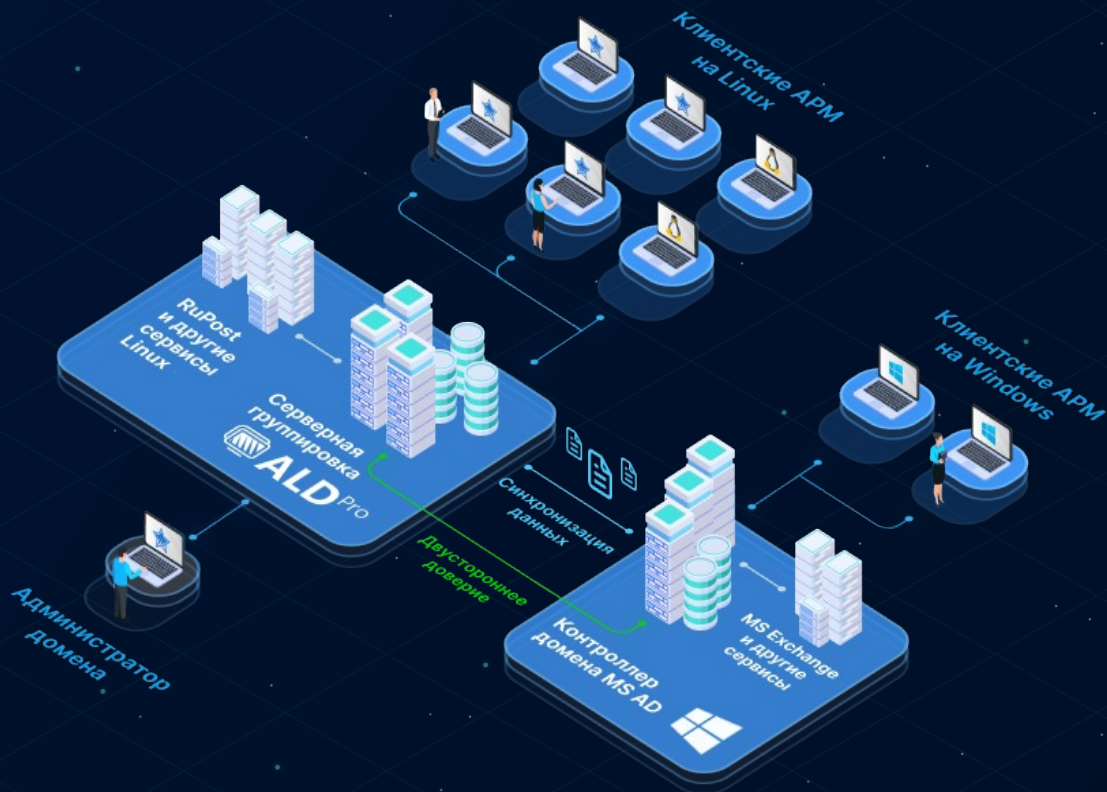


Порядок и централизация управления пользователями, их правами и доступом



Единая точка для управления, которая снижает порог входа сотрудников, администрирующих ИС

Возможности служба каталога ALD Pro



- **Централизованное управление учётными записями**

Хранение и управление учётными записями пользователей, компьютерами и сервисами в одном месте и, как следствие, снижение расходов на администрирование

- **Единая точка сквозной аутентификации Kerberos v5**

Освобождает пользователей от необходимости повторного ввода пароля и его хранения в открытом виде в диспетчерах паролей

- **Делегирование полномочий**

Реализована возможность распределения зон ответственности между администраторами

- **Групповые политики**

Централизованное управления параметрами компьютеров и пользователей при помощи групповых политик на базе SaltStack

- **Автоматическое развертывание сервисов**

Возможно выполнять автоматическое развёртывание следующих сервисов: репозитории deb-пакетов, SMB файловый сервер, IPP сервер печати, DHCP, установка ОС по сети, мониторинг

✓ Запись в «Реестре российского программного обеспечения» №12159 от 30.11.2021

✓ Сертификат соответствия ФСТЭК (по 2 УД и ТУ) №4830 от 26.07.2024

Ключевые улучшения в релизе 3.0

ВЫШЕ НАДЕЖНОСТЬ. ПРОЩЕ ЭКСПЛУАТАЦИЯ. ЛЕГЧЕ МИГРАЦИЯ.

БЫСТРОЕ ВНЕДРЕНИЕ

Графические утилиты
для развертывания
ALD Pro

Типовые пилоты для
демонстрации
базового
функционала

2 ЧАСА
на развертывание
2 ДНЯ
на прохождение ПМИ

ЛЕГКАЯ МИГРАЦИЯ

Новый модуль
синхронизации –
перенос 10 000 учетных
записей за 2 часа

НАДЕЖНАЯ РАБОТА

Надежная работа ДДО
– возможность
пользователям Windows
работать в
инфраструктуре Linux и
наоборот

МУЛЬТИВЕНДОРНОСТЬ

Возможность ввести в
домен ALD Pro ПК под
ОС Windows, Ред и Альт

Ключевые улучшения в релизе 3.0

**В 10 РАЗ
ВЫШЕ**

производительность
системы относительно
релизов ниже версии 2.1

**В 2 РАЗА
БОЛЬШЕ**

клиентских подключений
к контроллеру домена
относительно релиза 2.3

30 РОЛЕЙ

предустановлены в системе
для более гибкого
администрирования

**> СНЯТЫ
ОГРАНИЧЕНИЯ**

на количество политик,
применяемых к одному
компьютеру или серверу

**> БЫСТРАЯ
СИНХРОНИЗАЦИЯ**

оптимизирована работа модуля
синхронизации данных между
доменами ALD Pro и MS AD

> ПОДДЕРЖКА 1.8.1

реализован клиент для
входа в домен для
версий 1.8.1 и 1.8.1 UU 1

Модуль инвентаризации в составе ALD Pro



ACM



ALD^{Pro}

Сделан на базе ACM 1.3.0

ФУНКЦИИ АСМ

- Аппаратная инвентаризация
- Инвентаризация установленного ПО
- Учет лицензий Astra Linux

СКОРО

- Единый артикул
- Отгрузка заказчиком бандлом
- Цена бандла = ALD Pro
- Позиции появятся в прайсе

Мультивендорность. Новые возможности для масштабирования

РЕАЛИЗОВАНА ПОДДЕРЖКА ОПЕРАЦИОННЫХ СИСТЕМ ALT LINUX И РЕД ОС

Начиная с версии ALD Pro 3.0.0 для
операционных систем
ALT Linux 10.4,
РЕД ОС 7.3 и РЕД ОС 8.



