АО «СберТех» (является дочерним обществом ПАО Сбербанк)

117105, Москва, Новоданиловская наб., д. 10

Продукт Platform V IDM (IDM)

Компонент Platform V IDM (IDMX)

Руководство по установке

Содержание

Системные требования продукта Platform V IDM (IDM)

Требования к окружению для компонента продукта

Настройки безопасности окружения и перечень платформенных (дополнительных внешних) продуктов, используемых для установки, настройки и контроля в конечной информационной системе, выбираются при разработке конечной ИС, исходя из характера обрабатываемой в ней информации и иных требований информационной безопасности, предъявляемых к ней.

Системное программное обеспечение

Для функционирования IDM необходима установка следующего программного обеспечения сторонних правообладателей.

Категория ПО	Обязательность установки*	Наименование ПО	Версия	Продукт, функциональная совместимость с которым подтверждена **	Назначение категории ПО
Операционная система	Да	ОС Альт 8 СП Сервер	8.4	Рекомендовано	ОС контейнеров для запуска модулей компонента
		Red Hat Enterprise Linux	3.10	Опционально	ОС контейнеров для запуска модулей компонента
Операционная система		Microsoft Windows 10	21H2	Опционально	Опциональная ОС, которая может быть использована для запуска IDM Connector Server на внешних узлах и контурах
Среда контейнеризации	Да	Kubernetes	1.0	Рекомендовано	Платформа контейнеризации для запуска компонентов сервиса
		Red Hat OpenShift	4.2	Опционально	Платформа контейнеризации для запуска компонентов сервиса
Средство контейнеризации	Да	Docker CE	20.10.0	Рекомендовано	Инструмент для автоматизации работы с контейнерами
Java-машина	Да	OpenJDK	11.X	Рекомендовано	Окружение для работы модулей компонента

Категория ПО	Обязательность установки*	Наименование ПО	Версия	Продукт, функциональная совместимость с которым подтверждена **	Назначение категории ПО
Утилита распаковки	Да	Unzip	6.X	Рекомендовано	Распаковщик zip-архивов для Linux, используется при сборке образов IDM
Система управления базами данных (СУБД)	Да	PostgreSQL	13.X	Рекомендовано. Правообладателем АО «СберТех» также рекомендована СУБД, основанная на PostgreSQL, – Platform V Pangolin SE, см. раздел «Платформенные зависимости»	ПО, взаимодействующее с конечными пользователями, приложениями и базой данных для сбора и анализа данных
Сервер приложений	Да	Nginx	10.20.1	Рекомендовано	СПО для тестирования, отладки и исполнения веб-приложений и балансировки внешних и внутренних запросов между сервисами
Браузер	Да	Яндекс	21.2.X	Рекомендовано	Браузер для входа в UI
		Google Chrome	80.0.3987	Опционально	Браузер для входа в UI
Сервис централизованного хранения репозиториев артефактов (хранилище артефактов)	Да	Nexus-Public	2.5.1	Рекомендовано	Интегрированная платформа для проксирования, хранения и управления зависимостями Java (Maven), образами, а также распространения ПО
		Nexus Repository Manager PRO	3.37.0-01	Опционально	
Сервис централизованного хранения репозиториев исходного кода	Да	GitLab Community Edition	15.0	Рекомендовано	Хранение конфигураций при автоматизированной установке

Категория ПО	Обязательность установки*	Наименование ПО	Версия	Продукт, функциональная совместимость с которым подтверждена **	Назначение категории ПО
		Bitbucket	7.6	Опционально	
Сервис интеграции и оркестрации микросервисов в облаке	Нет	Istio	1.15	Рекомендовано. Правообладателем АО «СберТех» также рекомендован сервис интеграции и оркестрации микросервисов в облаке, основанный на Istio, – Platform V Synapse Service Mesh, см. раздел «Платформенные зависимости»	Сервис интеграции микросервисов в облаке
Система мониторинга (сбор и хранение метрик)	Нет	Prometheus	2.31	Рекомендовано. Правообладателем АО «СберТех» также рекомендован Сервис для сбора прикладных и инфраструктурных метрик и отправки их в целевую систему хранения – Объединенный мониторинг Unimon Platform V Monitor, см. раздел «Платформенные зависимости»	Система для сбора и хранения численных метрик
Система мониторинга (визуализация)	Нет	Grafana	2.5.0	Рекомендовано	Система для визуализации численных метрик (предоставленных, например, Prometheus)

Примечание:

*

- *Да — категория ПО обязательна для функционирования сервиса (это означает, что сервис не может выполнять свои основные функции без установки данной категории ПО).*
- *Нет — категория ПО необязательна для функционирования сервиса (это означает, что сервис может выполнять свои основные функции без установки данной категории ПО).*

**

- **Рекомендовано** — рекомендованный правообладателем АО «СберТех» продукт.
- **Опционально** — альтернативный по отношению к рекомендованному правообладателем АО «СберТех» продукт.

Платформенные зависимости

Для настройки, контроля и функционирования компонента реализована интеграция с программными продуктами, правообладателем которых является АО «СберТех»:

Наименование продукта	Код	Версия продукта	Код и наименование компонента	Обязательность установки***	Описание	Аналог других производителей****
Platform V Audit SE	AUD	2.3	AUDT / Аудит	Нет	Сервис для аудирования событий	Сервис успешно прошел испытания и подтвердил свою работоспособность с компонентом AUDT. С аналогами других производителей не тестировался
Platform V IAM SE	IAM	1.3	AUTH / IAM Proxy	Нет	Сервис выполняет функции аутентификации/авторизации запросов и реализует Policy Enforcement Point (PEP). Взаимодействует с KCSE/AUTZ или другими провайдерами аутентификации/авторизации	Любой OIDC провайдер
Platform V Monitor	OPM	4.1	LOGA / Журналирование	Нет	Сервис для хранения лог-файлов	Любой сервис сбора записей о событиях, совместимый с fluent-bit, например: Elasticsearch, InfluxDB
Platform V Monitor	OPM	4.1	MONA / Объединенный мониторинг Unimon	Нет	Сервис для сбора прикладных и инфраструктурных метрик и отправки их в целевую систему хранения	Prometheus 2.21.0

