Описание функциональных характеристик

Продукта Platform V IAM SE (IAM)

ОГЛАВЛЕНИЕ

Описание программного решения

Назначение и задачи программного решения

Platform V IAM SE содержит набор инструментов для управления доступом к информационным ресурсам. Данные инструменты необходимы для аутентификации и авторизации пользователей. Они обеспечивают удобство подключения защищаемых приложений к провайдеру идентификации, поддерживают реализацию множества различных сценариев работы в соответствии с отраслевыми стандартами, такими как OpenID Connect, Oauth 2.0, SCIM 2.0.

Platform V IAM SE используется во время взаимодействия пользователей с бизнес-приложениями (runtime). Для обеспечения выполнения функций по администрированию учетных записей, управлению их полным жизненным циклом (admin time) необходимо использовать дополнительные к Platform V IAM SE инструменты Identity Management / Identity Governance.

Основные термины и определения

Термин	Определение
id-token	Токен в формате JWTs, который получен RP от OP в результате аутентификации пользователя платформы по OIDC, представляющий из себя защищенное аутентификационное решение со сроком действия и возможностью проверки токена на подлинность по цифровой подписи.
OIDC	**O**pen **ID** **C**onnect v1.
OP	**O**pen ID **P**rovider, сервер авторизации OAuth 2.0, который способен аутентифицировать конечного пользователя и предоставлять проверяющей стороне утверждения/данные о событии аутентификации и о конечном пользователе.
RP	**R**elaying **P**arty, клиентское приложение OAuth 2.0, требующее проверки подлинности конечного пользователя и проверки утверждений/данных от поставщика OpenID (OP).
JWTs	Подписанный токен, с данными (payload) в формате JSON (Json Web Token signed). Формат по RFC 7519.
ФП	Функциональная подсистема Platform V.
StandIn	Функциональное решение переключения контуров при аварии.
АС	(Автоматизированная система) Комплекс сервисов и средств автоматизации бизнес-процессов.
TLS	(Transport Socket Layer) Протокол защиты транспортного уровня, обеспечивающий защищённую передачу данных между узлами в сети Интернет, использует асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Структура программного решения

Продукт состоит из трех сервисов (компонентов), которые могут быть интегрированы между собой. Каждый из данных компонентов предназначен для выполнения отдельных функций. В рамках реализуемых заказчиком сценариев компоненты могут использоваться по отдельности или совместно.

Название компонента	Описание
KeyCloak.SE (KCSE)	Сервис, основанный на Open Source версии Keycloak, позволяющий реализовать провайдер идентификации пользователей (Identity Provider).
Объединённый сервис авторизации (OCA) (AUTZ)	Сервис позволяет реализовать централизованную точку (Policy Decision Point (PDP)) принятия решений о возможности доступа на основе политик, формируемых по ABAC модели.
IAM Proxy (AUTH)	Реверсивный Proxy-сервер, располагаемый между пользователями и защищаемыми приложениями, который интегрируется с провайдерами идентификации / авторизации и позволяет упростить реализацию аутентификации / авторизации для приложений.

KeyCloak.SE

Компонент «KeyCloak.SE» продукта «Platform V IAM SE» (далее - KeyCloak.SE) выполняет следующие основные функции:

- Аутентификация пользователя при доступе к приложению. В рамках функции аутентификации возможно:
  - Настраивать собственные сценарии (flow) аутентификации;
  - Использовать функции одноразовых паролей OTP: TOTP/HOTP;
  - Реализовать аутентификацию по X.509 сертификатам;
  - Использовать поддержку WebAuthn;
  - Настраивать парольные политики.
- Авторизация пользователя на выполнение операции / действия в приложении. В KeyCloak.SE реализованы базовые функции авторизации. Более расширенная функциональность авторизации возможна при использовании компонента OCA. В рамках функций авторизации в KeyCloak.SE возможно:
  - Реализовать ведение каталога ресурсных серверов / ресурсов / полномочий;
  - Настроить политики авторизации: User-Based, Role/Group-Based, JavaScript-Based, Time-Based, Client-Base, Aggregated;
  - Включать авторизационную информацию в JWT-токены.
- Поддержка сценариев в рамках отраслевых проколов: OpenID Connect, Oauth 2.0, SAML 2.0, User Managed Access (UMA).
- Хранение данных, включая данные аутентификационного профиля пользователя, аутентификационного профиля приложения (client), авторизационных данных. В рамках хранения данных обеспечивается выполнения следующих функций:
  - Персистентность данных в СУБД / LDAP каталоге;
  - Поддержка внешних хранилищ данных (federation);
  - Кэширование данных;
  - Identity Brokering;
  - Мультитенантность (realms).

- Функции самообслуживания пользователей (Self-service) включая функции:
  - Регистрации в Identity Provider;
  - Управление согласиями;
  - Личный кабинет (account console);
  - Account Linking.
- Функции администрирования, включая:
  - Admin REST API;
  - Административная консоль;
  - Управление учетными записями пользователей / сессиями;
  - Export / Import;
  - События / аудит.
- Функции управления аутентификационными профилями и дополнительные функции для защищаемых приложений (client), включая:
  - Регистрация приложений: OIDC. Dynamyc client registration, SAML v2 Entity Descriptors;
  - Политики регистрации, client registration cli;
  - Token Exchange.

Объединённый сервис авторизации (OCA)

Компонент «Объединённый сервис авторизации (OCA)» продукта «Platform V IAM SE» (далее – OCA) выполняет следующие основные функции:

- Механизмы Role-Based Access Control (RBAC) авторизации, включая:
  - RBAC с динамическим расчётом групп на основании атрибутов сеанса (например, канал);
  - Центральное хранилище ролевых моделей (XML в СУБД);
  - Клиентские библиотеки (java) с кешированием в распределённом сессионном хранилище;
  - UI, рабочее место администратора.
- Механизмы Attribute-Based Access Control (ABAC) авторизации, включая:
  - Поддержка языка политик - XACML (eXtensible Access Control Markup Language);
  - Формирование политик авторизации (конвертирование) из DSL.
- Функции принятия авторизационного решения - Policy Decision Point (PDP), включая:
  - Централизованный API: XAML JSON Profile;
  - Принятие авторизационного решения в клиентской библиотеке.
- Функции централизованного хранения / динамического получения из внешних источников атрибутов пользователя с привязкой к пользователям (Policy Information Point), включая:
  - REST API для получения атрибутов;
  - Административный UI для создания атрибутов.

IAM Proxy

Компонент «IAM Proxy» продукта «Platform V IAM SE» (далее – IAM Proxy) выполняет следующие основные функции:

- Аутентификация пользователя при доступе к приложению посредством какого-либо провайдера аутентификации (например KeyCloak.SE). В рамках функций аутентификации IAM Proxy поддерживает:
  - Взаимодействие с внешним провайдером аутентификации по OpenID Connect;
  - Поддержка custom IdP;

    - Передача проверенной информации о пользователе внутренним приложениям в удобном виде: JWT, http headers, custom;
- Функции авторизации, включая:
    - Авторизация доступа к защищаемым приложениям по ролям: дает возможность ограничить обращение к бэковым приложениям на основе ролей из токена (по маске роли, регулярное выражение);
    - Дает возможность на прокси ограничить обращение к серверам-приложений на основе обращения к внешнему серверу авторизации (дополнительный слой авторизации на основе URL(RBAC) и атрибутов запросов (ABAC)), что позволяет вынести функции безопасности на отдельный компонент(прокси) и упростить авторизацию на приложении;
    - Кэширование авторизационных политик. Возможность принятия локальных авторизационных решений.
- Проксирование, поддержка HTTP, включая:
    - Поддержка проксирования http 1/1.1/2, ws, sse - Предоставляет возможность заказчику использовать в своих web-приложениях технологии WebSocket и Server-send events;
    - Балансировка - Round Robin, Hash, IP Hash, Least Connections;
    - Mtls - Терминирование mtls, mtls с бэковыми сервисами;
    - Поддержка sticky-session (по комплексным критериям);
    - Ведение сессии прокси - позволяет ограничить время жизни по неактивности, абсолютному времени, выполнить привязку по ip (или любому другому критерию).