- Параметры групповых политик могут быть разработаны партнером-интегратором.
- Разработано подробное руководство с инструкцией и примерами.



Улучшения в архитектуре 3.0 на уровне enterprise+

> СНЯТЫ ОГРАНИЧЕНИЯ ПО ЧИСЛУ КД

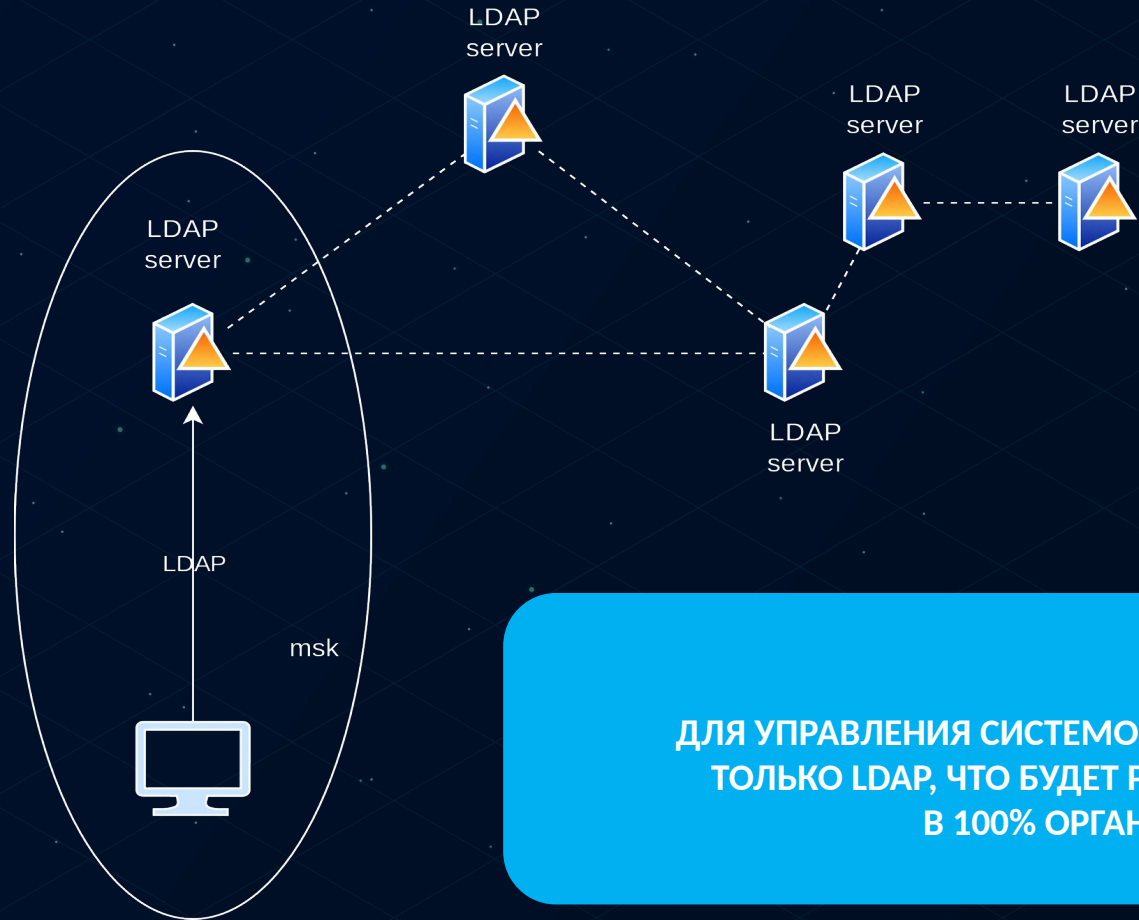
Компонент Salt Master накладывал ограничение в 10 КД, а компонент RabbitMQ — в 60 КД.

> УВЕЛИЧЕНА ПРОИЗВОДИТЕЛЬНОСТЬ

Нагрузки по суммированию ГП переложили на рабочие станции.

> РЕАЛИЗОВАЛИ УСТОЙЧИВОСТЬ К РАЗДЕЛЕНИЮ

Компоненты GlusterFS и RabbitMQ требовали полной сетевой связанности между контроллерами. Теперь хосту достаточно иметь доступ только к одному КД.



ДЛЯ УПРАВЛЕНИЯ СИСТЕМОЙ НУЖЕН
ТОЛЬКО LDAP, ЧТО БУДЕТ РАБОТАТЬ
В 100% ОРГАНИЗАЦИЙ.

Производительность интерфейсов 3.0

- Запросы UI оптимизированы под LDAP
- Добавили индексацию по ряду атрибутов
- Повысили производительность хеширования паролей

> ИНТЕРФЕЙС РАБОТАЕТ БЫСТРЕЕ > УСКОРИЛИ ЗА СЧЕТ ИНДЕКСОВ > УСКОРИЛИ LDAP BIND

Ранее использовали стандартный набор индексов, теперь добавили индексацию по нужным атрибутам для ускорения запросов.

Ранее мы пытались извлекать все объекты и строить постраничную навигацию. Теперь отображаем как в AD только первые 2000 элементов, что на порядок быстрее.

Ранее использовался очень безопасный, но не самый быстрый алгоритм хеширования паролей. Подняли к производительности AD.

Централизованное управление МКЦ/МРД + управление USB-накопителями



Теперь в интерфейсе ALD Pro можно управлять уровнями доступа пользователя



Централизованная настройка уровней и категорий МКЦ/МРД на рабочих станциях выполняется с помощью групповых политик ALD Pro, а допустимые значения для пользователя, выполняющего вход в систему, предоставляет служба SSSD.

**УПРАВЛЕНИЕ МОДУЛЕМ ЯДРА «PARSEC» —
КЛЮЧЕВАЯ ФУНКЦИЯ ДЛЯ ВСЕХ ИНСТАЛЛЯЦИЙ
«ВОРОНЕЖ» И «СМОЛЕНСК».**



Что такое МКЦ?