Наименование продукта	Код	Версия продукта	Код и наименование компонента	Обязательность установки***	Описание	Аналог других производителей****
Platform V Pangolin SE	PSQ	5.1.0	PSQL / Platform V Pangolin	Да	Система управления базами данных, основанная на PostgreSQL	PostgreSQL 13
Platform V DevOps Tools	DOT	1.2	CDJE / Deploy tools	Да	Сервис для развертывания и обновления компонентов Платформы и приложений потребителей, для настройки и обслуживания инфраструктуры Платформы	С аналогами других производителей не тестировался
Platform V Synapse Service Mesh	SSM	2.1.0	POLM / Управление политиками	Нет	Панель управления с открытым исходным кодом, служащая для взаимодействия, мониторинга и обеспечения безопасности контейнеров в среде контейнеризации Kubernetes	Istio Control Plane 1.12
Platform V Synapse Service Mesh	SSM	2.1.0	IGEG / Граничный прокси	Нет	Сервис для обеспечения управляемого вызова интеграционных сервисов прикладной части	Istio Proxy 1.12
Platform V Synapse Service Mesh	SSM	2.1.0	SVPX / Сервисный прокси	Нет	Сервис представляет собой подконтейнер (sidecar) контейнера с продуктом, обеспечивающий взаимодействие с Platform V Synapse Service Mesh	Istio Envoy Proxy 1.12
Platform V Backend	#BD	4.3.0	OTTS / One-Time Password (OTP) / OTT	Нет	Сервис для аутентификации и авторизации межсервисных взаимодействий	С аналогами других производителей не тестировался

Наименование продукта	Код	Версия продукта	Код и наименование компонента	Обязательность установки***	Описание	Аналог других производителей****
Platform V Secret Management	SCM	1.0	KMSS / Управление ключами/сертификатами	Нет	Сервис предоставляет средства обеспечения информационной безопасности в части хранения паролей и других секретов	Создание Kubernetes Secrets вручную средствами системы оркестрации контейниризированных приложений

Примечание:

***

- *Да — компонент или продукт необходим для функционирования сервиса (это означает, что сервис не может выполнять свои основные функции без установки данного компонента).*
- *Нет — необязательный для функционирования сервиса компонент или продукт (это означает, что сервис может выполнять свои основные функции без установки данного компонента).*

**** *— Рекомендуется установка программного продукта, правообладателем которого является АО «СберТех», при этом не исключена возможность (допускается правообладателем) использования аналога других производителей. Аналоги, в отношении которых продукт успешно прошел испытания и подтвердил свою работоспособность, указаны в разделе «Системное программное обеспечение».*

Аппаратные требования

Для компонента продукта требуется следующая минимальная конфигурация аппаратного обеспечения.

Компоненты с префиксом idmx *разворачиваются в едином пространстве имен (namespace). Компонент* idmx-engine *хранит данные в БД.*

Компонент	Назначение	Среда развертывания	Количество разворачиваемых экземпляров
idmx-ui	Front-end	Среда оркестрации контейнеризированных приложений	1 Deployment, 1 Pod
idmx-engine	Back-end	Среда оркестрации контейнеризированных приложений	1 Deployment, 1 Pod

Компонент	Назначение	Среда развертывания	Количество разворачиваемых экземпляров
idmx-connector-server	Back-end	Среда оркестрации контейнеризированных приложений	1 Deployment, 1 Pod
idmint-support-service	Back-end	Среда оркестрации контейнеризированных приложений	1 Deployment, 1 Pod
Platform V Pangolin SE	БД	ОС сервера	1

- Требования для каждого компонента IDM

  Для поддержания стабильной работоспособности IDM необходимо обеспечить следующую квоту ресурсов:

	Минимальная конфигурация	5000 пользователей	50.000 пользователей	100.000 пользователей
Количество ядер процессора (шт)	1	2	8	16
Оперативная память (ГБ)	4	8	16	32
Дисковое пространство (ГБ)	2	10	20	40

Обратите внимание, данные квоты ресурсов указаны исключительно для компонентов IDM. В случае использования опциональных интеграций, таких, как sidecar с агентами интеграций Platform V Monitor или разворачивания Istio (Platform V Synapse Mesh), выделяемую квоту ресурсов для компонентов и пространства имен следует увеличить согласно требованиям, указанным в документации на используемые интеграции.

В приведенной выше таблице размеров предполагается, что будет работать один экземпляр (узел) IDM. Экземпляры средней точки с несколькими узлами обычно развертываются из соображений высокой доступности, и это обычно двухузловые системы. В этом случае каждый узел должен быть рассчитан на полную нагрузку системы, поэтому оба узла должны быть развернуты в соответствии с таблицей выше.

Еще одна причина для многоузлового развертывания заключается в том, чтобы изолировать синхронную нагрузку (например, взаимодействие с пользователем) и асинхронную нагрузку (например, задачи и процессы). Однако универсального правила определения размеров такой системы не существует. В этом случае требуется индивидуальный анализ и измерения. Однако цифры, приведенные в таблице выше, можно использовать в качестве отправной точки.

- Требования базы данных

Для поддержания стабильной работы базы данных, использующейся для хранения данных IDM необходимо обеспечить следующие требования к ресурсам сервера:

	Минимальная конфигурация	*5000 пользователей*	*50.000 пользователей*	*100.000 пользователей*
Количество ядер процессора (шт)	*1*	*2*	*8*	*8*
Оперативная память (ГБ)	*2*	*4*	*16*	*16*
Дисковое пространство (ГБ)	*1*	*5*	*20*	*100*

При этом необходимо понимать, что нагрузка на СУБД наиболее чувствительна к размеру и характеру данных, а также к шаблонам использования, а также к типу и конфигурации используемой системы баз данных. Для точной оценки необходимо проводить расчеты под конкретные требования к системе.

Состав дистрибутива

Элемент дистрибутива	*Описание*
./bh/idm-connector-server.zip	*Сервис, содержащий коннекторы и позволяющий IDM проксировать через себя запросы к ресурсам, расположенным на других узлах или контурах*
./bh/idm-engine.zip	*Ядро IDM, предоставляющее основные функциональности продукта*
./bh/idm-ui.zip	*Сервис, предоставляющий пользовательский интерфейс для взаимодействия с IDM*
./bh/idmint-support-service.zip	*Вспомогательный сервис, содержащий дополнительные инструменты для работы IDM со специфически сконфигурированными ресурсами*
./conf/	*Директория с конфигурационными файлами для установки IDM при помощи Platform V DevOps Tools*
./conf/config/parameters/	*Директория содержащая конфигурационные файлы* *.conf *для установки IDM при помощи Platform V DevOps Tools*
./conf/idm-configs/	*Директория с инициализационными и пост-инициализационными конфигурационными файлами IDM, включая ролевую модель*
./conf/sql/	*Директория с конфигурационными скриптами для подготовки системной БД IDM перед установкой IDM*

Элемент дистрибутива	Описание
./conf/k8s/	Директория с предзаполненными шаблонизированными конфигурационными файлами для разворачивания IDM в среде оркестрации контейнеризированных приложений через Platform V DevOps Tools
./docker/	Директория содержащая Docker-образы модулей IDM

Пререквизиты

При настройке среды окружения IDM все системное ПО следует устанавливать согласно документации на это ПО. IDM не накладывает каких-либо дополнительных требований к настройке среды окружения.