Функции безопасности

IAM Proxy выполняет следующие функции безопасности:

- идентификация и аутентификация пользователей;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) ком-прометации средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- реализация необходимых методов (ролевой) и правил разграничения доступа;
- ограничение неуспешных попыток входа в информационную систему;
- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

Описание функциональных характеристик компонента IAM Proxy (AUTH)

Компонент IAM Proxy продукта Platform V IAM SE (далее – «IAM Proxy») - это реверсивный Proxy-сервер, который располагается между пользователем и защищаемым приложениями, который интегрируется с провайдерами идентификации / авторизации и позволяет упростить реализацию аутентификации / авторизации для приложений

Основные функции

- Аутентификация пользователя при доступе к приложению посредством какого-либо провайдера аутентификации (например компонента KeyCloak.SE продукта Platform V IAM SE). В рамках функций аутентификации IAM Proxy поддерживает:
  - Взаимодействие с внешним провайдером аутентификации по OpenID Connect;
  - Поддержка custom IdP;
  - Передача проверенной информации о пользователе внутренним приложениям в удобном виде: JWT, http headers, custom;

- Функции авторизации, включая:
  - Авторизация доступа к защищаемым приложениям по ролям: дает возможность ограничить обращение к бэковым приложениям на основе ролей из токена (по маске роли, регулярное выражение);
  - Дает возможность на прокси ограничить обращение к серверам-приложений на основе обращения к внешнему серверу авторизации (дополнительный слой авторизации на основе URL (RBAC) и атрибутов запросов (ABAC)), что позволяет вынести функции безопасности на отдельный компонент(прокси) и упростить авторизацию на приложении;
  - Кэширование авторизационных политик. Возможность принятия локальных авторизационных решений.

- Проксирование, поддержка HTTP, включая:
  - Поддержка проксирования http 1/1.1/2, ws, sse - Предоставляет возможность заказчику использовать в своих web-приложениях технологии WebSocket и Server-send events;
  - Балансировка - Round Robin, Hash, IP Hash, Least Connections;
  - Mtls - Терминирование mtls, mtls с бэковыми сервисами;
  - Поддержка sticky-session (по комплексным критериям);
  - Ведение сессии прокси - позволяет ограничить время жизни по неактивности, абсолютному времени, выполнить привязку по ip (или любому другому критерию).

Описание функциональных характеристик компонента Объединенный сервис авторизации (OCA) (AUTZ)

Компонент Объединенный сервис авторизации (OCA) продукта Platform V IAM SE (далее – OCA) – предназначен для авторизации доступа пользователей на основе: проверки ролей пользователей, наличия прав доступа и анализа правил атрибутов объектов и субъектов доступа.

Сервис обеспечивает возможность формирования политик авторизации на основе атрибутов и организует процедуру управления ролевыми моделями доступа сервисов Platform V, атрибутами объектов и субъектов доступа.

Сервис помогает защитить Platform V от несанкционированных операций злоумышленников и тем самым позволяет сохранить конфиденциальность и целостность информации.

