АО «СберТех» (является дочерним обществом ПАО Сбербанк)

117105, Москва, Новоданиловская наб., д. 10

Продукт Platform V IDM (IDM)

Компонент Platform V IDM (IDMX)

Описание функциональных характеристик

Дата	*Версия*	*Описание*
21.10.2022	*1.0*	*Версия продукта «Platform V IDM» впервые регистрируется в Реестре отечественного ПО*

Содержание

Термины и определения

Термин	Определение
IDM	Компонент IDMX продукта Platform V IDM. Система управления учетными записями и доступами
UI	User Interface. Графический интерфейс, через который пользователь взаимодействует с приложением
DataBase DB, БД	База данных
Система оркестрации контейнеризированных приложений	Kubernetes или OpenShift (опционально)
Docker images Docker-образ Образ	Исполняемый пакет, содержащий все необходимое для запуска приложения: код, среду выполнения, библиотеки, переменные окружения и файлы конфигурации
Registry Docker registry	Ресурс для хранения образов
Deploy	Установка/развертывание
Common репозиторий	Репозиторий с configmaps стендов
Configmap	Конфигурацинный файл
Namespace Пространство имен	Проектная область системы оркестрации контейнеризированных приложений
UI системы оркестрации контейнеризированных приложений	Интерфейс для управления компонентами системы оркестрации контейнеризированных приложений
Installer	Инструмент для автоматизированной установки. Продукт Platform V DevOps Tools, компонент Deploy tools (CDJE)
ISTIO	Настраиваемая сервисная сеть (service mesh) с открытым исходным кодом, служащая для взаимодействия, мониторинга и обеспечения безопасности контейнеров в кластере Kubernetes. Рекомендуется использовать сервис istio в составе продукта Platform V Synapse Service Mesh.
Платформа	Набор продуктов Platform V, правообладателем которых является АО «СберТех». Перечень таких продуктов обозначен в документации на конкретный Продукт.
Учетная карточка	Учетная запись пользователя в системе Platform V IDM
Учетная запись	Краткое название для учетной записи пользователя в какой-либо ИС, связанной с Platform V IDM

Термин	*Определение*
Юзер	*Учетная карточка пользователя как объект БД IDM, с которым проводятся операции*
Аккаунт	*Учетная запись пользователя в какой-либо ИС как объект IDM, с которым проводятся операции*
Ресурс	*Внешняя ИС, подключаемая к IDM для управления учетными записями*
ЛКМ	*Левая кнопка мыши*
ПКМ	*Правая кнопка мыши*
ПО	*Программное обеспечение*
ИС	*Информационная система*
IDE	*Integrated Development Environment, интегрированное окружение разработки*
UID	*User Identifier, идентификатор пользователя Unix*
GID	*Group Identifier, идентификатор группы Unix*
OID	*Object Identifier, идентификатор объекта IDM*

Цель создания

Platform V IDM — это система управления и обеспечения безопасности учетных записей (Identity Management / Identity Governance and Administration) пользователей, предназначенная для интеграции в существующую ИТ-среду предприятий. Хотя Platform V IDM может работать в небольших организациях, его основная цель — работать в средних и крупных организациях.

Platform V IDM также предназначена для автоматизация управления жизненным циклом учетных записей в различных автоматизированных системах Заказчика.

Platform V IDM обеспечивает исполнение процессов и регламентов по управлению правами доступа сотрудников к информационным ресурсам, предоставляет удобный интерфейс для работы системных и функциональных администраторов, и имеет модульную архитектуру, что позволяет разворачивать только требуемые элементы системы и легко масштабировать инсталляцию под нужды организации.

Целью Platform V IDM является синхронизация множества репозиториев, хранилищ и баз данных, хранящих учетные записи и управление ими. Platform V IDM может управлять такими системами, как Active Directory, приложениями, основанными на реляционных базах данных, приложениями, другими существующими IDM системами, и многими другими типами систем. Platform V IDM связывается с такими системами в основном с помощью коннекторов. В основе функциональности по реализации коннекторов также используется программное обеспечение с открытым исходным кодом ConnId framework.

Platform V IDM позволяет применять политики, такие как управление доступом на основе ролей (RBAC), разделение обязанностей (SoD), а также различные политики для обеспечения соответствия нормативным требованиям и рекомендациям.

Основные функции

Основные функции, которые предоставляет сервис:

№	Наименование функции	Потребитель	Аргументы	Описание
1	Автоматизация жизненного цикла учетных записей пользователей	Пользователи	-	Автоматическое создание, изменение и удаление учетных записей сотрудников согласно настроенным политикам управления доступами и данным кадровых систем
2	Ручное управление учетными записями пользователей	Администраторы	-	Администраторы могут вручную создавать, изменять и удалять учетные записи пользователей через интерфейс Platform V IDM
3	Направление и согласование заявок на доступ к информационным системам	Пользователи и администраторы	-	Platform V IDM предоставляет интерфейс самообслуживания (Self-Service), через который пользователи могут подавать заявки на получение доступа к требуемым им информационным системам. Администраторы, через свой интерфейс, обрабатывают эти заявки
4	Синхронизация учетных записей пользователей между несколькими информационными системами	Администраторы	-	Администраторы могут подключать различные информационные системы к Platform V IDM при помощи коннекторов и импортировать базы учетных записей пользователей с последующей синхронизацией учетных записей пользователя из разных систем. Для синхронизации также можно настроить политики разграничения доступов

Platform V IDM предоставляет возможность расширять набор подключаемых систем с помощью отдельных компонентов (коннекторов). Каждый из коннекторов имеет свою реализацию, и различные по зависимости настроечные конфигурации.

