Avanpost Directory Services

Полностью российская служба каталогов

IDM

Управление жизненным циклом учетных записей

Управление доступом

Централизованный аудит и контроль соответствия

Сервис самообслуживания пользователей

Управление паролями

IDM

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

FAM

Система единой аутентификации сотрудников в корпоративные ресурсы организации

PKI

Система управления всеми элементами инфраструктуры открытых ключей из единого центра

WEB SSO

Система единой аутентификации клиентов в порталы и бизнес-приложения

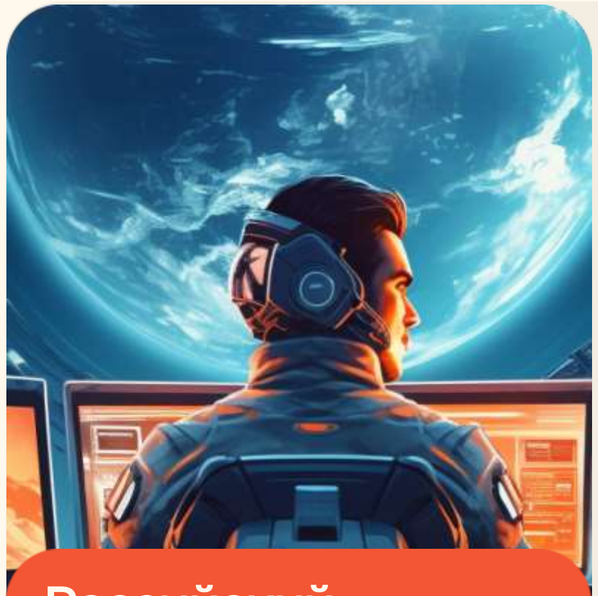
Управление доступом

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

AVANPOST

Разработчик систем аутентификации и управления доступом к информационным ресурсам предприятия

Технологические преимущества



Российский вендор новатор в области безопасности идентификационных данных

Развивает свою экспертизу с 2007 года.

Экспертиза команды и опыт сотен успешных внедрений позволяет решать задачи любой сложности независимо от отрасли и используемых предприятием систем.

Продукты Avanpost включены в реестр отечественного ПО, удовлетворяют требованиям безопасности информации и сертифицированы ФСТЭК, применимы в ГИС, ИСПДн, КИИ, КВО.

Современный технологический стек

Разработка ведется с помощью двух современных технологических стеков, в зависимости отсложности бизнес-логики и требований к производительности: Postgre SQL/.Net Core/EF/Akka.Net/Angular – для продуктов со сложной бизнес-логикой; Go/BadgerDB/NATS/Vue.js – для высокопроизводительных сервисов. Обеспечено соответствие стандартам: XACML, NIST RBAC, SCIM, OpenID Connect, SAML, FIDO U2F.

01

Соответствие требованиям безопасной разработки

При разработке продуктов используются стандарты SDL (Security Development Lifecycle), что закладывает необходимый уровень безопасности в основу разрабатываемой системы.

02

Простота масштабируемости

Используются технологии автоматического масштабирования ресурсов (Autoscaling), что позволяет сохранять стабильность работы при росте нагрузки и высвобождать неиспользуемые ресурсы при ее снижении.

03

AVANPOST

Технологические преимущества

Отказоустойчивость при высоких нагрузках

При разработке продуктов используются стандарты SDL (Security Development Lifecycle), что закладывает необходимый уровень безопасности в основу разрабатываемой системы.

04

Современный технологический стек

Поддерживаемые технологии:
- полный набор используемых в России дистрибутивов Linux;
- Windows;
- 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

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 всеми элементами инфраструктуры открытых ключей из единого центра

Облачная версия продукта в рамках базового сервиса ГосТеха

Облачная версия продукта

Мобильное приложение

AVANPOST FAM
FEDERATED ACCESS MANAGER

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

MULTI-FACTOR AUTHENTICATION (MFA+)

SINGLE-SIGN-ON (SSO)

WEB SSO STATE

WEB SSO - CIAM

AVANPOST PKI
PUBLIC KEY INFRASTRUCTURE

Система управления всеми элементами инфраструктуры открытых ключей из единого центра

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

Текущий функционал Avanpost DS

AVANPOST

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 основной функционал доменного клиента