Компонент OCA включает в себя следующие компоненты:

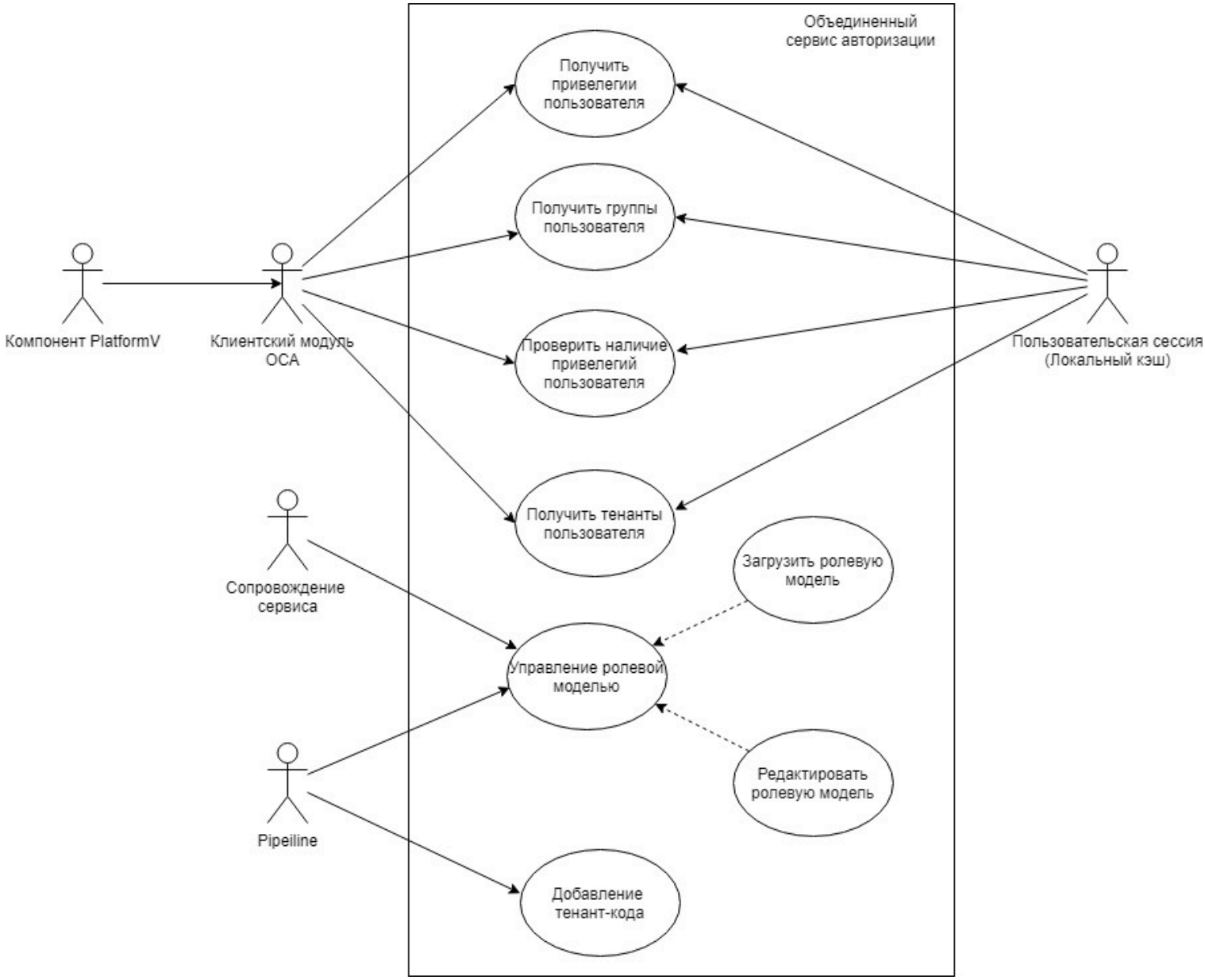
- Клиентский модуль – предоставление публичного Java API компонента;
- Сервис авторизации – предназначен для расчета привилегий пользователя;
- Загрузчик ролевой модели – предназначен для обновления ролевой модели;
- APM сервиса авторизации – предназначен для предоставления доступа к ролевой модели потребителей.

