IDM

Управление жизненным циклом учетных записей

Управление доступом

Централизованный аудит и контроль соответствия

Сервис самообслуживания пользователей

Управление паролями

Управление доступом

Система управления учетными записями и правами доступа пользователей к корпоративным ресурсам организации

AVANPOST

Разработчик систем аутентификации и управления доступом к информационным ресурсам предприятия

IDM
Система управления учетными записями и правами доступа пользователей к корпоративным ресурсам организации

FAM
Система единой аутентификации сотрудников в корпоративных ресурсах организации

PKI
Система управления всеми элементами инфраструктуры открытых ключей из единого центра

WEB SSO
Система единой аутентификации клиентов в порталах и внешних приложениях

Avanpost Directory Service

Полностью российская служба каталогов

AVANPOST

Разработчик систем аутентификации и управления доступом к информационным ресурсам предприятия

AVANPOST

Использование продукта на базе OSS → большое количество рисков и ограничений

Решение на базе FreeIPA

Обеспечивает только эмуляцию дерева домена за счет дополнительных атрибутов, структура каталога при этом остается плоской, что является ограничением масштабирования и выполнения ряда сценариев

В основе продукта много легаси кода, значительная часть функционала реализована на Python

Ориентирован на работу только с конкретным дистрибутивом. Другими клиентами Linux централизовано управлять придется с помощью иных программных средств

Avanpost Directory Service

Предлагается служба каталогов полностью собственной разработки

Изначально спроектирован с поддержкой полноценной древовидной структуры домена с возможностью вложенности подразделений, распределения каталога по узлам

Используется современный, высокопроизводительный, технологический стек: Golang, Badger DB, Nats

Поддерживает все Российские дистрибутивы Linux, как для контроллеров домена, так и в качестве доменных клиентов

Идеология Avanpost DS

В настоящий момент целевой схемой замещения операционных систем рабочих станций является применение российских дистрибутивов Linux.

Подход к построению Linux-инфраструктур традиционно отличается от плотно интегрированной закрытой экосистемы Windows. Основные постулаты, на которых строится ОС Linux и его окружение гласят:

- Пишите программы, которые делают что-то одно и делают это хорошо.
- Пишите программы, которые бы работали вместе.

В соответствии с этими постулатами реализовано большинство приложений и сервисов в Linux. И применение привычного подхода Microsoft не является оправданным и во многих случаях сильно ограничивает возможности эффективного построения целевых инфраструктур крупных предприятий.

Avanpost DS предлагает:

- Поддержку открытых протоколов в соответствии со стандартами;
- Поддержку точек расширения, позволяющую создать инфраструктуру, необходимую клиенту

Реализованный функционал уже сейчас позволяет решать задачи:

AVANPOST

01 Централизованная аутентификация по протоколу LDAP для приложений

02 Многофакторная аутентификация (интеграция с Avanpost FAM)

03 Сквозная аутентификация по протоколу Kerberos V5 (Kerberos Single Sign On)

04 Контроль доступа к ресурсам на основе членства в группах

05 Контроль доступа к объектам каталога на основе ролевой модели

06 Централизованное управление пользователями и компьютерами

07 Иерархическое хранение информации о пользователях и ресурсах

08 Георазпределенное отказоустойчивое хранение данных каталога

09 Централизованная аутентификация по протоколу Kerberos v5 при доступе к серверам и рабочим станциям

10 Обеспечение высокой доступности сервисов идентификации, аутентификации и авторизации

Текущий функционал Avanpost DS

LDAP каталог, как централизованное хранилище информации о пользователях и ресурсах

- Централизованное управление пользователями и компьютерами
- Поддержка авторизации доступа к ресурсам на основе групп
- Поддержка доменной иерархии (OU)
- Индексирование атрибутов
- Расширяемая схема

01

Реализован функционал репликации

- Мультимастер репликация (без необходимости назначения единого источника)
- Автоматическое построение топологии
- Встроенные механизмы разрешения конфликтов репликации
- Гибкая, отказоустойчивая топология межсайтовой репликации