Механизмы безопасности среды функционирования настраиваются согласно документации на эти продукты, и исходя из требований департамента информационной безопасности.

Установка

Установка через Installer

Установка дистрибутива производится автоматизированным способом через компонент Deploy tools (CDJE) продукта Platform V DevOps Tools (DOT).

Пререквизиты

Перед установкой IDM необходимо установить все обязательные и выбранные опциональные зависимости из списка ПО в разделе Системные требования. Установка и настройка ПО производится согласно документации на эти продукты.

Поддерживаемой системой приложений-контейнеров является Kubernetes (использование OpenShift – опционально), в инструкциях по настройке в именах переменных и параметрах системы могут встречаться названия систем контейнеризации, которые одинаковы и применимы для обоих сред контейнеризации.

Сборка образов IDM

Перед установкой необходимо собрать Docker-образы всех модулей IDM и поместить их в Registry. Сборка образов производится из компонентов дистрибутива IDM при помощи инструментов продукта Platform V DevOps Tools (рекомендовано) либо инструментами Docker (опционально) согласно стандартной инструкции использования этих инструментов.

Убедитесь, что базовый образ, на основе которого собираются Docker-образы IDM, содержит все нужное системное ПО:

- *ОС (рекомендуется ОС Альт 8 СП);*
- *Java-машина (рекомендуется OpenJDK);*
- *Утилита для распаковки zip-архивов (рекомендуется UnZip).*

Требуемые версии системного ПО смотрите в разделе Системные требования.

Подготовка системной БД

Перед запуском установки IDM также необходимо установить и настроить СУБД, которая будет использоваться для управления системной БД IDM. Установка производится согласно документации на выбранную СУБД (Platform V Pangolin SE или PostgreSQL). Для подготовки системной БД IDM:

1. *Войдите в СУБД под пользователем* postgres *и выполните следующие команды:*
   - *Создание пользователя:*

CREATE USER idm_user WITH PASSWORD 'password' LOGIN NOSUPERUSER NOCREATEDB NOCREATEROLE;

- *Создание БД:*

  CREATEDATABASE idm_db WITHOWNER = idm_user ENCODING = 'UTF8' TABLESPACE = pg_default LC_COLLATE = 'en_US.utf-8' LC_CTYPE = 'en_US.utf-8' CONNECTIONLIMIT = -1;

2. *Выйдите из УЗ* postgres *и войдите под созданным пользователем* idm_user. *Затем выполните для БД* idm_db *три скрипта подготовки БД в следующей последовательности:*

   1. postgres-new.sql
   2. postgres-new-audit.sql
   3. postgres-new-quartz.sql

Скрипты подготовки БД находятся в дистрибутиве в директории <distrib>/conf/sql/native-new.

Установка IDM

*Установка IDM включает в себя установку основных модулей развертывания (*idmx-engine, idmx-ui *и* idmx-connector-server*), а также вспомогательных сервисов (*idmint-support-service*). Установка всех модулей производится посредством компонента Deploy tools (CDJE) продукта Platform V DevOps Tools (DOT) (далее Installer).*

При установке используется типовая инструкция для работы Installer. Более подробную информацию можно найти в документации на Installer, документ **Руководство для операторов**. *Ниже приведена краткая инструкция:*

1. *В веб-интерфейсе Installer нажмите кнопку* **Собрать с параметрами**.
2. *На открывшейся странице с параметрами для сборки выберите:*
   - *DISTRIB_VERSION: ;*
   - *Выбрать OSE_CLUSTERS: ;*
   - *Выбрать версию платформы: ;*
   - *Выбрать сценарии запуска:* MIGRATION_FP_CONF*;*
3. *Нажмите кнопку* **Собрать**.
4. *Проверьте и настройте конфигурационные файлы и файл паролей в репозитории Installer.*
5. *Запустите Deploy Job с параметрами*FP_CONF_CHECK, OPENSHIFT_DEPLOY.

Примечания к процессу установки

1. *Миграция конфигурационных файлов.*

   В веб-интерфейсе Installer, перед установкой в среду системы оркестрации контейнеризированных приложений выберите и запустите шаг (playbook) ***Миграция конфигурационных файлов ФП*** *(MIGRATION_FP_CONF). В результате выполнения шага будут мигрироваться следующие файлы:*

   – idm-engine.conf

№	*Параметр файла*	*Описание*	*Значение по умолчанию*	*Возможные значения*
1	*idm-engine.ose.autoscaling.min_replicas*	*Параметр задает минимальное количество реплик, которые должны быть запущены для* idmx-engine	*1*	*Любое число в зависимости от доступных ресурсов*
2	*idm-engine.ose.route_url*	*Параметр задает URL, по которому должен быть доступен* idmx-engine	idm-engine-{{ lookup('custom_vars', 'global.multiClusters.openshiftNewRoute') }}	*Любая строка*
3	*idm-engine.ose.route_protocol*	*Параметр задает протокол подключения для Route к* idmx-engine	*http*	*http; https*
4	*idm-engine.java_opts_extra*	*Параметр задает дополнительные опции запуска для Java-машины*	*Отсутствует*	*Любые опции Java*
5	*idm-engine.ose.requests.cpu*	*Параметр задает минимальное количество мощности процессора, выделяемое для одной реплики* idmx-engine	*2*	*Любое число в зависимости от доступных ресурсов*
6	*idm-engine.ose.requests.memory*	*Параметр задает минимальное количество RAM, выделяемое для одной реплики* idmx-engine	*4Gi*	*Любое число в зависимости от доступных ресурсов*
7	*idm-engine.ose.limits.cpu*	*Параметр задает максимальное количество мощности процессора, которое может быть выделено для одной реплики* idmx-engine	*2*	*Любое число в зависимости от доступных ресурсов*