МКЦ (Модуль контроля целостности)

**Проверяет целостность файлов и приложений,
предотвращает несанкционированные изменения**



Мандатный контроль целостности (МКЦ)

УГРОЗЫ

Внедрение и использование вредоносного кода

Управление вредоносным кодом и компонентом

Повышение привилегий

Соккрытие действий

Получение доступа к другим компонентам

Неправомерный доступ или воздействие

ФУНКЦИИ ЗАЩИТЫ ASTRA LINUX

Мандатный контроль целостности

Стандартная
Операционная система



Стандартная
Операционная система
После атаки



Стандартная
Операционная система
Полная потеря данных



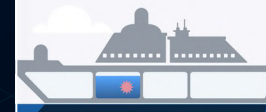
Операционная система
Astra Linux



Операционная система
Astra Linux
После атаки

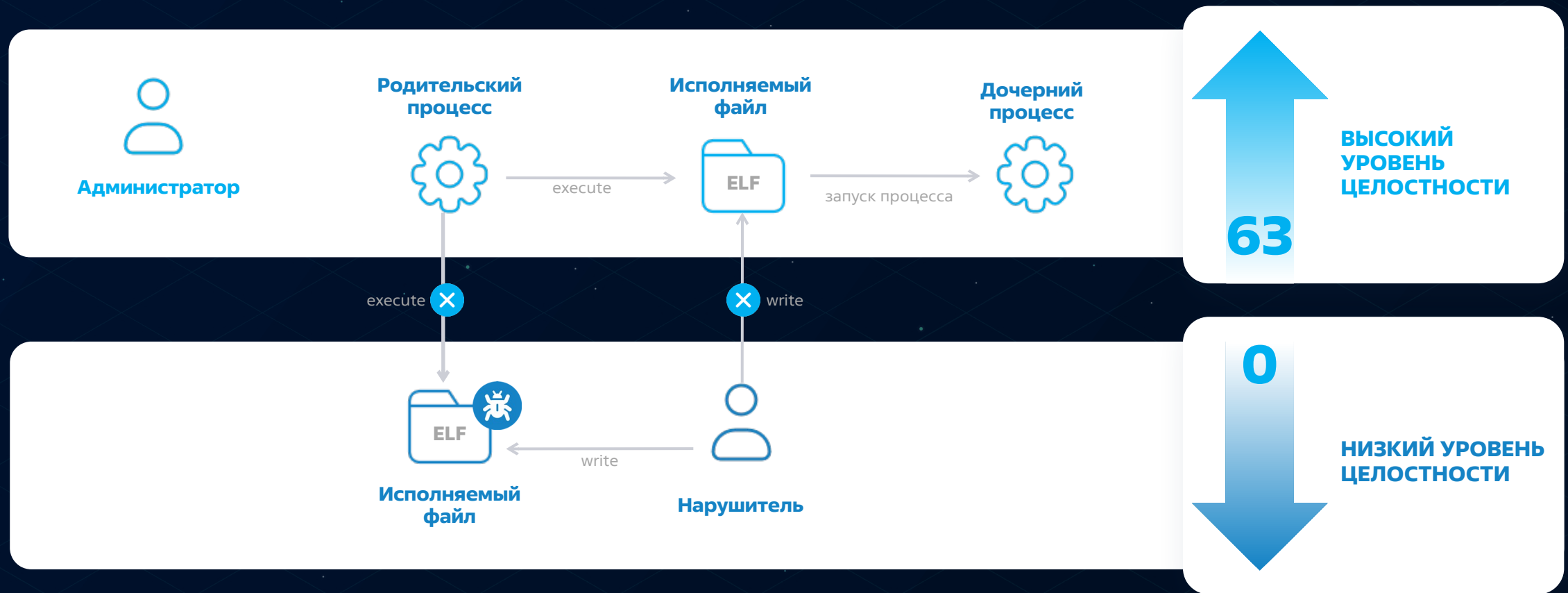


Операционная система **Astra Linux**
Изоляция поврежденного сектора
позволяет продолжать работу



Мандатный контроль целостности (МКЦ)

ПРИМЕР ИСПОЛЬЗОВАНИЯ МКЦ В ASTRA LINUX



Что такое МРД?

МРД

Мандатное управление доступом (Mandatory Access Control, MAC)

Механизм контроля доступа, основанный на уровнях секретности объектов и уровне допуска субъектов и категорий конфиденциальности.

Обеспечивает защиту информации, ограничивая доступ согласно правилам: "высокий читает низкий но не пишет, а низкий не видит высокий"



