ЮНИВЕРС
ДАТА

Руководство пользователя и администратора

Юниверс MDM HPE 6.11

2024

ООО «Юниверс Дата» оставляет за собой право вносить изменения в настоящий документ без предварительного уведомления.

Редакция от 18.06.2024.

Администратор системы

1. Редакция для высоконагруженных систем

Юниверс Управление Мастер Данными Высоконагруженная Редакция (далее – Юниверс MDM HPE) предназначена для обработки больших объемов данных (от 100 миллионов записей и выше).

Основная особенность системы – возможность загрузки больших объемов записей на высокой скорости. Высокая скорость загрузки достигается за счет оптимизированного алгоритма, способного работать с большими объемами данных.

Тип редакции определяется лицензией на систему. Информацию о редакции можно посмотреть в окне «О системе» в интерфейсе пользователя.

Для редакции HPE требуется обеспечение стабильного функционирования всей системы и ее компонентов; гарантия выдерживания больших скачков нагрузки. Эти особенности влияют, в первую очередь, на итоговую ИТ-инфраструктуру сервера, куда будет устанавливаться Юниверс MDM HPE.

Внедрение

HPE редакция требует специального подхода к общей архитектуре внедряемой системы, сценарию использования платформы и аппаратной части серверов.

Основная нагрузка платформы заключается в том, что необходимо загружать и поддерживать от 100 млн. записей постоянно, обрабатывать их (CRUD), обеспечивать качество данных (DQ), консолидировать дубликаты записей и т.д. При этом платформа должна иметь информационное взаимодействие с другими системами, что создает дополнительные требования, например, к обработке очередей сообщений.

2. Учетные записи

Содержание:

2.1. Создание, редактирование учетной записи

2.1.1. Создание учетной записи

Чтобы создать новую учетную запись:

1. Перейдите в раздел "Пользователи", если это не сделано ранее.
2. Нажмите кнопку ⊕ *Создать*, расположенную в нижней части панели управления пользователями.
3. В результате действия откроется окно создания новой учетной записи (Рисунок 1).
4. Во вкладке *Настройки пользователя* заполните основные свойства:
   - Обязательные поля для заполнения: **Логин**, **Имя/Фамилия**, **E-mail** и **Пароль**. Логин должен быть уникальным и состоять из букв латинского алфавита и цифр. Логин может начинаться с цифр. Также допустимо использование символов "-", "_", ".". Знак "@" и пробел в логине недопустимы.
   - **Роли**. Укажите одну или несколько ролей, требуемых для создаваемого пользователя. В случае конфликта нескольких ролей итоговые права пользователя вычисляются как объединение прав заданных ролей, пересечение трактуется в сторону повышения прав.
   - Секция "**Информация о пользователе**": отдельные поля могут быть *обязательными* для заполнения или доступными *только для чтения* в зависимости от настройки.
5. При необходимости заполните опциональные поля:
   - При включении свойства **Внешний** появится новое поле **Способ аутентификации**, в котором из выпадающего списка можно выбрать способ аутентификации (Рисунок 2): через LDAP или *Системная*

(аутентификация по умолчанию). Если пользователь отмечен как внешний, то для его работы в системе Юниверс используются данные входа во внешнюю систему (сторонний логин и пароль из внешней системы).

- Свойство **Суперпользователь** дает полные права на работу со всей системой вне зависимости от других настроек и назначенных ролей. Рекомендуется иметь минимум одну учетную запись с правами суперпользователя. Суперпользователю доступна возможность замены лицензии системы в специальном режиме.

6. При необходимости добавьте собственные метки безопасности в отдельной вкладке.
7. При необходимости добавьте заместителя текущего пользователя.
8. При необходимости отключите флаг **Учетная запись (не) активна**. Войти в систему от имени учетной записи можно только в случае, если она активна.
9. Нажмите кнопку *Сохранить*, расположенную в верхнем правом углу экрана, чтобы применить изменения.

    - Логин нельзя изменить после первого сохранения учетной записи.

Примечания:

- Создание/обновление настроек пользователя с включенным параметром "Внешний" недоступно, если у пользователя в качестве способа аутентификации выбран источник данных по умолчанию.
- Переход в другой раздел или обновление страницы в браузере может привести к потере несохраненных данных.
- Свойства учетной записи пользователь может просматривать в личном кабинете.
- В разделе Группы пользователей отображаются группы пользователя и его роли.

2.1.2. Редактирование учетной записи

Чтобы отредактировать учетную запись:

1. Выберите необходимую учетную запись из списка.
2. Внесите изменения.

    - Логин нельзя изменить после первого сохранения учетной записи.

3. Нажмите кнопку *Сохранить*, расположенную в верхнем правом углу экрана, чтобы внести изменения.

При редактировании настроек учетной записи изменения сразу вступают в силу. Перезаходить в учетную запись не требуется.

Ограничения:

- **Удаление** учетных записей через интерфейс недоступно. При необходимости учетная запись может быть деактивирована.

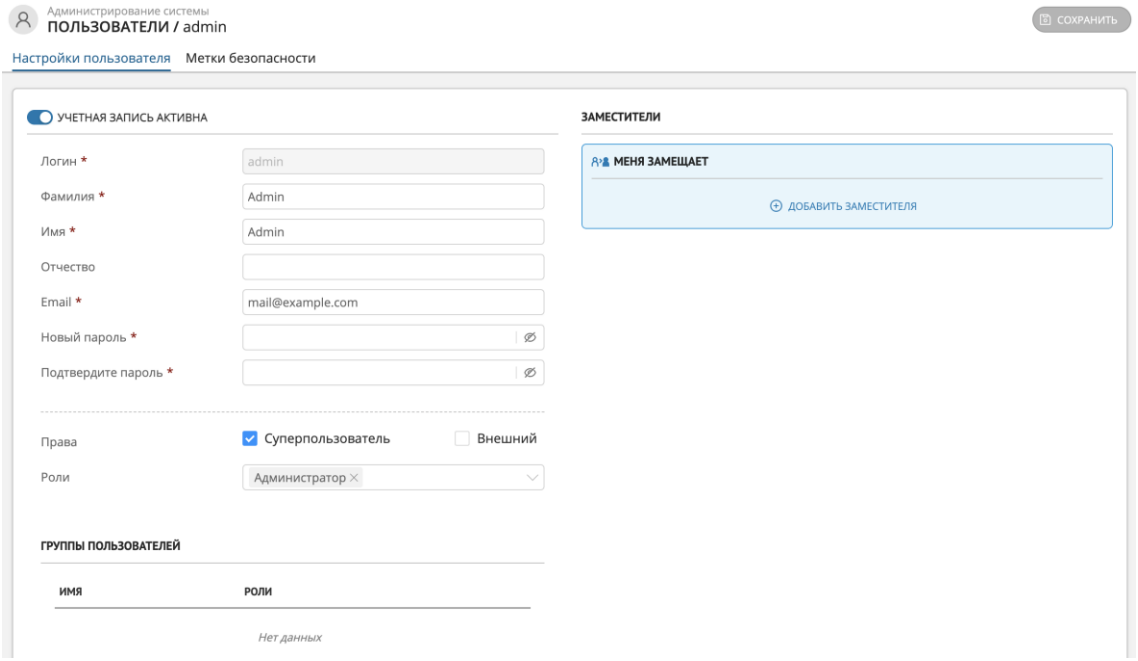


Рисунок 1 – Пример настройки параметров учетной записи

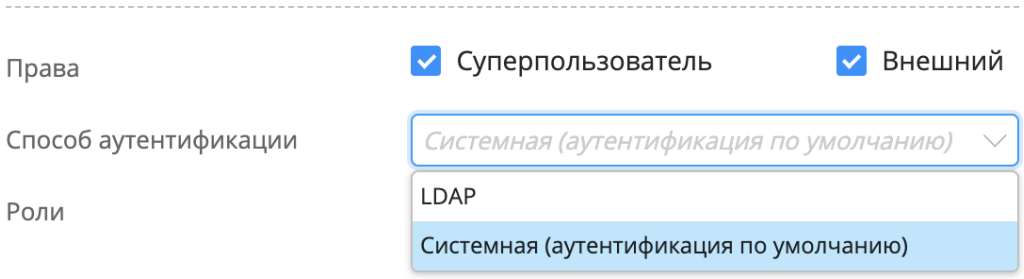


Рисунок 2 – Поле "Способ аутентификации"

2.2. Свойства учетной записи

Пользовательские свойства настраиваются в разделе "Пользователи", причем выполнение действий по настройке свойств ролей и пользователей может повлиять на работу последних.

Свойство	Описание	Комментарий
Активный	Признак	Если пользователь не активен, он не может

	активного пользователя	использовать систему. Может использоваться для временной деактивации учетных записей, например, для сотрудников в отпуске
Логин	Логин пользователя	Обязательное свойство. Логин пользователя должен быть уникальным и состоять из сочетания букв латинского алфавита с цифрами. Разрешенный формат: первый символ – буква; последующие символы – буквы, цифры. Логин также может содержать символы "-", "_", ".". Изменить логин существующего пользователя невозможно
Имя / Фамилия	Имя и фамилия пользователя	Обязательное свойство. Можно изменить после сохранения
Отчество	Отчество пользователя	Можно изменить после сохранения
Email	E-mail адрес пользователя	Обязательное свойство. Адрес электронной почты в общепринятом формате по RFC 2822
Пароль	Пароль учетной записи	Обязательное свойство. Необходим ввод и подтверждение пароля
Внешний	Признак внешнего пользователя	Если пользователь отмечен как внешний, то для его работы в системе Юниверс используются данные для входа во внешнюю систему (сторонний логин и пароль из внешней системы). При включении свойства появляется дополнительное поле "Способ аутентификации"
Способ аутентификации	Способ аутентификации внешнего пользователя	Поле появляется, если включен флаг "Внешний". Позволяет задать способ аутентификации в систему Юниверс через LDAP
Суперпользователь	Признак администратора системы	Система автоматически дает пользователю максимальные права на все объекты системы, вне зависимости от прочих настроек и назначенных ролей. Также пользователю доступна возможность замены лицензии системы в специальном режиме
Роли	Список ролей пользователя	Один пользователь может обладать несколькими ролями. В случае конфликта нескольких ролей итоговые права пользователя вычисляются как объединение прав заданных ролей, пересечение трактуется в сторону повышения прав
Информация о пользователе	Дополнительные свойства пользователя	Набор значений дополнительных свойств пользователей. Состав и количество полей настраиваются отдельно

2.3. Назначение меток учетной записи

Учетная запись получает метки безопасности от каждой из ролей, назначенных

пользователю в поле *Роли*. Такие метки безопасности находятся во вкладке *Метки безопасности* в секции *Заданы ролями*.

Помимо этого, учетной записи могут быть заданы собственные метки безопасности, при помощи которых расширяются права доступа к записям реестров/справочников.

Чтобы включить собственную метку безопасности для учетной записи:

1. Убедитесь, что учетная запись содержит минимум одну роль, имеющую минимум одну включенную метку безопасности.
2. Перейдите в закладку "Метки безопасности".
3. Нажмите на элемент **Выкл.** напротив требуемой метки для ее активации.
4. Нажмите ⊕ "Добавить значение", в результате чего станет доступен перечень атрибутов метки безопасности. Состав перечня зависит от того, как была настроена метка безопасности в соответствующем разделе, и содержать один или несколько атрибутов.
5. Укажите значение атрибутов в метке.
   - Если значение не указано, то оператору будут доступны все записи реестра/справочника, вне зависимости от того, какое значение принимает данный атрибут.
   - Если значение указано, то оператору будут доступны только те записи, у которых данный атрибут принимает указанное значение. Например, только физические лица с гражданством Российской Федерации.
   - Если метка безопасности содержит несколько атрибутов в перечне, то оператору будут доступны только те записи, которые подходят под все условия метки. Например, свечи зажигания с резьбой М12 и производителя DENSO.
6. При необходимости добавьте еще один перечень атрибутов метки безопасности.
   - Между перечнями атрибутов отображается разделитель "ИЛИ".
   - Если метка безопасности содержит несколько наборов, то оператору будут доступны записи, отвечающие условиям каждого набора. Например, 4 набора со значениями Philips, Polaris, Panasonic, Bosch позволяют оператору работать с записями указанных производителей.
7. После завершения всех настроек нажмите кнопку "Сохранить", расположенную в верхнем правом углу экрана.

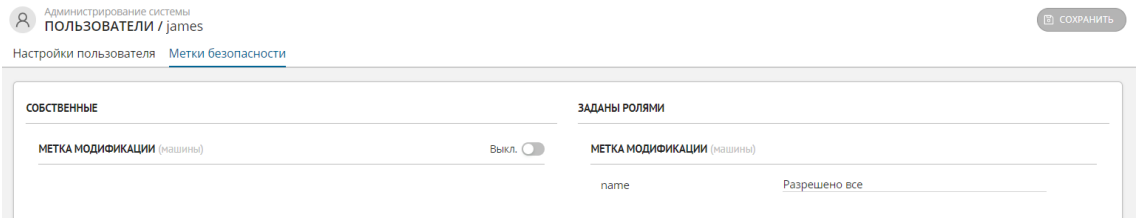


Рисунок 1 – Включение метки безопасности

2.4. Дополнительные параметры учетной записи

В системе Юниверс MDM предусмотрена настройка состава дополнительной информации о пользователе (например, отдел, должность и т.д.). Для этого:

- Нажмите кнопку "Настройка", расположенную в нижней части списка пользователей.
- В результате отобразится перечень дополнительных параметров в табличном виде (Рисунок 1).

Для создания дополнительного параметра:

- Нажмите кнопку *Добавить*.
- Укажите имя и отображаемое имя параметра.
- При необходимости: укажите параметр как обязательный (в таком случае параметр "только чтение" недоступен).
- При необходимости: укажите параметр как доступный только для чтения (в таком случае параметр "обязательный" недоступен).
- Нажмите кнопку "Сохранить".

Для редактирования дополнительного параметра:

- Наведите курсор на значение параметра и нажмите .
- Введите требуемое значение и нажмите "Сохранить".

Для удаления дополнительного параметра:

- В крайнем левом столбце отметьте флагами необходимые для удаления параметры.
- Нажмите кнопку *Удалить*.
- Сохраните изменения с помощью кнопки "Сохранить".

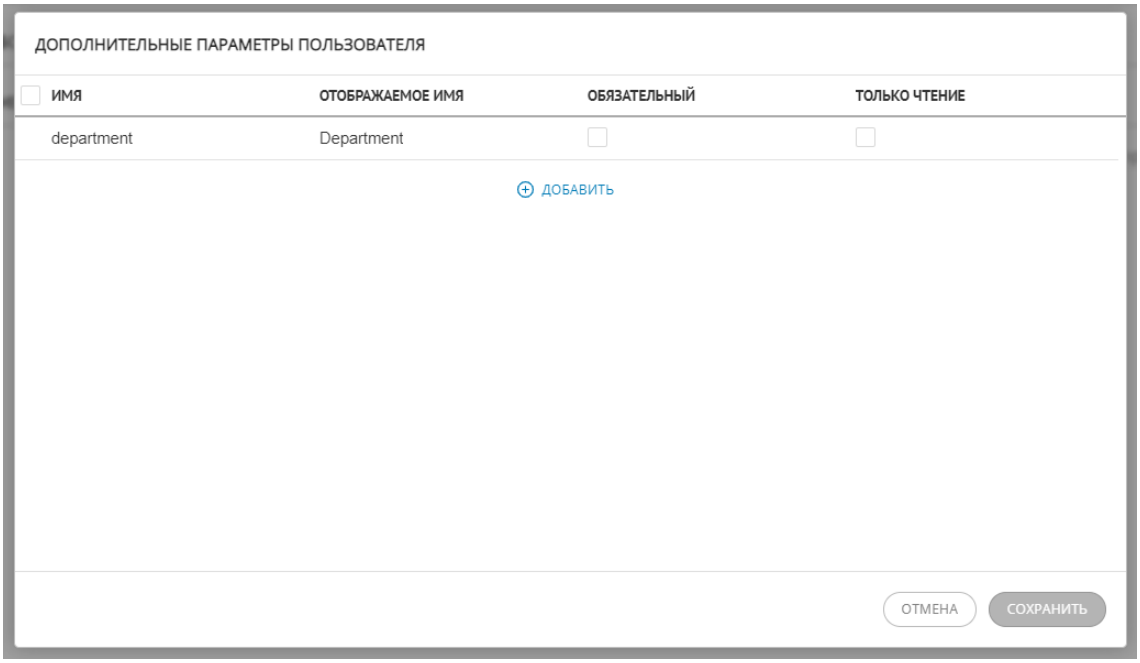


Рисунок 1 - Экран настройки дополнительных параметров пользователя

2.5. Замещение пользователей

В этой статье:

В системе Юниверс MDM предусмотрена возможность замещения пользователя на время его отсутствия, при этом пользователь-заместитель получает права и доступы того, кого он замещает.

Информация о замещениях отображается в разделе "Пользователи" (вкладка "Настройки пользователя"), в личном кабинете (вкладка "Заместители"), а также в разделе "Журнал".

Примечание:

Добавление заместителей доступно при включенном ресурсе "Администрирование замещений"

Совет:

Права пользователя-заместителя обновляются посредством операции, которая запускается ежедневно в 00:00, а также при старте системы. Исключение для пользователей, которым права передаются на текущую дату. Операции для таких пользователей запускаются при сохранении замещения

2.5.1. Создание замещения

Чтобы создать замещение пользователя:

1. Убедитесь, что открыт раздел "Пользователи" - вкладка "Настройки пользователя".
2. В правой части экрана в секции "Заместители" нажмите кнопку ⊕ "Добавить заместителя" (Рисунок 1).
3. В результате действия откроется модальное окно "Выбор заместителя" (Рисунок 2):
   - **Замещающий** - выберите пользователя из выпадающего списка, на которого назначаться права заместителя.
   - **Период замещения** - выберите дату начала и окончания замещения. Дата окончания не может быть раньше даты начала замещения, так же как и дата начала не может быть позже даты окончания замещения.
4. Нажмите *Добавить*.

Если текущий пользователь был назначен заместителем (другим пользователем) - замещение с наименованием "Я замещаю" также будет отображаться в секции "Заместители" *только для чтения* (Рисунок 3)

При наведении курсора на имя пользователя отобразится всплывающая подсказка с детальной информацией:

- Об учетной записи пользователя, которого будет замещать текущий пользователь - в секции "Я замещаю" (Рисунок 4).
- Об учетной записи пользователя, который замещает текущего пользователя (в секции "Меня замещает").

2.5.2. Удаление замещения

Чтобы удалить замещение:

1. Нажмите кнопку 🗑 "Удалить замещение", расположенную в конце строки с информацией о заместителе.
2. Подтвердите действие.

Примечания:

- Для неактивных пользователей блокируется возможность создания/редактирования замещений.
- Если в качестве заместителя указан пользователь, впоследствии ставший неактивным, то на экране в секции "Заместители" отобразится

соответствующее предупреждение.

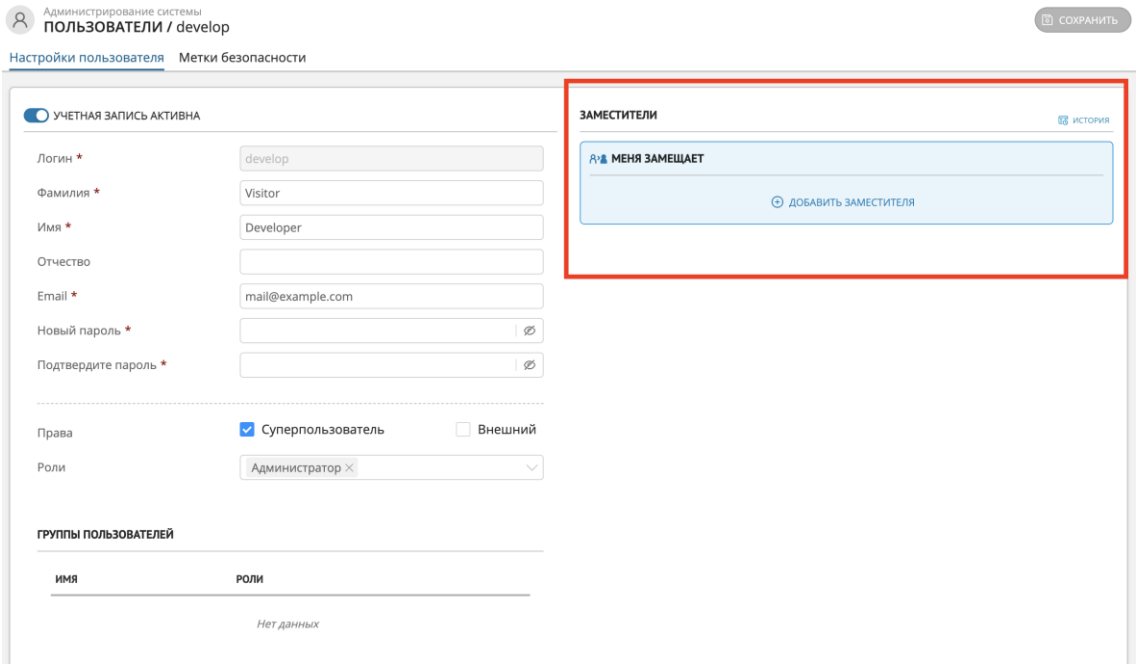


Рисунок 1 - Вкладка "Настройки пользователя" - секция "Заместители"

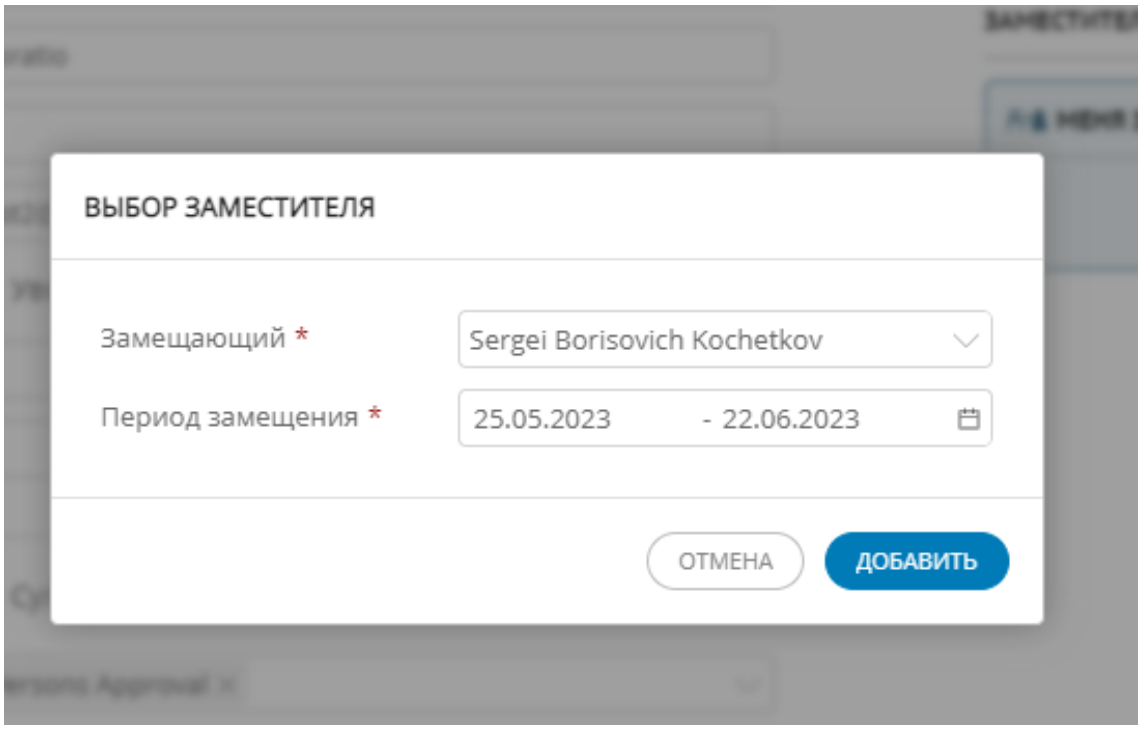


Рисунок 2 - Модальное окно "Выбор заместителя"

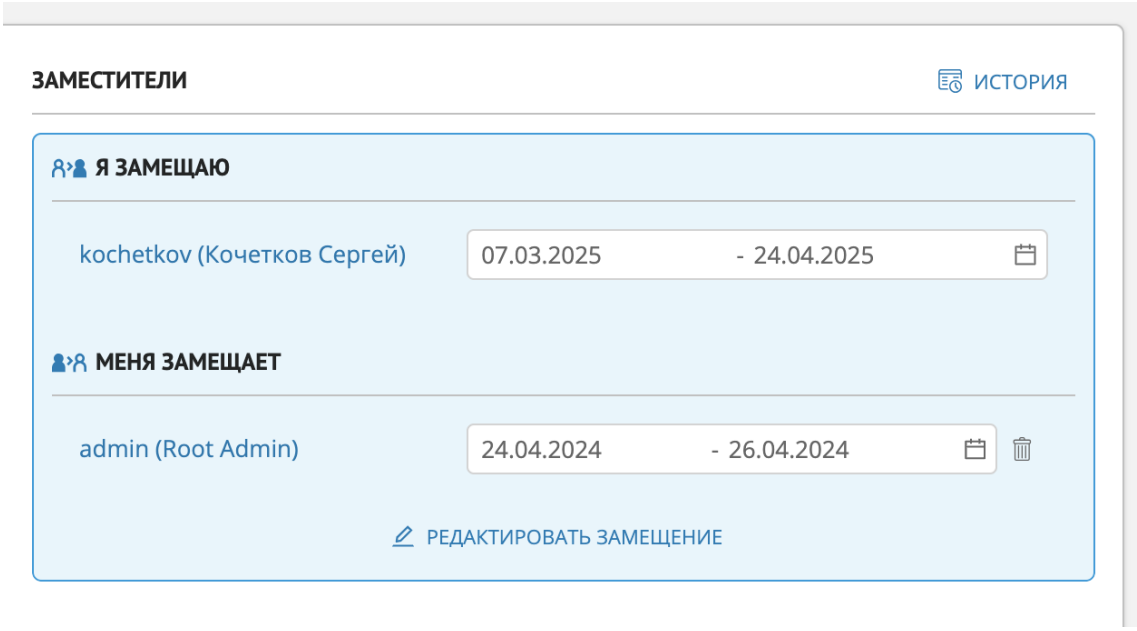


Рисунок 3 - Секция "Заместители" с информацией о том, кого замещает текущий пользователь

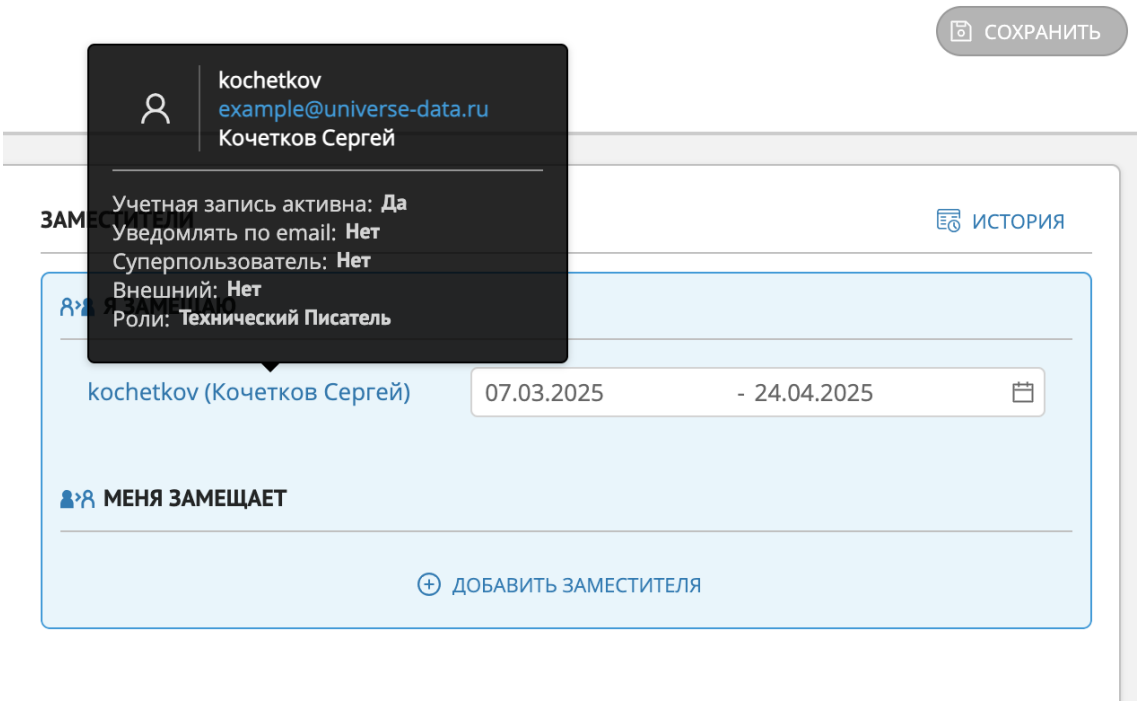


Рисунок 4 - Пример отображения всплывающей подсказки в секции "Я замещаю"

2.5.3. Просмотр истории замещений

Просмотр истории замещений доступен в 2 вариантах:

- Просмотр истории замещений **выбранного пользователя** осуществляется с

помощью кнопки "История" справа от заголовка "Заместители". Также просмотр окна доступен в настройках аккаунта.