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
8	idm-engine.ose.limits.memory	Параметр задает максимальное количество RAM, которое может быть выделено для одной реплики idmx-engine	4Gi	Любое число в зависимости от доступных ресурсов
9	idm-engine.repository.db.type	Параметр задает тип базы данных, используемой IDM для хранения внутренних данных	postgresql	**Не изменяйте данный параметр**
10	idm-engine.repository.db.username	Параметр задает имя пользователя, под которым IDM будет подключаться к БД	Отсутствует	Имя пользователя
11	idm-engine.repository.db.url	Параметр задает URL, по которому IDM будет подключаться к БД	Отсутствует	Любой URL для подключения к БД по протоколу JDBC
12	idm-engine.repository.db.mtls.enabled	Параметр определяет, будет ли использоваться mTLS для подключения idmx-engine к БД	false	true, false
13	idm-engine.ose.prometheus.io.scrape	Параметр определяет, будут ли собираться метрики Prometheus	true	true, false
14	idm-engine.ose.prometheus.io.port	Параметр задает порт эндпоинта, с которого будут собираться метрики Prometheus	8080	Любой порт
15	idm-engine.ose.prometheus.io.path	Параметр задает эндпоинт, с которого будут собираться метрики Prometheus	/midpoint/actuator/prometheus	**Не изменяйте данный параметр**
16	idm-engine.sp.username_header	Параметр определяет HTTP-заголовок, который будет использоваться при авторизации через Platform V IAM SE	Отсутствует	Любой HTTP-заголовок
17	idm-engine.sp.logout_url	Параметр определяет URL для выхода из учетной записи при авторизации через Platform V IAM SE	Отсутствует	Любой URL

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
18	idm-engine.config.base_path	Параметр задает путь до основной директории IDM	Отсутствует	**Не изменяйте данный параметр**
19	idm-engine.config.logs_path	Параметр задает путь до директории, в которую будут записываться журналы логов	/opt/midpoint/var/log	**Не изменяйте данный параметр**
20	idm-engine.config.tomcat.port_header	Параметр задает HTTP-заголовок для виртуального сервера Tomcat	X-Forwarded-Port	**Не изменяйте данный параметр**
21	idm-engine.internals_avoid_logging_change	Параметр определяет, можно ли вносить изменения в конфигурацию логирования через UI IDM	true	true, false
22	idm-engine.audit.url	Параметр задает URL, по которому в клиент Platform V Audit SE будут отправляться сообщения аудита	Отсутствует	Любой URL
23	idm-engine.audit.metamodel.version	Параметр задает версию метамодели аудита IDM для Platform V Audit SE	4	**Не изменяйте данный параметр**
24	idm-engine.cluster.enabled	Параметр определяет, включен ли кластерный режим работы IDM	false	true, false

- idm-ui.conf

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
1	idm-ui.ose.autoscaling.min_replicas	Параметр задает минимальное количество реплик, которые должны быть запущены для idmx-ui	1	Любое число в зависимости от доступных ресурсов
2	idm-ui.ose.route_url	Параметр задает URL, по которому должен быть доступен idmx-ui	idm-ui-{{ lookup('custom_vars', 'global.multiClusters.openshiftNewRoute') }}	Любая строка
3	idm-ui.ose.route_protocol	Параметр задает протокол подключения для Route к idmx-ui	http	http, https

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
4	idm-ui.ose.requests.cpu	Параметр задает минимальное количество мощности процессора, выделяемое для одной реплики idmx-ui	500m	Любое число в зависимости от доступных ресурсов
5	idm-ui.ose.requests.memory	Параметр задает минимальное количество RAM, выделяемое для одной реплики idmx-ui	1Gi	Любое число в зависимости от доступных ресурсов
6	idm-ui.ose.limits.cpu	Параметр задает максимальное количество мощности процессора, которое может быть выделено для одной реплики idmx-ui	500m	Любое число в зависимости от доступных ресурсов
7	idm-ui.ose.limits.memory	Параметр задает максимальное количество RAM, которое может быть выделено для одной реплики idmx-ui	1Gi	Любое число в зависимости от доступных ресурсов

- idm-connector-server.conf

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
1	idm-connector-server.ose.autoscaling.min_replicas	Параметр задает минимальное количество реплик, которые должны быть запущены для idmx-connector-server	1	Любое число в зависимости от доступных ресурсов
2	idm-connector-server.ose.requests.cpu	Параметр задает минимальное количество мощности процессора, выделяемое для одной реплики idmx-connector-server	500m	Любое число в зависимости от доступных ресурсов
3	idm-connector-server.ose.requests.memory	Параметр задает минимальное количество RAM, выделяемое для одной реплики idmx-connector-server	1Gi	Любое число в зависимости от доступных ресурсов

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
4	idm-connector-server.ose.limits.cpu	Параметр задает максимальное количество мощности процессора, которое может быть выделено для одной реплики idmx-connector-server	500m	Любое число в зависимости от доступных ресурсов
5	idm-connector-server.ose.limits.memory	Параметр задает максимальное количество RAM, которое может быть выделено для одной реплики idmx-connector-server	1Gi	Любое число в зависимости от доступных ресурсов
6	idm-connector-server.ose.custom_class_path	Параметр задает classpath с необходимыми библиотеками для idmx-connector-server	ib/asm-analysis-9.1.jar:lib/asm-commons-9.1.jar:/lib/asm-tree-9.1.jar:lib/asm-util-9.1.jar:lib/nashorn-core-15.3.jar:lib/ojdbc8.jar	Не изменяйте данный параметр
7	idm-connector-server.fluent.log_level	Параметр задает уровень логирования в Platform V Monitor для idmx-connector-server	INFO	ERROR, WARN, INFO. Рекомендуется оставить на INFO
8	idm-connector-server.config.logs_path	Параметр задает путь до директории, в которую будут записываться журналы логов	/app/connid-connector-server/logs/	Не изменяйте данный параметр

- idm-connectors.conf

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
1	idm.connector.exchange.url	Параметр определяет URL для подключения к ресурсу через коннектор ADExchange	Отсутствует	Любой URL
2	idm.connector.exchange.host	Параметр определяет хоста для подключения к ресурсу через коннектор ADExchange	Отсутствует	Любой хост
3	idm.connector.exchange.authentication	Параметр определяет тип аутентификации при подключения к ресурсу через коннектор ADExchange.	Отсутствует	Basic, Default, Kerberos