Platform V IDM имеет возможность надстройки уже существующими коннекторами (в виде JAR-файлов).

Также Platform V IDM поддерживает работу коннекторов (взаимодействие с подключенными системами) на получение и передачу информации, а также обработку данных в многопоточном режиме с возможностью распределения по нескольким физическим или виртуальным серверам.

Поддержка ряда коннекторов включена в базовые услуги поддержки Platform V IDM. Перечень основных коннекторов перечислен ниже.

Идентификационные коннекторы

Коннектор	Описание
Active Directory Connector (LDAP/LDAPS)	Коннектор для подключения к AD/Exchange на основе LDAP/winRm
DatabaseTable Connector (опционально)	Коннектор для подключения к таблицам реляционных баз данных
SCIM v2 Generic Connector (опционально)	Коннектор для подключения к серверам на основе SCIM 2
ISIM Connector (опционально)	Коннектор для подключения к серверам на основе IBM Security Identity Manager
Refcursor Connector (опционально)	Коннектор IDM для выполнения хранимых процедур

Кроме уже существующих коннекторов, Platform V IDM может использовать коннекторы, совместимые с ConnId, из различных источников.

ConnId — платформа, которая выполняет большую часть операций подготовки в Platform V IDM.

Основной концепцией ConnId является коннектор. Коннектор — это (обычно) часть Java кода, который с одной стороны управляется единым интерфейсом Java, а с другой стороны использует различные протоколы и интерфейсы для подключения к ресурсу.

Сценарии использования

Работа с учетными записями пользователей

1. *Администратор авторизуется и заходит в интерфейс администратора Platform V IDM.*
2. *Администратор может управлять учетными записями в системе Platform V IDM следующим образом:*
   - *Создать новую учетную запись в IDM;*
   - *Синхронизировать учетную запись IDM с подключенными системами. При этом, в зависимости от настроенных политик, учетные записи в подключенных системах будут автоматически созданы, удалены или изменены;*
   - *Удалить учетную запись в IDM;*
   - *Изменить организацию, роли, назначения и доступы учетной записи.*

Конфигурация системы

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор может управлять конфигурацией инсталляции IDM следующим образом:*
   - *Вносить изменения в конфигурацию через онлайн-редактор конфигурационных файлов;*
   - *Импортировать новые конфигурационные файлы в формате XML, YAML или JSON.*

Основные кадровые сценарии работы с карточками сотрудников в IDM

Прием нового сотрудника

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в список учетных карточек пользователей IDM.*
3. *Администратор создает карточку для нового сотрудника и заполняет ее данными.*
4. *Администратор переходит в созданную карточку и добавляет сотруднику назначения на положенные ему ресурсы.*

5. *IDM автоматически генерирует учетные записи в управляемых им ресурсах и заполняет их согласно назначениям и данным из учетной карточки IDM.*

Увольнение сотрудника

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*
3. *Администратор указывает в свойствах карточки дату увольнения и сохраняет изменения.*
4. *IDM автоматически блокирует учетную карточку и все существующие учетные записи сотрудника при наступлении указанной даты увольнения.*

Длительное отсутствие сотрудника

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*
3. *Администратор указывает в свойствах карточки дату начала отсутствия сотрудника.*
4. *Если после указанной даты начала отсутствия проходит больше 28 дней, IDM автоматически блокирует учетную карточку и все существующие учетные записи сотрудника.*
5. *При возвращении сотрудника администратор указывает в свойствах карточки дату окончания отсутствия сотрудника, и IDM автоматически разблокирует учетную карточку и учетные записи.*

Декретный отпуск

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*
3. *Администратор указывает в свойствах карточки даты начала и окончания отсутствия сотрудника, а также код типа отсутствия, соответствующий декретному отпуску.*
4. *IDM автоматически блокирует учетную карточку и учетные записи сотрудника на период между указанными датами, добавляет специальную роль для сотрудников в декрете и отключает все остальные роли.*
5. *По окончании указанного периода IDM разблокирует учетную карточку и учетные записи сотрудника и восстанавливает роли.*

Блокировка доступа при неактивности сотрудника

1. *Сотрудник не выполняет вход в учетную запись управляемого ресурса в течение более чем 28 дней.*
2. *IDM автоматически блокирует данную учетную запись сотрудника.*

Ручное назначение группы Active Directory сотрудника

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*
3. *Администратор указывает в свойствах карточки дополнительные группы AD с их параметрами CN и DC.*
4. *IDM передает изменения в Active Directory, и учетная запись сотрудника включается в указанные группы.*

Перевод сотрудника на новую должность

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*
3. *Администратор указывает в свойствах карточки код и название новой должности сотрудника.*
4. *IDM обновляет данные в карточке, добавляет или удаляет роли, организации и назначения согласно новой должности, и обновляет информацию в существующих учетных записях сотрудника.*

Блокировка сотрудника при инциденте КБ

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*
3. *Администратор указывает в свойствах карточки административный статус “Отключен”.*
4. *IDM автоматически блокирует учетную карточку и все учетные записи сотрудника.*

Ручное изменение персональных данных в карточке сотрудника

1. *Администратор авторизуется и заходит в интерфейс администратора IDM.*
2. *Администратор переходит в карточку сотрудника.*

3. *Администратор изменяет какие-либо персональные данные сотрудника в свойствах карточки.*

4. *IDM производит перерасчет связанных с измененными данными (например, изменяет ФИО, если было изменена фамилия или имя сотрудника) и вносит изменения в данные учетных записей сотрудника.*