Основные функции

Основные функции реализованы через интерфейсы компонента:

- Графический интерфейс компонента предназначен для загрузки и управления ролевых моделей;
- API сервиса расчета привилегий предназначен для расчета привилегий пользователя на основе двух механизмов авторизации:
    - Role-Based Access Control (RBAC) – контроль доступа на основа ролевой модели;
    - Attribute-Based Access Control (ABAC) – контроль доступа на основе атрибутов.

- Pipeline API — предназначен для обновления ролевой модели;
- SOAP API - предназначен для управления учетными записями и ролей.



Сценарии использования

Основные элементы диаграммы:

- Компонент Platform V - любой потребитель компонента OCA;
- Клиентский модуль компонента OCA - Spring Boot Starter для обращений в серверную часть компонента OCA;
- Сопровождение сервиса - пользователь или система, оказывающие услуги по администрированию и сопровождению сервиса;
- Pipeline - это последовательность стадий (они же stages), внутри которых расположены задачи (инструкции) для загрузки ролевой модели;
- Пользовательская сессия - это локальный кэш для оперативных и справочно-конфигурационных данных в привязке к клиенту.

Получить привилегии

Главный сценарий

1. Компонент Platform V обращается к клиентскому модулю OCA.
2. Клиентский модуль OCA проверяет наличие привилегий пользователя в пользовательской сессии локальный кэш).
3. Если в пользовательской сессии нет привилегий, клиентский модуль OCA передает пользовательские атрибуты в компоненте OCA.
4. OCA возвращает список привилегий.
5. Клиентский модуль OCA записывает список привилегий пользователя в пользовательскую сессию (локальный кэш).

Исключительные сценарии:

Ошибка получения пользовательских атрибутов заключается в том, что Компонент Platform V делает запись в журналирование об ошибке получения пользовательских атрибутов.

Получить группы пользователя

Главный сценарий

1. Компонент Platform V обращается к клиентскому модулю OCA.
2. Клиентский модуль OCA проверяет наличие групп пользователя в пользовательской сессии (локальный кэш).
3. Если в пользовательской сессии нет групп, клиентский модуль OCA передает пользовательские атрибуты в компоненте OCA.
4. OCA возвращает список групп.
5. Клиентский модуль OCA записывает список групп в пользовательскую сессию.

Исключительные сценарии

Ошибка получения пользовательских атрибутов заключается в том, что Компонент Platform V делает запись в журналирование об ошибке получения пользовательских атрибутов.

Проверить наличие привилегии

Главный сценарий

1. Компонент Platform V обращается к клиентскому модулю OCA.
2. Клиентский модуль OCA проверяет наличие привилегий пользователя в пользовательской сессии (локальный кэш).
3. Если в пользовательской сессии нет привилегий, клиентский модуль OCA передает пользовательские атрибуты в OCA.
4. OCA возвращает список привилегий.
5. Клиентский модуль OCA записывает список привилегий пользователя в пользовательскую сессию.
6. Клиентский модуль проверяет наличие запрашиваемой привилегии в списке привилегий.

Исключительные сценарии

Ошибка получения пользовательских атрибутов заключается в том, что Компонент Platform V делает запись в журналирование об ошибке получения пользовательских атрибутов.

Получить тенанты пользователя

Главный сценарий

1. Компонент Platform V обращается к клиентскому модулю OCA.
2. Клиентский модуль OCA проверяет наличие тенант-кодов в пользовательской сессии (локальный кэш).
3. Если в пользовательской сессии нет тенант-кодов, клиентский модуль OCA передает пользовательские атрибуты в OCA.
4. OCA возвращает список тенант-кодов пользователя.
5. Клиентский модуль OCA записывает список тенант-кодов пользователь в пользовательскую сессию.

Исключительные сценарии

Ошибка получения пользовательских атрибутов заключается в том, что Компонент Platform V делает запись в журналирование об ошибке получения пользовательских атрибутов.