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
4	idm.connector.exchange.username	Параметр определяет учетную запись для подключения к ресурсу через коннектор ADExchange	Отсутствует	Любая строка
5	idm.connector.exchange.load.classes	Параметр определяет типы Active Directory, которые нужно подгрузить через коннектор ADExchange	Отсутствует	Любая строка
6	idm.connector.kis.departments_port	Параметр определяет порт для подключения IDM к БД с кадровой информацией по подразделениям	Отсутствует	Любой порт
7	idm.connector.kis.departments_host	Параметр определяет URL для подключения IDM к БД с кадровой информацией по подразделениям	Отсутствует	Любой URL
8	idm.connector.kis.departments_database	Параметр определяет URL для подключения IDM к БД с кадровой информацией по подразделениям	Отсутствует	Любой URL
9	idm.connector.kis.departments_user	Параметр определяет логин для подключения IDM к БД с кадровой информацией по подразделениям	Отсутствует	Любая строка
10	idm.connector.kis.departments_table	Параметр определяет таблицу БД с кадровой информацией по подразделениям, из которой будет браться информация	Отсутствует	Любая строка
11	idm.connector.kis.departments_keycolumn	Параметр определяет ключевой параметр таблицы БД с кадровой информацией по подразделениям	Отсутствует	Любая строка
12	idm.connector.kis.sap.employees_port	Параметр определяет порт для подключения IDM к БД с кадровой информацией по сотрудникам	Отсутствует	Любой порт
13	idm.connector.kis.sap.employees_host	Параметр определяет URL для подключения IDM к БД с кадровой информацией по сотрудникам	Отсутствует	Любой URL
14	idm.connector.kis.sap.employees_database	Параметр определяет URL для подключения IDM к БД с кадровой информацией по сотрудникам	Отсутствует	Любой URL
15	idm.connector.kis.sap.employees_user	Параметр определяет логин для подключения IDM к БД с кадровой информацией по сотрудникам	Отсутствует	Любая строка

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
16	idm.connector.kis.sap.employees_table	Параметр определяет таблицу БД с кадровой информацией по сотрудникам, из которой будет браться информация	Отсутствует	Любая строка
17	idm.connector.kis.sap.employees_keycolumn	Параметр определяет ключевой параметр таблицы БД с кадровой информацией по сотрудникам	Отсутствует	Любая строка

- idm-support-service.conf

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
1	idmint-support-service.ose.autoscaling.min_replicas	Параметр задает минимальное количество реплик, которые должны быть запущены для idmint-support-service	1	Любое число в зависимости от доступных ресурсов
2	idmint-support-service.ose.limits.cpu	Параметр задает минимальное количество мощности процессора, выделяемое для одной реплики idmint-support-service	400m	Любое число в зависимости от доступных ресурсов
3	idmint-support-service.ose.limits.memory	Параметр задает минимальное количество RAM, выделяемое для одной реплики idmint-support-service	800Mi	Любое число в зависимости от доступных ресурсов
4	idmint-support-service.ose.requests.cpu	Параметр задает максимальное количество мощности процессора, которое может быть выделено для одной реплики idmint-support-service	200m	Любое число в зависимости от доступных ресурсов
5	idmint-support-service.ose.requests.memory	Параметр задает максимальное количество RAM, которое может быть выделено для одной реплики idmint-support-service	800Mi	Любое число в зависимости от доступных ресурсов

- idm.all.conf

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
1	idm.ose.image.path	Параметр определяет путь к Docker-образу IDM для развертывания	Отсутствует	Любой URL

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
2	idm.ose.hashicorp.role	Параметр определяет роль для доступа к секретам IDM в компоненте KMSS	Отсутствует	Любая строка
3	idm.ose.hashicorp.key	Параметр определяет ключ для доступа к секретам IDM в компоненте KMSS	Отсутствует	Любая строка
4	idm.ose.hashicorp.namespace	Параметр задает пространство имен, в котором расположен экземпляр компонента KMSS, используемый для IDM	Отсутствует	Любой URL
5	idm.ose.hashicorp.enabled	Параметр определяет, будет ли использоваться компонент KMSS для хранения секретов IDM	false	true, false
6	idm.fluent.brokers	Параметр определяет брокеров Kafka, через которых будут отправляться журналы логов IDM в Platform V Monitor	Отсутствует	Обратитесь к документации компонента LOGA Platform V Monitor
7	idm.fluent.topics	Параметр определяет топики Kafka, в которых будут отправляться журналы логов IDM в Platform V Monitor	Отсутствует	Обратитесь к документации компонента LOGA Platform V Monitor
8	idm.fluent.log_level	Параметр определяет уровень логирования IDM для Platform V Monitor	Отсутствует	Обратитесь к документации компонента LOGA Platform V Monitor
9	idm.fluent.ca_path	Параметр задает путь в vault для CA сертификата от Platform V Monitor	Отсутствует	Любая строка
10	idm.fluent.cert_path	Параметр задает путь в vault для клиентского сертификата от Platform V Monitor	Отсутствует	Любая строка
11	idm.fluent.cert_key_path	Параметр задает путь в vault для ключа клиентского сертификата от Platform V Monitor	Отсутствует	Любая строка
12	idm.fluent.image.name	Параметр задает имя Docker образа сайдкара компонента LOGA Platform V Monitor	Отсутствует	Любая строка
13	idm.fluent.image.tag	Параметр задает тэг Docker образа сайдкара компонента LOGA Platform V Monitor	Отсутствует	Любая строка

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
14	idm.fluent.image.path	Параметр задает путь до Docker образа сайдкара компонента LOGA Platform V Monitor	Отсутствует	Любой URL
15	idm.fluent.requests.cpu	Параметр задает минимальное количество мощности процессора, выделяемое для сайдкара компонента LOGA Platform V Monitor	100m	Любое число в зависимости от доступных ресурсов
16	idm.fluent.requests.memory	Параметр задает минимальное количество RAM, выделяемое для сайдкара компонента LOGA Platform V Monitor	16Mi	Любое число в зависимости от доступных ресурсов
17	idm.fluent.limits.cpu	Параметр задает максимальное количество мощности процессора, которое может быть выделено для сайдкара компонента LOGA Platform V Monitor	200m	Любое число в зависимости от доступных ресурсов
18	idm.fluent.limits.memory	Параметр задает максимальное количество RAM, которое может быть выделено для сайдкара компонента LOGA Platform V Monitor	32Mi	Любое число в зависимости от доступных ресурсов

- idm.istio.all.conf

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
1	idm.ose.istio.enabled	Параметр определяет, будет ли использоваться интеграция с Platform V Synapse Service Mesh (Istio)	false	true, false
2	idm.ose.istio.egress.deployment.spec.template	Параметр задает шаблон для Istio	Отсутствует	Любая строка
3	idm.ose.istio.ingress.deployment.instance	Параметр определяет имя экземпляра Istio Control Plane для Ingress	Отсутствует	Любая строка
4	idm.ose.istio.ingress.deployment.ca_addr	Параметр определяет адрес Istio Control Plane для Ingress	Отсутствует	Любой URL
5	idm.ose.istio.egress.deployment.instance	Параметр определяет имя экземпляра Istio Control Plane для Egress	Отсутствует	Любая строка