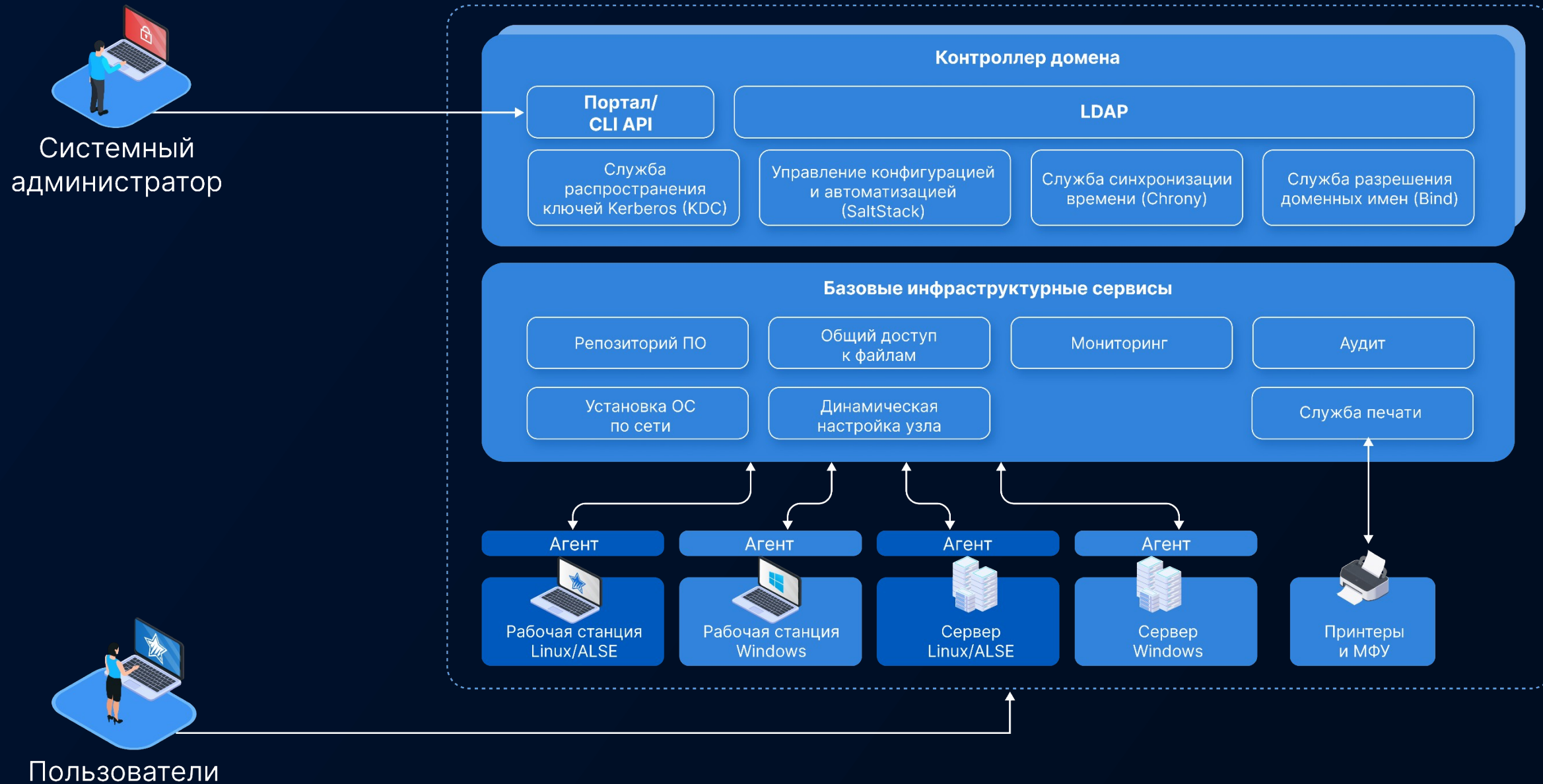
Мандатное управление доступом

ASTRA LINUX
DESKTOP

ASTRA LINUX
SERVER



Архитектура ALD Pro



Миграция домена

Сценарий импортозамещения

Миграция или синхронизация данных из домена MS Active Directory

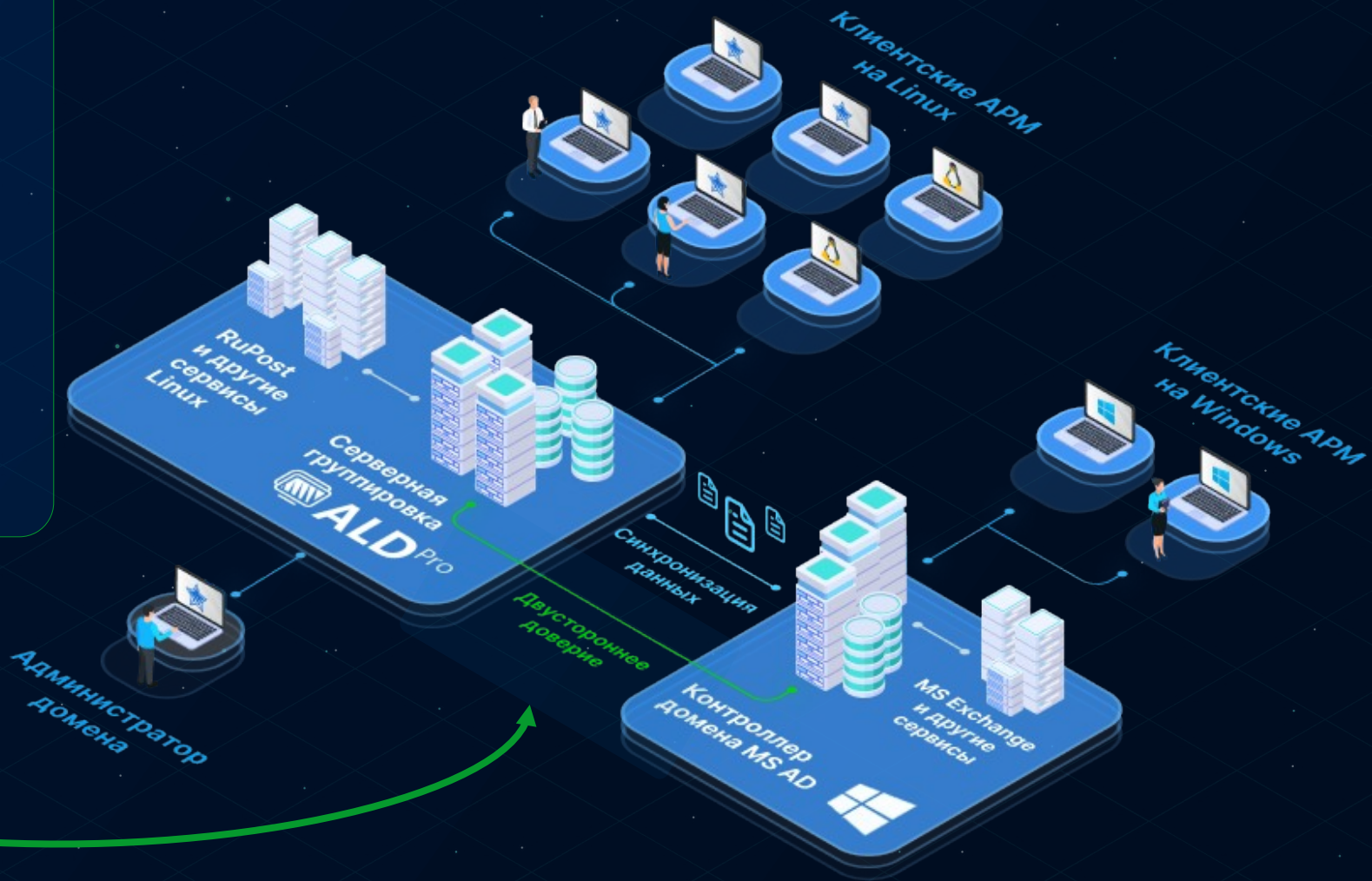
- Орг.структура (OU)
- Учетные записи пользователей
- Группы
- Пароли



Построение гетерогенной инфраструктуры

Сценарий импортозамещения

Двусторонние доверительные отношения позволяют делегировать доступ к ресурсам между доменами и обеспечивают взаимную аутентификацию пользователей