Управление ролевой модели

Главный сценарий

1. Сотрудник сопровождения заходит в АРМ ОСА.
2. Сотрудник сопровождения выбирает нужную вкладку в АРМ ОСА.
3. Сотрудник сопровождения редактирует ролевую модель.
4. Изменения ролевой модели применяются.

Исключительные сценарии

Ошибка редактирования ролевой модели заключается в том, что сотрудник сопровождения получает в АРМ сообщение об ошибке сохранения ролевой модели.

Управление ролевой модели

Главный сценарий

1. Pipeline загружает файл с ролевой моделью в импортер ОСА.
2. Импортер сервиса авторизации проверяет загружаемую ролевую модель.
3. Импортер ОСА сохраняет загружаемую ролевую модель.

Исключительные сценарии

Ошибка редактирования ролевой модели заключается в том, что сервис авторизации выдает ошибку о сохранении ролевой модели.

Добавление тенант-кода

Главный сценарий

1. Pipeline передает тенант-код в заголовке запроса при загрузке ролевой модели.
2. Импортер ОСА проверяет наличие тенант-кода в справочнике авторизации.
3. Импортер ОСА сохраняет новый тенант-код в справочнике авторизации.

Исключительные сценарии:

Исключительные сценарии отсутствуют

Описание функциональных характеристик компонента KeyCloak.SE

Компонент KeyCloak.SE продукта Platform V IAM SE - это сервис, основанный на Open Source версии Keycloak, позволяющий реализовать функции провайдера идентификации пользователей (Identity Provider).

Основные функции

- Аутентификация пользователя при доступе к приложению. В рамках функции аутентификации возможно:
  - Настраивать собственные сценарии (flow) аутентификации;
  - Использовать функции одноразовых паролей OTP: TOTP/HOTP;
  - Реализовать аутентификацию по X.509 сертификатам;
  - Использовать поддержку WebAuthn;
  - Настраивать парольные политики.
- Авторизация пользователя на выполнение операции / действия в приложении. В компоненте KeyCloak.SE продукта Platform V IAM SE реализованы базовые функции авторизации. Более расширенная функциональность авторизации возможна при использовании компонента Объединенный сервис авторизации (ОСА) продукта Platform V IAM SE. В рамках функций авторизации в компоненте KeyCloak.SE продукта Platform V IAM SE возможно:
  - Реализовать ведение каталога ресурсных серверов / ресурсов / полномочий;
  - Настроить политики авторизации: User-Based, Role/Group-Based, JavaScript-Based, Time-Based, Client-Base, Aggregated;
  - Включать авторизационную информацию в JWT-токены.
- Поддержка сценариев в рамках отраслевых проколов: OpenID Connect, Oauth 2.0, SAML 2.0, User Managed Access (UMA).
- Хранение данных, включая данные аутентификационного профиля пользователя, аутентификационного профиля приложения (client), авторизационных данных. В рамках хранения данных обеспечивается выполнения следующих функций:
  - Персистентность данных в СУБД / LDAP каталоге;
  - Поддержка внешних хранилищ данных (federation);
  - Кэширование данных;
  - Identity Brokering;
  - Мультитенантность (realms).
- Функции самообслуживания пользователей (Self-service) включая функции:
  - Регистрации в Identity Provider;
  - Управление согласиями;
  - Личный кабинет (account console);
  - Account Linking.
- Функции администрирования, включая:
  - Admin REST API;
  - Административная консоль;
  - Управление учетными записями пользователей / сессиями;
  - Export / Import;
  - События / аудит.

- Функции управления аутентификационными профилями и дополнительные функции для защищаемых приложений (client), включая:
    - Регистрация приложений: OIDC. Dynamyc client registration, SAML v2 Entity Descriptors;
    - Политики регистрации, client registration cli;
    - Token Exchange.