- Просмотр истории **всех замещений** с помощью кнопки "История замещений" внизу списка всех пользователей (справа от кнопки создания нового пользователя).

2.5.3.1. История замещений отдельного пользователя

Переход к истории замещений осуществляется с помощью кнопки "История" справа от заголовка "Заместители".

По умолчанию открывается экран с пользователями, которых замещает текущий пользователь. Для перехода на экран с информацией о пользователях, которые замещают текущего (Рисунок 5), используйте переключатель "Я замещаю" в правом верхнем углу окна.

Замещения отображаются в виде таблицы со столбцами: имя замещаемого/заместителя, период замещения и статус.

Для столбцов "Период замещения" и "Статус" доступна фильтрация:

- Нажмите на кнопку справа от заголовка столбца.
- Выберите нужный период или значение статуса ("Активный" - в процессе замещения; "Завершенный" - процесс замещения уже завершен) и нажмите *Применить*.

Рисунок 5 - Пример отображения истории замещений отдельного пользователя

2.5.3.2. Просмотр истории всех замещений

Просмотр окна истории всех замещений, а также кнопка перехода к окну, доступны пользователям с включенным правом "Администрирование замещений пользователей" на чтение. В противном случае отображаются только те замещения, для которых текущий пользователь является замещающим/замещаемым/создателем замещения.

Замещения отображаются в виде таблицы со столбцами: кто и кого замещает, период замещения и статус (Рисунок 6).

Для столбцов таблицы доступна фильтрация:

- Нажмите на кнопку  справа от заголовка столбца.
- Выберите нужного пользователя, период или значение статуса ("Активный" - в процессе замещения; "Завершенный" - процесс замещения уже завершен) и нажмите *Применить*.

Замещения, еще не вступившие в силу (т.е. назначенные на будущие даты), считаются отложенными. На UI этот статус не отображается, при этом в карточке пользователя такие замещения отображаются как активные. В истории замещений отображаются только активные и завершенные замещения.

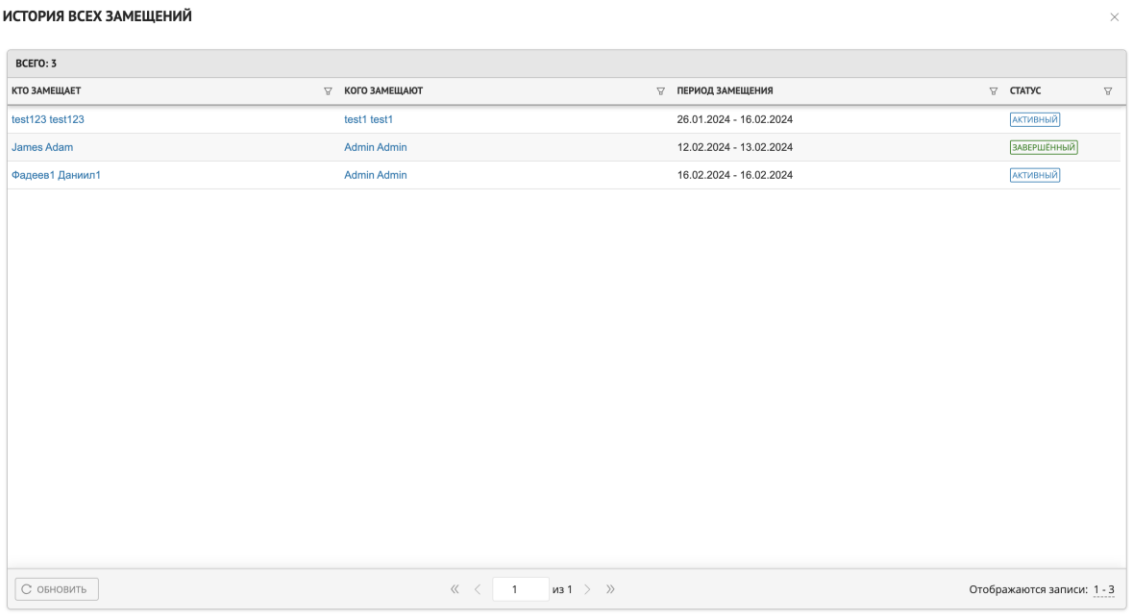


Рисунок 6 - Пример отображения окна истории всех замещений

3. Роли

Примечание:

Управление ролями доступно пользователям, имеющим соответствующие права доступа. В новой системе это Суперпользователь

Содержание:

3.1. Создание, редактирование и удаление ролей

Чтобы создать роль:

1. Перейдите в раздел "Роли", если это не сделано ранее.
2. Нажмите кнопку ⊕ *Создать*, расположенную в нижней части списка ролей.
3. В результате действия откроется окно создания новой роли (Рисунок 1).
4. По умолчанию открыта закладка "Настройка". Оставайтесь в ней.
5. Заполните секцию *Информация о роли*:
   - **Название** и **Отображаемое название**. Название роли должно быть уникальным и состоять из букв латинского алфавита; может содержать цифры, символы "-", "_".
   - Секция "**Дополнительно**": отдельные поля могут быть *обязательными* для заполнения или доступными *только для чтения* в зависимости от настройки.
6. Включите необходимые метки безопасности и укажите значения атрибутов.
7. Перейдите на закладку "Права доступа" (Рисунок 2).
8. Установите необходимые права доступа к ресурсам системы.
9. Нажмите кнопку *Сохранить*, расположенную в верхнем правом углу экрана, чтобы применить изменения.
   - Название нельзя изменить после первого сохранения роли.

Примечание:

Переход в другой раздел или обновление страницы в браузере может

привести к потере несохраненных данных

Чтобы отредактировать роль:

1. Выберите необходимую роль из списка существующих.
2. Внесите изменения.
   - Название нельзя изменить после первого сохранения роли.
3. Нажмите кнопку *Сохранить*, расположенную в верхнем правом углу экрана, чтобы внести изменения.

Если ранее были добавлены обязательные поля в информации о роли, то требуется заполнить эти поля для сохранения.

Чтобы удалить роль:

1. Выберите необходимую роль из списка существующих.
2. Нажмите кнопку *Удалить*, расположенную в верхнем правом углу экрана.
3. Подтвердите действие в диалоговом окне.

Примечание:

- При удалении роли, на которую назначены пользователи, в диалоговом окне отобразиться уведомление с предупреждением (Рисунок 3).

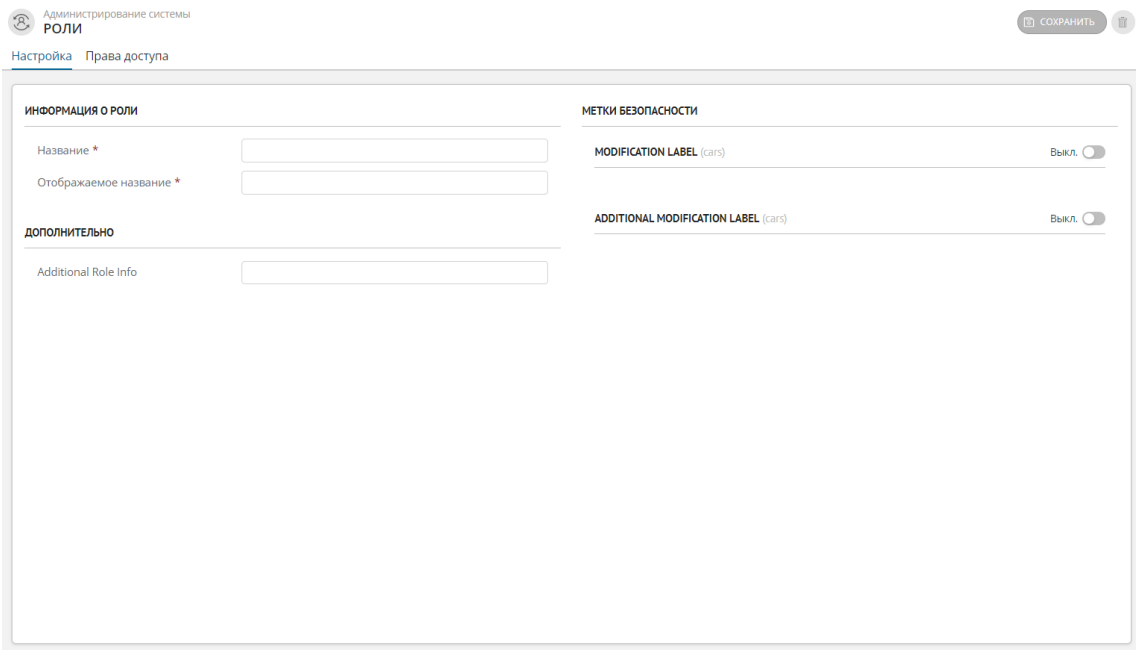


Рисунок 1 – Экран настройки свойств роли

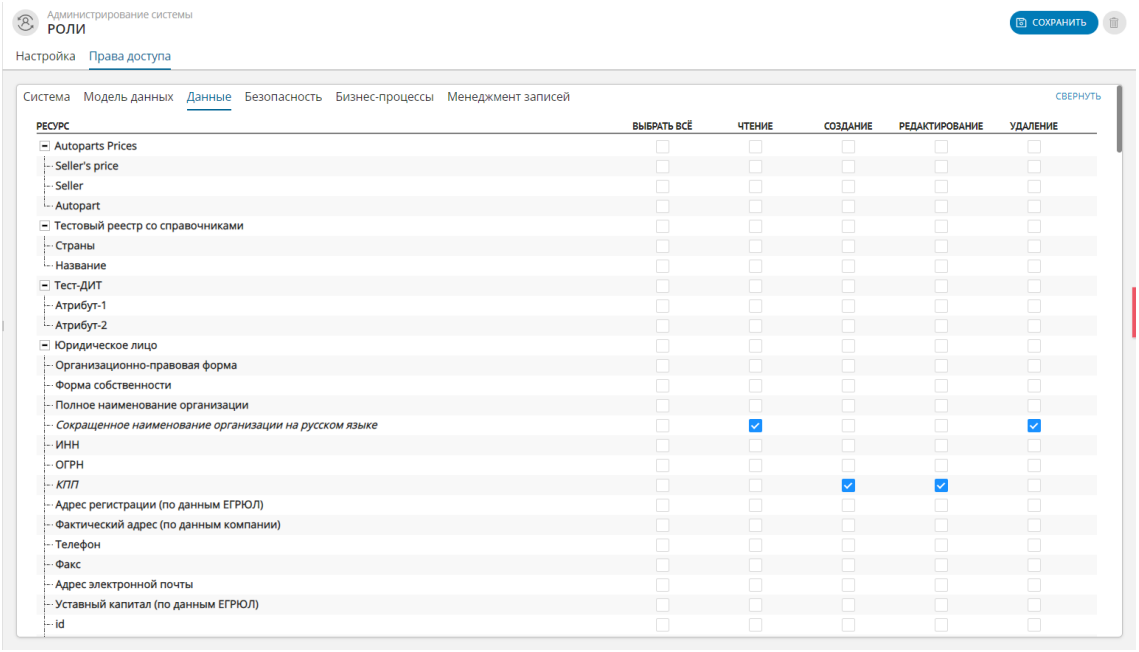


Рисунок 2 – Закладка настройки прав доступа

Уведомление при удалении роли с назначенным на нее пользователем

Рисунок 3 – Уведомление при удалении роли с назначенным на нее пользователем

3.2. Описание прав системы

Права доступа настраиваются в разделе "Роли" → закладка "Права доступа".

Права указываются для каждой категории прав отдельно.

> **Совет:**
>
> Применение прав распространяется по иерархии сверху вниз: права могут задаваться глобально на любом уровне (такой уровень будет считаться родительским), а переопределяться - на дочернем.

Блоки прав:

- Система
- Модель данных
- Данные
- Классификаторы
- Безопасность
- Бизнес-процессы
- Менеджмент записей

3.2.1. Система

Группа прав **Администрирование системы** определяет доступ к:

- Разделу "Библиотеки" (переопределяется правом **Библиотеки**);
- Разделу "Потоки выполнения" (переопределяется правом **Потоки выполнения**);
- Разделу "Журнал" (переопределяется правом **Управление журналом аудита**);
- Разделу "Параметры системы" (переопределяется правом **Параметры системы**);
- Разделу "Операции" (переопределяется правом **Операции**);
- Запуску операций (переопределяется правом **Запуск операций** при условии, что включено право **Операции** на чтение);
- Колонкам по умолчанию, которые будут использованы в выдаче таблицы результатов поиска.
- Разделу "Каталог доступа" (переопределяется правом **Каталог доступа**).

Доступные виды прав:

- **Полные**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).

3.2.2. Модель данных

Примечание:
При настройке прав на модель данных ознакомьтесь с примечаниями

Группа прав **Администрирование моделей** определяет доступ к:

1. Группе **Администрирование модели качества данных**. Определяет доступ к разделу "Качество данных". Вложенные ресурсы определяют доступ к:
   - Закладке "Правила качества" (определяется правом: **Категории**, **Правила качества**, **Функции**)
   - Закладке "Наборы правил" (определяется ресурсами: **Категории**, **Наборы правил**, **Правила качества**, **Функции**)
   - Закладке "Назначения" (определяется ресурсами: **Категории**, **Наборы правил**, **Назначения**, **Правила**, **Функции**)
   - Закладке "Функции" (определяется ресурсом **Функции**)
   - Закладке "Фазы выполнения" (определяется ресурсами: **Категории**, **Наборы правил**, **Назначения**, **Правила**, **Функции**)
   - Закладке "Категории правил качества" (определяется ресурсом

Категории)

2. Праву **Администрирование модели правил сопоставления**. Определяет доступ к редактированию правил сопоставления.
3. Право **Модель данных** определяет доступ к:
   - Разделу "Модель данных";
   - Разделу "Источники данных";
   - Разделу "Единицы измерения";
   - Разделу "Перечисления";
   - Разделу "Импорт/экспорт".
4. Право **Администрирование модели бизнес-процессов** определяет доступ к разделу "Бизнес-процессы".
5. Право **Администрирование модели классификаторов** определяет доступ к разделу "Классификаторы". Учитывает права, предоставленные во вкладке "Классификаторы". В списке классификаторов пользователю будут доступны только те классификаторы, к которым предоставлен доступ.
   - **Полные**: совокупность прав на Чтение + Редактирование
   - **Чтение**: определяет доступ к разделу "Классификаторы", а также просмотр метаинформации, версий и узлов и экспорт классификаторов.
   - **Редактирование**: определяет доступ к редактированию метаинформации, версий и узлов и импорту классификаторов. Создание нового классификатора доступно, если предоставлен доступ на редактирование верхнего уровня во вкладке "Классификаторы".

Примечания:

- Права на закладки в разделе "Правила качества" взаимосвязаны между собой, поэтому доступ к определенной закладке определяется сразу несколькими правами доступа.
- Чтобы пользователь мог создавать правила качества данных, он должен иметь права: **Модель данных** (чтение) и **Администрирование модели качества данных** (полные права). Если нет прав **Модель данных** (чтение), то в расширенном режиме не будут видны реестры / справочники, кроме существующих назначений; в простом режиме не будут видны реестры / справочники.
- Для редактирования **фаз выполнения** необходимо право на изменение ресурса "Администрирование модели качества данных".
- Для доступа к **простому режиму создания правил** необходимо иметь права на чтение и обновление ресурса "Администрирование модели качества

данных".
- Для импорта модели качества данных: право на изменение ресурса "Администрирование модели качества данных".
- Для экспорта модели качества данных: право на чтение ресурса "Администрирование модели качества данных".

Доступные виды прав:

- **Выбрать все**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).
- **Чтение**: просмотр существующих объектов.
- **Редактирование**: редактирование существующих объектов. Убедитесь, что включено право на чтение.

3.2.3. Данные

Группа прав **Данные** настраивает права доступа для каждого реестра/справочника отдельно. Также доступна настройка прав на каждый атрибут реестра/справочника.

Доступные виды прав на реестр/справочник:

- **Выбрать все**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).
- **Чтение**: просмотр существующих объектов.
- **Создание**: создание новых объектов. Убедитесь, что включено право на чтение.
- **Редактирование**: редактирование существующих объектов. Убедитесь, что включено право на чтение.
- **Удаление**: удаление существующих объектов. Убедитесь, что включено право на чтение.

Доступные виды прав на атрибуты:

- **Выбрать все**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).
- **Чтение**: просмотр атрибута в карточке записи.
- **Создание**: возможность заполнить атрибут для новой записи, которая еще не опубликована. Убедитесь, что включено право на чтение.
- **Редактирование**: возможность редактировать атрибут для записи, которая уже опубликована. Атрибут для новой записи при этом заполнять нельзя. Это право также позволяет удалять значения атрибутов. Убедитесь, что включено

право на чтение.
- **Удаление** не работает для атрибутов.

Если права доступа не назначены на реестр/справочник (а права назначены только на атрибуты), то у пользователя не будет прав на этот реестр/справочник.

3.2.4. Классификаторы

Группа прав **Классификаторы** настраивает права доступа для каждого классификатора отдельно.

Права верхнего уровня (родительский уровень "Классификаторы"):

- Предоставляют права на все дочерние элементы. Если выбраны права на чтение на верхнем уровне, автоматически добавляются права на чтение при создании нового классификатора.
- Дают доступ на создание и импорт новых классификаторов (если во вкладке "Модель данных" предоставлен доступ на редактирование к *Администрированию модели классификаторов*).

Права дочернего уровня (по именам классификаторов):

- **Выбрать все**: совокупность прав на Чтение + Редактирование.
- **Чтение**: предоставляет права на выбор узлов классификатора в карточке записи (вкладка "Классификация").
- **Редактирование**: предоставляет права на редактирование и импорт выбранного классификатора, его версий и узлов (если во вкладке "Модель данных" предоставлен доступ на редактирование к *Администрированию модели классификаторов*).

Примечания:

- Поиск и редактирование классификатора доступны, если есть право *Администрирование модели классификаторов* на чтение + редактирование и на конкретный классификатор (права только на конкретный классификатор не дают возможности его редактировать).
- Права только на чтение конкретных классификаторов без права *Администрирование модели классификаторов* дают возможность: видеть информацию в записях во вкладке "Классификация", которая относится только к доступным классификаторам; а также возможность добавлять/удалять эту информацию при наличии необходимых прав на редактирование записи.
- Вкладка "Назначения" активна всегда. Если у пользователя нет прав на

чтение модели данных, просмотр вкладки будет ограничен.

3.2.5. Безопасность

Группа прав **Администрирование подсистемы безопасности** определяет доступ к:

- Разделу "Пользователи" (переопределяется правом **Пользователи**). Право на чтение не дает доступ к разделу Пользователи;
- Разделу "Роли" (переопределяется правом **Роли** при условии, что включено право **Метки безопасности** на чтение).
- Разделу "Метки безопасности" (переопределяется правом **Метки безопасности**);
- Функции "Замещение пользователей" в разделе "Пользователи" (переопределяется правом **Администрирование замещений пользователей**);
- Разделу "Группы пользователей" (переопределяется правом **Группы пользователей**):
  - Право на *чтение* предоставляет доступ к разделу "Группы пользователей".
  - Право на *редактирование* предоставляет доступ к созданию групп, изменению пользователей в группах, добавлению ролей на группу, удалению группы. Группы, пришедшие из LDAP, не редактируются, но доступно добавление ролей и пользователей.
  - Пользователь с доступом к редактированию Групп, Ролей, Пользователей и Меток безопасности может редактировать свои группы, роли, учетную запись.

Доступные виды прав:

- **Выбрать все**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).
- **Чтение**: просмотр существующих объектов.
- **Редактирование**: редактирование существующих объектов.

3.2.6. Бизнес-процессы

Группа прав **Бизнес-процессы** настраивает права на действия для каждого бизнес-процесса.

- **Удаление процесса**. Право дает доступ на удаление бизнес-процессов.

Также у каждого существующего процесса есть список отдельных прав:

- **Процессы** - работа с процессами (в закладке "Процессы" раздела "Задачи");
- **Задачи** - работа с задачами (в закладке "Задачи" раздела "Задачи");
- **Выбор исполнителя** - выбор исполнителя конкретной задачи;
- **Переназначение задач** - переназначение задач на себя или других пользователей;
- **Редактирование комментариев и вложений**.

Доступные виды прав. **Полные**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).

3.2.7. Менеджмент записей

Группа прав **Менеджмент записей** определяет доступ к:

- Отключению лимита на пакетные операции (переопределяется правом **Отключить лимит на пакетные операции с записями**). Отменяет ограничение оператору данных на единовременную обработку до 30 записей за операцию.
- Просмотру истории записи в карточке записи (переопределяется правом **История записи**);
- Разделу "Дубликаты" (переопределяется правом **Дубликаты**):
    - *Полные* права предоставляют доступ к работе с разделом "Дубликаты", а также к возможности сравнивать и объединять дубликаты записей.
    - Доступ к дублирующимся записям регулируется через группу прав "Данные"
- Просмотру истории консолидации в карточке записи (переопределяется правом **История консолидации**);
- Возможности физически удалять записи (переопределяется правом **Физическое удаление**).

Группа прав **пользовательские пакетные операции** определяет доступ к:

- Импорту записей;
- Экспорту записей;
- Модификации записей;
- Удалению записей.
    - При отсутствии прав - соответствующие действия ("Импорт", "Экспорт", "Модификация", "Удаление") будут неактивны.

Доступные виды прав. **Полные**: совокупность всех доступных прав. Автоматически включает права на создание, чтение, редактирование и удаление (если есть).

3.3. Назначение меток ролям

В секции *Метки безопасности* доступен перечень существующих меток, которые можно включать и настраивать для каждой отдельной роли (категории пользователей). Метки создаются и редактируются в соответствующем разделе.

Чтобы включить метку безопасности для роли:

1. Выберите требуемую роль, если это не сделано ранее.
2. Нажмите на элемент *Выкл.* напротив метки безопасности, которую требуется активировать.
3. В результате действия метка будет включена для текущей роли.
4. Нажмите кнопку ⊕ "Добавить значение" под названием включенной метки (Рисунок 1).
5. В результате действия станет доступен перечень атрибутов метки безопасности. Состав перечня зависит от того, как была настроена метка безопасности в соответствующем разделе, и содержит один или несколько атрибутов.
6. При необходимости: укажите значение атрибутов в метке.
   - Если значение не указано, то оператору будут доступны все записи реестра/справочника, вне зависимости от того, какое значение принимает данный атрибут.
   - Если значение указано, то оператору будут доступны только те записи, у которых данный атрибут принимает указанное значение. Например, только физические лица с гражданством Дании.
   - Если метка безопасности содержит несколько атрибутов в перечне, то оператору будут доступны только те записи, которые подходят под все условия метки. Например, свечи зажигания с резьбой M12 и производителя DENSO.
7. При необходимости: нажмите "Добавить значение" повторно, чтобы добавить еще один перечень атрибутов метки безопасности.
   - Между перечнями атрибутов отображается разделитель "ИЛИ".
   - Если метка безопасности содержит несколько наборов, то оператору будут доступны записи, отвечающие условиям каждого набора.

Например, 4 набора со значениями Philips, Polaris, Panasonic, Bosch позволяют оператору работать с записями указанных производителей.

8. После завершения всех настроек нажмите кнопку *Сохранить*, расположенную в верхнем правом углу экрана.

Примечания:

- Ограничения на доступ к данным расширяются метками безопасности от учетной записи и от ролей.
- Ограничения по одному атрибуту расширяют доступ к записям с указанными значениями атрибута. Например, если в метке1 (назначенной на роль) указан материал: сталь; в метке2 (назначенной на роль) указан материал: дерево, и в метке3 (назначенной на учетную запись) указан материал: пластик, то пользователю доступны записи со всеми указанными типами материала.
- Ограничения по разным атрибутам реестра/справочника дополняют условия доступа к записи. Например, записей с атрибутом "Материал: Сталь" будет найдено 8620, а записей с атрибутами "Материал: Сталь" и "Марка стали: 60С2А" всего 206.
- В случае если учетная запись получает права от меток безопасности, регулирующих разные реестры/справочники, то увеличивается список доступных атрибутов реестров/справочников.

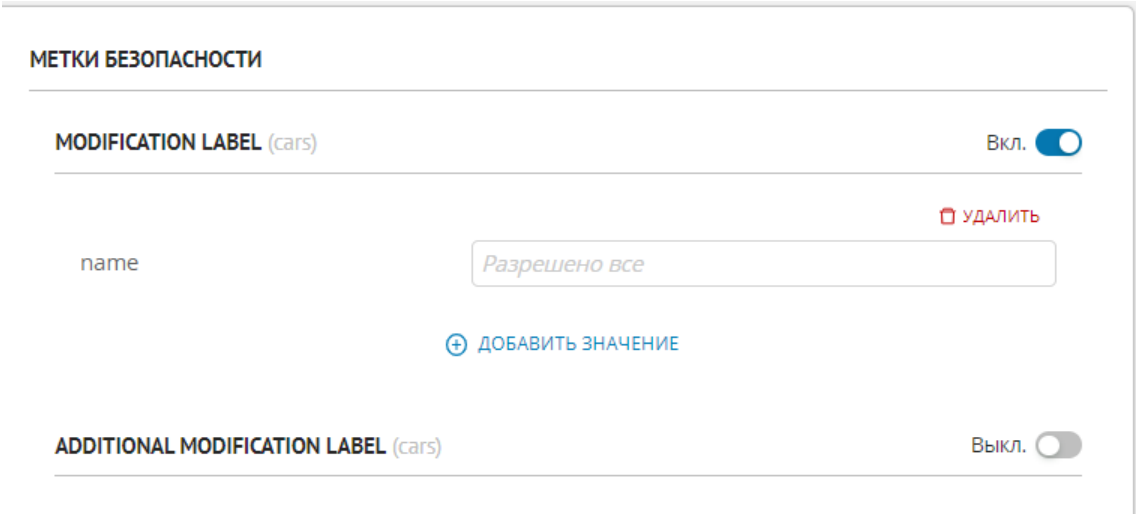


Рисунок 1 – Включение метки безопасности

3.4. Дополнительные параметры ролей

Для того, чтобы перейти к настройке дополнительных параметров роли (например, добавить поля для указания департамента, отдела и т.д.), выполните действия:

1. Нажмите кнопку "Настройка", расположенную в нижней части списка ролей.
2. В результате отобразится перечень дополнительных параметров в табличном виде (Рисунок 1).