02

Реализован функционал Kerberos v5 KDC

- AS и TGS обмен ключами
- Сквозная аутентификация
- Аутентификация на основе сертификатов

03

Реализована ролевая модель доступа к объектам службы каталогов

- Гранулярный доступ на уровне атрибутов
- Механизм наследования разрешений
- Контроль доступа на основе членства в группах

04

AVANPOST

Журнал безопасности

- Учет событий привязки LDAP
- Учет событий выдачи ключей
- Kerberos
- Учет изменений в каталоге
- Передача событий в SIEM

05

Веб консоль администратора дает возможность управления вышеизложенным функционалом, в частности:

- Управление объектами каталога в режиме иерархии и в плоском виде
- Доступ к журналу безопасности
- Управление DNS зонами

06

Доменный клиент

- Автоматизация введения компьютера в домен
- Настройка диспетчера аутентификации (sssd)
- Настройка сквозной аутентификации по протоколу Kerberos v5
- Обновление Kerberos ключей по расписанию
- Обновление DNS записей
- Поддержка Alt, Astra, RED OS, ROSA и других по запросу

07

Интеграция с DNS сервером:

- Хранение данных DNS зоны в каталоге
- Безопасные динамические обновления

08

Многофакторная проверка подлинности, интеграция с Avanpost MFA+

(Federated Access Management)

09

AVANPOST

Технологические преимущества

Отказоустойчивость при высоких нагрузках

Продукты разрабатываются с учетом требований к масштабированию крупных компаний и обеспечивают высокую производительность и отказоустойчивость в высоконагруженных средах.

04

Современный технологический стек

Разработка ведется с помощью технологий для высокопроизводительных сервисов:
- Go/BadgerDB/Vue.js

Поддерживаемые технологии:
- полный набор используемых в России дистрибутивов Linux;
- контейнеризация Doker & Kubernets;
- Cloud Ready;
- популярные Open Source решения;
- популярные проприетарные решения.

05

Современные WEB-интерфейсы

Web-интерфейсы продуктов разработаны с использованием популярных Frameworks, что обеспечивает совместимость и поддержку браузерами. Широкие возможности по брендированию и кастомизации.

06

Гибкая интеграционная шина

Продукты адаптируются к архитектуре и системам заказчика, могут быть внедрены на сложной неоднородной мультидоменной ИТ инфраструктуре. Открытые API у всех продуктов и компонентов.