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

02

Журнал безопасности

- Учет событий привязки LDAP
- Учет событий выдачи ключей Kerberos

03

AVANPOST

Реализован функционал Kerberos v5 KDC

- AS и TGS обмен ключами
- Сквозная аутентификация

04

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

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

05

Реализован функционал репликации

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

06

Реализована ролевая модель доступа к объектам службы каталогов

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

07

Многофакторная проверка подлинности, интеграция с Avanpost FAM

(Federated Access Management)

08

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

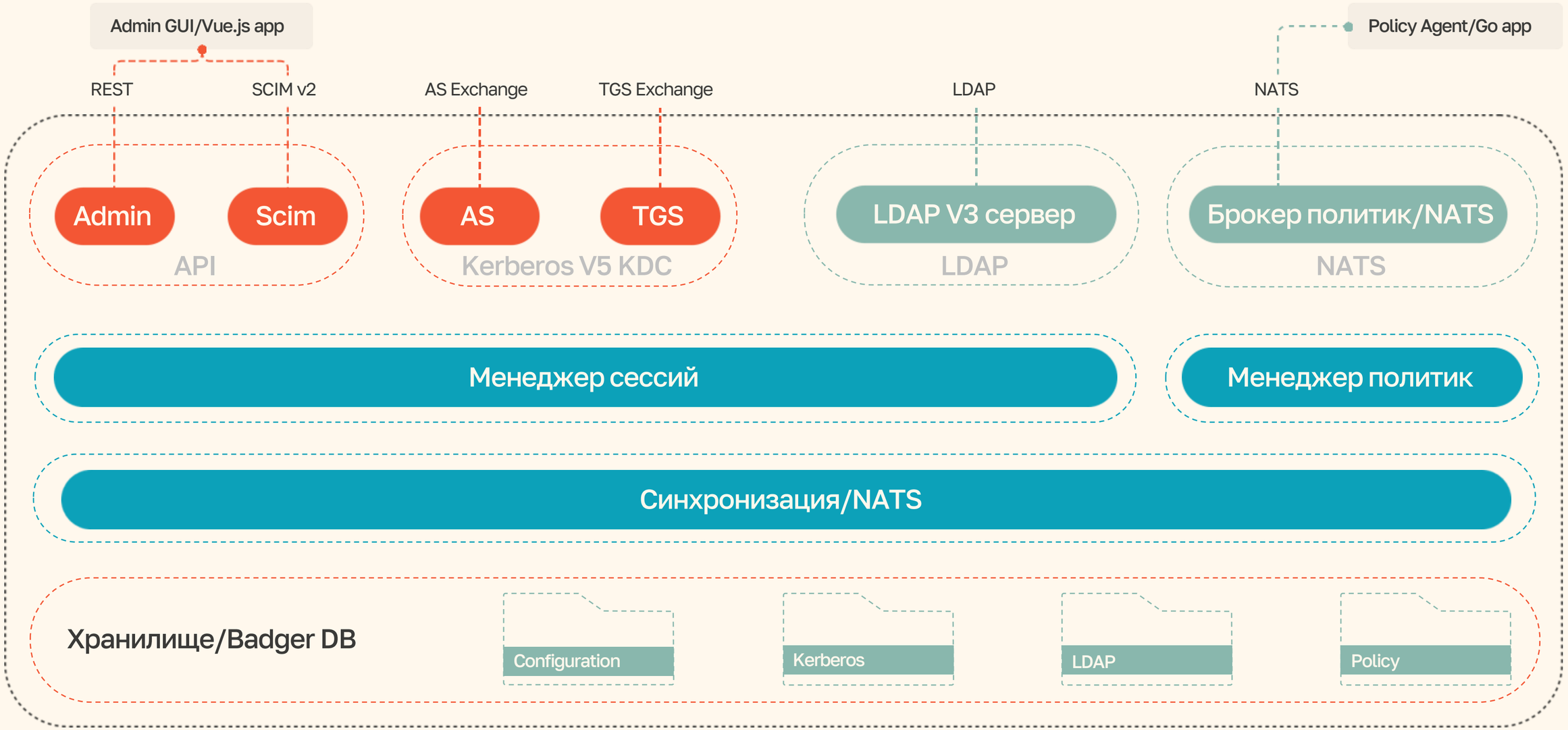
Дополнительный функционал

Интеграции с инфраструктурными сервисами	• Система управления конфигурацией • Служба DNS • Служба NTP	Сервисы, необходимые для функционирования домена с возможностью выбора решения в зависимости от потребностей заказчика
Корпоративный удостоверяющий центр		Замена Active Directory Certificate Services
Поддержка современных протоколов аутентификации		Посредством интеграции с Avanpost FAM
Доменный клиент		Поддержка всех отечественных дистрибутивов Linux