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
6	idm.ose.istio.egress.deployment.ca_addr	Параметр определяет адрес Istio Control Plane для Egress	Отсутствует	Любой URL
7	idm.ose.istio.ingress.route_url	Параметр определяет URL для Route, создаваемого для Ingress	ingress-{{ lookup('custom_vars', 'global.multiClusters.openshiftNewRoute') }}	Любая строка
8	idm.ose.istio.ingress.ca_certs_path	Параметр задает путь к сертификатам CA для Ingress	Отсутствует	Любой путь
9	idm.ose.istio.ingress.certs_path	Параметр задает путь к клиентским сертификатам для Ingress	Отсутствует	Любой путь
10	idm.ose.istio.egress.ca_certs_path	Параметр задает путь к сертификатам CA для Egress	Отсутствует	Любой путь
11	idm.ose.istio.egress.certs_path	Параметр задает путь к клиентским сертификатам для Egress	Отсутствует	Любой путь
12	idm.ose.istio.egress.db_repository_host	Параметр задает хост для доступа к БД Egress	Отсутствует	Любой хост
13	idm.ose.istio.egress.db_repository_ip	Параметр задает IP-адрес для доступа к БД Egress	Отсутствует	Любой IP-адрес
14	idm.ose.istio.ingress.deployment.requests.cpu	Параметр задает минимальное количество мощности процессора, выделяемое для одной реплики Ingress	400m	Любое число в зависимости от доступных ресурсов
15	idm.ose.istio.ingress.deployment.requests.memory	Параметр задает минимальное количество RAM, выделяемое для одной реплики Ingress	700Mi	Любое число в зависимости от доступных ресурсов
16	idm.ose.istio.ingress.deployment.limits.cpu	Параметр задает максимальное количество мощности процессора, которое может быть выделено для одной реплики Ingress	600m	Любое число в зависимости от доступных ресурсов

№	Параметр файла	Описание	Значение по умолчанию	Возможные значения
17	idm.ose.istio.ingress.deployment.limits.memory	Параметр задает максимальное количество RAM, которое может быть выделено для одной реплики Ingress	900Mi	Любое число в зависимости от доступных ресурсов
18	idm.ose.istio.egress.deployment.requests.cpu	Параметр задает минимальное количество мощности процессора, выделяемое для одной реплики Egress	200m	Любое число в зависимости от доступных ресурсов
19	idm.ose.istio.egress.deployment.requests.memory	Параметр задает минимальное количество RAM, выделяемое для одной реплики Egress	256Mi	Любое число в зависимости от доступных ресурсов
20	idm.ose.istio.egress.deployment.limits.cpu	Параметр задает максимальное количество мощности процессора, которое может быть выделено для одной реплики Egress	400m	Любое число в зависимости от доступных ресурсов
21	idm.ose.istio.egress.deployment.limits.memory	Параметр задает максимальное количество RAM, которое может быть выделено для одной реплики Egress	512Mi	Любое число в зависимости от доступных ресурсов

3. *Выпуск сертификатов.*

   Если вы планируете использовать SSL для подключения IDM к БД Platform V Pangolin SE, следует выполнить следующие действия:

   1. *Получите у администраторов вашей БД следующие сертификаты:*
      - *сертификат клиента;*
      - *ключ сертификата;*
      - *CA сертификат.*
   2. *Поместите их в инсталляцию компонента KMSS продукта Platform V Secret Management, подключенную к IDM.*
   3. *Измените следующие параметры в конфигурационных файлах IDM:*
      - idm-engine.repository.db.mtls.enabled *в* true*;*
      - idm-engine.repository.db.url *— добавьте в данный URL пути до сертификатов, например:*

jdbc:postgresql://pangolin.db.mycorp.ru:5432/idmx-1?prepareThreshold=0&ssl=true&sslmode=verify-full&sslcert=/vault/secrets/postgres.crt&sslkey=/vault/secrets/postgres.pk8&sslrootcert=/vault/secrets/postgres_ca.crt

4. *Добавление сертификатов в* common *репозиторий.*

   В common репозиторий добавьте сертификаты, указанные в таблице.

Наименование	*Расположение*
Ingress, Egress, OTT, БД	idm_common_dev/<директория стенда>/ansible/files/ssl
Серверы OTT	idm_common_dev/<директория стенда>/ansible/files/ssl

В common *репозиторий добавьте описание параметров обращения к сертификатам.*

Наименование	*Расположение*
custom_property.conf.yml	idm_dev/ift/conf/

Например:

```
# комментарий
kubernetes/openshift:
project: 'tribe-sc-ift-idm'
# Istio
# Ingress
ingressKeyStoreFile: 'ansible/files/ssl/idm/idm-ingress.jks'
ingressKeyStorePass: 'idm.ssl.ose.istio.keyStore.ingress.password'
ingressRootCertAlias: 'root'
ingressCertAlias: 'idm-ingress'
ingressPrivateKeyAlias: 'idm-ingress'

# Egress
egressKeyStoreFile: 'ansible/files/ssl/idm/idm-egress.jks'
egressKeyStorePass: 'idm.ssl.ose.istio.keyStore.egress.password'
egressRootCertAlias: 'root'
egressCertAlias: 'idm-egress'
egressPrivateKeyAlias: 'idm-egress'

##OTT сертификаты
# Сами кейсторы разместить в commons среды, пути до кейсторов указать в репозитории ФП в `conf/custom_property.conf.yml`
idmCertStoreName: 'idm.p12'
idmOttCertStorePath: 'ansible/files/ssl/idm/idm.p12'
```

```
ottTrustStoreName: 'ift_sol_std3_ott_public.p12'
ottTrustStorePath: 'ansible/files/ssl/ift_sol_std3_ott_public.p12'
```

4. *Заполнение паролей и секретов.*

   В common репозитории в файл _passwords.conf *(либо в vault, если используется компонент KMSS) добавьте следующие секреты:*

   - idm_connector_exchange_password — *Пароль для подключения через коннектор ADExchange;*
   - idm_connector_kis_departments_password — *Пароль для подключения к БД с кадровой информацией по подразделениям;*
   - idm_connector_kis_sap_employees_password — *Пароль для подключения к БД Oracle с кадровой информацией по сотрудникам;*
   - idm_engine_keystore_password — *Пароль от хранилища ключей IDM;*
   - idm_engine_repository_db_password — *Пароль для подключения к системной БД (Platform V Pangolin SE) IDM;*
   - istio_egress_ca — *Сертификат CA для Egress;*
   - istio_egress_cert— *Клиентский сертификат для Egress;*
   - istio_egress_key — *Клиентский ключ для Egress;*
   - istio_ingress_ca — *Сертификат CA для Ingress;*
   - istio_ingress_cert — *Клиентский сертификат для Ingress;*
   - istio_ingress_key — *Клиентский ключ для Ingress;*
   - keystore — *Хранилище ключей и сертификатов IDM;*
   - logger_ca — *Сертификат CA для Platform V Monitor;*
   - logger_cert — *Клиентский сертификат для Platform V Monitor;*
   - logger_key — *Клиентский ключ для Platform V Monitor;*