Проблемы импортозамещения

1

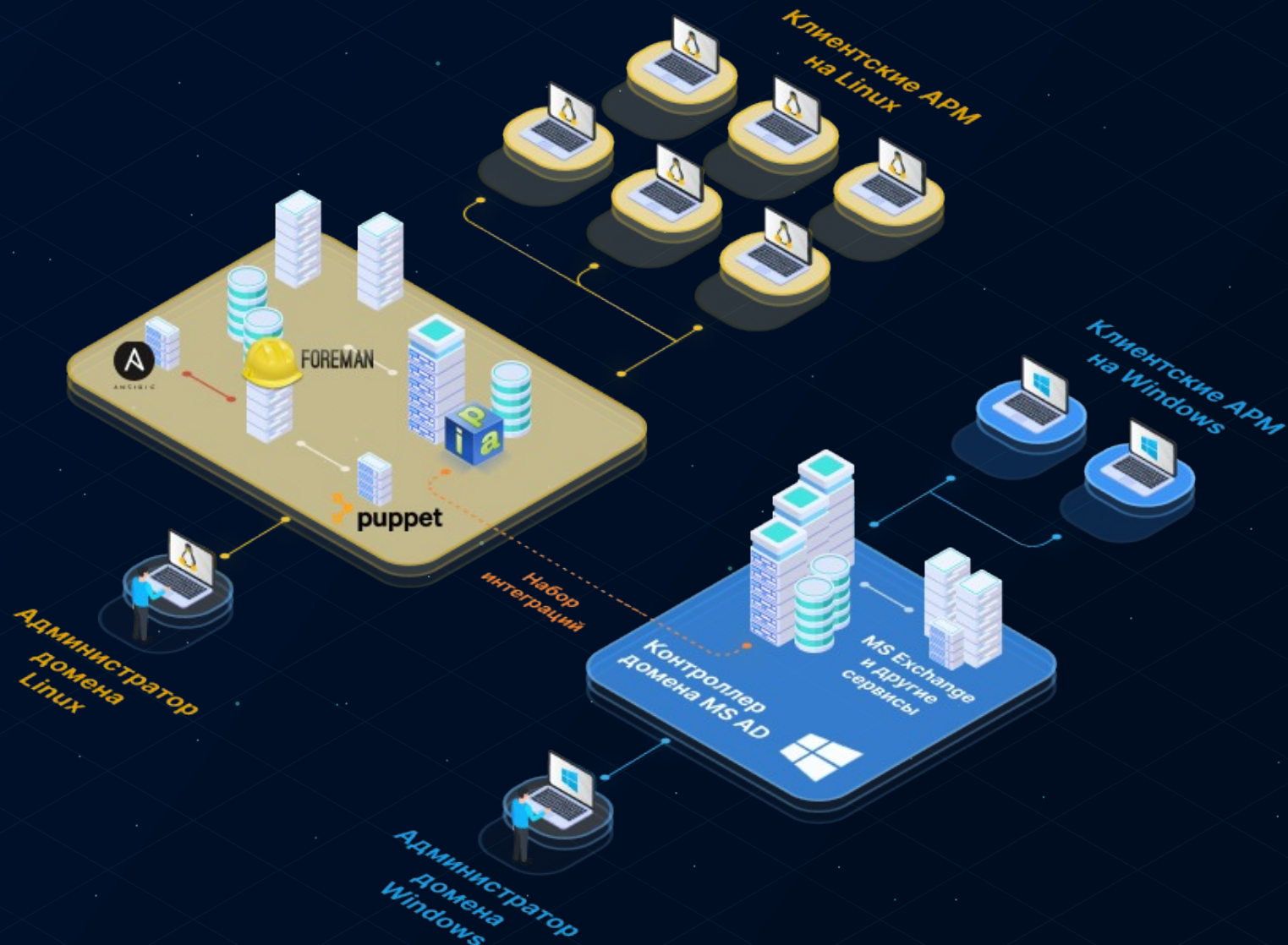
технологически сложные
решения без описания
лучших практик

2

отсутствует техническая
поддержка и описание
сценариев миграции и
внедрения

3

нужна поддержка
совместной работы
с MS Active Directory



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

1

анализ текущей инфраструктуры



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

1

анализ текущей инфраструктуры

2

развертывание и настройка
ALD Pro



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

1

анализ текущей инфраструктуры

2

развертывание и настройка
ALD Pro

3

настройка доверительных
отношений



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

4

синхронизация данных
между двумя доменами

5

ввод новых компьютеров в
домен, установка ОС и ПО по
сети на компьютеры под
Linux



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

4

синхронизация данных между двумя доменами

5

ввод новых компьютеров в домен, установка ОС и ПО по сети на компьютеры под Linux

6

настройка параметров компьютеров и пользователей через групповые политики



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

7

перенос сервисов из домена MS AD в домен ALD Pro



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

7

перенос сервисов из домена MS AD в домен ALD Pro

8

завершение миграции
всех компьютеров и
пользователей на
отечественное ПО



Шаги по внедрению ALD Pro и Astra Linux в инфраструктуру MS

7

перенос сервисов из домена MS AD в домен ALD Pro

8

завершение миграции всех компьютеров и пользователей на отечественное ПО

9

масштабирование домена с ростом организации



47+

интеграций на август 2025 г.

20+

интеграций в планах до конца 2025

40+

интеграций в планах за 2026

100+

интеграций к концу 2026



Kaspersky
Unified Monitoring
and Analysis Platform



КонсультантПлюс
надежная правовая поддержка



FOREMAN



Комьюнити профессионалов

←

ALD Профессионалы 🚀

1 437 участников

📄

Лента

ALD Профессионалы 🚀: Всем прошаренным ...

#

Информирование (readme) ⓘ

13.05.2025

ALD Профессионалы 🚀: Вышло глобальн...

📁

Материалы по продукту

20.05.2025

ALD Профессионалы 🚀: SIEM-системы (Se...

🗨️

Курилка

11:20

Фещенко: Ну к нам они не приходили, кейса инт...

🌐

Групповые политики

27.03.2025

Nikita: Коллеги а подскажите какая сейчас актуал...

🐾

Интеграции

10.06.2025

ALD Профессионалы 🚀: ! Коллеги, спешим вам со...

★

Вакансии

09.06.2025

ALD Профессионалы 🚀: В команду ALD Pro и...

📖

Курс по службе каталога ALD Pro

03.12.2024

ALD Профессионалы 🚀: Часть 1. Astra Linux ⭐ Срав...

🔔

PreSale

28.11.2024

ALD Профессионалы 🚀: Во время презентации A...

📅

Интеграция ALD Pro с КонсультантПл...