Не входящие в состав продукта функции

Поддержка Windows клиентов	Не планируется поддержка клиентов Windows, так как это потребует реализации проприетарных протоколов MS
Интеграция со службой установки ОС по сети PXE	Задачи установки ОС по сети решаются собственным функционалом отечественных ОС
Интеграция со службой DHCP	Служба DHCP присутствует в составе всех российских дистрибутивов Linux и не требует интеграции со службой каталогов
Служба удаленного помощника Служба инвентаризация ПК	Функционал инвентаризации и удаленного помощника относится к другому классу ПО и решается отдельными продуктами российских вендоров

Как устроен Avanpost DS



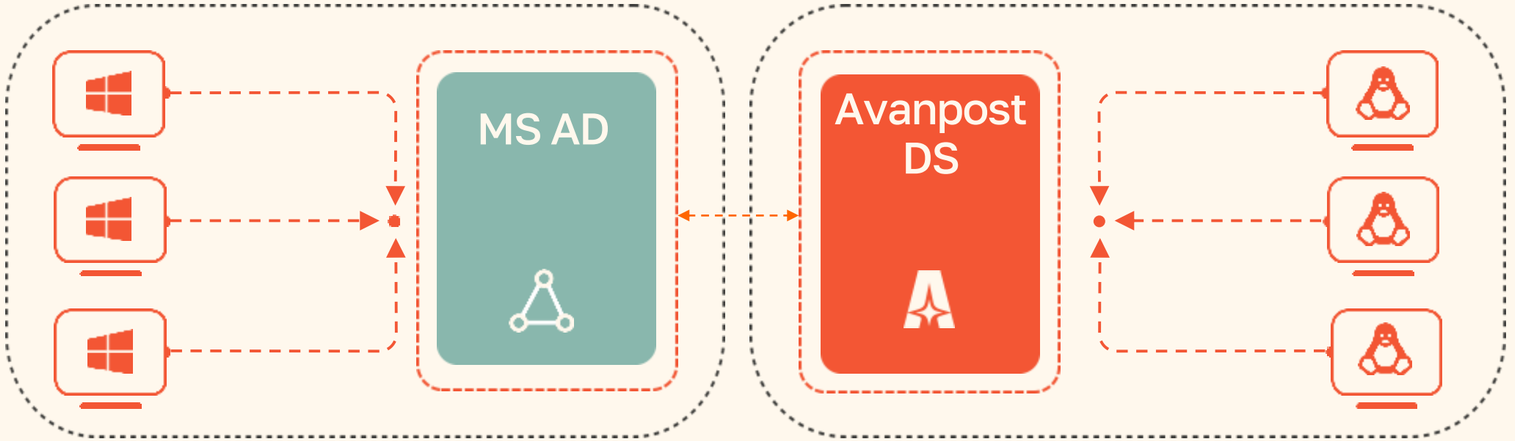
Использование в гибридных и переходных инфраструктурах

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.