07

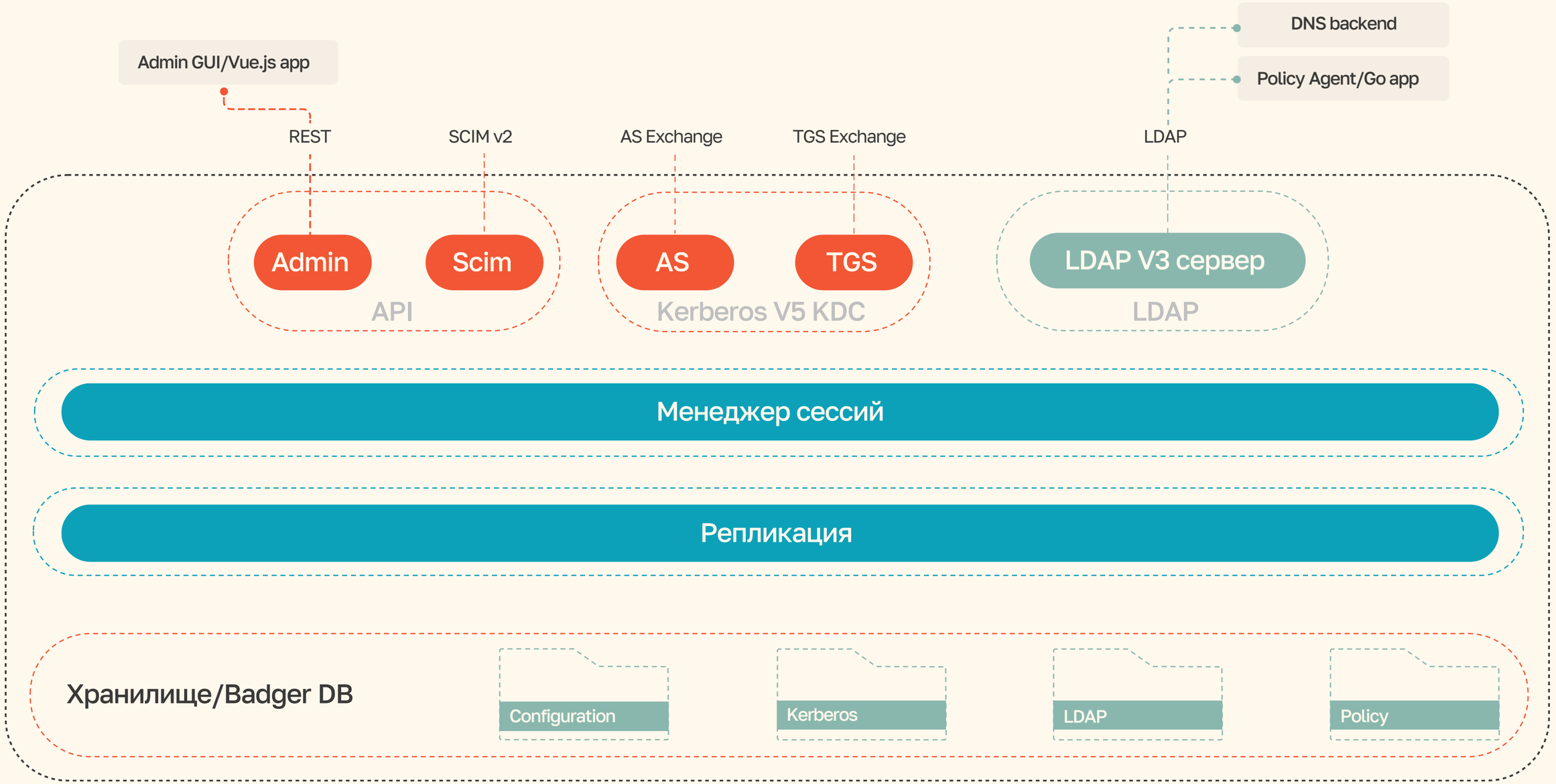
Поддержка клиентов 24/7

Доступность 24/7.
Гибкость планов технической поддержки позволяет выбрать оптимальное соотношение цены и комплекса услуг.