02.10.2024

Timur: Коллеги, всем привет! Выкладываем финальн...

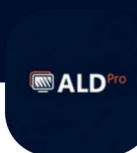
Интеграции

5 сообщений

Основано в ноябре 2024 года

- 1IDM
- 1C:Предприятие
- Ankey IDM
- Astra.Disk
- Bitrix
- DION
- Directum RX
- ELMA365
- Foreman
- GitFlic
- GranulexRecovery
- Ideco NGFW
- Kaspersky Unified Monitoring and Analysis Platform
- Keycloak
- MaxPatrol SIEM
- MikoPBXco
- MS Exchange
- MTS Link
- NGFW UserGate 7.1
- OpenVPN
- PKI Aladdin
- Pragmatic Tools
- Printum
- PRO32
- Proxmox VE
- RuBackup
- RuPost
- SafeTechCA
- Solar Dozor
- Solar inRights
- Solar SafeConnect
- Solar SafeInspect

Подписаться



@ALD_PROFESSIONALS

ОТКРЫТЫЙ ОНЛАЙН КУРС

370 000+

просмотров

64 000+

посетителей

10+

человеко-лет
исследований



Опубликован в ноябре 2024
года

Доступная онлайн документация

ДОСТУПНАЯ ОНЛАЙН ДОКУМЕНТАЦИЯ

<https://www.aldpro.ru/materials/3.0.0/>



Найти

Руководство администратора.
Быстрый старт

+ Руководство Администратора.
Часть 1

Общие сведения

Развертывание
контроллеров домена и
подсистем

Обновление подсистем

Матрицы совместимости и
обновлений

+ Руководство Администратора.
Часть 2

Руководство администратора.
Редакция Free

Руководство Пользователя

+ Программа и методика
испытаний

Выбрать версию:

Версия 3.0.0

Главная > Руководство Администратора. Часть 1

Развертывание контроллеров

Для установки серверной части **ALD Pro** (контроллер домена, подсистема) необходимо выполнить предварительных настроек.

При переустановке ALD Pro на сервер/компьютер (контроллер домена) необходимо предварительно убедиться, что этот хост присутствует в каталоге. Подробнее в разделах Вывод компьютера из домена и И

Развертывание первого контроллера

Подготовка окружения сервера к установке

Требования к ОС

Продукт **ALD Pro** можно установить на хостах под управлением операционной системы. Для контроллеров домена и других подсистем требуется максимальная версия операционной системы, установленная в системе с любым уровнем защищенности.

При установке продукта необходимо учитывать список поддерживаемых версий операционной системы → **Матрицы совместимости и обновлений** → **Матрица совместимости** → **1.7.xxx** - актуального оперативного обновления.

Для проверки версии и уровня защищенности операционной системы

```
cat /etc/astra/build_version
sudo astra-modeswitch getname
```

Результат выполнения команд:

Приложения к презентации

(Дополнительные материалы)

Приложения к презентации

- **Основные улучшения последней версии**
- Сертификация ФСТЭК
- Сравнение FreeIPA и Samba
- Доверие домена ALD Pro с другим доменом ALD Pro, или альтернатива замены леса MS AD

ОСНОВНЫЕ УЛУЧШЕНИЯ В РЕЛИЗЕ 2.5.0

✓ Оптимизирован механизм выбора источников для синхронизации времени

Изменения значительно повышают надежность протокола аутентификации Kerberos и других технологий. Решения конкурентов на базе Samba AD не имеют решения этой задачи.

✓ Доработки групповых политик

В форме редактирования групповых политик реализована возможность при назначении объектов на подразделения выбирать OU из дерева, что упростит работу с одноименными отделами в больших компаниях

✓ Решение для управления паролями локальных администраторов (LAPS)

Позволяет централизованно управлять паролями на компьютерах домена. Адекватное решение есть только у Альтов, которые задействовали те же атрибуты, которые использует MS.

✓ Новый инструмент экспорта/импорта объектов групповой политики (GPO)

Значительно упрощает управление настройками окружения. Теперь можно быстро переносить уже настроенные объекты в продуктивную среду

в **10** раз выше

производительность системы
относительно релизов ниже версии 2.1

в **2** раза больше

клиентских подключений к контроллеру
домена относительно релиза 2.3

30 ролей

предустановлены в системе для
более гибкого администрирования

СНЯТЫ ОГРАНИЧЕНИЯ

на количество политик, применяемых
к одному компьютеру или серверу

БЫСТРАЯ СИНХРОНИЗАЦИЯ

оптимизирована работа модуля синхронизации
данных между доменами ALD Pro и MS AD

ПОДДЕРЖКА 1.8.1

реализован клиент для входа в
домен для версий 1.8.1 и 1.8.1 UU 1

Приложения к презентации

- Основные улучшения последней версии
- **Сертификация ФСТЭК**
- Сравнение FreeIPA и Samba
- Доверие домена ALD Pro с другим доменом ALD Pro, или альтернатива замены леса MS AD

Кому необходима сертификация ФСТЭК



Энергетический сектор

Приказ ФСТЭК №17

Приказ ФСТЭК №239

Приказ ФСТЭК №31

Приказ ФСТЭК №21



Государственный сектор

Приказ ФСТЭК №17

Приказ ФСТЭК №239

Приказы МО РФ

Приказы ФСБ

Приказ ФСТЭК №21



Финансовый сектор

Приказ ФСТЭК №21

ГОСТ 57580

Приказ ФСТЭК №239

Положения ЦБ

Приказы ФСБ



Нефтегазовый сектор

Приказ ФСТЭК №31

Приказ ФСТЭК №239

Приказы ФСБ



Промышленный сектор

Приказ ФСТЭК №31

Приказ ФСТЭК №239

Приказы ФСБ

Ответственность за нарушение требований ИБ

Административная ответственность:
штрафы для должностных лиц
компаний от 20 000 до 300 000 руб.