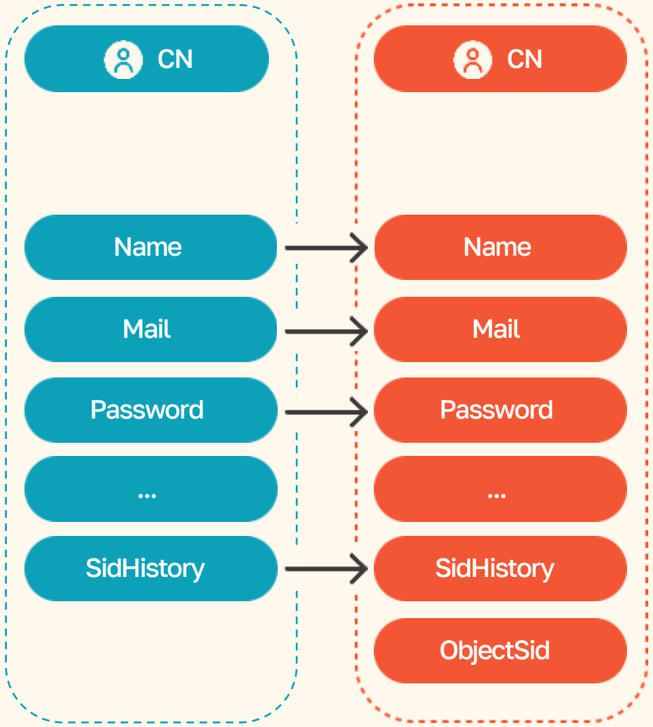


Доступ к ресурсам в период существования

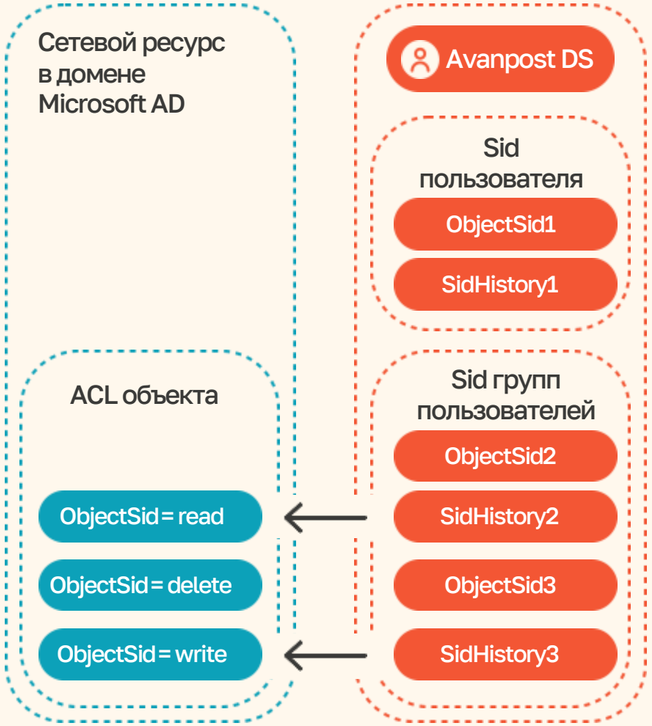
Реализация глобального каталога

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.