Для создания дополнительного параметра:

1. Нажмите кнопку *Добавить*.
2. Укажите имя и отображаемое имя параметра.
3. При необходимости: укажите параметр как обязательный (в таком случае параметр "только чтение" недоступен).
4. При необходимости: укажите параметр как доступный только для чтения (в таком случае параметр "обязательный" недоступен).
5. Нажмите кнопку "Сохранить".

Для редактирования дополнительного параметра:

- Наведите курсор на значение параметра и нажмите .
- Введите требуемое значение и нажмите "Сохранить".

Для удаления дополнительного параметра:

- В крайнем левом столбце отметьте флагами необходимые для удаления параметры.
- Нажмите кнопку *Удалить*.
- Сохраните изменения с помощью кнопки "Сохранить".

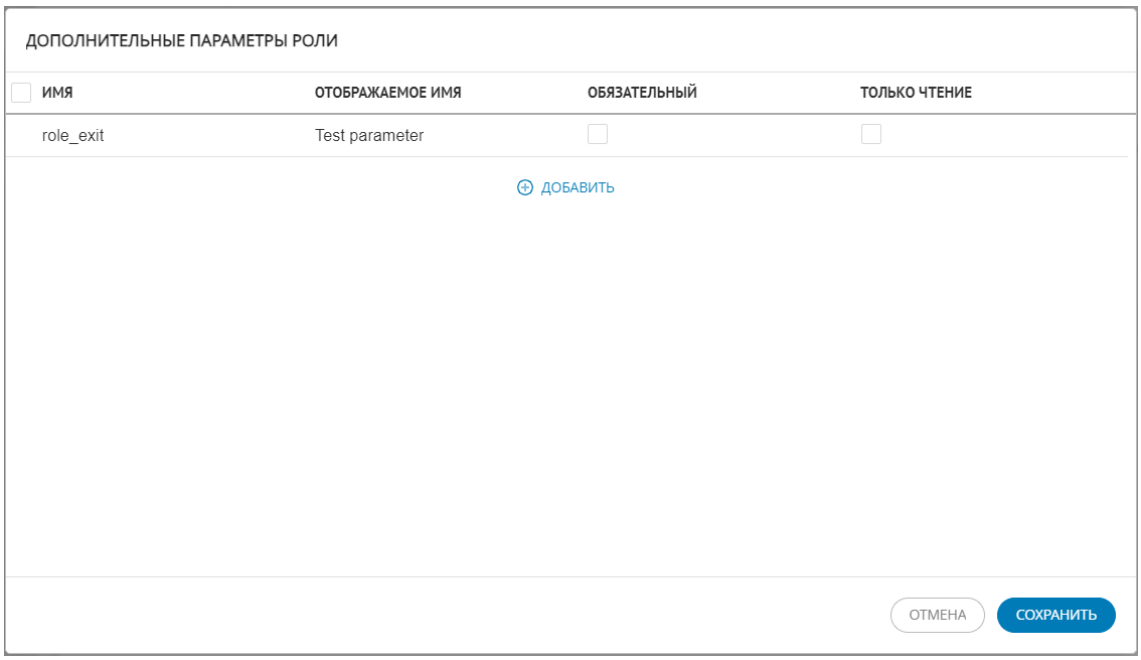


Рисунок 1 - Настройка дополнительных параметров роли

3.5. Настройка роли для гостевого доступа

Гостевой доступ позволяет просматривать некоторые реестры/справочники без входа в систему. Гостю доступны разделы "Главная" и "Данные".

Доступ к данным реализуется через специальную роль.

За настройку гостевого доступа отвечают следующие **параметры в backend.properties**:

- com.unidata.mdm.ee.guest.mode=${GUEST_MODE:false} - *гостевой доступ отключен при {GUEST_MODE:false}*
- com.unidata.mdm.ee.guest.role=${GUEST_ROLE:guest}
- com.unidata.mdm.ee.guest.username=${GUEST_USERNAME:guest}
- com.unidata.mdm.ee.guest.password=${GUEST_PASSWORD:guest}

По умолчанию гостевой доступ выключен. Чтобы его включить, измените значение параметра com.unidata.mdm.ee.guest.mode на {GUEST_MODE:true}. Это можно сделать перед первым запуском docker-образа или в любой момент после. При изменении параметров backend.properties необходимо перезапустить систему.

Остальные параметры гостевого доступа меняются при тех же условиях с последующей перезагрузкой системы.

Чтобы настроить гостевой доступ:

1. Перейдите в раздел "Роли".
2. Откройте роль guest (имя роли соответствует com.unidata.mdm.ee.guest.role). Роль создана автоматически.
3. Настройте права доступа для роли. Можно регулировать только права на *просмотр* реестров/справочников и их отдельных атрибутов. При попытке добавить права доступа к другим разделам и функциям будет выдана ошибка.
4. Сохраните роль. Нажмите "Сохранить" в правом верхнем углу экрана.

Чтобы просмотреть текущие настройки гостевого доступа:

1. Перейдите в раздел "Параметры системы".
2. Найдите набор настроек "Параметры гостевого режима".

Примечание:
В разделе "Параметры системы" настройки недоступны для редактирования

4. Метки безопасности

Содержание:

4.1. Метки безопасности

4.1.1. Описание

Метки безопасности ограничивают пользователя при работе с объектами. Метка используется для разграничения прав доступа к данным в пределах одного реестра/справочника и представляет собой проверяемый набор атрибутов реестра.

Пользователю, к роли которого назначена метка, указывается список разрешенных значений атрибутов. Пользователь может работать только с записями реестра, значение атрибутов которых совпадает с разрешенными.

Метки используются только для атрибутов следующих типов:

- Строковый,
- Целочисленный,
- Ссылка на справочник.

4.1.2. Ограничение доступа с помощью меток

Логика ограничений доступа к данным:

- Если в метке участвуют несколько атрибутов, то пользователь видит записи, в которых значение указанных атрибутов совпадает с разрешенными значениями, настроенными для пользователя (т.е. внутри метки действует логическое "И").
- Если для пользователя настроено несколько экземпляров одной метки, то пользователь видит записи, целиком удовлетворяющие одному из экземпляров меток (т.е. между метками действует логическое "ИЛИ").
- Если для пользователя настроено несколько разных меток, то пользователь видит записи, удовлетворяющие всем меткам (т.е. логическое "И" между метками). При этом внутри меток действуют правила 1 и 2.

Под ограничением в доступе следует понимать:

- Поисковые запросы возвращают только данные, удовлетворяющие меткам.

4.1.3. Порядок назначения меток безопасности

Для настройки и последующего назначения меток безопасности:

1. Создать метки безопасности.
2. В разделе "Роли" назначить набор меток на выбранную роль.
3. В разделе "Пользователи" назначить роль на необходимого пользователя.
4. Включить метки безопасности для учетной записи.

4.2. Управление метками безопасности

4.2.1. Создание метки безопасности

Чтобы создать метку безопасности:

1. Перейдите в раздел "Метки безопасности", если это не сделано ранее.
2. Нажмите кнопку ⊕ *Создать*, расположенную в нижней части списка меток.
3. В результате действия в рабочей области отобразится перечень параметров метки.
4. Укажите название и отображаемое название метки. При необходимости добавьте описание метки.
5. Выберите реестр/справочник, на котором будет работать метка[1].
6. Укажите один или несколько атрибутов выбранного реестра/справочника.
   - Метки используются только для атрибутов: Строковый, Целочисленный, Ссылка на справочник.
   - В разделах "Роли" и "Пользователи" для указанных атрибутов можно будет добавить разрешенные значения.
7. Сохраните метку. Нажмите кнопку 💾 "Сохранить", расположенную в правом верхнем углу экрана.

Обновление страницы в браузере может привести к потере несохраненных данных.

Примечания:

- Работа меток безопасности для иерархических справочников не предусмотрена.

Чтобы отредактировать ранее созданную метку:

1. Выберите необходимую метку из списка существующих.

2. Введите требуемые значения свойств.
3. Нажмите  "Сохранить".

Чтобы удалить метку безопасности:

1. Выберите необходимую метку.
2. Нажмите кнопку  *Удалить*, расположенную в правом верхнем углу экрана.
3. Подтвердите действие.

Если для разных атрибутов одного реестра/справочника необходимо установить разное количество допустимых значений, то рекомендуется создавать несколько меток безопасности на один реестр/справочник.

4.2.2. Свойства метки безопасности

№	Свойство	Описание	Комментарий
1	Название	Логическое имя метки	Имя метки должно быть уникальным и состоять из сочетания букв латинского алфавита с цифрами, первый символ - всегда буква. Допустимы символы "-", "_". Изменить имя существующей метки невозможно
2	Отображаемое название	Отображаемое имя метки	Используется для отображения в интерфейсе. Может состоять из сочетания произвольного набора букв кириллического и латинского алфавита с цифрами
3	Описание	Текстовое описание метки	Дополнительная информация о метке
4	Объект модели	Реестр/справочник, для которого настраивается метка	Реестр/справочник, для которого создается метка
5	Атрибутивный состав	Набор атрибутов реестра/справочника, участвующих в метке	Возможно задание нескольких полей для одной метки

Пользователю доступны для просмотра только те записи, которые полностью удовлетворяют меткам безопасности. В случае, если доступ к записи определяется сразу несколькими метками, то такая запись будет доступна пользователю только при условии, что условия для каждой метки совпадают. Например, если заданы метки на атрибут "тип материала" со значением "дуб" и атрибут "вид изделия" со значением "доска", то пользователю будут доступны записи, в которых оба атрибута содержат заданные условия.

Если запись не соответствует хотя бы одной метке, то такая запись недоступна.

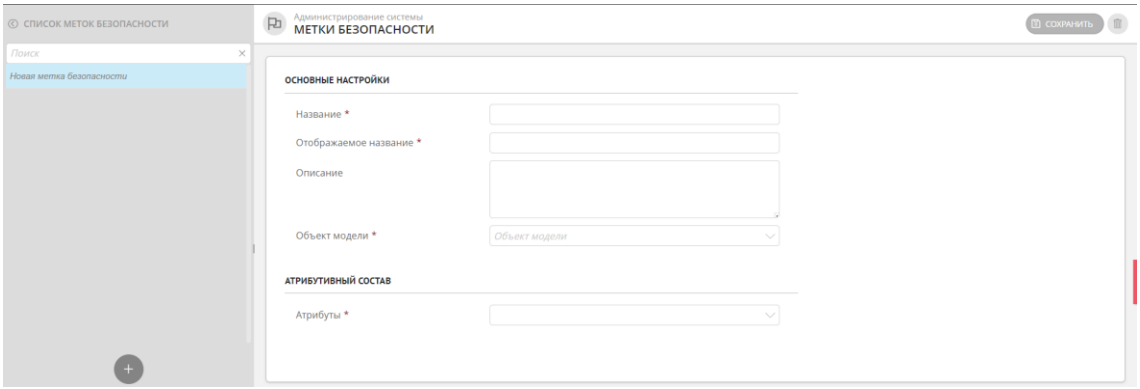


Рисунок 1 – Общий вид раздела

5. Группы пользователей

Группы пользователей предназначены для настройки прав доступа с помощью объединения различных пользователей в группы. Также группы могут содержать в себе подгруппы, которые наследуют настройки ролей от родительской.

Порядок расположения дочерних групп внутри родительской можно изменить с помощью удерживания строки нужной группы и ее перемещения вверх/вниз.

> Примечание:
>
> Раздел "Группы пользователей" доступен для работы, если пользователю назначена роль с правом *Группы пользователей*

5.1. Создание группы

Чтобы создать группу:

1. Перейдите в раздел "Группы пользователей".
2. Наведите курсор на строку корневой группы и нажмите ⊕ "Добавить вложенную группу".
3. Введите имя новой группы и нажмите Enter.
4. В результате действия отобразится экран настроек группы (Рисунок 1).
5. В секции *"Основные настройки"* заполните основные параметры:
   - **Отображаемое имя**. Обязательный. Имя группы для отображения в интерфейсе.
   - **Описание**. Дополнительное описание группы.
   - **Внешний**. Флаг проставляется автоматически, если группа была загружена из внешней системы. Внешние группы недоступны для удаления.
   - **Способ авторизации**. Выпадающий список, в котором указаны способы авторизации. Universe - учетная запись, созданная в Юниверс MDM; ldap - учетная запись, созданная через Active Directory. Способ авторизации может быть скрыт, если выключен флаг "Внешний".
   - **Роли**. Выпадающий список ролей, назначаемых группе. Могут быть выбраны несколько ролей.
   - **Унаследованные роли**. Если создаваемая группа является подгруппой, ячейка автоматически заполнит ее той ролью, которую она наследует от родительской группы.
6. В секции *"Пользователи"* нажмите кнопку ⊕ в верхнем правом углу

таблицы и выберите пользователей из списка для добавления в группу.

7. В результате действия строки пользователей будут отображаться в таблице с лейблом "Добавлена".
   - Подробная информация об учетной записи пользователя отображается во всплывающей подсказке при наведении курсора на имя пользователя. При наличии в настоящий момент у пользователя заместителя - имя этого пользователя в таблице подсвечивается оранжевым цветом, а при появлении подсказки также будет загружен доп.блок с информацией о периоде замещения, где оранжевым цветом будет выделен пользователь, который замещает просматриваемого пользователя. Если заместитель назначен на будущие даты - имя пользователя будет иметь стандартное отображение.
   - Чтобы удалить пользователя из таблицы, наведите курсор на нужную строку и нажмите *Удалить*.
8. Нажмите *Сохранить* в верхнем правом углу экрана, чтобы применить изменения.

5.2. Редактирование группы

Чтобы отредактировать группу:

1. Выберите необходимую группу из списка.
2. Внесите изменения.
   - При удалении пользователя из таблицы строка будет отмечена лейблом "Удалена" до сохранения изменений. При необходимости нажмите "Отменить удаление".
3. Нажмите *Сохранить* в верхнем правом углу экрана, чтобы внести изменения.

5.3. Удаление группы

Чтобы удалить группу:

1. Выберите необходимую группу из списка существующих.
2. В верхнем правом углу экрана нажмите *Удалить*.
3. Подтвердите действие.
   - При удалении родительской группы все дочерние перемещаются в

корень иерархии.

- При удалении группы, на которую назначены пользователи, в диалоговом окне отобразиться уведомление с предупреждением (Рисунок 2).

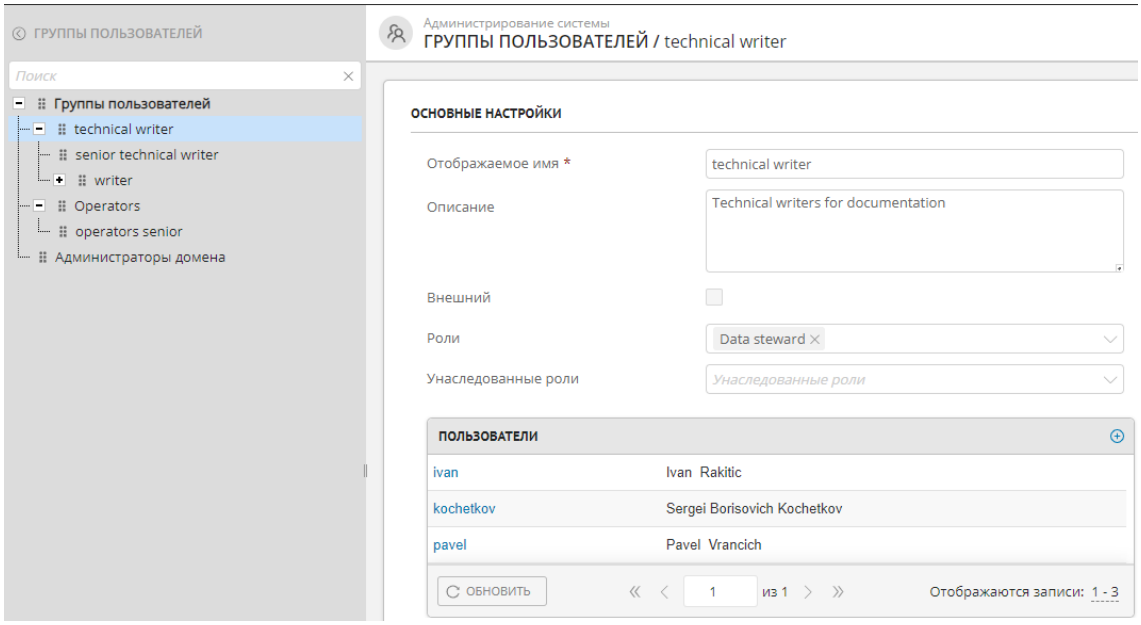


Рисунок 1 - Пример создания группы пользователей

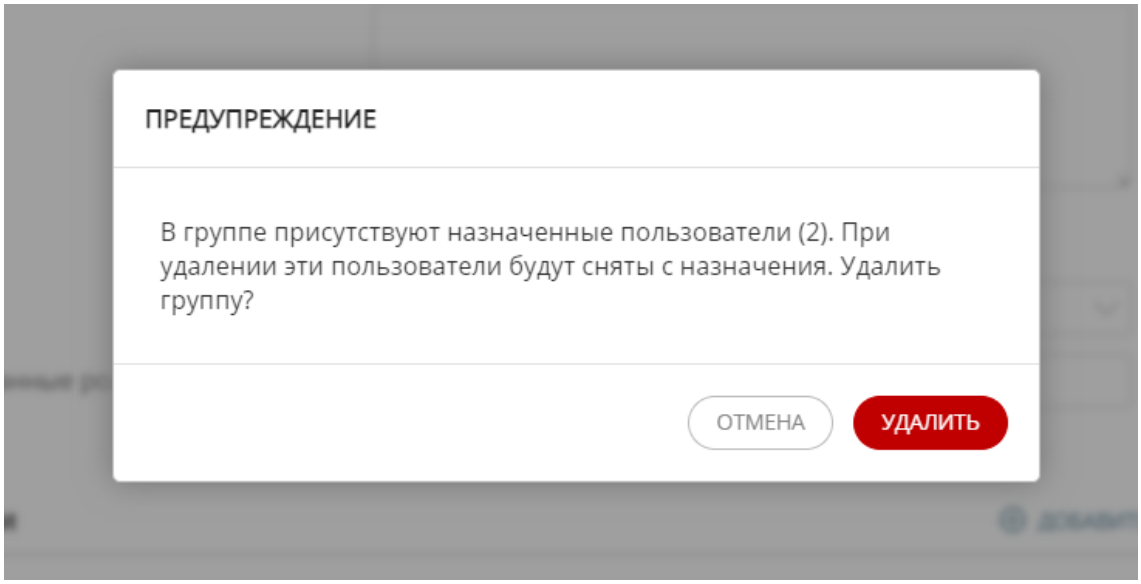


Рисунок 2 - Уведомление при удалении группы с назначенными на нее пользователями

6. Каталог доступа

В этой статье:

6.1. Общее описание

Статья описывает интеграцию с Active Directory через создание LDAP-подключения в разделе "Каталог доступа".

Взаимодействие с Active Directory (AD) связывает учетные записи пользователей Windows с пользователями Юниверс MDM. Позволяет авторизоваться через учетную запись Windows и получать права доступа в Юниверс MDM.

> Примечание:
>
> Раздел "Каталог доступа" доступен для работы, если пользователю назначена роль с правом *Каталог доступа*

Протокол LDAP используется в Юниверс MDM для взаимодействия с Active Directory (и другими способами аутентификации).

Для интеграции создается LDAP-сервер и подключается к Active Directory. Active Directory имеет собственную структуру объектов, которая настраивается под требуемую IT-инфраструктуру.

Также разные версии Active Directory могут использовать разные фильтры. Для проверки настройки фильтров используйте кнопку "Проверить подключение".

Структура запроса для LDAP может быть создана администратором Active Directory.

При возникновении сложностей с настройкой интеграции воспользуйтесь поиском в интернете. Полезные ссылки:

- Обозреватель Active Directory версии 1.52
- Доменные службы Active Directory
- Lightweight Directory Access Protocol

6.2. Создание LDAP-подключения

Чтобы создать подключение:

1. Убедитесь, что открыт раздел "Каталог доступа".
2. Нажмите кнопку ⊕ *Создать* в нижней части списка подключений.
3. Заполните основные параметры во вкладке "**LDAP-подключения**" (Рисунок 1):
   - **URL сервера**. Обязательный.
   - **Порт**. Обязательный. Значения по умолчанию: с ssl сертификатом - 636, без сертификата - 389.
   - **Логин**. Обязательный. Указывается значение атрибута AD "distinguishedName" (например, "CN=mdmADTest,CN=Users,DC=achrf,DC=ru").
   - **Пароль**. При обновлении не требуется указание пароля, если он не был изменен.
   - **Использовать SSL сертификат**. Включение флага подразумевает, что в java на сервере mdm установлен сертификат.
   - **Участники**. Имя атрибута, в котором указан список групп, где участвует пользователь. Заполняется на основании настроек AD. Если поле пустое или некорректно заполненное - пользователь не будет привязан к своим группам.
   - **Максимальное количество пользователей**. По умолчанию, количество записей в AD - не более 1000. Пагинация отсутствует. Если настройки сервера AD изменены в большую сторону, то параметр можно отредактировать, но не более, чем указано в настройках сервера (подробности см. в официальной документации).
4. При необходимости нажмите кнопку ⚙ "Проверить подключение", чтобы осуществить проверку корректности подключения.
5. Принудительный запуск операции синхронизации доступен при нажатии кнопки "Синхронизировать".
6. Перейдите во вкладку "**Домены безопасности**".
7. Нажмите кнопку + *Создать* в верхнем правом углу экрана.
8. Заполните основные параметры домена (Рисунок 2):
   - **Домен безопасности**. Обязательный. Имя домена безопасности.
   - **Базовый поиск пользователей**. База для поиска. Например, при "distinguishedName" выглядит как

"CN=mdmADTest,CN=Users,DC=achrf,DC=ru", в поле "Базовый поиск пользователей" нужно указать "CN=Users,DC=achrf,DC=ru".

- **Фильтр пользователей**. Дополнительный фильтр пользователей. Чтобы найти пользователя с именем "mdmADTest", необходимо указать фильтр (&(objectcategory=user)(CN=mdmADTest)). Фильтр поддерживает поиск по маске. Чтобы найти пользователей "mdmADTest_1", "mdmADTest_2", "mdmADTest", необходимо указать фильтр (&(objectcategory=user)(CN=mdmADTes*)).
- **Базовый поиск групп**. Заполняется аналогично параметру "Базовый поиск пользователей" - только для групп.
- **Фильтр групп**. Заполняется аналогично параметру "Фильтр пользователей" - только для групп. Например, указав в поле "Фильтр пользователей" (|(CN=Администратор*)), будут доступны все группы, начинающиеся с "Администратор" (Администраторы, Администратор ролей и т.д)

9. Нажмите кнопку "Предварительный просмотр", чтобы убедиться, что параметры верны и производится выборка необходимых групп/пользователей. В результате действия будут получены и отображены пользователи и группы согласно фильтрам в настройках домена с сервера AD.
10. Чтобы настроить регулярность синхронизации - перейдите во вкладку "**Расписание**".
11. Нажмите кнопку *Создать* в верхнем правом углу экрана.
12. В поле **CRON выражение** задайте периодичность запуска синхронизации. При наведении курсора на значок в конце строки отобразится всплывающая подсказка с возможными вариантами расписания.
13. После внесения всех необходимых изменений - нажмите "Сохранить" в верхнем правом углу экрана.

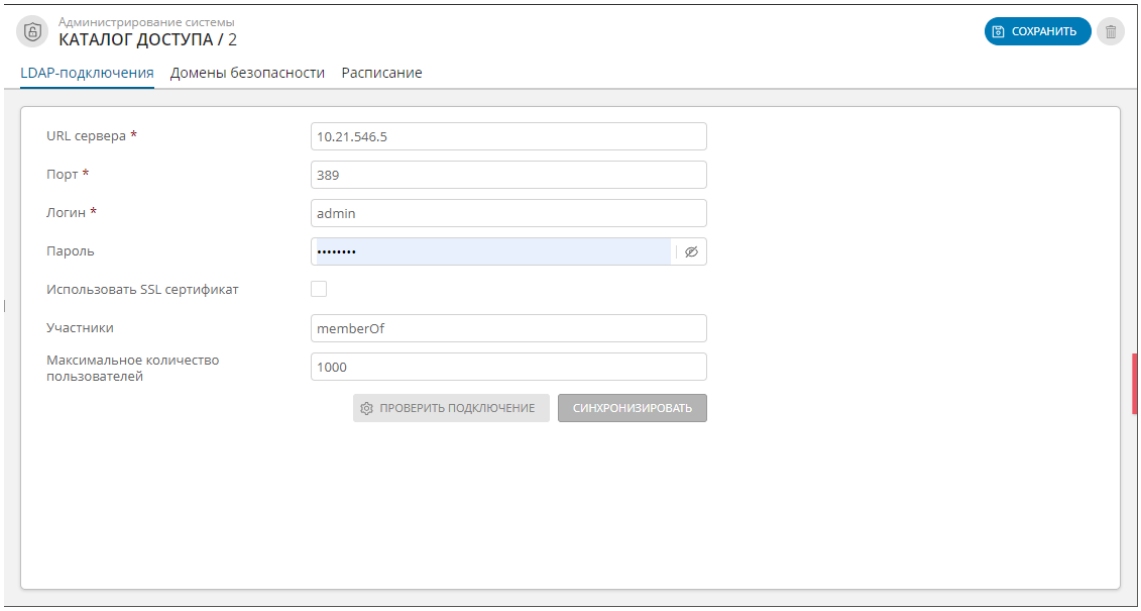


Рисунок 1 – Вкладка "LDAP-подключения"

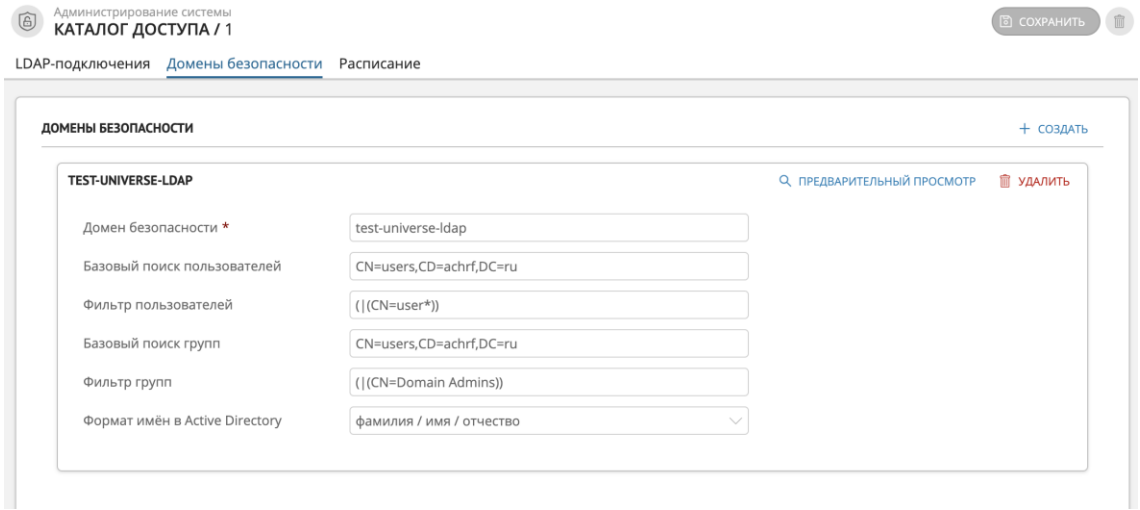


Рисунок 2 – Вкладка "Домены безопасности"

6.3. Сохранение данных атрибутов из AD

Чтобы сохранять данные атрибутов Active Directory в данные пользователя системы Юниверс MDM, необходимо создать дополнительные параметры пользователя.