Статья 13.11	Статья 13.32
Статья 13.15	Статья 13.39
Статья 13.31	

Ст. 272 УК РФ
Ст. 283 УК РФ
Ст. 274.1 УК РФ

**Помимо штрафов могут
применяться и другие санкции**

Приостановка
деятельности
организации сроком до
90 дней

Приостановка деятельности
организации пока нарушения
не будут исправлены в
установленные сроки

Лишение лицензии на
постоянной основе

Преимущества сертификации ФСТЭК

- Гарантировано может использоваться в ГИС, КИИ, АСУТП, ИСПДН
- Исключение сложностей при прохождении аттестации ФСТЭК в ИС в целом
- ALD Pro наиболее исследованная служба каталога ФСБ/ФСТЭК
- Гарантия безопасности доменной инфраструктуры, включая механизм доверия между доменами и интерфейс администратора
- Дополнительная защита в конкурсах

Приложения к презентации

- Основные улучшения последней версии
- Сертификация ФСТЭК
- **Сравнение FreeIPA и Samba**
- Доверие домена ALD Pro с другим доменом ALD Pro, или альтернатива замены леса MS AD



FreeIPA vs Samba AD

FreeIPA vs Samba AD



Samba

После создания невозможно увеличить размер БД

В Samba отсутствуют возможности управления SUDO-правилами и нет политик доступа к узлу (HBAC)

В домене нет идентификаторов POSIX, поэтому служба SSSD вынуждена выполнять пересчет

Сложность
расширения
БД

SUDO и HBAC

Поддержка
UID и GID

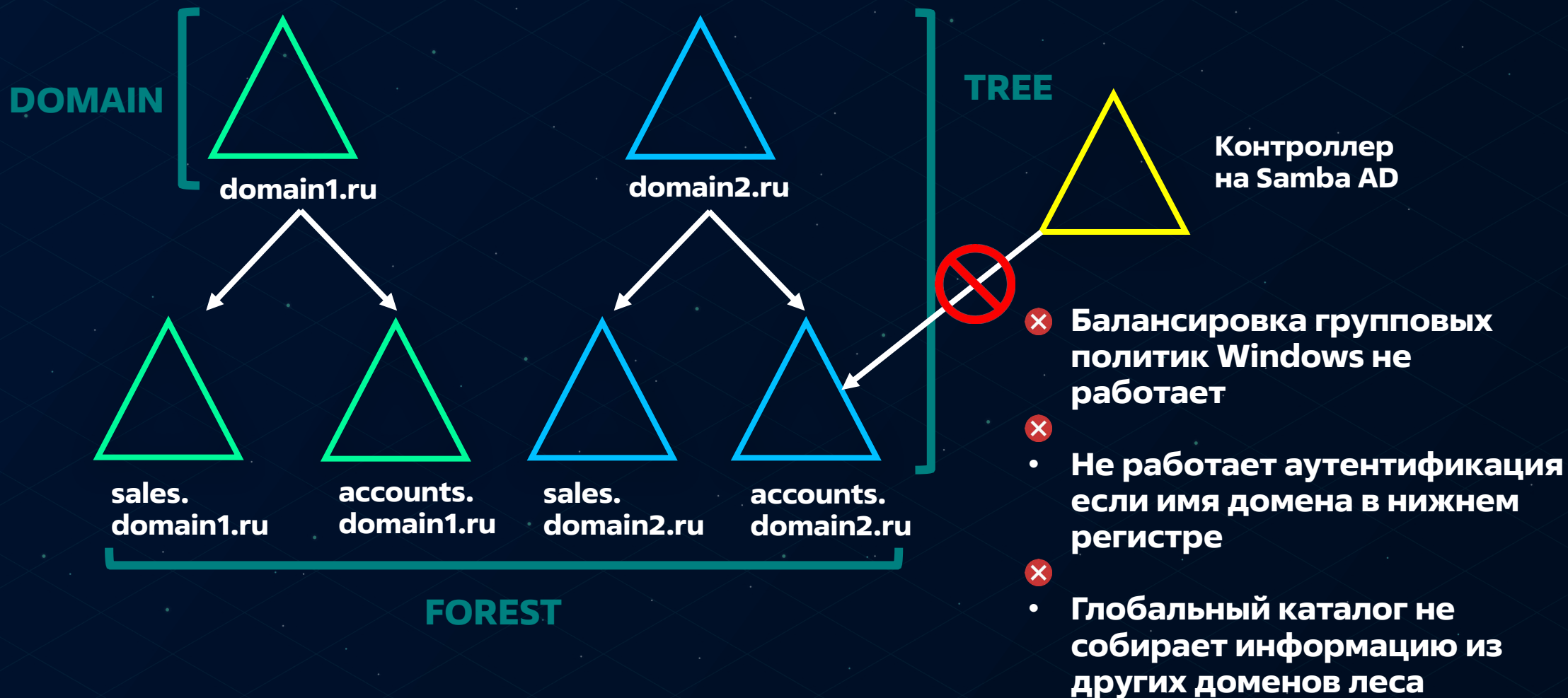
ALD Pro

Размер базы данных LDAP каталога зависит только от размера файловой системы

Имеет инструменты управления правилами SUDO и HBAC политиками, как консольные, так и графические.

Изначально работает с POSIX-идентификаторами в Linux среде.