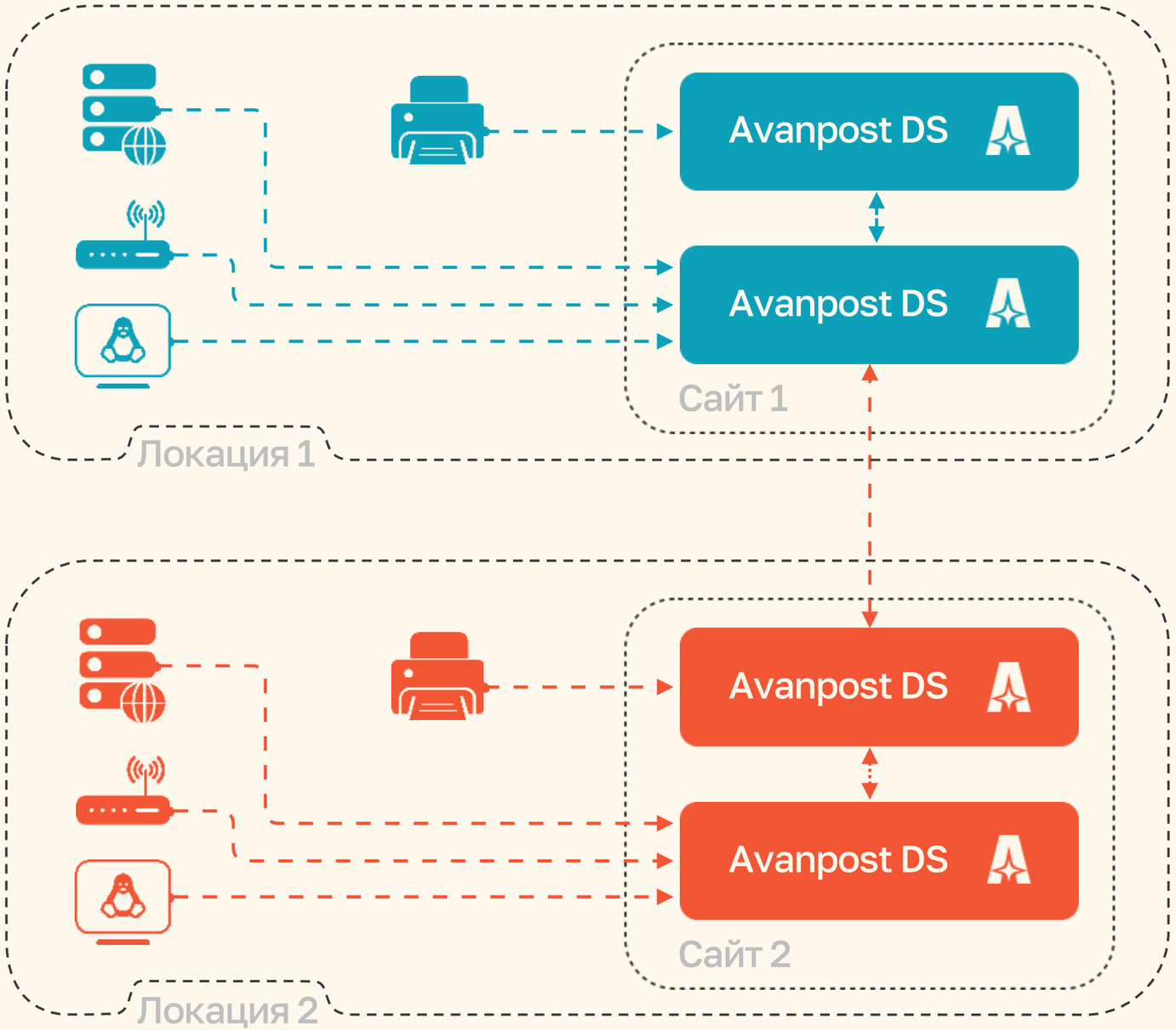
При миграции пользователя в Avanpost DS генерируется новый идентификатор, а старый SID копируется как значение атрибута SidHistory.



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

Использование в географически распределенных инфраструктурах

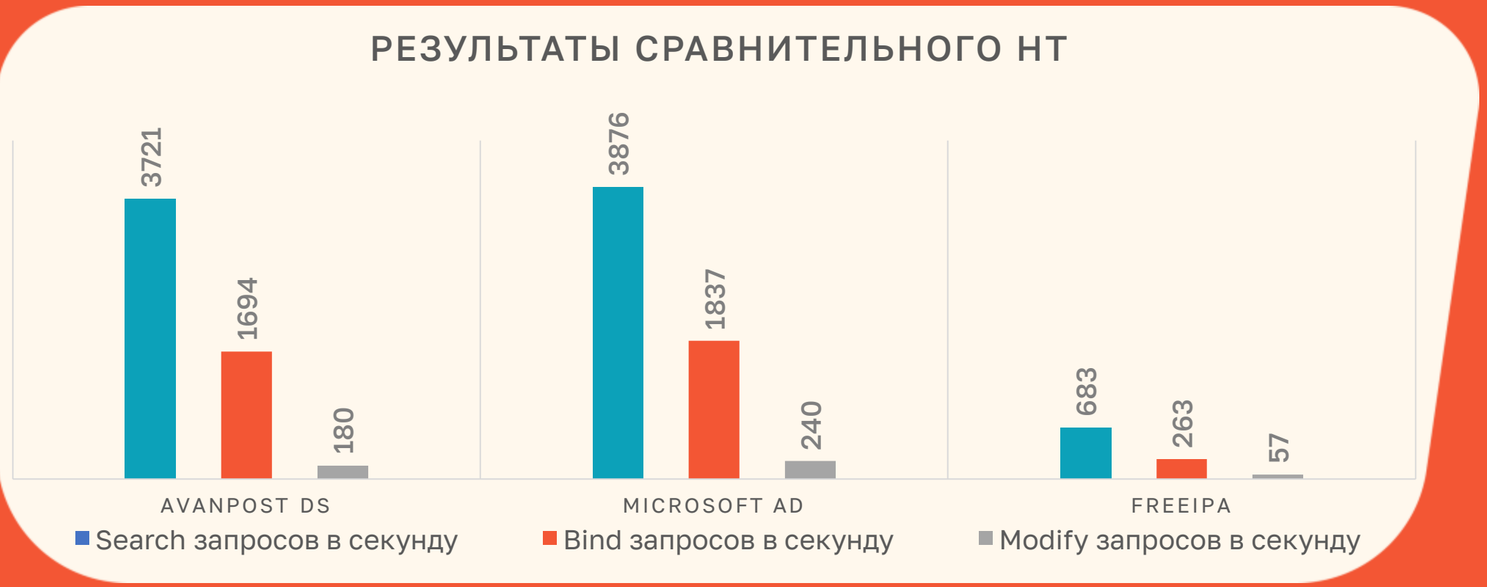
Avanpost Directory Services поддерживает репликацию объектов каталога и сессий, что позволяет использовать его для централизованного управления доступом и аутентификации в географически распределенной инфраструктуре.