08

AVANPOST

Как устроен Avanpost DS

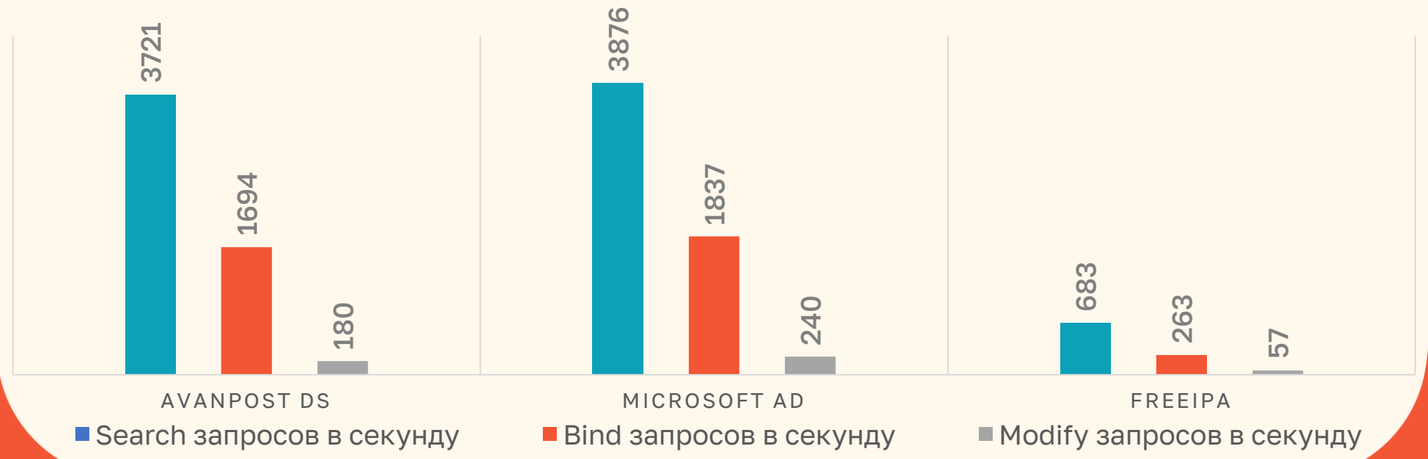


Нагрузочное тестирование

При **нагрузочном тестировании** наша платформа-ядро показала на порядок **большую производительность**, в сравнении с FreeIPA и унаследованными от нее решениями.

В ходе нагрузочного тестирования контроллер домена Avanpost DS показывал стабильную работу при одновременной обработке более **100 000 запросов** (50 000 на один контроллер домена).

РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО НТ



Сравнительное нагрузочное тестирование проводилось на стенде с 3 500 000 объектов, из них:

- 600 000 пользователей
- 300 000 групп;
- 1 000 000 прочих объектов (учетных записей хостов и служб);
- 1 600 000 ключей Kerberos

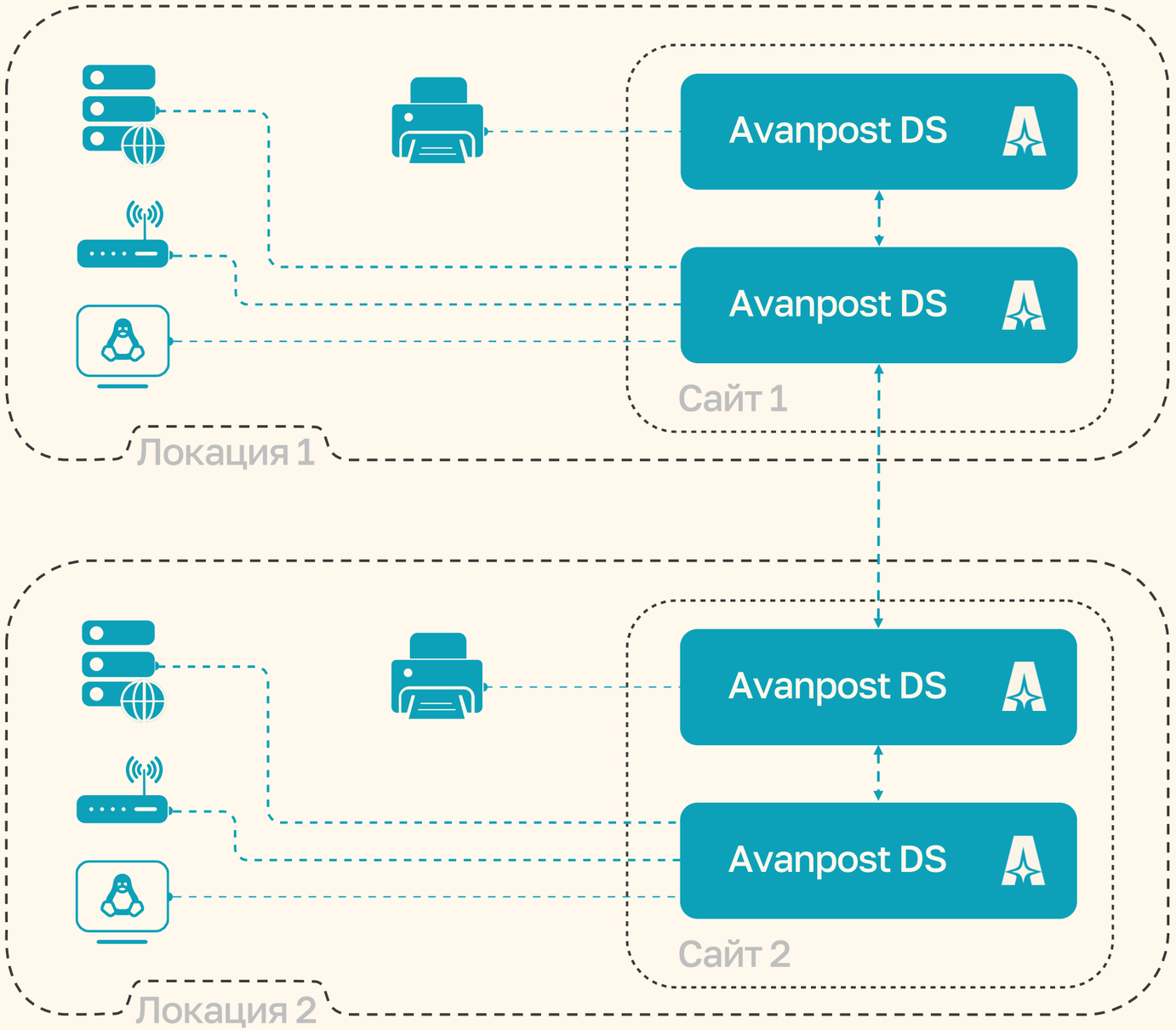
Использование в георасределенных инфраструктурах