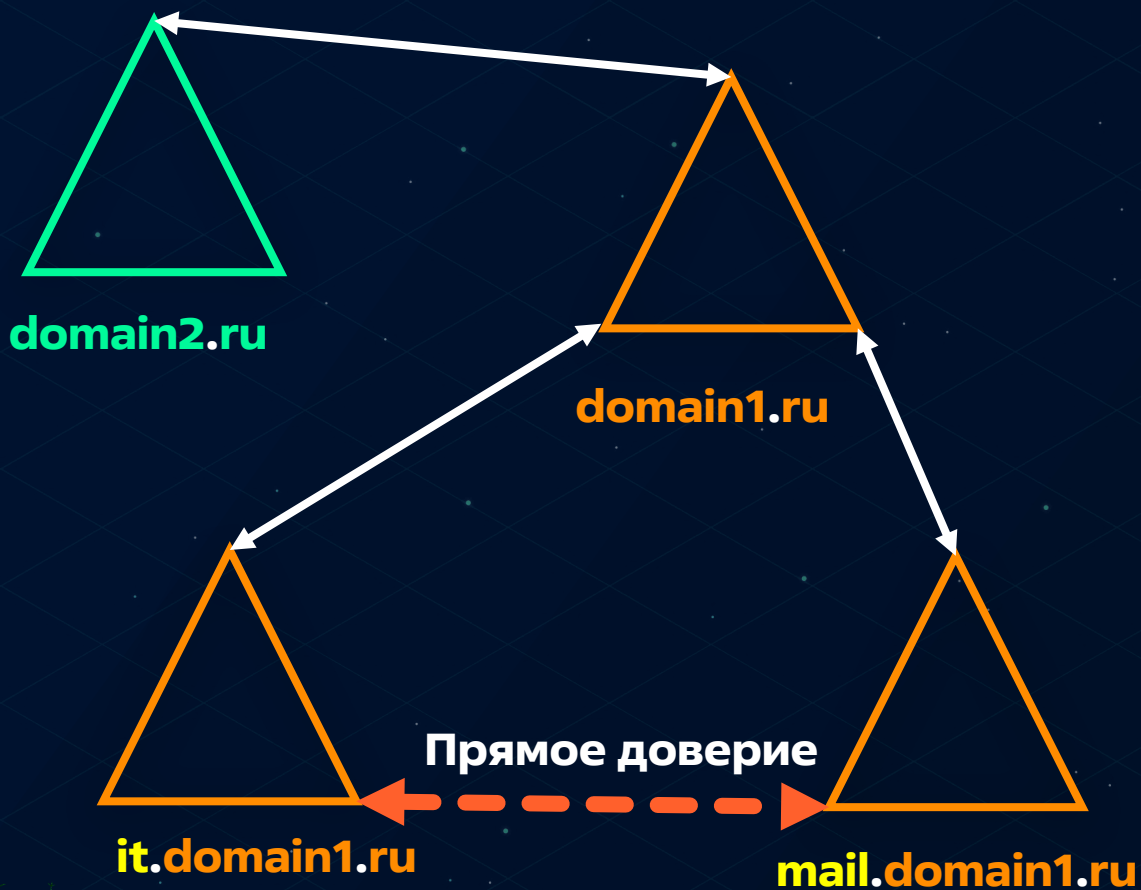
НЕВОЗМОЖНО ЗАМЕНИТЬ MS AD НА SAMBA AD



Приложения к презентации

- Основные улучшения последней версии
- Сертификация ФСТЭК
- Сравнение FreeIPA и Samba
- **Доверие домена ALD Pro с другим доменом ALD Pro, или альтернатива замены леса MS AD**

ЗАЧЕМ НУЖЕН ЛЕС В ACTIVE DIRECTORY ?



- **Периметр администрирования**

В лесу доменов MS AD администраторы могут делегировать полномочия на управление доменом, при этом домен MS AD не является периметром безопасности

- **Снижение требований к контроллерам**

В лесу доменов MS AD при делении большой инфраструктуры на маленькие домены снижаются требования по ОЗУ на контроллерах домена

- **Доверительные отношения**

В лесу доменов MS AD между доменами автоматически выстраиваются двусторонние транзитивные ДДО

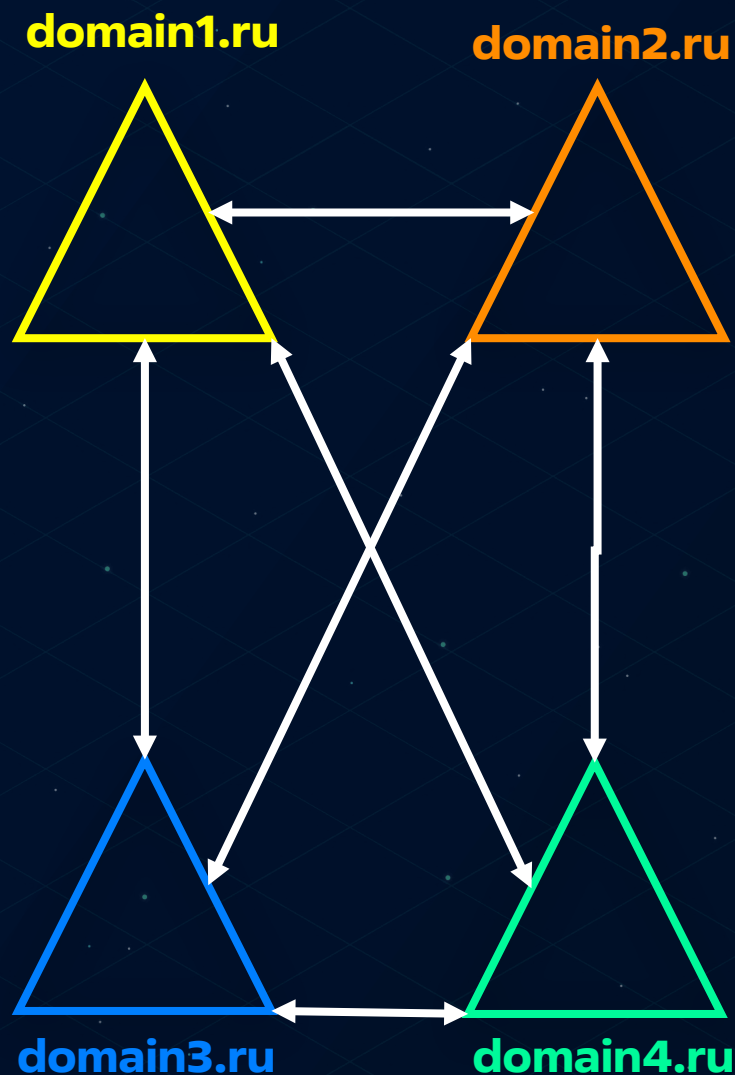
- **Общая схема каталога**

В лесу доменов MS AD используется общая схема, т. е. набор атрибутов, классов объектов и т.д.

- **Общая DNS-зона**

В лесу доменов MS AD можно создавать дочерние поддомены, которые будут использовать общую DNS-зону

КАКИЕ ЗАДАЧИ РЕШАЮТ ДДО МЕЖДУ ДОМЕНАМИ ALD PRO



- **Периметр администрирования**

В инфраструктуре ALD Pro администраторы могут передать полномочия на управление доменом, при этом домен ALD Pro является еще и периметром безопасности.

- **Снижение требований к контроллерам**

В инфраструктуре ALD Pro при делении большой инфраструктуры на несколько доменов ALD Pro снижаются требования по ОЗУ на контроллерах

- **Доверительные отношения**

В инфраструктуре ALD Pro между доменами можно вручную выстроить доверительные отношения «все со всеми», что полностью решает данную задачу

- **Общая схема каталога**

В инфраструктуре ALD Pro можно вручную во всех доменах обеспечить одинаковую схему, которая будет содержать тот же набор атрибутов, классов объектов и т. д. Использование общей схемы не является преимуществом.

- **Общая DNS-зона**

В инфраструктуре ALD Pro каждый домен должен иметь собственное имя, поэтому все домены нужно будет создавать на одном уровне. Использование общей DNS-зоны не является преимуществом.