- Поле "Имя" - имя параметра - должно совпадать со значением имени атрибута AD.
- После синхронизации дополнительные параметры будут заполнены значениями из атрибутов пользователя AD.
- Если изменить значения доп.параметров через интерфейс Юниверс

MDM - при следующей синхронизации они будут перезаписаны значениями из AD.

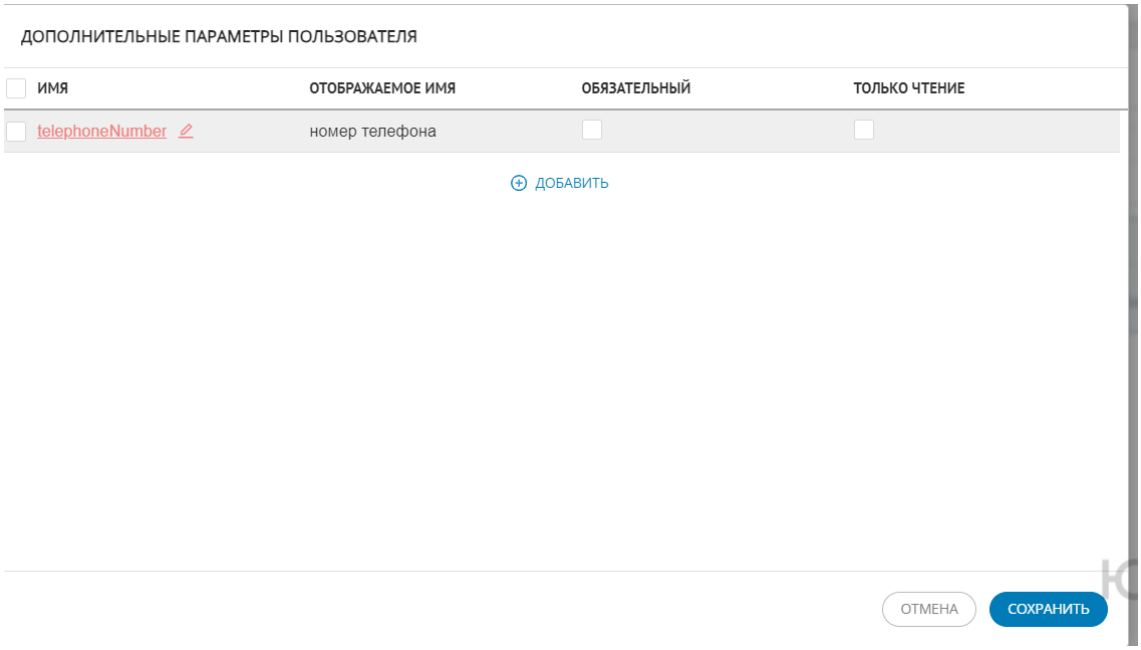


Рисунок 3 – Создание дополнительного параметра учетной записи

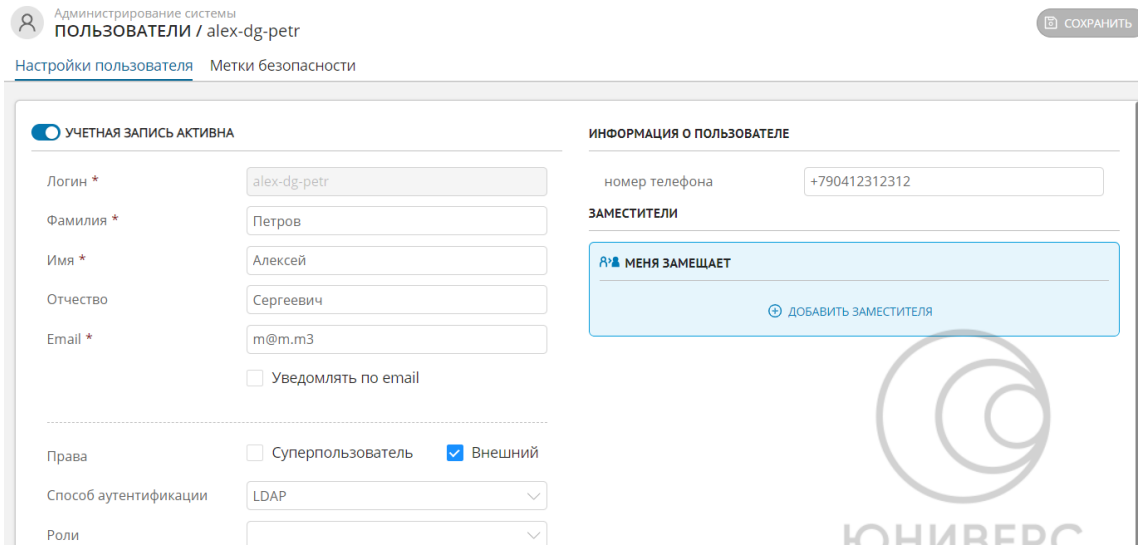


Рисунок 4 – Загрузка учетной записи вместе с дополнительным параметром

6.4. Выбор формата импорта ФИО из AD

При настройке интеграции с Active Directory есть возможность выбирать формат для разбора атрибута из учетной записи пользователя на сервере AD `name` .

В качестве значения по умолчанию выставлен формат "Фамилия / Имя / Отчество".

Пример:

Учетная запись на сервере AD содержит поля "Имя" и "Фамилия".

Создано 2 пользователя: либо в разных доменах (порядок имени и отчества различается); либо оба пользователя в одном домене, но имя и фамилия одного перепутаны местами:

- Имя "Петр", фамилия "Александров",
- Имя "Петров", фамилия "Александр".

Настройка:

В настройках раздела "Каталог доступа" во вкладке "Домены безопасности" необходимо создать 2 домена с разными фильтрами:

Первый:

- Базовый поиск пользователей: `CN=Users,DC=achrf,DC=ru`
- Фильтр пользователей: `(&(objectcategory=user)(CN=Петр Александров))` (формат имени "Имя/Фамилия")

Второй:

- Базовый поиск пользователей: `CN=Users,DC=achrf,DC=ru`
- Фильтр пользователей `(&(objectcategory=user)(CN=Петров Александр))` (формат имени "Фамилия/Имя")

В результате в процессе выполнения операции синхронизации в системе сохраняются два пользователя с корректным заполнением имени и фамилии.

6.5. Авторизация через AD

Авторизация через AD происходит без применения дополнительных настроек. Пользователь будет загружен, сохранен и добавлен в группы, которые уже существуют в системе Юниверс MDM. Для авторизации используется логин от учетной записи Windows.

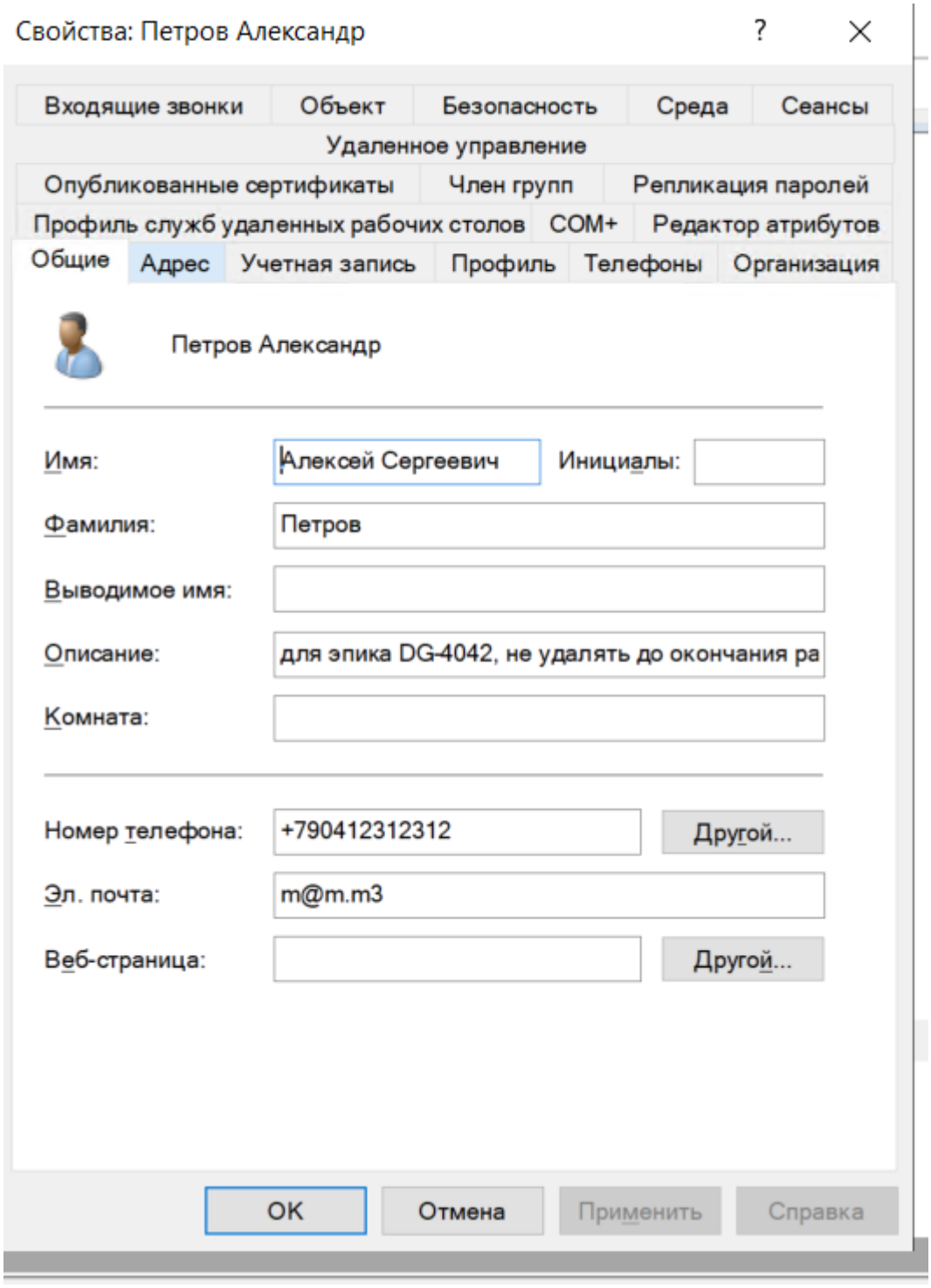
6.6. Синхронизация с AD

1. Конфигурация Active Directory читается из БД.
2. По всем доменам загружаются группы, далее сохраняются или обновляются в Юниверс MDM. Группы, неудовлетворяющие фильтрам, удаляются из системы.
3. Далее загружаются пользователи (по всем доменам), сохраняются или

обновляются в системе. Если пользователь уже существует (например, создан через интерфейс), то он не будет сохранен или обновлен информацией из AD.

4. Пользователям, имеющим доступы к ресурсам безопасности: "Роли" и "Пользователи", будет доступен отчет в Уведомлениях системы. При этом учитываются только персональные роли - роли из групп игнорируются. Детализация отчета доступна по одноименной кнопке.

Отображение дополнительных параметров учетной записи Active Directory в Windows (Рисунок 5/6):


Свойства: Петров Александр
Входящие звонки
Объект
Безопасность
Среда
Сеансы
Удаленное управление
Опубликованные сертификаты
Член групп
Репликация паролей
Профиль служб удаленных рабочих столов
COM+
Редактор атрибутов
Общие
Адрес
Учетная запись
Профиль
Телефоны
Организация
Петров Александр
Имя:
Алексей Сергеевич
Инициалы:
Фамилия:
Петров
Выводимое имя:
Описание:
для эпика DG-4042, не удалять до окончания ра
Комната:
Номер телефона:
+790412312312
Другой...
Эл. почта:
m@m.m3
Веб-страница:
Другой...
OK
Отмена
Применить
Справка

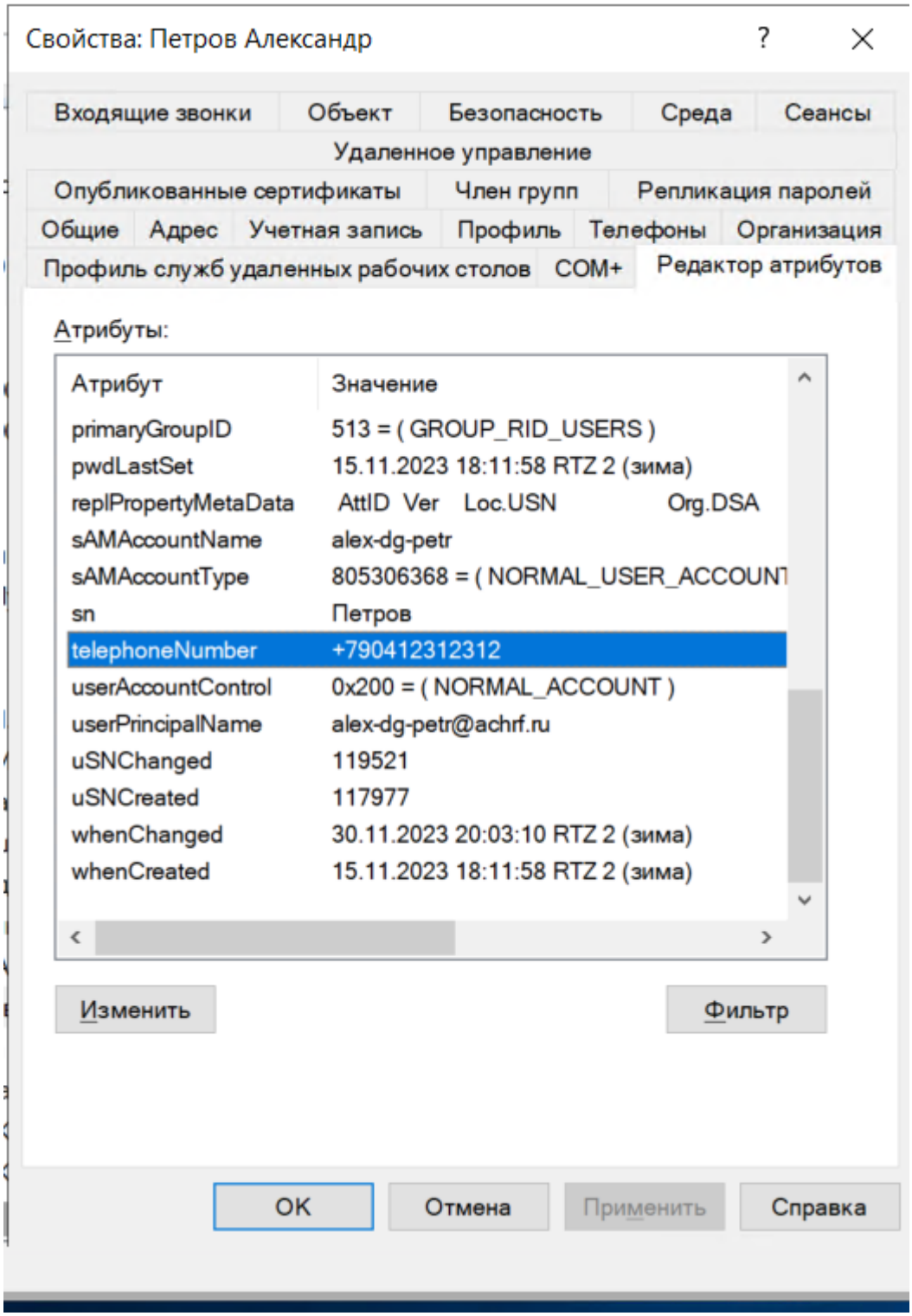


Рисунок 5/6 – Отображение дополнительного параметра

6.7. Вопросы и ответы

Сокращения:

- AD - active directory
- Система - платформа Юниверс

Как мне загрузить больше 1000 пользователей?

Выставить необходимое число в поле "Максимальное количество пользователей". Это количество пользователей, которое будет выгружено из каждого домена.

Когда система получает свежие данные о пользователе AD?

Данные пользователя в системе обновляются только в процессе операции синхронизации или после успешной авторизации.

Я изменил данные пользователя в Системе. После синхронизации поля изменились на поля из учетной записи AD

Информация из AD считается приоритетной, каждый раз после синхронизации/успешной авторизации пользователя в Системе, его данные будут обновлены на актуальные из AD.

Я заблокировал учетную запись в Системе, но пользователь может продолжать работу после синхронизации с AD

Информация из AD считается приоритетной, каждый раз после синхронизации/успешной авторизации пользователя в Системе, его учетная запись будет деактивирована/активирована согласно AD.

Я заблокировал пользователя в AD, но он продолжил работать в Системе

Система обновляет учетные записи пользователей только при синхронизации/авторизации в Системе. После синхронизации учетная запись пользователя станет неактивной, пользовательская сессия будет завершена.

У меня не выгрузился пользователь

userPrincipalName используется в Системе как логин пользователя. Пользователь без заполненного атрибута userPrincipalName не будет сохранен в Системе. Если login пользователя содержит недопустимые символы, пользователь не будет сохранен в Системе. Допустимые символы: латинские буквы, цифры, символы тире, подчеркивания (_) и точки (.). Логин может начинаться с цифры, знак @ в логине недопустим, пробел в логине недопустим.

У меня выгрузился пользователь без фамилии/имени/отчества или ФИО перепутано местами

Имя пользователя читается из атрибута sn, фамилия из givenName , отчество из initials, т.к. многие компании указывают отчество работника в поле "Инициалы".

Система при считывании пользователя формирует строку sn givenName initials , что соответствует паттерну разбора "имя / фамилия / отчество". Если в AD в поле "Имя" записывается Имя Отчество, поле "Инициалы" не заполняется, то необходимо изменить паттерн разбора ФИО на "имя / отчество / фамилия".

Я изменил "userPrincipalName" у пользователя в AD, в Системе теперь 2 пользователя

userPrincipalName используется в Системе как логин пользователя. Если userPrincipalName изменен, в системе будет создан новый пользователь.

В конфигурации домена я указал фильтр на группы, но пользователи в них не добавились

Фильтр групп отвечает только за выгрузку групп, если фильтр пользователей не задан, пользователи не будут выгружены.

Я указал фильтр пользователей и фильтр групп, но пользователи не добавились в группы

Проверьте, что поле "Участники" заполнено. Значение должно соответствовать настройкам AD, чаще всего это memberOf или members. Пользователи должны входить в группы AD.

Я хочу выгрузить только активных пользователей

В большинстве случаев достаточно добавить в фильтр пользователей выражение `(!userAccountControl:1.2.840.113556.1.4.803:=2)`. Если фильтр работает некорректно, обратитесь к документации AD.

Я хочу выгрузить всех пользователей с именем, начинающимся на букву П

Используйте в фильтре *. Добавьте в фильтр пользователей выражение (SN=П*).

При неуспешной авторизации по SSO в Журнале аудита не отображается логин пользователя

На этапе авторизации через SSO система не имеет данных о логине доступа, в лог записывается пустое значение.

При синхронизации у меня возникает ошибка LDAP: error code 3 - Timelimit Exceeded

Увеличьте значение переменной `com.universe.mdm.ldap.integration.default.ldap.connection.time.limit`

При блокировке учетной записи непосредственно в Системе (в интерфейсе

пользователя) сессия пользователя закрывается

Это корректное поведение. Так как учетная запись заблокирована, то и текущая сессия должна быть немедленно завершена.

Что если пользователь не попал по фильтрам ни в одну из групп?

Если внешний пользователь не попал по фильтрам ни в одну из групп, полученных из AD, то пользователь зайти в Систему сможет, но объекты в Системе не увидит.

7. Операции

Содержание:

7.1. Общая информация

Раздел предназначен для управления запуском операций, настройки параметров и просмотра информации о статусе операции.

7.1.1. Создание и изменение операций

Чтобы создать новую операцию:

1. Перейдите в раздел "Операции".
2. Нажмите кнопку ⊕ *Создать*, расположенную в нижней части списка операций.
3. Заполните **обязательные** свойства операции:
   - **Активна**: Флаг, который определяет операцию как активную, то есть актуальную и доступную для запуска (в том числе и по расписанию).
   - **Тип**: Выпадающий список с типом операции, например, задача переиндексации или задача экспорта данных. От типа зависит набор параметров в секции "Параметры". При подключении стороннего пакета операций, перечень доступных значений будет дополнен соответствующими пунктами. Типы операций отсортировываются по алфавиту.
   - **Название**: Имя операции, которое будет отображаться в списке операций.
4. *Опционально.* Заполните дополнительные свойства операции:
   - **Описание**: Дополнительная информация об операции.
   - **Cron-выражение**: Настройка периодичности выполнения операции (расписания) посредством Cron-выражений.
   - При необходимости используйте теги.
5. При необходимости настройте запуск операции относительно других

операций в секции "**Запуск следующей операции**".

- Из выпадающего списка выберите операцию, после успешного или неудачного запуска которой будет запускаться текущая операция.
- Информация о запуске операции по цепочке будет отображаться в журнале аудита.

6. Укажите параметры операции.
7. Нажмите кнопку  *Сохранить*, расположенную в верхнем правом углу экрана.

> Примечание:
> Сохранить новую операцию можно только после заполнения обязательных полей, а также при условии ввода корректного формата CRON-выражения. При попытке сохранения операции с верным CRON-выражением, но содержащим нерекомендуемый временной промежуток (например, запуск операции каждую секунду), будет предложено подтвердить сохранение действия.

Чтобы отредактировать ранее созданную операцию:

1. Выберите ее из списка существующих операций.
2. Введите требуемые значения свойств. Тип операции изменить нельзя.
3. Нажмите кнопку *Сохранить*.

Чтобы удалить операцию:

1. Выберите операцию из списка и нажмите кнопку  *Удалить* в правом верхнем углу экрана.
2. Подтвердите или отмените действие в появившемся окне.

7.1.2. Клонирование операций

1. Выберите необходимую операцию из перечня созданных, и в правой части строки нажмите кнопку  *Клонировать*.
2. В результате действия откроется копия операции для редактирования параметров.
3. Задайте уникальное имя для клонированной операции и измените как минимум один параметр.
4. Сохраните операцию.

7.1.3. Сортировка операций

При нажатии на элемент  "Фильтровать" доступны инструменты сортировки

и фильтрации перечня операций:

- По тегам;
- По активности: активные, неактивные, все операции;
- По ID, названию или типу операции.

7.1.4. Использование тегов

Любую операцию можно отметить одним или несколькими тегами. Тег может быть как на английском, так и на русском языках. Использование тегов отмечает произвольные наборы операций и в последствии искать их. Например, можно отметить все операции для первоначальной загрузки большого объема записей.

Для создания тега:

1. Выберите необходимую операцию из перечня существующих или создайте новую.
2. В поле "Теги" введите значение тега (любые символы).
3. Нажмите клавишу "Enter" или кликните левой кнопкой мыши по предлагаемым тегам (если они есть).
4. Сохраните операцию.

Удаление тега из поля "Теги" доступно несколькими способами: стереть текст (клавиша Backspace); убрать тег, щелкнув левой кнопкой мыши по правой части тега, выбрать выделенное значение в выпадающем списке.

Все теги, использованные хотя бы в одной сохраненной операции, доступны в выпадающем списке. Теги импортируются и экспортируются вместе с набором операций и доступны любому пользователю, у которого есть права на работу с разделом.

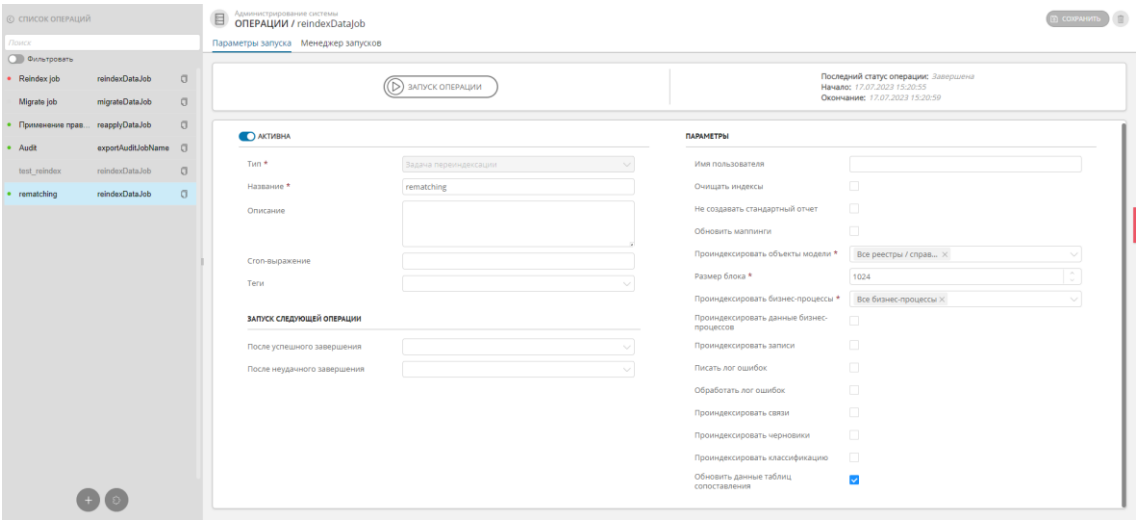


Рисунок 1 - Раздел "Операции" (закладка "Параметры")

7.2. Дополнительные действия с операциями

7.2.1. Запуск операций

Операция может запускаться вручную или автоматически по расписанию (при помощи Cron-выражений).

Чтобы запустить операцию вручную:

1. Выберите необходимую операцию из списка в разделе "Операции".
2. В результате на экране отобразится закладка "Параметры запуска" с параметрами выбранной операции.
3. Нажмите кнопку "Запуск операции", расположенную в верхней части экрана.
4. В результате действий:
   - Кнопка "Запуск операции" сменит вид на "Остановить операцию".
   - В закладке "Параметры запуска" над областью параметров операции будет отображен статус последнего запуска.
   - В закладке "Менеджер запусков" будет отображен последний запуск операции: дата и время начала и окончания, текущий статус запуска.
   - В списке операций индикатор выполнения текущей операции изменит свой цвет на синий (Рисунок 1). В случае успешного выполнения операции индикатор становится зеленого цвета, если операция завершится с ошибкой - красного.