AVANPOST

Avanpost Directory Services

Обеспечивает:

- Мультимастер репликацию
  - Автоматическое построение топологии в пределах сайта
  - Гибко настраиваемую топологию межсайтовой репликации
  - Репликацию по уведомлению (Notify-Pull) и по расписанию
- Структуру сайтов
  - Контроль межсайтовой репликации и использования WAN линков
  - Локализацию сетевых служб - привязку доменных клиентов к контроллерам домена сайта на основе подсетей
- Катастрофоустойчивость
  - Все контроллеры домена Avanpost DS равноправны и имеют полную копию каталога
  - Каждый контроллер домена имеет весь необходимый набор сервисов для обслуживания доменных клиентов



Групповые политики

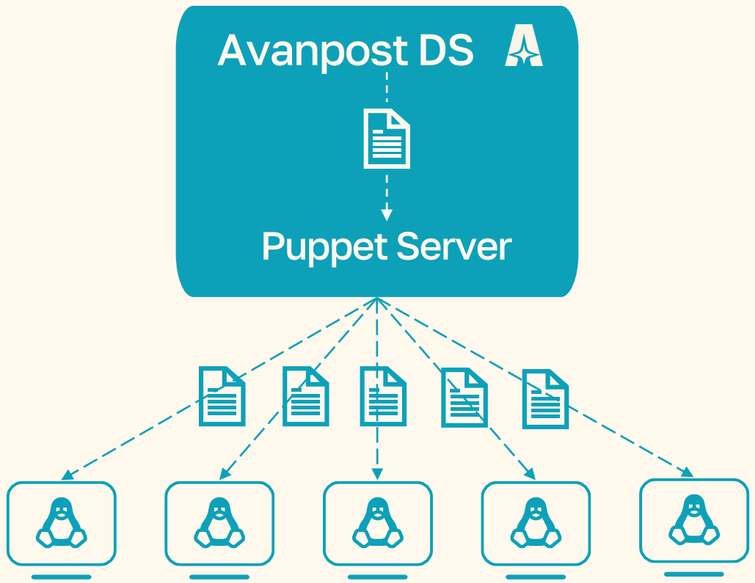
AVANPOST

Avanpost Directory Services

Реализует функционал групповых политик посредством интеграции с системой управления конфигурациями (Puppet)

Avanpost DS обеспечивает привязку политик к подразделениям и передает инструкции по применению конфигураций в Puppet.