5. *Корректировка параметров в configmap.*

   Скорректируйте в репозитории Docker CE или Bitbucket (опционально) параметры:

   - /conf/config/parameters/idm-engine.conf*:*
     - *Параметры подключения к БД.*
   - /conf/config/parameters/idm.all.conf*:*
     - *URL образа IDM и секрет для доступа в Docker Registry;*
     - *Секрет с паролем к keystore.*
   - /conf/config/parameters/idm-connector-kis.conf*:*
     - *Параметры для доступа IDM к нужным таблицам БД с кадровой информацией.*

Установка Connector Server

Компонент idm-connector-server *(далее Connector Server) предназначен для подключения IDM к ресурсам, расположенным вне контура, в котором находится инсталляция IDM. Connector Server устанавливается на сервер или виртуальную машину с ОС на базе Linux (рекомендуется ОС Альт 8 СП), либо с ОС Windows 10 (опционально).*

Пререквизиты:

1. *Установлен OpenJDK версии не ниже 11.*
2. *В переменные среды добавлена переменная* JAVA_HOME.

Установка:

1. *Скопируйте из дистрибутива IDM на сервер файл* idm-connector-server.zip*, расположенный в директории дистрибутива* <distrib>/bh/.
2. *Разархивируйте скопированный архив* idm-connector-server.zip *в директорию* idm-connector-server.
3. *Если в директории* <server>/idm-connector-server/connid-connector-server/lib/ *есть файл* connector-common-1.5.0.0.jar*, удалите его.*
4. *Отредактируйте файл* <server>/idm-connector-server/connid-connector-server/conf/connectorserver.properties*, изменив значение параметра* connectorserver.protocol *на* WEB_SOCKET*, и сохраните изменения.*
5. *Откройте командную строку (консоль), перейдите в директорию* connid-connector-server *и выполните следующую команду:*
   - *Если ОС — Альт 8 СП или Linux:* bin/ConnectorServer.sh -setKey -key <SECRET_KEY> -properties conf/connectorserver.properties*;*
   - *Если ОС — Windows 10:* .\bin\ConnectorServer.bat /setkey <SECRET_KEY> /properties .\conf\connectorserver.properties*;*

     , где <SECRET_KEY> *— ключ доступа (пароль) для подключения IDM к Connector Server. При выборе ключа доступа руководствуйтесь требованиями кибербезопасности к паролям. Рекомендуется избегать спецсимволов в ключе доступа, так как могут возникнуть проблемы с подключением.*

После выполнения шагов выше, Connector Server будет установлен.

Для запуска Connector Server откройте командную строку, перейдите в директорию <server>/idm-connector-server/connid-connector-server *и выполните команду:*

- *Если ОС — Альт 8 СП или Linux:* bin/ConnectorServer.sh -run -properties conf/connectorserver.properties*;*
- *Если ОС — Windows 10:* .\bin\ConnectorServer.bat /run /properties .\conf\connectorserver.properties.

Если запуск успешен, в консоли командной строки будет отражена строка вида o.i.f.s.tcp.ConnectorServerImpl - Connector Server started at <дата> <время>. *После этого окно командной строки нельзя закрывать, так как это завершит работу Connector Server.*

Импорт конфигурации Connector Server в IDM

Чтобы IDM мог использовать установленный и запущенный Connector Server, необходимо добавить конфигурацию этого компонента в IDM. Для этого:

1. *Перейдите в любое IDE или текстовый редактор с возможностью создания xml-файлов.*
2. *Создайте новый файл и вставьте в него следующий XML код, заменив соответствующие значения параметров значениями для своих стендов:*

```
<connectorHost xmlns="http://midpoint.evolveum.com/xml/ns/public/common/common-3" xmlns:t="http://prism.evolveum.com/xml/ns/public/types-3" xmlns:protocol="http://midpoint.evolveum.com/xml/ns/public/connector-host-protocol-extension" oid="d7c941c0-1cf4-4fe7-b231-32e1a1c40bcf">

  <name>My local connector</name> //имя создаваемой конфигурации в IDM
  <hostname>localhost</hostname> //имя хоста на котором развернут Connector Server
  <port>9999</port> //порт для подключения к Connector Server
  <sharedSecret>
    <t:clearValue>admin</t:clearValue> //укажите здесь то же значение, которое было задано как ключ доступа к Connector Server во время установки
  </sharedSecret>
  <extension>
    <protocol:connectionProtocol>WEB_SOCKET</protocol:connectionProtocol>
    <protocol:path>/</protocol:path>
  </extension>

</connectorHost>
```

3. *Сохраните файл в файловую систему сервера.*
4. *Войдите в UI установленной инсталляции IDM.*
5. *Импортируйте созданный файл согласно инструкции из документа* ***Руководство оператора****, раздел* ***Параметры настройки****, подраздел Импорт конфигурационных файлов.*

Интеграции с платформенными зависимостями

Для интеграции IDM с большинством платформенных зависимостей следует:

1. *Установить и настроить зависимости согласно их документации.*
2. *Перед установкой IDM указать корректные значения в параметрах конфигурационных файлов, отвечающих за взаимодействие с интеграциями. Например, для подключения интеграции с Platform V IAM SE следует заполнить параметры* idm-engine.sp.username_header *и* idm-engine.sp.logout_url.
3. *Установить IDM.*

Процесс отличается для следующих зависимостей:

- *Platform V Secret Management: Для интеграции следует заполнить соответствующие параметры в* idm.all.conf*, и перед установкой IDM следует поместить нужные секреты в vault Platform V Secret Management.*
- *Platform V Synapse Service Mesh: Для установки IDM с интеграцией с Istio следует установить Platform V Synapse Mesh согласно документации на продукт SSM, заполнить конфигурационный файл* idm.istio.all.conf *корректными значениями, и при установке через Installer использовать playbook с установкой Istio.*
- *Platform V Backend: Никаких дополнительных действий для подключения интеграции со стороны IDM не требуется, установите и настройте компонент OTTS согласно документации на продукт #BD.*

Обновление

Обновление дистрибутива производится через Installer с использованием Job Deploy, в которой необходимо выбрать шаг (playbook) ***Установка в*** *Kubernetes или* ***Openshift*** *(опционально). Обновление происходит со стратегией Rolling Update, удаление предыдущей версии IDM не требуется.*

Для обновления используется типовая инструкция по развертыванию окружения под Installer job [Deploy, Service].

Обновление версии БД выполняется согласно инструкциям в документации по используемой СУБД (Platform V Pangolin SE или PostgreSQL).