Примечание:
Повторное выполнение операции, вызываемое при нажатии кнопки "Перезапуск операции" в закладке "Менеджер запусков", в текущей реализации недоступно

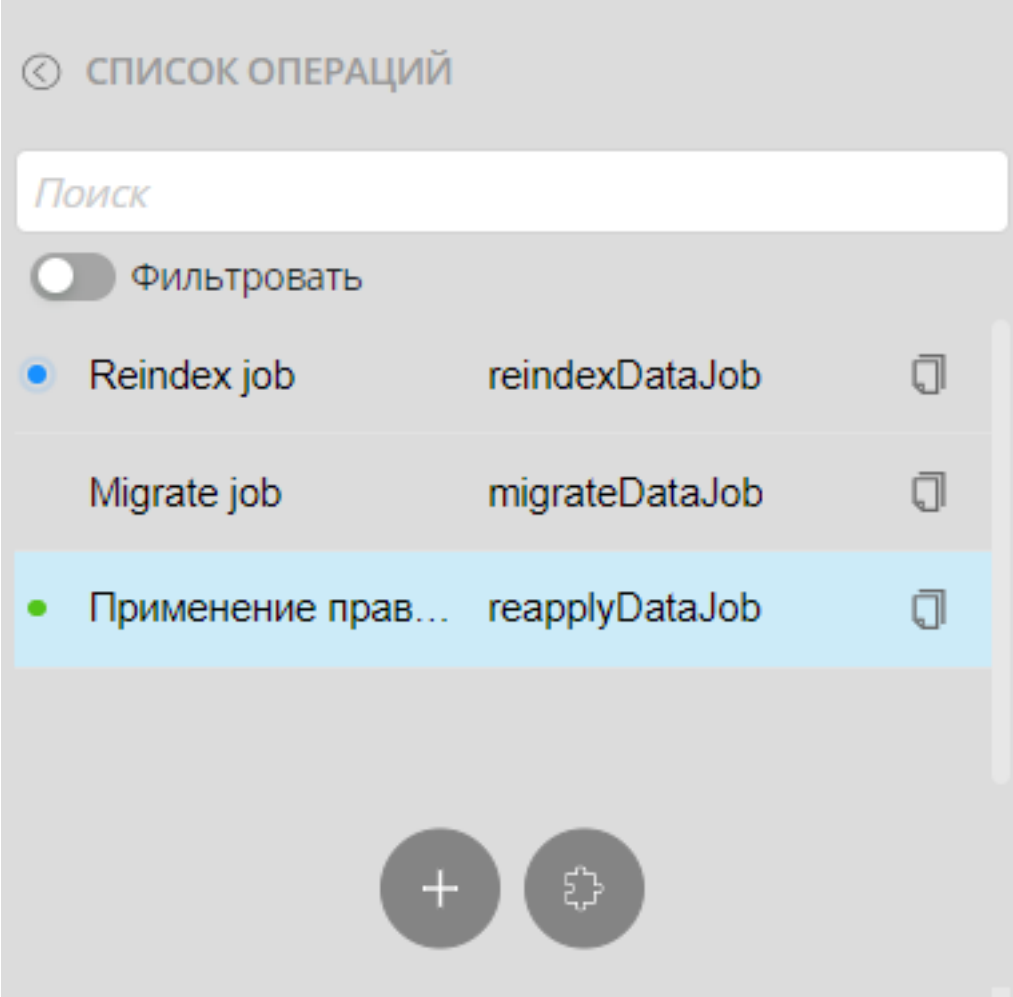


Рисунок 1 - Цветовые индикаторы выполнения операции

Для просмотра детализации выполнения:

1. Перейдите в закладку "Менеджер запусков".
2. Выберите необходимую запись о запуске операции.
3. В результате действия в нижней части экрана раскроется секция "Шаги операций", содержащая данные по каждому шагу выполнения операции.
4. Для ознакомления с ошибкой нажмите кнопку "Детали", расположенную в правой части соответствующей строки детализации шага (Рисунок 2).

Если в процессе выполнения операции возникнет ошибка, в текущем статусе операции будет отображено значение "Ошибка". Все успешные шаги операции будут иметь статус "Завершена", прерванные – статус "Остановлена".

Чтобы прервать выполнение, нажмите кнопку "Остановить операцию".

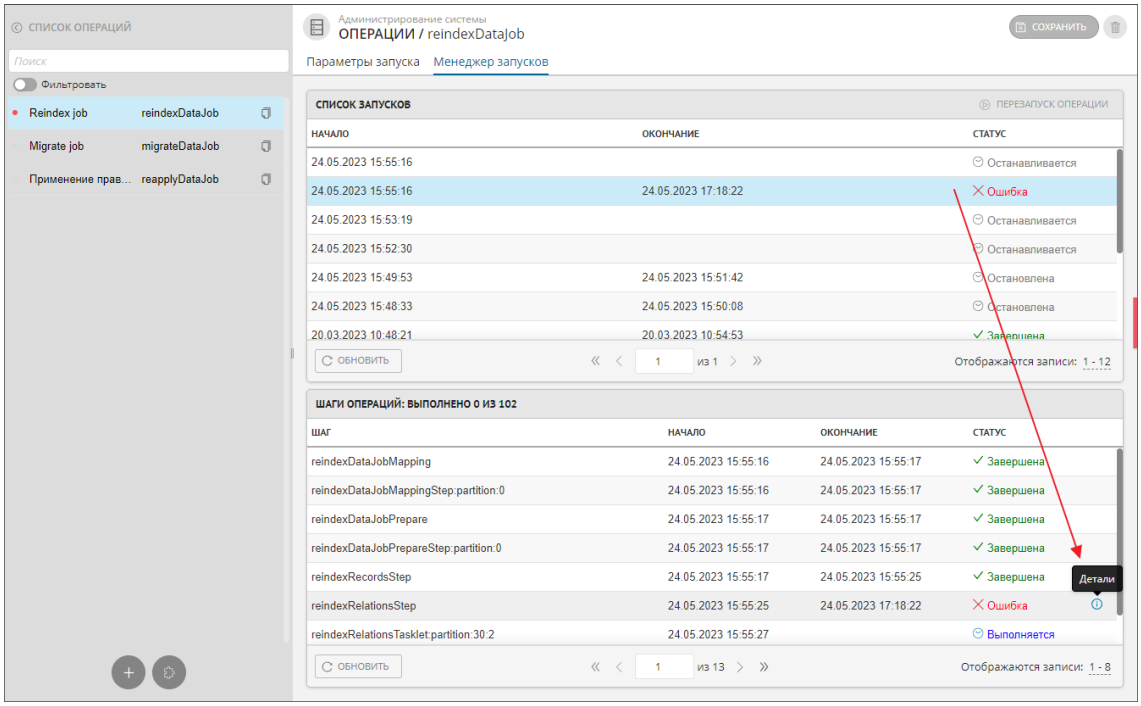
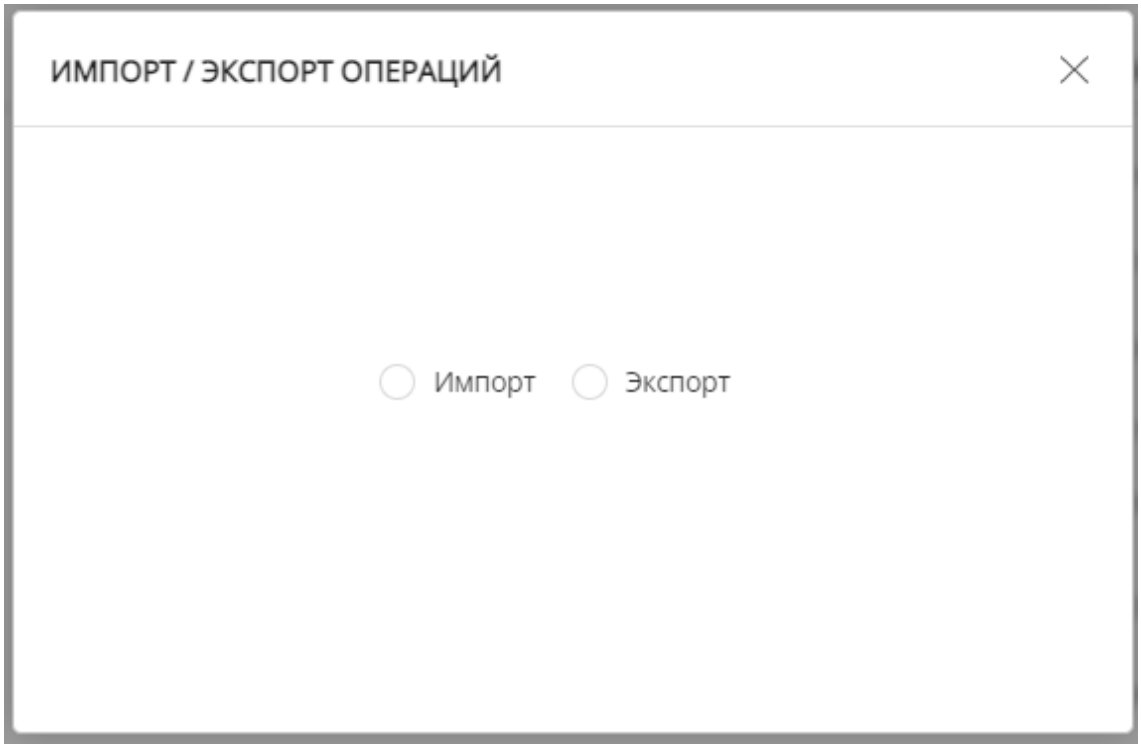


Рисунок 2 - Просмотр деталей ошибки операции

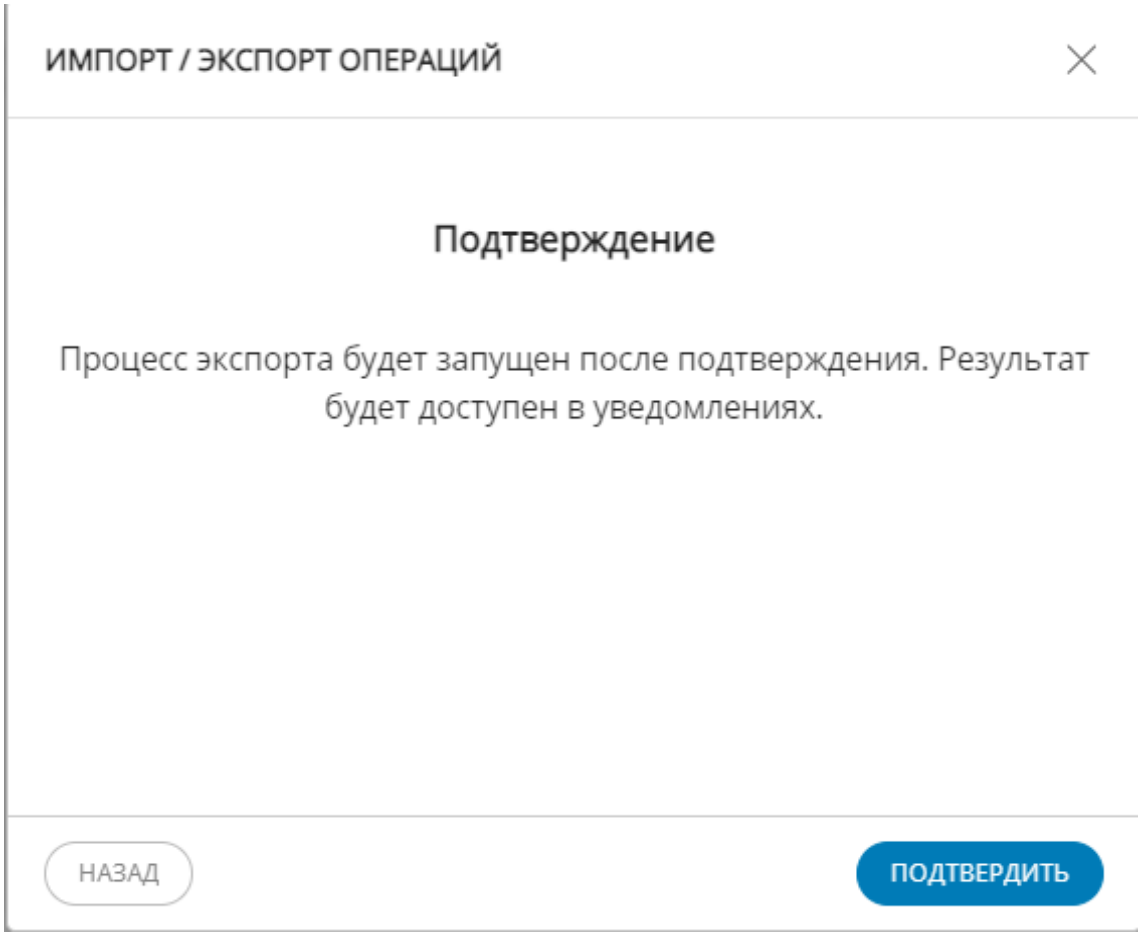
7.2.2. Импорт и экспорт операций

Чтобы импортировать или экспортировать набор операций, которые были созданы ранее в системе, необходимо воспользоваться соответствующим мастером. Для этого нажмите кнопку "Импорт/экспорт", расположенную в нижней части перечня созданных операций.

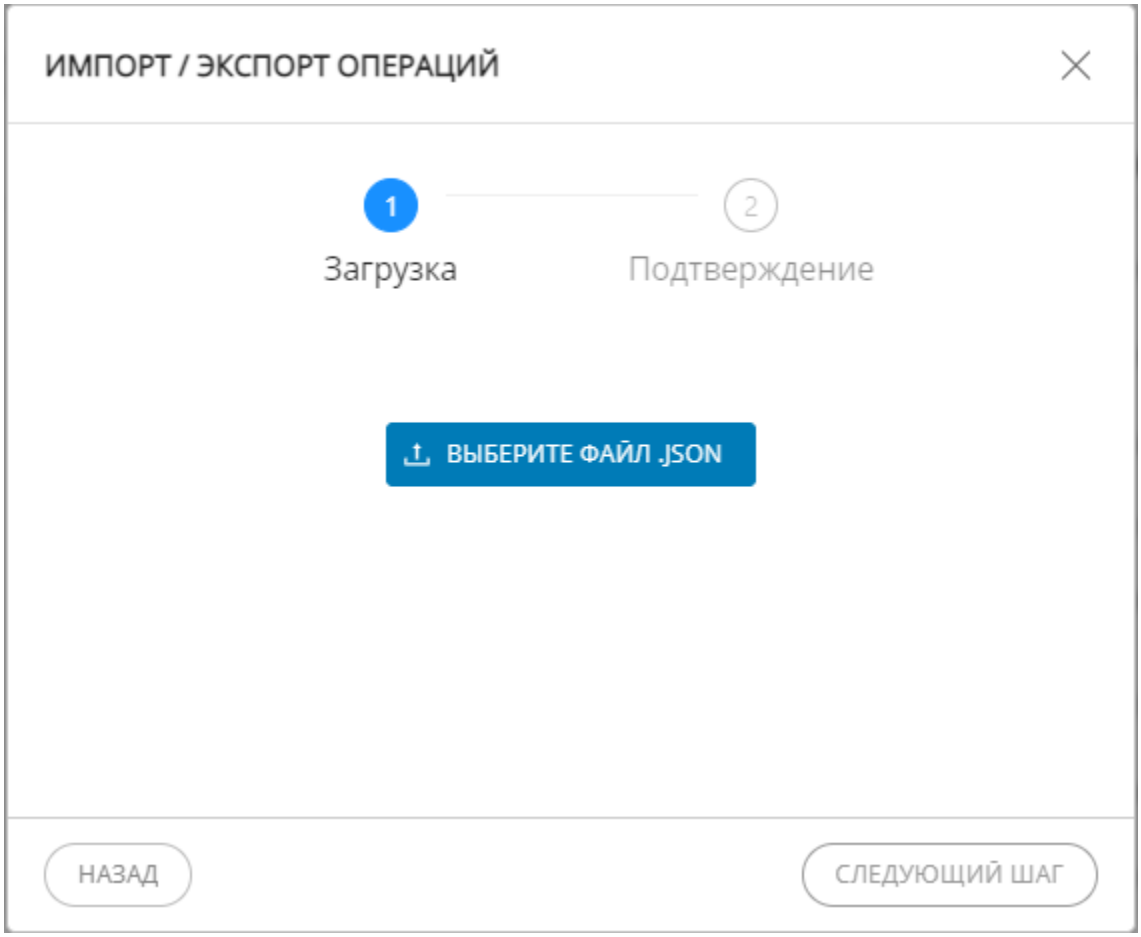
Шаг 1. Выберите требуемое действие. Экспорт выполняется в 2 шага. Импорт в 3 шага.



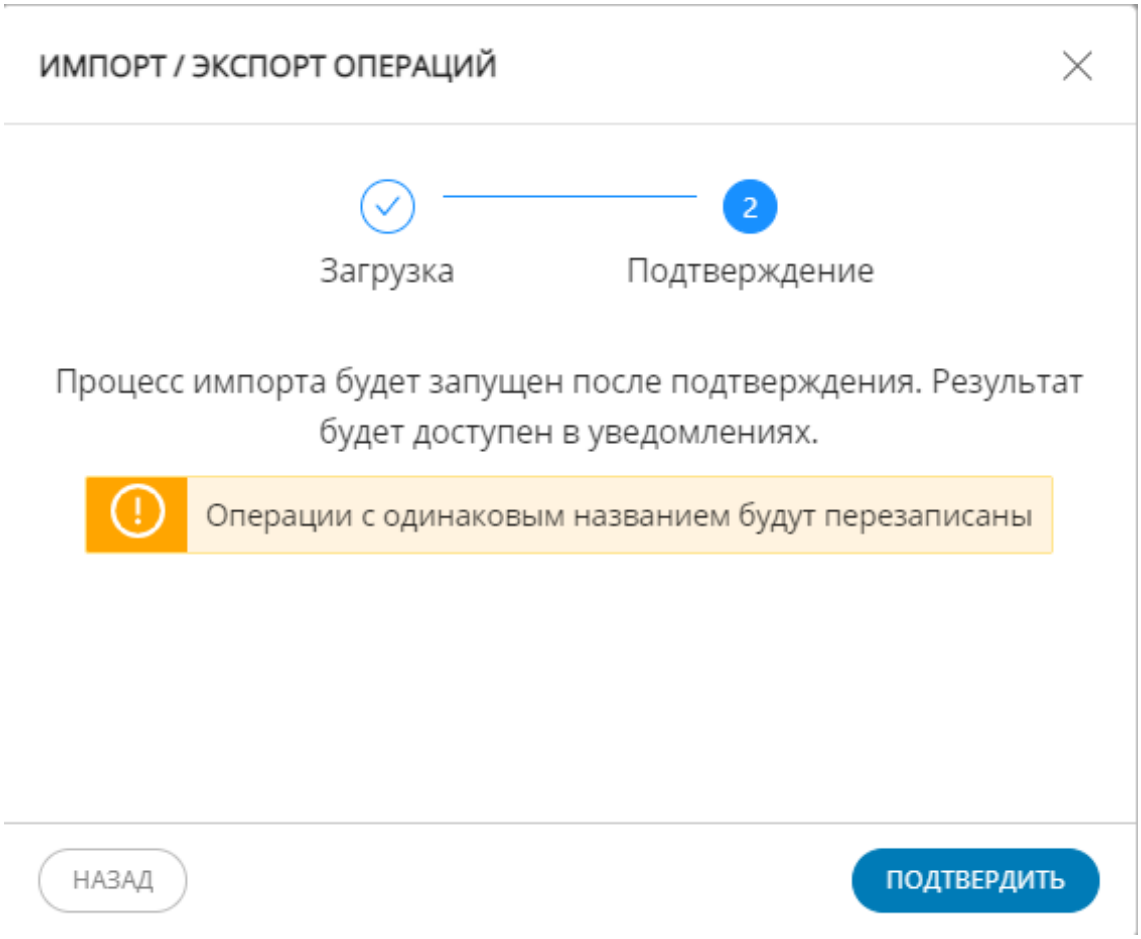
Шаг 2. Экспорт. Для экспорта не предусмотрены дополнительные настройки. Подтвердите действие, после чего начнется экспорт, результаты которого можно скачать в Уведомлениях.



Шаг 2. Импорт. Выберите файл с набором операций (формат .json). Для продолжения нажмите "Следующий шаг".



Шаг 3. Импорт. Подтвердите действие. Сообщение о результатах импорта отобразится в Уведомлениях.



7.3. Описание основных операций

Содержание:

7.3.1. Операция импорта данных (importDataJob)

Операция импорта предназначена для внесения данных из сторонней информационной системы в Юниверс MDM HPE.

Входными данными операции являются записи сторонней информационной

системы.

Результатом выполнения операции являются данные, импортированные в Юниверс MDM HPE.

Для операции импорта данных указываются следующие параметры:

- jobUser (строковый) – логин учетной записи. Определяет, с правами какой учетной записи будет запускаться операция. Если поле пустое, то при запуске по Cron-выражению у операции будут полные права на любой реестр/справочник; при запуске через интерфейс у операции будут права текущей учетной записи. Для учетной записи оператора данных может понадобиться настроить права на реестры/справочники;
- dataSetSize (список) – выбор режима для импорта данных. Доступны режимы SMALL и LARGE.

Режим SMALL использует JDBC batch, вставляя пакетный файл, размер которого регулирует unidata.job.import_data.commit_interval. Вставка производится непосредственно в рабочие таблицы.

Режим LARGE предназначен для больших объемов данных (от 3-5 млн. записей). При выборе режима в процессе импорта будет использоваться ступенчатый способ загрузки, подразумевающий копирование данных через двоичный протокол во временные таблицы для выполнения первоначальной трансформации и загрузки, с последующим копированием обработанных данных в постоянные таблицы. Режим требует для своей работы больше ресурсов, чем режим SMALL. При выборе значения LARGE необходимо предотвратить возможность изменения данных через другие интерфейсы, например, через SOAP-интерфейс.

- blockSize (целочисленный) – количество записей в партиции, которую получает узел кластера. Значение blockSize делится на unidata.job.import_data.commit_interval при непосредственной вставке в базу. При определении размера партиции нужно стремиться к тому, чтобы количество получившихся партиций не превышало 200 - 250 (особенность функционирования spring-batch в том, что объекты партиций держатся в памяти на узле координаторе. При большом количестве партиций можно спровоцировать OOM). По умолчанию установлено значение 1000;
- initialLoad – флаг для первоначальной загрузки. При значении true запускается выполнение первоначальной загрузки в пустую БД по оптимизированному алгоритму: каждая запись будет расцениваться как новая и не будет подвергаться различным проверкам. При возможности обновления существующих данных параметр не рекомендуется использовать. Если

параметр выставлен в false, то ошибки DQ не попадут в отчет об импорте;
- auditLevel (список) – уровень фиксируемых сообщений в разделе «Журнал» (0 – аудит запрещен, 1 – только ошибки, 2 – все сообщения);
- usersSelector (список, выбор нескольких вариантов) – перечень учетных записей. Позволяет выбрать получателей сообщений о результатах выполнения задачи;
- databaseUrl (строковый) – JDBC URL базы данных, содержащей данные для загрузки вместе с данными аутентификации;

В качестве значения параметра можно указать ссылку на стороннюю базу данных. Пример jdbc:postgresql://import.host.org/staging_db?current

Schema=import_data&user=postgres&password=postgres

- operationId (строковый) – идентификатор загрузки. Если параметр не заполнен, то он будет сгенерирован при запуске операции. Может использоваться для отчетности;

В случае отсутствия введенного значения идентификатор генерируется автоматически. В случае, если operationId операции импорта совпадает с operationId одного из предыдущих выполнений этой операции, то в результатах загрузки будут: записи, которые загружались при предыдущем выполнении (в их прошлом состоянии) + записи, которые загружаются при текущем выполнении. Например, если физически загружается 10 записей, то за два прохода importDataJob будет получено 20 записей, что может использоваться для сравнения изменений записей, их количества и т.п.

- definitionContent (строковый) – JSON-маппинг загружаемых данных, выполненный в соответствии со схемой платформы Юнидата. Используется для загрузки данных из внешних источников.
- processingBatchCrashes (флаг, по умолчанию включен) – отслеживание необрабатываемых ошибок при вставке/обновлении batch (пачки) записей. В случае, если одна из записей в пачке имеет ошибки (например, нарушена ссылочная целостность), то текущая пачка загружается по алгоритму, в котором каждая запись из пачки импортируется отдельно. При большом количестве пачек, в которых обнаруживаются ошибки, время работы операции увеличится. Результат работы параметра логируется в unidata_backend.log.
- skipDq – флаг пропуска проверки качества данных в процессе импорта записей (true = пропустить);
- skipMatching – флаг пропуска процедуры поиска дубликатов в процессе

импорта записей (true = пропустить);
- skipIndexing – флаг пропуска процедуры создания поискового индекса Elasticsearch (true = пропустить);
- skipNotifications – флаг, позволяет пропустить рассылку сообщений об обновлениях (true = пропустить);
- skipIndexRebuild – флаг пропуска процедуры перестроения индексов базы данных при первоначальной загрузке. Только для режима LARGE (true = пропустить);
- skipMove – не используется. Служебный параметр, который будет удален в следующих релизах.
- mergeWithPreviousVersion (флаг) – считать разницу между старой и вновь пришедшей версиями данных и создавать новую версию только в том случае, если данные отличаются. Рассчитывается для совпадающих систем-источников. Низкая скорость выполнения за счет ресурсоемкости.
- resolveByMatching (флаг) – При активном флаге: во время вставки записи производится проверка. Если запись не была идентифицирована по ключам (по внешнему ключу, ключу эталона, ориджина), то будет осуществлен поиск дубликатов в Elasticsearch (по правилам с предварительной кластеризацией). В случае, если будут обнаружены дубликаты, запись будет вставлена как update для первого из найденных эталонов, при этом изменения не будут отображены на экране «Исходная запись». Работает только в режиме SMALL

После импорта данных может потребоваться выполнение переиндексации.

Импорт модели данных возможен не только полным архивом, но и частично, например, только записи, только связи или данные классификаторов с данными записей. Доступны любые сочетания элементов модели данных: записей, классификаторов, связей.

В результате выполнения операции в уведомлениях доступен архив с отчетами о выполнении: отчет о данных и отчет о связях. Количество записей в отчете настраивается в <CONF_DIR>/backend.properties параметром unidata.job.import_data.report_size. При установке значения «-1» происходит выборка всех.

Пропуск данных настраивается в JSON-маппинге путем изменения полей processRecords, processClassifiers, processRelations.

7.3.1.1. Параметры операции

- **Имя пользователя** (поле ввода). Логин учетной записи. Определяет, с правами какой учетной записи будет запускаться операция. Если поле пустое, то при запуске по Cron-выражению у операции будут полные права на любой реестр/справочник; при запуске через интерфейс у операции будут права текущей учетной записи. Для учетной записи оператора данных может понадобиться настроить права на реестры/справочники.
- **Очищать индексы** (флаг). Удаляет старые индексы и создает новые.
- **Не создавать стандартный отчет** (флаг). Отключает запись событий в журнал аудита.
- **Обновить маппинги** (флаг). Обновляет маппинги индекса.
- **Проиндексировать объекты модели** (выпадающий список). Реестр/справочник для которого будет выполнена переиндексация (доступен выбор нескольких). По умолчанию установлено значение All - операция выполняется для всех реестров/справочников.
- **Размер блока** (поле ввода). Размер блока загружаемых данных (количество записей). Значение по умолчанию 1024.
- **Проиндексировать бизнес-процессы** (выпадающий список). Выбирает имена бизнес-процессов, данные которых будут переиндексированы. Если параметр отключен, то процессы не индексируются. Параметр доступен при наличии модуля бизнес-процессов.
- **Проиндексировать данные бизнес-процессов** (флаг). Отключает или включает параметр. Параметр доступен при наличии модуля бизнес-процессов.
- **Проиндексировать записи** (флаг). Запускает переиндексацию записей.
- **Проиндексировать связи** (флаг). Запускает переиндексацию связей.
- **Проиндексировать черновики записи** (флаг). Запускает индексацию черновиков записей и их дочерних сущностей (связей и т.п.) в индексы черновиков выбранных реестров/справочников.
- **Проиндексировать черновики** (флаг). Выполняет индексацию черновиков в индекс `default_default_[draft]`
- **Проиндексировать модель данных** (флаг). Выполняет индексацию модели данных в индекс `default_default_[model]`
- **Проиндексировать классификацию** (флаг). Запускает переиндексацию классификации.
- **Обновить данные таблиц сопоставления** (флаг). Запускает процесс поиска дубликатов записей по настроенным правилам. См. отличие от matchingJob.
- **Писать лог ошибок** (флаг). Сохраняет данные неудачных интервалов

фиксации в БД.