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).



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

Roadmap Avanpost DS

на оставшееся полугодие 2023 год

Q3 → Интеграция с DNS сервером, поддержка хранения зон DNS в каталоге, динамические обновления

Q3 → Ролевая модель доступа к объектам каталога, делегирование, гранулярный контроль доступа

Q3 → Управляемая межсайтовая топология репликации

Q4 → Интеграция с сервером мониторинга, витрины мониторинга, оповещения о состоянии системы (Zabbix, Prometheus)

Q4 → Расширение функционала журналирования: сбор дополнительных событий

Q4 → Интеграция с сервером журналирования, передача журналов в SIEM системы

Roadmap Avanpost DS

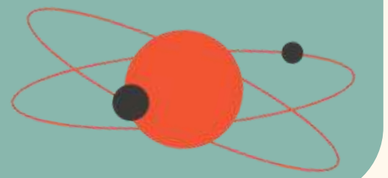
на первое полугодие 2024 год

Q1 → Групповые политики, стандартные шаблоны и возможность добавления параметров

Q1 → Функционал доверительных отношений между доменами - Реализация двусторонних доверительных отношений с MS AD

Q1 → Автоматизация миграции данных из MS AD, миграция паролей из MS AD

Q1 → Функционал доверительных отношений между доменами. Доверительные отношения между доменами ADS



Q2 → Поддержка мультидоменной структуры леса доменов

Q2 → Поддержка фреймворка SASL

Q2 → Открытое API системы по стандарту SCIM 2.0

Q2 → Корпоративный удостоверяющий центр, шаблоны сертификатов, политики выдачи сертификатов

Q2 → Корзина службы каталогов

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

AVANPOST

Существенные сложности и задержку сроков при использовании решений на базе FreeIPA могут вызвать:

01 Отсутствие выбора компонентов окружения: серверов DNS, систем управления конфигурациями в зависимости от потребностей клиента и масштаба внедрения

02 Ограничения системы управления конфигурацией, не поддерживающей интеграцию со сторонними системами

03 Ограничения по построению гибкой топологии репликации без лимита по количеству контроллеров домена и связей репликации

04 Ограничения по количеству клиентов поддерживаемых контроллером доменов, отсутствие поддержки облачной инфраструктуры

05 Прочие ограничения вызванные отсутствием возможности быстрой модификации продукта

За счет реализации механизма двухсторонних доверительных отношений,

Avanpost DS позволит плавно провести миграцию с Microsoft AD, без прерывания обслуживания в переходный период (доступ к КИС с рабочих станций Windows, доступ к не прошедшим миграцию КИС с рабочих станций под управлением любых отечественных дистрибутивов Linux).

Директор по разработке

Александр Махновский

amahnovsky@avanpost.ru

Владелец продукта DS

Дмитрий Закорючкин

dzakoryuchkin@avanpost.ru

+7 (903) 523-07-85

На текущий момент Avanpost Directory Service

- Внесен в реестр отечественного ПО в 2022 г.
- Сертифицируется по требованиям ФСТЭК, получение сертификата ожидается во 2-м квартале 2024 г.