Применение политик обеспечивается клиентом системы управления конфигурацией



Базовый набор политик включает в себя:

- Парольные политики
- Управление доступом к USB-устройствам и съемным носителям
- Подключение сетевых дисков и перенаправление папок
- Настройки безопасности ОС
- Выполнение сценариев
- Настройка доступа к приложениям и системным командам
- Централизованная установка пакетов
- Настройка сетевых параметров
- Настройка принтеров и других устройств
- Управление настройками электропитания
- Управление обновлением и репозиториями пакетов

Возможность расширения политик, через загрузку собственных шаблонов конфигурации

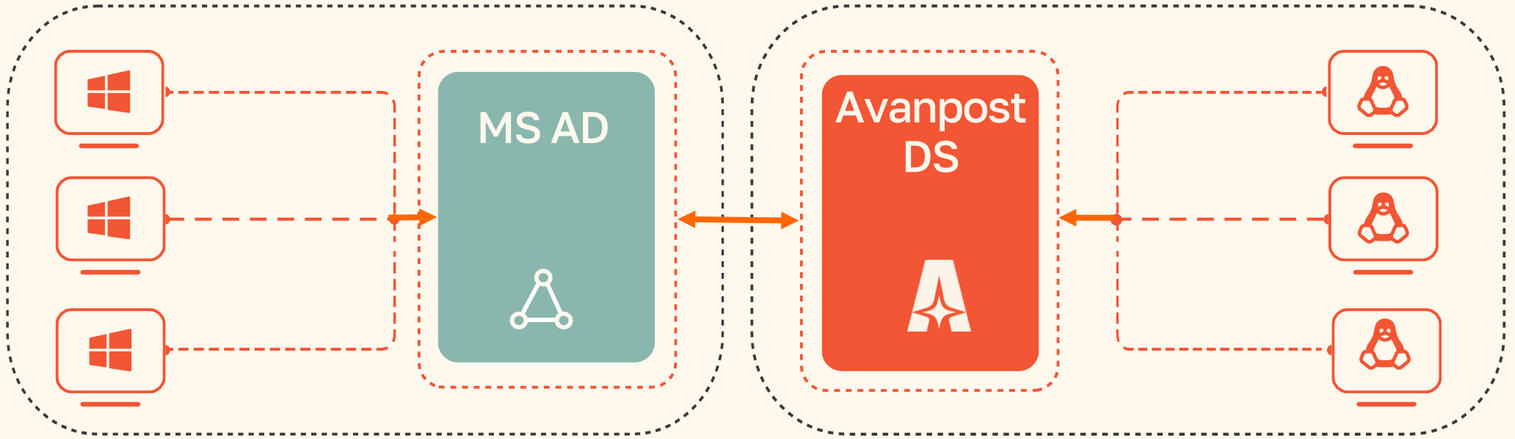
Использование в гибридных и переходных инфраструктурах

Двусторонние доверительные отношения

позволят осуществить плавный переход
без прерывания обслуживания

Переход от MS-инфраструктуры к импортонезависимой

в организациях будет осуществляться постепенно,
путем переноса рабочих станций,
сервисов и приложений в новую инфраструктуру,
создаваемую параллельно с имеющейся.