- **Обработать лог ошибок** (флаг). Активирует режим дообработки накопленных неудачных запросов.

7.3.1.2. Когда применяется

Операция запускается в случаях:

- Если производились значимые изменения модели данных, записях, классификации, таблицы сопоставления и т.д.
- Если есть сомнения в актуальности данных в индексе. Например, не отображается часть записей.
- Если было загружено много данных, и они не отображаются.
- Если индекс данных был очищен вручную.

Периодичность запуска определяется администратором системы с учетом рабочих задач по обслуживанию Юниверс MDM.

7.3.1.3. Лог ошибок

> Примечание:
>
> Одновременно должен быть включен только один параметр: Писать лог ошибок (writeIdLog) ИЛИ Обработать лог ошибок (processIdLog)

Писать/Обработать лог ошибок сохраняет в БД информацию о записях, не попавших в индекс, чтобы при дальнейшем запуске была возможность дообработать только неудачно завершившуюся часть, что существенно экономит время на полную переиндексацию большого количества записей.

Параметры используются в случае, когда происходит прерывание очереди индексации Opensearch и завершение индексирующих запросов с ошибкой *EsRejectedExecutionException*. Во всех остальных случаях параметры должны быть **отключены**.

В случае, если необходимо переиндексировать большие данные:

- сперва запускается операция с *Писать лог ошибок*.
- затем, если остаются неиндексированные данные, то запустить операцию повторно, выключив *Писать лог ошибок* и включив *Обработать лог ошибок*.

Также при больших данных можно отключать параметры *Очищать индексы* и *Обновить маппинги*.

7.3.1.4. Механизм работы параметра "Размер блока" (blockSize)

Все количество обрабатываемых записей делится на части по blockSize записей.

Затем в каждой части обрабатывается одним тредом по `com.unidata.mdm.job.reindex.data.commit.interval` записей (в памяти держится информация по этому количеству записей, при переходе к следующим записям память очищается), пока не кончатся записи.

Параметр `com.unidata.mdm.job.reindex.data.commit.interval`, как правило, не нуждается в редактировании. Рекомендуемого значения 1024 достаточно для большинства задач. Чем больше этот параметр, тем больше памяти может быть занято в один момент времени. Если этот параметр больше, чем blockSize, то фактически этот параметр будет равен blockSize.

`org.unidata.mdm.job.reindex.data.threads` – количество одновременно обрабатываемых тредов.

Параметры `com.unidata.mdm.job.reindex.data.commit.interval` и `org.unidata.mdm.job.reindex.data.threads` задаются в **backend.properties**.

Таким образом, следует выбирать `org.unidata.mdm.job.reindex.data.threads` по количеству логических ядер процессора (использовать равное или меньшее число, в зависимости от наличия другой нагрузки на процессор).

При указании небольшого blockSize легче отслеживать прогресс операции через UI (менеджер запусков > выбрать запуск > количество выполненных шагов). С точки зрения производительности лучше использовать достаточно большой blockSize, чтобы количество мигрируемых записей было примерно равно **N * blockSize * com.unidata.mdm.job.reindex.data.threads**, где N – не слишком большое натуральное число, например, 1.

Если blockSize слишком большой (например, 500000), то часть данных может не записаться, но при этом операция завершится успешно.

Настройка blockSize необходима для баланса между объемом обрабатываемых данных и количеством потоков. Плохо, когда создается очень много потоков, и так же плохо когда 1 поток обрабатывает слишком много данных сразу. Поэтому желательно выбирать средние значения исходя из доступных ресурсов сервера.

Также blockSize необходимо выбирать в соответствии с общим количеством данных чтобы количество партиций не было слишком большим. На таких больших данных, как в справочнике с адресами, оптимальным вариантом является 500-2000 партиций.

Обработка данных происходит последовательно: записи > связи > классификаторы > бизнес-процессы > матчинг. Сначала завершается обработка одного типа данных, затем происходит переход к другому. Обрабатываются те типы данных, которые есть в наличии.

7.3.2. Операция переиндексации данных (reindexDataJob)

Операция переиндексации данных предназначена для запуска индексации поисковой системы при значимых изменениях в структуре записей или при добавлении новых данных. Индексированные данные ускоряют поиск и отображаются в интерфейсе пользователя.

По условиям лицензирования у операции reindexDataJob может быть отключена многопоточность. В таком случае операция будет запускаться только на одном узле кластера.

7.3.2.1. Параметры операции

- **Имя пользователя** (поле ввода). Логин учетной записи. Определяет, с правами какой учетной записи будет запускаться операция. Если поле пустое, то при запуске по Cron-выражению у операции будут полные права на любой реестр/справочник; при запуске через интерфейс у операции будут права текущей учетной записи. Для учетной записи оператора данных может понадобиться настроить права на реестры/справочники.
- **Очищать индексы** (флаг). Удаляет старые индексы и создает новые.
- **Не создавать стандартный отчет** (флаг). Отключает запись событий в журнал аудита.
- **Обновить маппинги** (флаг). Обновляет маппинги индекса.
- **Проиндексировать объекты модели** (выпадающий список). Реестр/справочник для которого будет выполнена переиндексация (доступен выбор нескольких). По умолчанию установлено значение All - операция выполняется для всех реестров/справочников.
- **Размер блока** (поле ввода). Размер блока загружаемых данных (количество записей). Значение по умолчанию 1024.
- **Проиндексировать бизнес-процессы** (выпадающий список). Выбирает имена бизнес-процессов, данные которых будут переиндексированы. Если параметр отключен, то процессы не индексируются. Параметр доступен при наличии модуля бизнес-процессов.
- **Проиндексировать данные бизнес-процессов** (флаг). Отключает или включает параметр. Параметр доступен при наличии модуля

бизнес-процессов.

- **Проиндексировать записи** (флаг). Запускает переиндексацию записей.
- **Проиндексировать связи** (флаг). Запускает переиндексацию связей.
- **Проиндексировать черновики записи** (флаг). Запускает индексацию черновиков записей и их дочерних сущностей (связей и т.п.) в индексы черновиков выбранных реестров/справочников.
- **Проиндексировать черновики** (флаг). Выполняет индексацию черновиков в индекс `default_default_[draft]`.
- **Проиндексировать модель данных** (флаг). Выполняет индексацию модели данных в индекс `default_default_[model]`.
- **Проиндексировать классификацию** (флаг). Запускает переиндексацию классификации.
- **Обновить данные таблиц сопоставления** (флаг). Запускает процесс поиска дубликатов записей по настроенным правилам. См. отличие от matchingJob.
- **Писать лог ошибок** (флаг). Сохраняет данные неудачных интервалов фиксации в БД.
- **Обработать лог ошибок** (флаг). Активирует режим дообработки накопленных неудачных запросов.

7.3.2.2. Когда применяется

Операция запускается в случаях:

- Если производились значимые изменения модели данных, записях, классификации, таблицы сопоставления и т.д.
- Если есть сомнения в актуальности данных в индексе. Например, не отображается часть записей.
- Если было загружено много данных, и они не отображаются.
- Если индекс данных был очищен вручную.

Периодичность запуска определяется администратором системы с учетом рабочих задач по обслуживанию Юниверс MDM.

7.3.2.3. Лог ошибок

Примечание:
Одновременно должен быть включен только один параметр: Писать лог ошибок (writeIdLog) ИЛИ Обработать лог ошибок (processIdLog)

Писать/Обработать лог ошибок сохраняет в БД информацию о записях, не попавших в индекс, чтобы при дальнейшем запуске была возможность

дообработать только неудачно завершившуюся часть, что существенно экономит время на полную переиндексацию большого количества записей.

Параметры используются в случае, когда происходит прерывание очереди индексации Opensearch и завершение индексирующих запросов с ошибкой *EsRejectedExecutionException*. Во всех остальных случаях параметры должны быть **отключены**.

В случае, если необходимо переиндексировать большие данные:

- сперва запускается операция с *Писать лог ошибок*.
- затем, если остаются неиндексированные данные, то запустить операцию повторно, выключив *Писать лог ошибок* и включив *Обработать лог ошибок*.

Также при больших данных можно отключать параметры *Очищать индексы* и *Обновить маппинги*.

7.3.2.4. Механизм работы параметра "Размер блока" (blockSize)

Все количество обрабатываемых записей делится на части по blockSize записей.

Затем в каждой части обрабатывается одним тредом по `com.unidata.mdm.job.reindex.data.commit.interval` записей (в памяти держится информация по этому количеству записей, при переходе к следующим записям память очищается), пока не кончатся записи.

Параметр `com.unidata.mdm.job.reindex.data.commit.interval`, как правило, не нуждается в редактировании. Рекомендуемого значения 1024 достаточно для большинства задач. Чем больше этот параметр, тем больше памяти может быть занято в один момент времени. Если этот параметр больше, чем blockSize, то фактически этот параметр будет равен blockSize.

`org.unidata.mdm.job.reindex.data.threads` – количество одновременно обрабатываемых тредов.

Параметры `com.unidata.mdm.job.reindex.data.commit.interval` и `org.unidata.mdm.job.reindex.data.threads` задаются в **backend.properties**.

Таким образом, следует выбирать `org.unidata.mdm.job.reindex.data.threads` по количеству логических ядер процессора (использовать равное или меньшее число, в зависимости от наличия другой нагрузки на процессор).

При указании небольшого blockSize легче отслеживать прогресс операции через UI (менеджер запусков > выбрать запуск > количество выполненных шагов). С точки зрения производительности лучше использовать достаточно большой

blockSize, чтобы количество мигрируемых записей было примерно равно **N * blockSize * com.unidata.mdm.job.reindex.data.threads**, где N – не слишком большое натуральное число, например, 1.

Если blockSize слишком большой (например, 500000), то часть данных может не записаться, но при этом операция завершится успешно.

Настройка blockSize необходима для баланса между объемом обрабатываемых данных и количеством потоков. Плохо, когда создается очень много потоков, и так же плохо когда 1 поток обрабатывает слишком много данных сразу. Поэтому желательно выбирать средние значения исходя из доступных ресурсов сервера.

Также blockSize необходимо выбирать в соответствии с общим количеством данных чтобы количество партиций не было слишком большим. На таких больших данных, как в справочнике с адресами, оптимальным вариантом является 500-2000 партиций.

Обработка данных происходит последовательно: записи > связи > классификаторы > бизнес-процессы > матчинг. Сначала завершается обработка одного типа данных, затем происходит переход к другому. Обрабатываются те типы данных, которые есть в наличии.

7.3.3. Операция переприменения данных (reapplyDataJob)

Операция переприменяет правила качества данных к записям, запускает правила, индексирует и сохраняет в БД результаты.

Параметры операции определяют, на каких объектах модели (реестрах/справочниках) какие наборы правил качества запускать. Например, если набор правил X настроен на реестры 1 и 2, а в параметрах операции выбраны набор X и только реестр 1, то переприменяться будут только правила набора X для данных реестра 1.

7.3.3.1. Параметры операции

- **Имя пользователя** (поле ввода). Логин учетной записи. Определяет, от имени какого пользователя фиксируются изменения - пишутся аудит и штампы в индексе и БД. Отчет о выполнении приходит пользователю, запустившему операцию. Проверка прав не происходит.
- **Наборы правил** (выпадающий список). Перечень наборов правил качества, созданных в разделе "Качество данных".
- **Переприменить для объектов модели** (выпадающий список). Перечень

реестров/справочников, для которых будет применена операция.
- **Размер блока** (поле ввода). Размер блока загружаемых данных. По умолчанию 1024.

Примечания:

- Операция не проводит ремаппинг модели данных;
- Не может запускаться повторно в случае возникновения ошибок;
- Не инициирует сопоставление записей;
- Отчет о выполнении не содержит информацию о количестве обработанных записей.

7.3.3.2. Когда применяется

Операция запускается в случаях:

- Если производились значимые изменения в правилах качества данных.
- При обновлении модели данных, добавлении новых атрибутов, а также при создании новых правил качества или изменении существующих.
- Если есть сомнения в актуальности правил качества.
- Если необходимо заново переприменить качества данных к записям.

Периодичность запуска определяется администратором системы с учетом рабочих задач по обслуживанию Юниверс MDM.

7.3.3.3. Взаимосвязь с потоками выполнения

Операция переприменения имеет собственные потоки выполнения: [BATCH_RECORD_UPSERT_START]${reapply-records-bulk-pipeline} (общий массовый поток) и [RECORD_UPSERT_START]${reapply-records-worker-pipeline} (поток, определяющий действия с каждой записью отдельно).

- Для корректной работы с наборами правил, настроенными на фазу ETALON, необходимо добавить сегмент типа Point - RECORD_UPSERT_QUALITY_ETALON в поток {reapply-records-worker-pipeline}.
- Операция не применяется для работы с наборами правил, настроенными на фазу ORIGIN.

7.3.3.4. Механизм работы параметра "Размер блока" (blockSize)

Все количество обрабатываемых записей делится на части по blockSize записей.

Затем в каждой части обрабатывается одним тредом по

`com.unidata.mdm.job.reapply.data.commit.interval` – записей (в памяти держится информация по этому количеству записей, при переходе к следующим записям память очищается), пока не кончатся записи.

Параметр `com.unidata.mdm.job.reapply.data.commit.interval`, как правило, не нуждается в редактировании. Рекомендуемого значения 1024 достаточно для большинства задач. Чем больше этот параметр, тем больше памяти может быть занято в один момент времени. Если этот параметр больше, чем blockSize, то фактически этот параметр будет равен blockSize.

`org.unidata.mdm.job.reapply.data.threads` – количество одновременно обрабатываемых тредов.

Параметры `com.unidata.mdm.job.reapply.data.commit.interval` и `org.unidata.mdm.job.reapply.data.threads` задаются в **backend.properties**.

Таким образом, следует выбирать `org.unidata.mdm.job.reapply.data.threads` по количеству логических ядер процессора (использовать равное или меньшее число, в зависимости от наличия другой нагрузки на процессор).

При указании небольшого blockSize легче отслеживать прогресс операции через UI (менеджер запусков > выбрать запуск > количество выполненных шагов). С точки зрения производительности лучше использовать достаточно большой blockSize, чтобы количество мигрируемых записей было примерно равно **N * blockSize * com.unidata.mdm.job.reapply.data.threads**, где N – не слишком большое натуральное число, например, 1.

Если blockSize слишком большой (например, 500000), то часть данных может не записаться, но при этом операция завершится успешно.

Настройка blockSize необходима для баланса между объемом обрабатываемых данных и количеством потоков. Плохо, когда создается очень много потоков, и так же плохо когда 1 поток обрабатывает слишком много данных сразу. Поэтому желательно выбирать средние значения исходя из доступных ресурсов сервера.

Также blockSize необходимо выбирать в соответствии с общим количеством данных чтобы количество партиций не было слишком большим. На таких больших данных, как в справочнике с адресами, оптимальным вариантом является 500-2000 партиций.

Обработка данных происходит последовательно: записи > связи > классификаторы > бизнес-процессы > матчинг. Сначала завершается обработка одного типа данных, затем происходит переход к другому. Обрабатываются те типы данных, которые есть в наличии.

7.3.4. Операция консолидации данных (duplicateJob)

Операция предназначена для объединения кластера записей, их очищения и сопоставления записей из таблиц.

Операция выполняет объединяет кластера записей, но не производит поиск дублирующихся записей. После объединения кластеров дубликатов операция снова проверяет получившиеся наборы записей на дубликаты (т.е. уже сами объединенные записи могут сформировать кластера).

Для поиска новых / обновления существующих дубликатов записей используется Операция сопоставления данных (matchingJob).

7.3.4.1. Параметры операции

- **Имя пользователя** (поле ввода). Логин учетной записи, от имени которой будут выполняться действия операции.
- **Наборы правил** (выпадающий список). Перечень наборов правил, которые будут обработаны операцией (будут консолидированы, обновлены или удалены кластера только для выбранных правил).
- **Размер блока** (поле ввода). Размер блока загружаемых данных. По умолчанию 1024.
- **Назначенная сущность** (выпадающий список). Сущность, записи которой будут консолидированы по выбранным наборам. Если оставить параметр пустым - будут консолидироваться записи по каждой сущности.

7.3.4.2. Когда применяется

Операция запускается в случаях:

- Если необходимо объединить кластера дубликатов записей, найденных ранее (в ходе работы Операции сопоставления данных (matchingJob)).
- Если производились значимые изменения в таблицах сопоставления записей.
- Если есть сомнения в актуальности кластеров дубликатов.

Периодичность запуска определяется администратором системы с учетом рабочих задач по обслуживанию Юниверс MDM.

С помощью триггеров можно настроить последовательное выполнение операций matchingJob > duplicateJob.

7.3.5. Операция экспорта аудита (exportAuditJobName)

Операция выгружает логи аудита.

7.3.5.1. Параметры операции

- **Куда сохранить лог** - по умолчанию значение: Notification (Уведомления системы).
- **Включить заголовок в файл** - флаг, включающий строки с датой выгрузки и описание форматов в файл экспорта.
- **Формат экспорта** - выпадающий список: CEF или SEQ.
- **От какой даты выгрузить логи** - дата начала периода выгрузки. Если дата не указана, то проставляется текущая - количество дней из параметра "Период выгрузки". Если указана конкретная дата - количество дней из параметра "Период выгрузки".
  - `a - b = ç` где **a** - параметр "От какой даты выгрузить логи", **b** - параметр "Период выгрузки", **c** - диапазон выгрузки логов.
- **Имя пользователя** - системное имя пользователя, имеющего права на экспорт.
- **Период выгрузки** - количество дней для отображения в выгрузке (по умолчанию 1d). Указывается число и далее символ m (минуты), h (часы), d (дни), M (месяцы), y (годы).
- **Размер блока экспортируемых данных** - размер блока загружаемых данных, по умолчанию = 5000.
- **Источник логов для экспорта** - выпадающий список: opensearch (поисковый индекс) или db (база данных).

7.3.5.2. Когда применяется

Операция запускается при необходимости. В случае, если необходимо выгрузить логи аудита и сохранить их.

7.3.6. Операция экспорта данных (exportDataJob)

Операция экспорта данных предназначена для выгрузки данных в стороннюю информационную систему.

7.3.6.1. Параметры операции

- **Пропустить связи** (флаг). Флаг пропуска связанных записей.
- **Дата среза** (дата). Экспортировать период, актуальный на этот момент времени.
- **ID операции** (поле ввода). Идентификатор загрузки.
- **Описание структуры данных** (поле ввода). Описание загружаемых данных

в формате JSON, выполненное в соответствии со схемой Юниверс MDM.

- **Пропустить удаленные** (флаг). Флаг пропуска записей, помеченных как удаленные.
- **Обновлено после** (дата). Выбор только записей, имеющих версии после указанной даты (то есть будут экспортированы только те записи, которые были обновлены после этой даты).
- **URL базы данных** (поле ввода). JDBC URL базы данных для выполнения экспорта.
- **Размер блока** (поле ввода). Размер блока загружаемых данных. По умолчанию 1024.

7.3.6.2. Когда применяется

Операция запускается при необходимости. В случае, если необходимо выгрузить данные в другую информационную систему.

7.3.7. Операция сопоставления данных (matchingJob)

Операция предназначена для поиска новых / обновления существующих дубликатов записей в выбранных наборах правил сопоставления. Операция обновляет таблицы сопоставления, формируя тем самым кластеры дубликатов.

Операция выполняет первичный поиск и формирование кластеров, но не объединяет кластера. Для объединения используется Операция консолидации данных (duplicateJob).

7.3.7.1. Параметры операции

- **Имя пользователя** (поле ввода). Логин учетной записи, от имени которой будут выполняться действия операции.
- **Размер блока наборов правил** (поле ввода). Количество одновременно обрабатываемых наборов правил при запуске операции. По умолчанию 10.
- **Наборы правил** (выпадающий список). Список наборов правил, которые следует обработать операции.
- **Размер блока обновления таблиц** (поле ввода). Количество одновременно обрабатываемых записей (в таблице сопоставления) при запуске операции. По умолчанию 1024.

Примечания:

- В операцию не входит функция консолидации кластеров, вне зависимости от того, включена автоконсолидация или нет.

- В уведомлении о завершении операции выводится количество полученных кластеров. Можно скачать csv файл с их описанием.

7.3.7.2. Когда применяется

Операция запускается в случаях:

- Если необходимо сформировать кластера дубликатов записей (найти дубликаты в данных).
- При обновлении модели сопоставления данных (например, если добавлена новая колонка). В этом случае следует пересчитать и таблицы, и кластера записей.
- При изменении алгоритма поиска (регистронезависимый --> регистрозависимый, точный --> нечеткий). В этом случае следует пересчитать кластера записей.
- При пакетной загрузке записей с отключенным real-time matching (XLSX/REST/Custom). В результате формируются таблицы сопоставления, следует пересчитать матчинг. Затем рекомендуется включить real-time matching, чтобы поиск дубликатов работал после одиночных вставок.

Периодичность запуска определяется администратором системы с учетом рабочих задач по обслуживанию Юниверс MDM.

С помощью триггеров можно настроить последовательное выполнение операций matchingJob > duplicateJob.

7.3.7.3. Сравнение с reindexDataJob

Операцию переиндексации (reindexDataJob) стоит запускать, когда поменялась модель данных, и необходимо обновить под нее поисковые индексы; либо, когда с индексами что-то произошло, и нужно их починить.

Операцию сопоставления данных (matchingJob) стоит запускать, когда поменялась модель сопоставления данных или когда необходимо произвести массовое сопоставление.

reindexDataJob с флагом "Обновить данные таблиц сопоставления" в части индексов сопоставления:

1. Обновляет таблицы матчинга (с ними работают алгоритмы матчинга).
2. Вычисляет кластеры дубликатов: если включен real-time матчинг (параметр org.unidata.mdm.matching.data.real.time.matching.enabled в backend.properties).

Особенности reindexDataJob: можно выбирать, записи **каких**

реестров/справочников будут затронуты.

matchingJob делает следующее:

1. Обновляет таблицы матчинга (с ними работают алгоритмы матчинга).
2. Вычисляет кластеры дубликатов вне зависимости от того, включен real-time или нет.

Особенности matchingJob:

- Можно выбирать, по каким **наборам правил сопоставления** будут затронуты записи.
- Более подробное уведомление по результату работы операции.

7.4. Маппинг данных

Соответствие загружаемых данных модели задается в файле преобразования данных формата JSON.

Основные объекты модели данных – справочники и реестры, каждый из которых должен быть представлен отдельно в файле преобразования данных. Объект содержит поля, описывающие основные параметры, необходимые для интеграции, а также массивы внутренних объектов (атрибутов и связей), составляющих структуру основного.

В свою очередь, объекты реестров должны быть объединены в массив реестров (*entities*), а справочники – в массив справочников (*lookupEntities*). Задание соответствия данных модели требуется для операции экспорта данных.

Содержание маппингов помещается в Описание структуры данных операции экспорта. Кроме того, в операции должна быть указана ссылка на базу данных (поле URL базы данных).

7.4.1. Маппинг экспорта данных

Элементом маппинга первого уровня может выступать:

- *entities* – в случае описания реестров;
- *lookupEntities* – в случае описания справочников.

Ниже приведена структура маппинга для описания реестров/справочников.

Таблица 1 – Структура маппинга операции экспорта данных

Элементы				Значения	Описание
1 уровня	2 уровня	3 уровня	4 уровня		
entities					Описание реестров
	name				Имя реестра/справочника
	@type			DB	Тип источника данных
	fields				Атрибуты реестра
		name			Имя атрибута
		@type		DB	Тип источника данных
		column			Столбец базы данных для экспорта информации
	updateMark				Метка обновления
		update MarkType		TIMESTAMP	Тип метки обновления
		@type		DB	Тип источника данных
		column			Столбец БД для экспорта информации
		source System Column			Столбец БД, в который будет выгружено название источника данных записи
	multi Version			true, false	Применяется при обновлении записей с одинаковым External ID (если таковые существуют) [#]
	joins				SQL запрос для объединения данных
	natural Key				Идентификатор записи во внешней системе
		@type		DB	Тип источника данных
		alias			Псевдоним для полученного ключа
		column			Столбец базы данных для экспорта информации
		type			Тип значения атрибута [#]
	dqErrors Section				Секция ошибок качества данных
		@type		DB	Тип источника данных
		table			Таблица базы данных

		external IdField			Внешнее поле идентификатора
		status Field			Поле статуса
		ruleName Field			Поле имени правила
		message Field			Поле сообщения
		severity Field			Поле критичности правила
		category Field			Поле категории
	source System				Название источника данных
	tables				Таблицы базы данных, в которые будут экспортированы данные
	version Range				Описание периодов актуальности
		normalize From		true, false	Признак нормализации даты начала периода [#]
		normalize To		true, false	Признак нормализации даты конца периода [#]
		valid From			Актуален от
			name		Имя атрибута
			@type	DB	Тип источника данных
			column		Столбец базы данных для экспорта информации
			type	"java.lang.String", "java.lang.Integer", "java.sql.Timestamp"	Тип атрибута
		validTo			Актуален до
			name		Имя атрибута
			@type	DB	Тип источника данных
			column		Столбец базы данных для экспорта информации
			type	"java.lang.String", "java.lang.Integer", "java.sql.Timestamp"	Тип атрибута

		isActive			Признак активности периода/всей записи данных/связей [#]_

Примечания:

- **multiVersion** - Применяется в случае, если существуют дублирующиеся по External ID записи. Это может быть необходимо для дозагрузки накопленных/обновившихся данных или для обновления разных периодов актуальности в пределах одной записи.
  - *False* – при загрузке записи будут восприниматься как разные, даже если имеют одинаковый External ID.
  - *True* – несколько версий одной записи будут загружаться как обновления одной записи. Если нет явной цели объединения записей, то рекомендуется как более безопасный вариант использовать значение false. Если порядок вставки важен, то необходимо сортировать записи (связи). При этом, сортировка не влияет на процесс формирования эталонной записи. Параметр используется для записей и всех видов связей.
- **type** (для naturalKey) - Тип значения атрибута указывается из пакета java.lang.
  - *Время, дата и дата/время*: java.lang.Date или java.lang.Timestamp.
  - *Логический*: java.lang.Boolean.
  - *Строковый*: java.lang.String.
  - *Численный*: java.lang.Double.
  - *Целочисленный*: java.lang.Integer или java.lang.Long.
  - *Файл и текстовый файл* не импортируются и не экспортируются.
- **normalizeFrom** - Если установлено значение *true*, то часы, минуты и миллисекунды даты начала периода будут обнулены, т.е. приведены к виду: 00:00:00:000.
- **normalizeTo** - Если установлено значение *true*, то часы, минуты и миллисекунды даты конца периода будут приведены к виду 23:59:59:999.
- **isActive** - Необходима возможность привести значение такого поля к булеву значению. Пример: "isActive" : { "name" : "IS_ACTIVE", "@type" : "DB", "column" : "v.is_active", "type" : "java.lang.Boolean" }.