Удаление

Для удаления IDM из системы оркестрации контейнеризированных приложений необходимо удалить средствами системы оркестрации следующие объекты:

- *Deployment* idmx-ui*;*
- *Deployment* idmx-connector-server*, если он был установлен;*
- *StatefulSet* idmx-engine*;*
- *В случае если использовался OpenShift — Route и Services для* idmx-ui*,* idmx-engine *и* idmx-connector-server*;*
- *Если использовались компоненты из раздела Платформенные зависимости — удалите их согласно документации на эти компоненты.*

Системная БД IDM удаляется согласно документации на используемую СУБД (Platform V Pangolin SE или PostgreSQL).

Проверка работоспособности

Проверка включает следующие действия:

- *Получить корректный статус при завершении Job Deploy Installer = Success;*
- *Проверить статус readiness и liveness проб контейнеров IDM в интерфейсе системы оркестрации контейнеризированных приложений. Если в процессе запуска возникли какие-либо ошибки, они будут отражены в пробах;*
  - idmx-engine*;*
  - idmx-ui*;*
  - idmx-connector-server*;*
  - idmint-support-service*;*
- *Работоспособность БД проверяется согласно инструкции на СУБД (Platform V Pangolin SE или PostgreSQL).*

Проверка работоспособности интеграций с платформенными зависимостями

Проверка работоспособности платформенных зависимостей производится согласно их документации. Для проверки работоспособности интеграций:

- *Для Platform V DevOps Tools:*
  - *Прямой интеграции нет, Platform V DevOps Tools используется для установки IDM. Если Platform V DevOps Tools был установлен некорректно - будет невозможно установить IDM.*
- *Для Platform V Synapse Service Mesh и Platform V Backend (компонент OTTS):*
  - *Сервисы не имеют применимого UI, проверьте работоспособность интеграции, отправив несколько запросов от IDM к ресурсам, защищаемым этими зависимостями. Если запросы успешны, интеграция работает корректно.*
- *Для Platform V IAM SE:*
  - *Если интеграция с Platform V IAM SE работает корректно, при попытке входа в IDM пользователь будет перенаправлен на страницу входа в IAM.*
- *Для Platform V Secret Management:*
  - *Если интеграция с Platform V Secret Management работает корректно, IDM сможет запуститься и инициализироваться, так как в vault хранятся секреты для доступа IDM к системной БД.*
- *Для остальных зависимостей:*
  - *Перейдите в интерфейс соответствующего сервиса и проверьте наличие сведений, получаемых от IDM. Так, для интеграций с Platform V Audit SE или Platform V Monitor в журналах данных сервисов должны появиться сообщения и метрики IDM.*

Откат

Для отката необходимо откатить:

- *компоненты системы оркестрации контейнеризированных приложений.*

Откат дистрибутива производится следующим образом:

1. *Удалите текущую версию дистрибутива со стенда по инструкции из раздела Удаление.*
2. *Установите требуемую предыдущую версию дистрибутива по инструкции из раздела Установка через Installer.*

Откат БД проводится средствами используемой СУБД (Platform V Pangolin SE или PostgreSQL) и согласно документации на данную СУБД. Рекомендуется проводить регулярные резервные сохранения (backup) системной БД IDM.

Часто встречающиеся проблемы и пути их устранения

Не подключается интеграция с какой-либо платформенной зависимостью

Убедитесь, что все параметры для подключения к инсталляции интеграции заполнены корректными значениями, соответствующими стенду и окружению, где разворачивается IDM:

- *Platform V IAM SE — Параметры* idm-engine.sp.username_header*,* idm-engine.sp.logout_url *конфигурационного файла* idm-engine.conf*;*
- *Platform V Audit SE — Параметры* idm-engine.audit.url*,* idm-engine.audit.metamodel.version *конфигурационного файла* idm-engine.conf*;*
- *Platform V Secret Management — Параметры* idm.ose.hashicorp.enabled*,* idm.ose.hashicorp.role*,* idm.ose.hashicorp.key*,* idm.ose.hashicorp.namespace *конфигурационного файла* idm.all.conf*;*
- *Компонент LOGA (Журналирование) продукта Platform V Monitor — Параметры группы* idm.fluent. *конфигурационного файла* idm.all.conf*;*
- *Platform V Synapse Service Mesh — Параметры группы* idm.ose.istio. *конфигурационного файла* idm.istio.all.conf*;*

Подробнее о параметрах смотрите в разделе Установка через Installer, подраздел ***Миграция конфигурационных файлов****.*

Также убедитесь, что используемые платформенные зависимости корректно установлены и настроены, руководствуясь документацией на эти продукты.

Не запускается Connector Server, установленный отдельно

Основной причиной того что Connector Server не запускается является некорректная версия установленной Java-машины. Проверьте версию OpenJDK на соответствие Системным требованиям, и установите корректную версию в случае расхождения.

Не собирается образ с модулем IDM

Если сборка Docker-образов с модулями IDM прерывается с ошибкой — скорее всего в базовом образе, на основе которого собираются образы IDM, отсутствует утилита распаковки zip-архивов. Удостоверьтесь, что в базовом образе добавлена такая утилита (например, UnZip для ОС Альт 8 СП или Linux).

Чек-лист валидации установки

1. *На сервере развернуто необходимое ПО из раздела Системные требования;*
2. *Развернута и настроена БД Platform V Pangolin SE или PostgreSQL;*
3. *БД доступна по порту (по умолчанию 5432) из кластера системы оркестрации контейнеризированных приложений.*
4. *Созданы docker-образы* idmx-engine, idmx-ui, idmx-connector-server, idmint-support-service *(раздел* ***Установка через Installer****, подраздел Сборка образов IDM);*
5. *Выделен проект системы оркестрации контейнеризированных приложений;*
6. *Произведена настройка проекта системы оркестрации контейнеризированных приложений;*
7. *Произведена первоначальная настройка БД (раздел* ***Установка через Installer****, подраздел Подготовка системной БД);*
8. *Выпущены клиентские и/или серверные сертификаты для подключения к БД Platform V Pangolin SE по SSL при необходимости.*
9. *Подготовлено окружение в соответствии с типовой инструкцией по настройке Job [Deploy, Service] при установке через Installer.*
10. *Приложения установлены при помощи Installer (job завершен со статусом* ***SUCCESS****) (раздел* ***Установка через Installer****, подраздел Установка IDM).*
11. *Для каждого из модулей IDM —* idmx-engine, idmx-ui, idmx-connector-server, idmint-support-service *— readiness и liveness пробы используемой системы оркестрации контейнеризированных приложений возвращают статус Ready.*