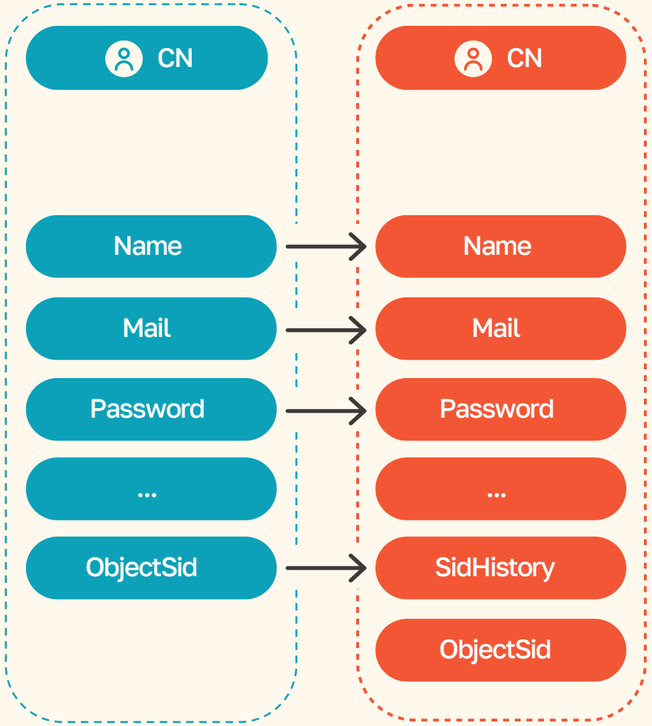


Доступ к ресурсам в период существования

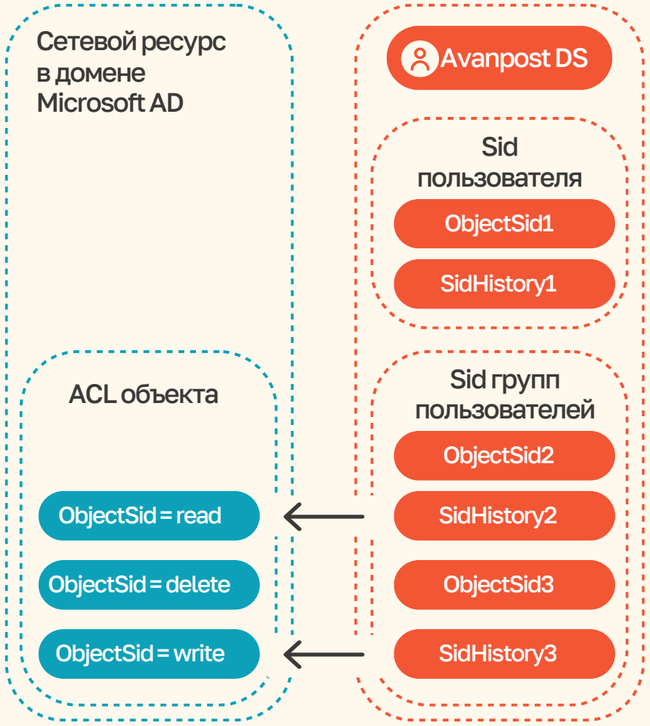
Реализация глобального каталога

В Avanpost DS позволит сохранить доступ пользователей прошедших миграцию к ресурсам в домене Windows за счет реализации совместимой схемы Microsoft AD.

В то время как доверительные отношения обеспечивают прозрачную аутентификацию, поддержка атрибутов **ObjectSID** и **SIDHistory** обеспечивает прозрачную авторизацию для пользователей с сохранением всех уровней доступа.



При миграции пользователя в Avanpost DS генерируется новый идентификатор, а старый SID копируется как значение атрибута SidHistory.



При доступе к ресурсам в домене Microsoft AD авторизация происходит с использованием атрибута SidHistory.

Продуктовый портфель

AVANPOST

AVANPOST DS
DIRECTORY SERVICE

Общая информационная инфраструктура для управления и систематизации ресурсов: тома, папки, файлы, принтеры, пользователи, группы, устройства, телефонные номера и др. объекты.

AVANPOST IDM
IDENTITY MANAGEMENT

Система управления учетными записями и доступом к корпоративным ресурсам предприятия

AVANPOST PAM
PRIVILEGED ACCESS MANAGEMENT

Система управления доступом администраторов к серверам и сетевому оборудованию

AVANPOST FAM
FEDERATED ACCESS MANAGER

Современный центр управления многофакторной аутентификацией в корпоративных приложениях с поддержкой федерации удостоверений

AVANPOST PKI
PUBLIC KEY INFRASTRUCTURE

Система управления всеми элементами инфраструктуры открытых ключей из единого центра

MULTI-FACTOR AUTHENTICATION (MFA)

SINGLE-SIGN-ON (SSO)

WEB SSO STATE

WEB SSO - CIAN

Облачная версия продукта в рамках базового сервиса ГосТеха

Облачная версия продукта

Мобильное приложение

Владелец продукта DS

Дмитрий
Закорючкин

dzakoryuchkin@avanpost.ru

Подпишитесь на наш ТГ канал

@AVANPOST_IDM

На текущий момент Avanpost Directory Service

- Внесен в реестр отечественного ПО в 2022 г.
- Сертифицируется по требованиям ФСТЭК
- Сертификат АМ Test Lab по результатам независимого тестирования