8. Библиотеки

8.1. Описание

Раздел "Библиотеки" предназначен для загрузки пользовательских библиотек в формате **.jar**, расширяющих функциональность системы.

Библиотеки могут использоваться для:

- Добавления пользовательской функции обработки данных.
- Расширения бизнес-процессов: добавления новых сервисных задач и слушателей для различных событий.
- Добавления пользовательских сегментов пайплайнов.
- Добавление другого пользовательского кода.

Файлы библиотек могут содержать описания объектов одного или нескольких типов.

Например, один .jar-файл библиотеки может включать в себя описания краулера БД PostgreSQL и пользовательской функции очистки данных. Далее описание необходимого объекта будет добавляться в систему с помощью мастера библиотек соответствующего раздела: описание краулера БД PostgreSQL – в разделе "Краулеры" при добавлении нового краулера, описание функции очистки – в разделе "Качество данных" при создании новой функции.

8.2. Добавление новой библиотеки

Чтобы добавить библиотеку:

1. Нажмите кнопку ┼ "Добавить библиотеку", расположенную в правом верхнему углу раздела (Рисунок 1).
2. В результате действия откроется модальное окно загрузки новой библиотеки (Рисунок 2).
3. Чтобы загрузить библиотеку, нажмите *Выбор файла*. После чего выберите необходимый файл с расширением **.jar**.
    - Если загружен неверный файл - наведите курсор на имя файла, при этом справа появится кнопка 🗑 "Удалить файл", на которую следует нажать.
    - Если загружен файл с некорректным расширением, система выдаст ошибку и не даст сохранить библиотеку. В таком случае нажмите *Отмена* или выберите другой файл с расширением **.jar**.

- Для успешной загрузки файл не должен превышать 2Гб (в браузерах Internet Explorer и Mozilla Firefox). Браузеры Google Chrome и Opera допускают загрузку файлов более 4Гб.

4. В поле *Версия в системе* введите порядковый номер версии файла библиотеки.
5. В поле *Описание* доступен ввод краткого описания добавляемой библиотеки.
6. Нажмите кнопку *Загрузить*. Если требуется прервать загрузку – нажмите кнопку *Отмена*.
7. В результате действий в таблицу будет загружена новая библиотека. Загрузка больших файлов может занять более продолжительное время.

Примечания:

- Библиотеки определяются сразу после загрузки, и не требуют перезапуска системы.
- Столбец *Тип* отображает тип библиотеки, который автоматически определяется системой в зависимости от того, какой класс (несколько классов) содержит файл библиотеки. Если в таблице отображается библиотека без типа, то это может быть либо ранее загруженная библиотека, либо библиотека с неизвестными для системы классами. Тип библиотеки отображается только для чтения и не подлежит редактированию. Одна библиотека может иметь несколько типов:
  - Генератор значений атрибутов,
  - Алгоритм,
  - Функция,
  - Краулер,
  - Наблюдатель за задачами,
  - Генератор external ID,
  - Обработчик задач,
  - Наблюдатель за исполнением.

8.3. Управление перечнем библиотек

Обновление библиотек

Если в систему уже загружена библиотека с определенным именем и номером версии, то при повторной загрузке библиотеки (имя и номер версии у которой тоже совпадает), то содержимое библиотеки обновляется. Если у библиотеки отличается имя или версия, то библиотека загружается как новая.

Например, если загружается новая библиотека с функцией обработки данных, то в модели качества данных потребуется выбрать новую функцию (если при этом у функции в старой и в новой библиотеке было одинаковое имя, то в списке будет две функции с одинаковыми именами; если планируется частое обновление функций, то рекомендуется менять не только версию библиотеки, но и добавлять версию в имя функции). Аналогично и с другим содержимым библиотек.

Для сортировки библиотек используйте фильтры:

- **По имени файла**. Нажмите кнопку  "Фильтр", расположенную в правой части столбца *Имя файла*. В пустом поле введите имя, по которому необходимо отфильтровать имеющиеся файлы. Нажмите *Применить*.
- **По версии**. Нажмите кнопку  "Фильтр", расположенную в правой части столбца *Версия*, и включите флаг *Только последние версии*. В результате перечень файлов будет сгруппирован в более сокращенный, где останутся только последние добавленные версии файлов.
- **По типу**. Нажмите кнопку  "Фильтр", расположенную в правой части столбца *Тип*, и выберите необходимые типы библиотек, по которым будет отфильтрована таблица имеющихся файлов. Нажмите *Применить*.

Для удаления библиотеки:

1. В крайнем левом столбце отметьте флагами необходимые для удаления библиотеки.
2. В верхнем правом углу экрана нажмите  *Удалить*.
3. Подтвердите действие.

Для скачивания файла библиотеки:

1. Наведите курсор на строку с необходимой библиотекой.
2. Нажмите  "Скачать" в правом конце строки. Кнопка отображается только при наведении курсора на строку.
3. В результате действия файл будет автоматически скачан на ваше устройство.

8.4. Список библиотек по умолчанию

С дистрибутивом поставляются следующие библиотеки:

- *system-cleanse-functions.jar* - стандартные функции обработки данных. Используются в правилах качества данных.
- *postgresMatchingStorage-algorithms.jar* - стандартный алгоритм поиска дубликатов данных по точному совпадению.

- *data-cleanse-functions.jar* - функции обработки данных для MDM: Проверка уникальности атрибутов, Получение данных из индекса, Получение данных из JDBC, Проверка консистентности ссылок, Проверка значения справочников. Используются в правилах качества данных.
- *system-delegate-executors.jar* - обработчик бизнес-процессов, используется для отправки уведомлений на почту.
- *postgres-sql-crawler.jar* - краулер для БД PostgreSQL.

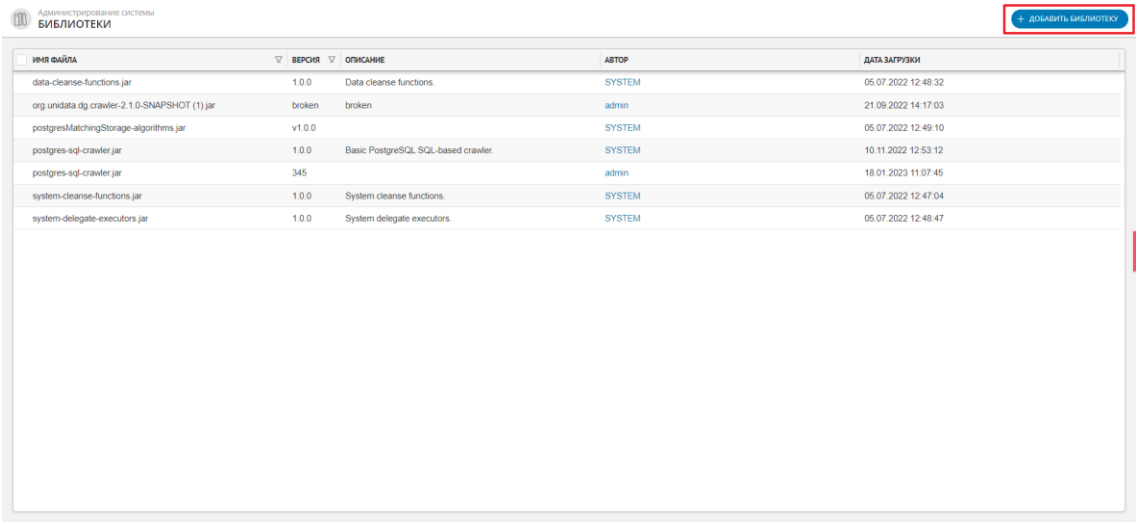


Рисунок 1 - Раздел "Библиотеки" и кнопка "Добавить библиотеку"

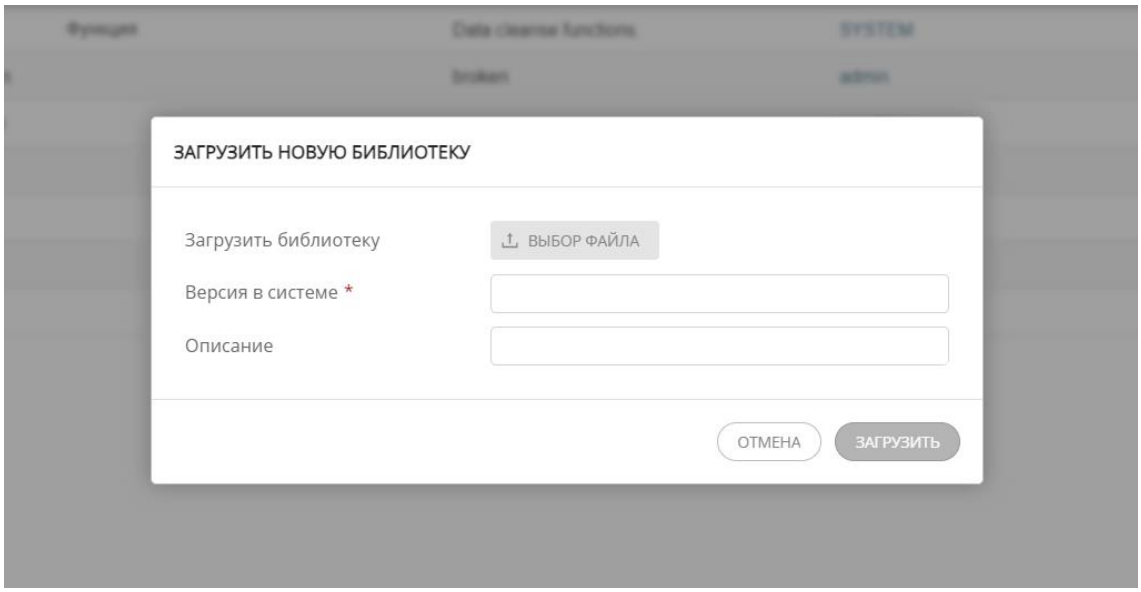


Рисунок 2 - Окно загрузки новой библиотеки

9. Потоки выполнения

Содержание:

9.1. Общие сведения

Раздел "Потоки выполнения" предназначен для редактирования стандартных цепочек операций над данными, используемых системой Юниверс MDM.

За счет редактирования становится доступно:

- Изменение порядка цепочек действий при работе с данными.
- Временное отключение определенных звеньев цепочки действий.
- Интегрирование дополнительных цепочек действий, необходимых для заказчика.

9.1.1. Создание потока выполнения

1. Перейдите в раздел "Потоки выполнения".
2. Нажмите кнопку ⊕ *Создать*, расположенную в нижней части списка потоков выполнения.
3. В результате откроется список стартовых сегментов, из которых нужно выбрать один.
   - **Обязательно**. Если сегмент не был выбран сразу, то задайте сегмент в области **Start**: нажмите кнопку "Выбрать сегмент" и выберите сегмент из списка.
4. Введите имя объекта в поле "Объект", расположенное над блоком стартовых сегментов.
5. Задайте сегмент типа **Point**, в котором будет выполняться основная логика потока. Для этого нажмите кнопку "Добавить сегмент", расположенную под областью "Start" и выберите требуемый сегмент.
6. При необходимости задайте сегмент типа **Connector**, через который будет подключаться новый поток выполнения. Для этого нажмите кнопку "Добавить сегмент", расположенную под областью "Start" и выберите требуемый сегмент.
   - Наличие сегментов Point и Connector зависит от выбранного стартового

сегмента.
- Сегментов типа Point и Connector может быть несколько.
- Доступна настройка порядка запуска таких сегментов.

7. При необходимости задайте сегмент, который будет обрабатывать ошибку выполнения потока. Для этого в области **Fallback** нажмите кнопку "Выбрать сегмент" и выберите требуемый сегмент из списка.
   - Наличие такого сегмента зависит от выбранного стартового сегмента.
8. **Обязательно.** Задайте сегмент, которым будет завершаться поток выполнения. Для этого в области **Finish** нажмите кнопку "Выбрать сегмент" и выберите требуемый сегмент из списка.
9. Нажмите кнопку "Сохранить", расположенную в правом верхнем углу экрана.

9.1.2. Редактирование потока выполнения

1. Выберите требуемый поток выполнения, указанный в списке потоков.
2. Измените или удалите необходимые сегменты потока. Описание выбора сегментов см. выше.
3. Нажмите кнопку "Сохранить", расположенную в правом верхнем углу экрана.

Чтобы удалить поток выполнения, нажмите кнопку *Удалить*, расположенную в правом верхнем углу экрана.

9.1.3. Типы сегментов потока выполнения

- **Start**. Сегмент, с которого будет начинаться поток выполнения. Все последующие сегменты потока предлагаются контекстно, в зависимости от выбранного стартового сегмента.
- **Point**. Сегмент выполнения основной логики потока. Поток выполнения может содержать сразу несколько сегментов Point. Порядок запуска сегментов зависит от порядка их расположения.
- **Connector**. Сегмент подключения новых потоков выполнения. Используется в случае, если в работе одного потока необходимо задействовать другой поток (например, в потоке получения записей использовать поток получения связей).
- **Selector**. Сегмент ветвления стандартного потока на несколько других.
- **Fallback**. Сегмент обработки ошибки выполнения потока. Запускается в случае, если основная логика потока (**Start**, **Point** и **Connector**) завершилась с ошибкой.
- **Finish**. Сегмент, которым будет завершаться поток выполнения.

Примечания:

- В сегментах с типом "Connector" можно просматривать и редактировать данные поля startId и subjectId.

9.1.4. Поиск сегментов потока выполнения

В левой верхней части списка сегментов расположено поисковое поле. Поиск регистронезависимый, ищет сегменты потоков выполнения по их id и description.

Кнопка "Фильтровать" активирует варианты фильтрации сегментов:

- Стартовые сегменты. Поиск только среди стартовых сегментов (обозначены лейблом Start).
- Все сегменты. Поиск среди сегментов всех типов.

Если кнопка "Фильтровать" неактивна, то поиск производится по стартовым сегментам.

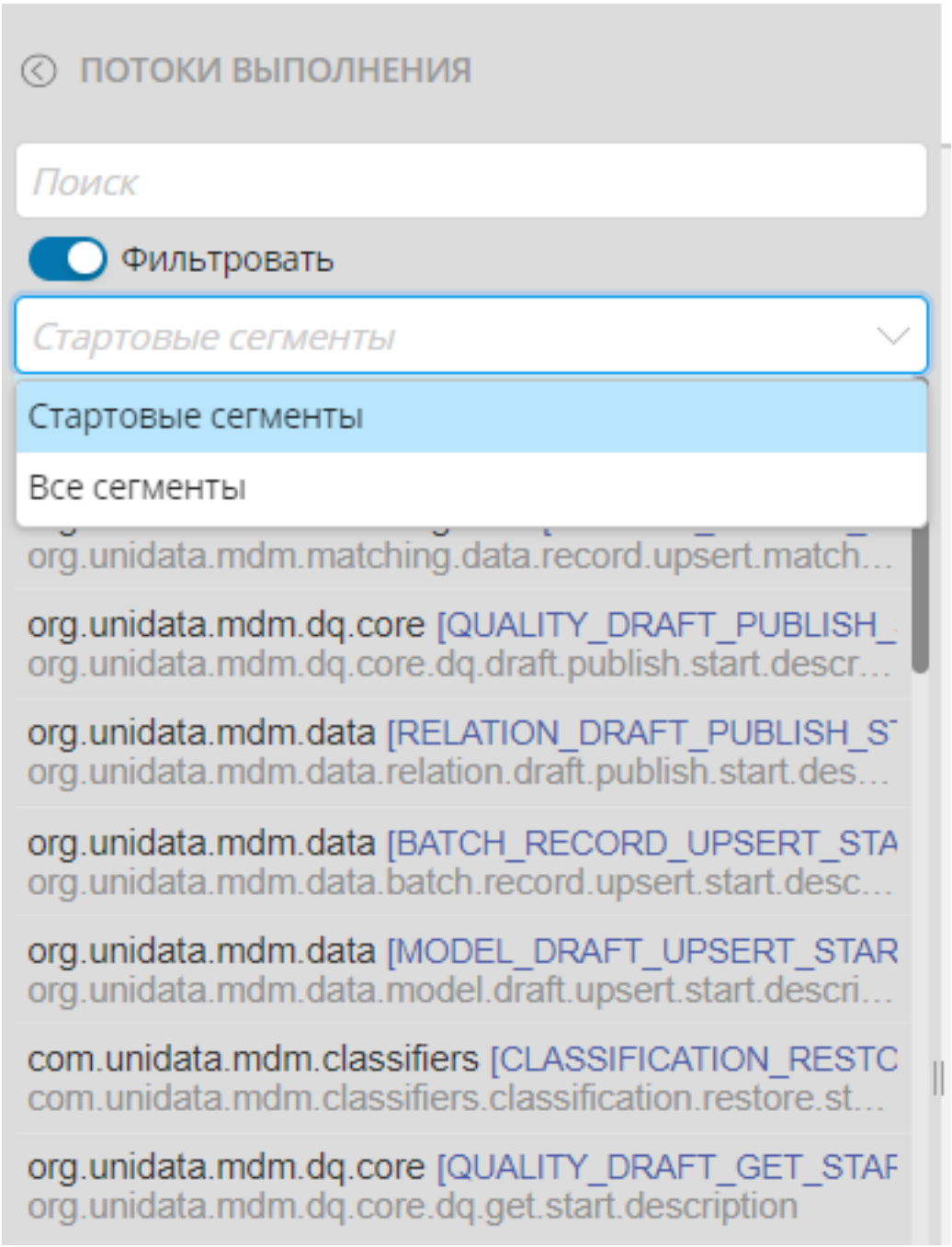


Рисунок 1 - Панель поиска с выбором вариантов фильтрации

9.1.5. Описание основных потоков выполнения

От настройки потоков выполнения напрямую зависит работа основных функций системы. С помощью потоков выполнения также можно редактировать стандартный порядок действий при работе с данными. Все базовые потоки выполнения включены в официальный комплект поставки Юниверс MDM.

Примеры стандартных потоков выполнения:

- Для настройки связей
- Для правил сопоставления
- Для правил качества
- Для бизнес-процессов

9.2. Примеры потоков выполнения

Содержание:

9.2.1. Поток создания и обновления связей

9.2.1.1. Основной поток создания/обновления связей

1. Стартовый сегмент потока: [RELATION_UPSERT_START] - обеспечивает базовую валидацию исходного контекста (наличие связи, проверку существования левого и правого концов связи, корректность статуса записи обновляемой связи). Выполняет настройку исходного контекста.
2. Сегменты типа Point:
   - [RELATION_UPSERT_ACCESS] - выполняет проверку прав пользователя на создание/обновление связи;
   - [RELATION_UPSERT_MEASURED] - нормализует измеряемые атрибуты связи перед сохранением;
   - [RELATION_UPSERT_PERIOD_CHECK] - проверяет корректность границ периода актуальности создаваемой/обновляемой связи.
3. Сегмент типа Selector: [RELATION_UPSERT_SELECTOR] - определяет по какой ветви потока исполнения пойдет процесс создания/изменения связи: черновик [DRAFT] или регулярный поток [REGULAR].
4. Финишный сегмент: [RELATION_UPSERT_FINISH] - возвращает результат создания/обновления связи.

Ветвь потока [DRAFT]:

- [RELATION_UPSERT_MODBOX] - выполняет подготовку внесенных изменений перед вычислением обновленного таймлайна связи;

- [RELATION_UPSERT_TIMELINE] - вычисляет обновленный таймлайн связи. Применяет внесенные изменения к текущему таймлайну связи, вычисляет периоды актуальности, создает эталонную запись связи;
- [RELATION_UPSERT_DRAFT] - выполняет сохранение/обновление черновика связи;
- [RELATION_UPSERT_POSTPROCESSING] - выполняет постобработку атрибутов связи. Вычисляет отображаемые значения для атрибутов типа "Перечисление" и "Ссылка на справочник", заполняет шаблоны ссылок на веб-ресурсы;

Ветвь потока [REGULAR]:

- [RELATION_UPSERT_VALIDATE] - выполняет валидацию атрибутов создаваемой/обновляемой связи и проверяет согласованность данных.
- [RELATION_UPSERT_INDEXING] - вычисляет изменения в поисковом индексе при создании/обновлении связи.
- [RELATION_UPSERT_PERSISTENCE] - применяет изменения, вычисленные при создании/обновлении связи, в базу данных и поисковый индекс.

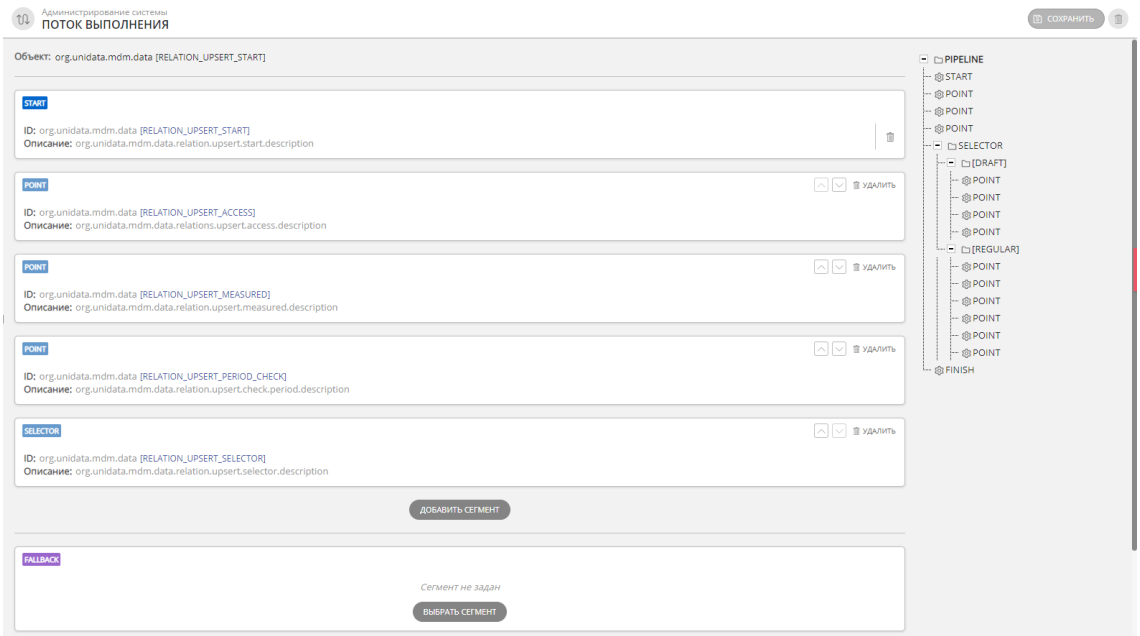


Рисунок 1 - Пример готового потока выполнения

9.2.2. Поток сопоставления данных

Настройка перечисленных потоков выполнения осуществляет сопоставление данных в режиме реального времени в следующих условиях:

- При сохранении изменений записи

- При удалении записи
- Для формирования кластеров запрашиваемой записи
- При пакетном сохранении изменений записей
- При пакетном удалении записей

9.2.2.1. При сохранении изменений записи

1. Стартовый сегмент: [RECORD_UPSERT_START].
2. Сегмент типа Connector: [RECORD_UPSERT_MATCHING_CONNECTOR].
3. Финишный сегмент: [RECORD_UPSERT_FINISH].

9.2.2.2. При удалении записи

1. Стартовый сегмент: [RECORD_DELETE_START].
2. Сегмент типа Connector: [RECORD_DELETE_MATCHING_CONNECTOR].
3. Финишный сегмент: [RECORD_DELETE_FINISH].

9.2.2.3. Для формирования кластеров запрашиваемой записи

1. Стартовый сегмент: [RECORD_GET_START].
2. Сегмент типа Connector: [RECORD_GET_MATCHING_CONNECTOR].
3. Финишный сегмент: [RECORD_GET_FINISH].

9.2.2.4. При пакетном сохранении изменений записей

1. Стартовый сегмент: [BATCH_RECORD_UPSERT_START].
2. Сегмент типа Connector: [BATCH_RECORD_UPSERT_MATCHING_CONNECTOR].
3. Финишный сегмент: [BATCH_RECORD_UPSERT_FINISH].

9.2.2.5. При пакетном удалении записей

1. Стартовый сегмент: [BATCH_RECORD_DELETE_START].
2. Сегмент типа Connector: [BATCH_RECORD_DELETE_MATCHING_CONNECTOR].
3. Финишный сегмент: [BATCH_RECORD_DELETE_FINISH].

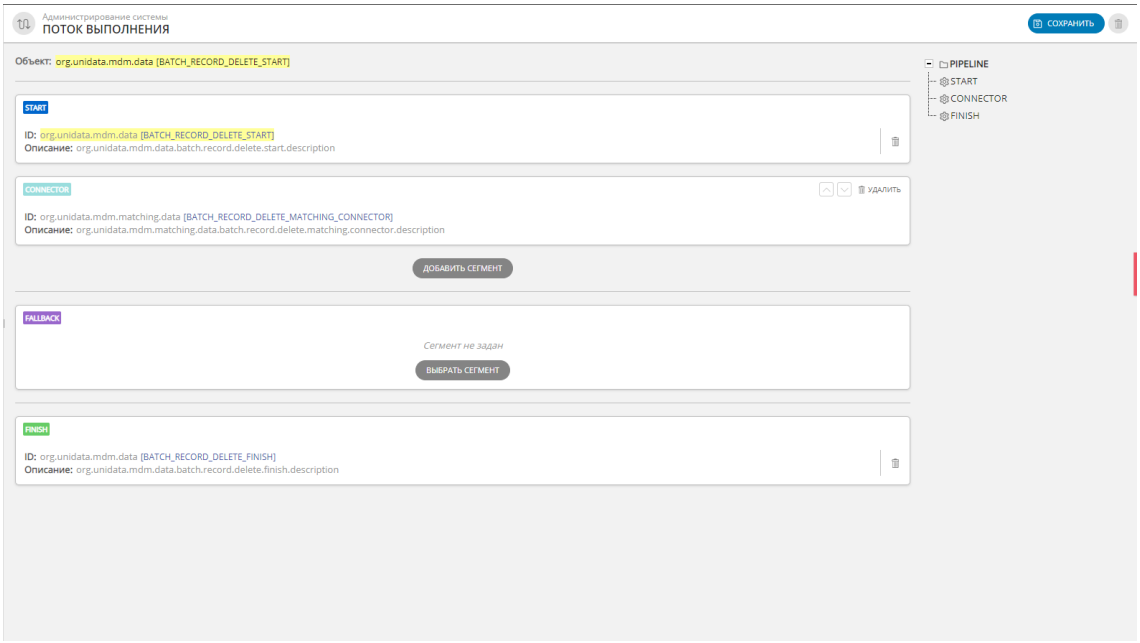


Рисунок 1 - Пример готового потока выполнения

9.2.3. Потоки выполнения правил качества данных

9.2.3.1. Выполнение правил качества

1. Стартовый сегмент: [RECORD_UPSERT_QUALITY_START] - определяет реестр/справочник, для которого будут выполняться правила качества.
2. Сегмент типа Point: [RECORD_UPSERT_QUALITY_POINT] - выполняет назначенные правила качества для всех периодов актуальности записи.
3. Сегмент типа Gate: [RECORD_UPSERT_QUALITY_GATE] - индексирует вычисленные ошибки правил качества и применяет результаты обогащения для записи.
4. Финишный сегмент: [RECORD_UPSERT_QUALITY_FINISH] - возвращает результат исполнения правил качества.

9.2.3.2. Выполнение правил качества при сохранении изменений записи

1. Стартовый сегмент: [RECORD_UPSERT_START] - сохранение изменений записей.
2. Сегмент типа Connector: [RECORD_QUALITY_CONNECTOR] - выполняет проверку назначенных на реестр/справочник наборов правил качества и в случае их наличия запускает поток выполнения правил качества для записей.
3. Финишный сегмент: [RECORD_UPSERT_FINISH] - возвращает результат

сохранения изменений записей.

9.2.3.3. Формирование ошибок правил качества для записи

1. Стартовый сегмент: [RECORD_GET_START].
2. Сегмент типа Connector: [RECORD_GET_QUALITY_CONNECTOR] - получает вычисленные ошибки правил качества для запрашиваемой записи.
3. Финишный сегмент: [RECORD_GET_FINISH].

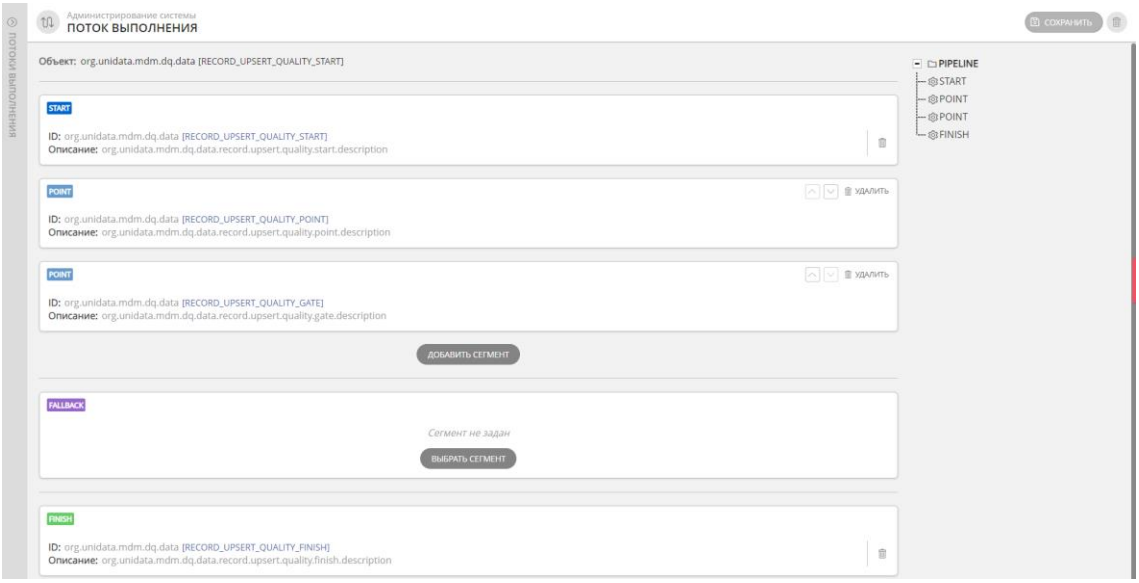


Рисунок 1 - Пример готового потока выполнения

9.2.4. Поток публикации черновика записи

9.2.4.1. Поток стандартной публикации черновика

1. Стартовый сегмент: [RECORD_DRAFT_PUBLISH_START] - выполняет публикацию черновика записей.
2. Финишный сегмент: [RECORD_DRAFT_PUBLISH_FINISH] - завершает публикацию черновика записи.

9.2.4.2. Публикация с учетом наличия бизнес-процессов

1. Стартовый сегмент: [RECORD_DRAFT_PUBLISH_START] - выполняет публикацию черновика записей.
2. Сегмент типа Selector: [RECORD_DRAFT_PUBLISH_WORKFLOW_SELECTOR] - селектор, который добавляет ветвление в стандартный поток (Рисунок 1).

- Если на реестр/справочник назначен бизнес-процесс согласования, то селектор выполнит сегмент [RECORD_DRAFT_PUBLISH_START_WORKFLOW], запускающий процесс согласования изменений, а поток выполнения публикации черновика записи будет прерван.
- Если реестр/справочник не имеет назначенных бизнес-процессов, селектор выполнит пустой сегмент [EMPTY_POINT], и поток выполнения публикации черновика продолжится.

3. Финишный сегмент: [RECORD_DRAFT_PUBLISH_FINISH] - завершает публикацию черновика записи.

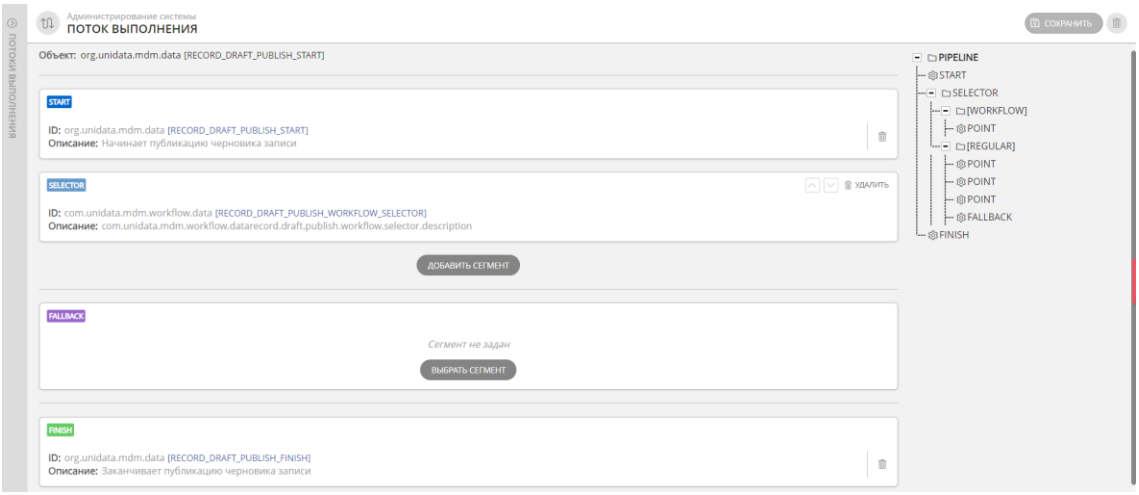


Рисунок 1 - Пример готового потока выполнения

10.Журнал аудита

10.1. Описание

Раздел "Журнал" представляет собой таблицу и предназначен для аудита действий пользователей с данными, а также для просмотра активности пользователей (Рисунок 1). В журнале регистрируются и хранятся события – различные действия, совершенные пользователем (например, создание/изменение или удаление записей реестра/справочника, учетных записей, ролей, операций, групп пользователей и т.д).

События могут быть связаны одной операцией (например, в рамках пакетной обработки данных или фоновой очистке логов в базе данных).

Информация о пользователе, совершившем действия, отображается в столбце "**Имя пользователя**" и подсвечивается оранжевым цветом, если для него существуют заместители. Подробная информация о замещении отображается во всплывающей подсказке при наведении курсора на имя пользователя.

Информация о произошедшем событии отображается в столбце "**Тип сообщения**", подробная детализация события - в столбце "**Детали**".

> **Совет:**
>
> При наведении курсора на сообщение в столбце "Детали" появится всплывающая подсказка с полным описанием события и его деталей (например, Источник [MANUAL] в тексте сообщения означает, что событие - создание/изменение или удаление - было выполнено вручную)

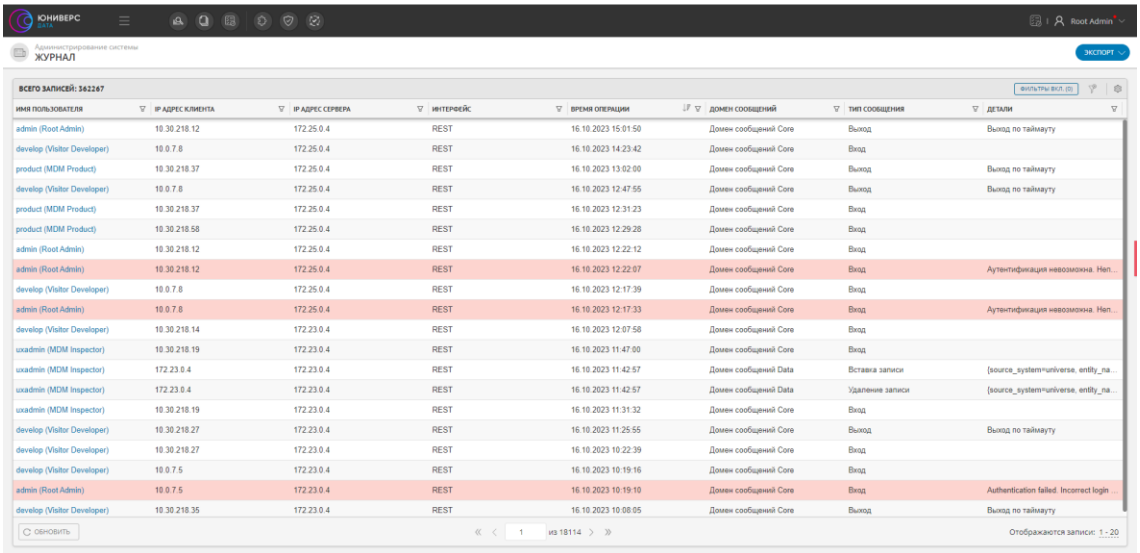


Рисунок 1 - Пример отображения записей в журнале событий

10.2. Навигация по списку событий

В нижней части экрана расположена панель с кнопкой обновления результатов, элементом переключения страниц и выпадающим списком для выбора количества записей, отображаемых на странице (Рисунок 2).

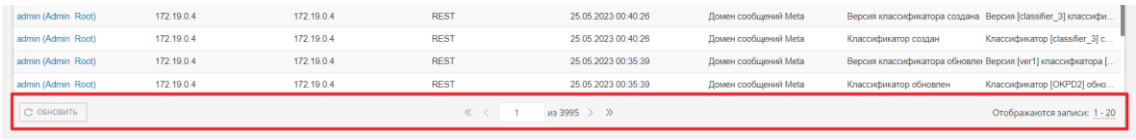


Рисунок 2 - Панель навигации по страницам записей

10.3. Настройка колонок

Для настройки отображения колонок журнала нажмите кнопку "Настройка колонок" в правом верхнем углу таблицы. В результате действия раскроется выпадающее меню со списком колонок (Рисунок 3). Установите флаги колонкам, необходимым для отображения в таблице, или используйте флаг "Включить все".

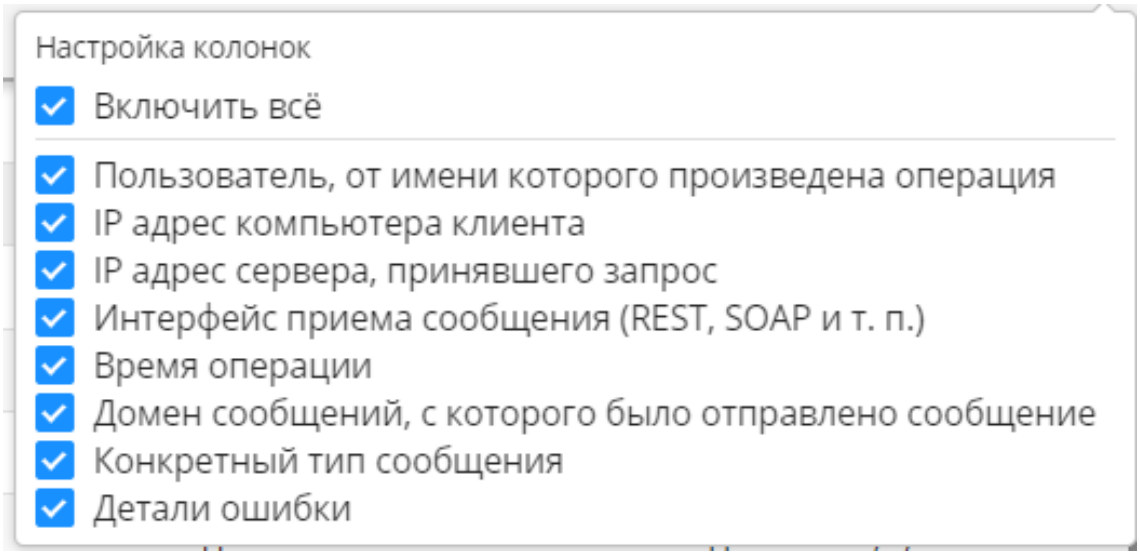


Рисунок 3 - Настройка колонок журнала

10.4. Сортировка журнала

1. Нажмите на значок "Фильтр" , расположенный справа от заголовка колонки, и задайте один или несколько фильтров в появившемся поле. В зависимости от колонки поле может иметь вид выпадающего списка, элемент выбора даты, текстовое поле и т.п. Возможна фильтрация сразу по нескольким значениям из списка.

2. Нажмите "Применить". В результате действия таблица будет отфильтрована по заданным параметрам.
3. Включить и выключить одновременно все заданные фильтры можно нажав кнопку *Фильтры выкл.* в правом верхнем углу таблицы. В результате действия кнопка изменит свой вид на *Фильтры вкл ( )*. В скобках будет указано число примененных фильтров.
4. Для сброса параметров фильтрации нажмите кнопку "Сбросить фильтры"  в правом верхнем углу таблицы.

10.5. Экспорт данных журнала

Данные журнала можно выгрузить в файл Excel (**.xlsx**). Нажмите кнопку "Экспорт" в правом верхнем углу экрана. Затем выберите вариант экспорта:

- *Экспорт текущей страницы*. В результатах будут содержаться только строки, которые были отфильтрованы ранее. В отчет попадают строки, которые уместились на текущую страницу результатов. Например, страница 6.
- *Экспорт всего журнала*. В результатах будут содержаться только строки, которые были отфильтрованы ранее. В отчет попадают строки со всех страниц журнала. Например, 210 из 210 страниц.

После формирования отчета результаты доступны в уведомлениях.

Ниже представлено соответствие полей по типу события для расшифровки содержимого отчета.

- login; Вход
- logout; Выход
- role_create; Создание роли
- role_delete; Удаление роли
- role_update; Обновление роли
- label_create; Создание метки
- label_delete; Удаление метки
- label_update; Обновление метки
- audit_xlsx_export; Экспорт аудита в xlsx
- user_create; Создание учетной записи
- user_update; Обновление учетной записи
- user_roles_update; Изменение ролей пользователя
- user_deactivate; Деактивация учетной записи
- user_activate; Активация учетной записи

- user_password_update; Изменение пароля учетной записи
- auth_block; Блокировка аутентификации
- role_labels_update; Изменение меток безопасности роли
- job_create; Создание операции
- job_update; Изменение операции
- job_delete; Удаление операции
- job_launch; Запуск операции
- job_stop; Остановка операции
- job_activate; Активация операции
- job_deactivate; Деактивация операции
- classification-upsert; Вставка классификации
- classification-delete; Удаление классификации
- classifier-create; Классификатор создан
- classifier-update; Классификатор обновлен
- classifier-delete; Классификатор удален
- version-create; Версия классификатора создана
- version-update; Версия классификатора обновлена
- version-delete; Версия классификатора удалена
- start-workflow; Старт процесса
- complete-task; Окончание задачи
- assign-task; Присвоение задачи
- add-comment; Добавление комментария
- edit-comment; Редактура комментария
- delete-comment; Удаление комментария
- add-attachment; Добавление вложения
- edit-attachment; Редактирование вложения
- delete-attachment; Удаление вложения
- create_user_replacement; Создание замещения пользователя
- update_user_replacement; Изменение замещения пользователя
- delete_user_replacement; Удаление замещения пользователя
- users_group_create; Создание группы пользователей
- users_group_update; Изменение группы пользователей
- users_group_roles_update; Изменение ролей группы
- users_group_delete; Удаление группы пользователей
- record-upsert; Вставка записи (отображается при редактировании и при создании записи)
- record-delete; Удаление записи
- record-get; Получение записи

- record-restore; Восстановление записи
- meta-draft-remove; Удаление черновика
- meta-draft-apply; Применение черновика
- meta-draft-upsert; Вставка черновика
- source-system-create; Создание источника данных
- source-system-update; Изменение источника данных
- source-system-delete; Удаление источника данных
- crawler-create; Создание краулера
- crawler-update; Изменение краулера
- crawler-delete; Удаление краулера
- crawler-connector-create; Создание подключения
- crawler-connector-update; Изменение подключения
- crawler-connector-delete; Удаление подключения
- crawler-instance-create; Создание набора данных
- crawler-instance-update; Изменение набора данных
- crawler-instance-delete; Удаление набора данных
- runtime_properties_update; Изменение параметров системы
- workflow-model-change; Обновление модели бизнес-процессов

11.Параметры системы

Раздел "Параметры системы" содержит перечень конфигурационных параметров, доступных для просмотра и редактирования в интерфейсе системы. Параметры разбиты на группы, каждая из которых отвечает за отдельные функции системы Юниверс MDM: очередь сообщений, периоды актуальности и т.д. (Рисунок 1).

Перечень параметров формируется посредством последовательного чтения параметров из источников данных: файла **backend.properties**, базы данных **PostgreSQL** и **Hazelcast**. Каждый следующий прочитанный источник сравнивается с предыдущим, что соответствует логическому выражению backend.properties AND PostgreSQL > AND Hazelcast.

В процессе сравнения новые параметры добавляются, а существующие перезаписываются, становясь равными последнему прочитанному источнику. Таким образом формируется полный и актуальный перечень параметров системы Юниверс MDM.

В разделе доступно изменение значений отдельных параметров, а также импорт/экспорт параметров.

Примечания:

- Приоритетным считается задание значений параметров через интерфейс - такие значения будет невозможно переопределить в файлах *.env*, *docker-compose.yml* и *backend.properties*.
- Файл *backend.properties* содержит некоторые параметры, недоступные для чтения и редактирования через интерфейс - они могут быть заданы через редактирование файла. См. описание файла backend.properties.

Содержание:

11.1. Перечень параметров системы

11.1.1. Настройки лицензии

Путь к файлу лицензии / com.unidata.mdm.license.file (поле ввода):

Хранение истории лицензий / com.unidata.mdm.license.history (флаг): включен

11.1.2. Параметры гостевого режима

Гостевой режим включен / com.unidata.mdm.ee.guest.mode (флаг): выключен

Пароль / com.unidata.mdm.ee.guest.password (поле ввода): guest

Роль / com.unidata.mdm.ee.guest.role (поле ввода): guest

Имя пользователя / com.unidata.mdm.ee.guest.username (поле ввода): guest

11.1.3. Свойства классификаторов

Максимально допустимая длина описания объекта / com.unidata.mdm.classifiers.model.description.length (поле ввода): 255

Максимально допустимая длина отображаемого имени объекта / com.unidata.mdm.classifiers.model.display.name.length (поле ввода): 255

Максимально допустимая длина имени объекта / com.unidata.mdm.classifiers.model.name.length (поле ввода): 255

Размер блока переиндексации классификатора / com.unidata.mdm.classifiers.model.reindex.batch.size (поле ввода): размер блока, которым будут отправляться узлы для переиндексации в OpenSearch. По умолчанию = 1024.

Размер блока загружаемых из БД узлов для переиндексации классификатора / com.unidata.mdm.classifiers.model.reindex.load.size (поле ввода): размер блока, которым будут загружаться узлы из БД. По умолчанию = 65536.

11.1.4. Параметры безопасности приложения

Включить возможность ручной пролонгации пользовательской сессии / org.unidata.mdm.core.security.token.manual.prolongation.enabled (флаг):

Если параметр включен, то для продления времени сессии пользователя учитываются следующие действия: click - клик мышью, scroll - прокрутка окна, resize - изменение размера окна, keypress - нажатие символьной клавиши, mousemove - движение курсора. Если параметр выключен, то учитываются только запросы к серверу через Rest API. Если пользователь определенное время не производит ни одно из указанных действий, то от последнего действия отсчитывается таймер org.unidata.mdm.core.security.token.ttl и сессия завершается автоматически.

Время жизни пользовательской сессии (в сек.) / org.unidata.mdm.core.security.token.ttl (поле ввода): 1800. Значение 0 - бесконечность, максимальное конечное - 2147483647 (Integer.MAX_VALUE). В целях безопасности не рекомендуется использовать бесконечное или слишком большое значение.

11.1.5. Системные настройки

Язык интерфейса по умолчанию / org.unidata.mdm.system.default.locale (поле ввода):

Диапазон используемых значений соответствует стандарту BCP47.

Режим разработчика / org.unidata.mdm.system.developer.mode (флаг):

Влияет на ранее установленные и успешно запущенные модули системы. Триггер параметра срабатывает при старте системы (сервера). Если флаг включен, то миграции всегда запускаются. Применяет обновления системы.

Формат хранения данных / org.unidata.mdm.system.dump.target.format (поле ввода): PROTOSTUFF

Time-out воспроизведения события / org.unidata.mdm.system.event.replay.timeout (поле ввода): 3000. Параметр синхронизации между узлами (нодами) системы. Например, если в node1 обновилась модель, она ждет `event.replay.timeout` миллисекунд, пока остальные ноды не отреагируют на обновление. Максимальное значение = 9223372036854775807 (Long.MAX_VALUE).

Путь к начальной конфигурации потоков выполнения / org.unidata.mdm.system.initial.pipelines (поле ввода): file:///usr/share/tomcat/conf/universe//enterprise-pipelines.json

Идентификатор узла / org.unidata.mdm.system.node.id (поле ввода): node0

Версия системы / org.unidata.mdm.system.platform.version (поле ввода): 6.11.0-SNAPSHOT

Включить профилировщик / org.unidata.mdm.system.simon.enabled (флаг):

Используется для измерения производительности системы. Рекомендуется включать только для тестов, так как профилировщик забирает часть производительности.

11.1.6. Параметры системных операций модуля core

Cron-выражение запуска операции очистки бинарных данных /

org.unidata.mdm.core.job.clean.binaries.cronex (поле ввода): 0 0 0/1 * * ?. См. подробнее.

Отключение операции очистки бинарных данных / org.unidata.mdm.core.job.clean.binaries.disabled (флаг):

Если флаг включен, то автоматическая очистка неиспользуемых файлов не будет запускаться. Очищает неиспользуемые (например, не прикрепленные к записям) файлы из таблиц:

- org_unidata_mdm_core.binary_data
- org_unidata_mdm_core.character_data

Время жизни откреплённых бинарных данных (в минутах) / org.unidata.mdm.core.job.clean.binaries.lifetime (поле данных): 10080. Определяет период времени, в течение которого на сервере будут храниться файлы, неприкрепленные ни к одной из записей. Максимальное значение - число минут от -1000000000-01-01T00:00Z до текущего момента.

11.1.7. Почтовые настройки

Включить email-уведомления / org.unidata.mdm.core.email.enabled (флаг)

Адрес системы / org.unidata.mdm.core.email.frontend_url (поле ввода): например, *http://localhost:8082/*. Указывает адрес frontend-приложения системы. Почтовый сервер использует этот адрес, чтобы получать информацию о событиях в системе, на основе которых создается почтовая рассылка.

Пароль / org.unidata.mdm.core.email.password (поле ввода): password

Адрес почтового сервера / org.unidata.mdm.core.email.server_host (поле ввода): localhost

Порт почтового сервера / org.unidata.mdm.core.email.server_port (поле ввода): 5025

Путь к шаблонам уведомлений / org.unidata.mdm.core.email.templates_folder (поле ввода): *file:///usr/share/tomcat/conf/universe//templates*

Логин / org.unidata.mdm.core.email.username (поле ввода): universe@example.com

11.1.8. Настройки хранения паролей

Cron-выражение запуска операции очистки неактивных паролей / org.unidata.mdm.core.job.clean.inactive.passwords.cronex (поле ввода): 0 0 2 1/1 * ? * (значение по умолчанию - запуск в два часа ночи каждый день). См. подробнее.

Срок действия пароля администратора (в днях) /
org.unidata.mdm.core.password.policy.admin.expiration.days (поле ввода): 91. Влияет на учетные записи с флагом "Суперпользователь".

Разрешение смены пароля /
org.unidata.mdm.core.password.policy.allow.password.change (флаг): да / нет. Если включен, то становится доступным механизм изменения паролей. Если параметр отключается, то у пользователей должны быть токены авторизации, иначе вход будет невозможен

Проверка попыток аутентификации по IP-адресу клиента включена /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.client.ip.enabled (флаг): да / нет. По умолчанию выключен

Лимит ошибок аутентификации по IP-адресу клиента /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.client.ip.limit (поле ввода): 5

Время ожидания после превышения лимита ошибок аутентификации по IP-адресу клиента, секунды /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.client.ip.timeout (поле ввода): 30

Время хранения в кэше записей об ошибках аутентификации по IP-адресу, минуты /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.client.ip.ttl (поле ввода): 30

Проверка аутентификации по имени пользователя включена /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.username.enabled (флаг): по умолчанию - выключен

Лимит ошибок аутентификации по имени пользователя /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.username.limit (поле ввода): 5

Время ожидания после превышения лимита ошибок аутентификации по имени пользователя, секунды /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.username.timeout (поле ввода): 30

Время хранения в кэше записей об ошибках аутентификации по имени пользователя, минуты /
org.unidata.mdm.core.password.policy.check.failed.authentication.count.by.username.ttl

(поле ввода): 30

Размер истории паролей при проверке нового пароля / org.unidata.mdm.core.password.policy.check.repetitions.count (поле ввода): 0

Время жизни записей неактивных паролей, дни (0 - не удалять записи) / org.unidata.mdm.core.password.policy.inactive.password.record.ttl (поле ввода): 60

Минимальная длина пароля / org.unidata.mdm.core.password.policy.min.length (поле ввода): 0

Допустимый формат пароля (регулярное выражение) / org.unidata.mdm.core.password.policy.regexp (поле ввода). Проверить регулярные выражения можно с помощью онлайн-инструмента https://regex101.com/ (необходимо выбрать Java 8).

Пример формата пароля / org.unidata.mdm.core.password.policy.regexp.example (поле ввода):

Срок действия пароля (в днях) / org.unidata.mdm.core.password.policy.user.expiration.days (поле ввода): 181

Максимальное количество сеансов пользователя / org.unidata.mdm.core.security.user.session.limit (поле ввода): 10000. Значение можно конфигурировать через переменную окружения `CORE_SECURITY_SESSION_LIMIT` Если при попытке авторизации количество сеансов пользователя достигло лимита, то на экране отобразится ошибка о превышении лимита параллельных сеансов.

11.1.9. Настройки загрузки файлов

Максимальное количество файлов / org.unidata.mdm.core.file.max.count (поле ввода): по умолчанию = 10. Количество файлов, которые можно прикрепить к одному атрибуту записи. Максимальное количество файлов, как и другие параметры, определяющие загрузку файлов в систему, определяется только характеристиками сервера системы и задачами пользователя. Важно сбалансировать количество файлов и их размер, а также количество записей, в которых используются прикрепленные файлы. Например, может быть 1000 записей, к каждой из которых прикреплено 20 файлов по 10Кб; либо 100 записей, к каждой из которых прикреплено 1 файл по 100Мб. Излишняя нагрузка на сервер может привести к проблемам производительности.

Временная директория для загрузок / org.unidata.mdm.core.upload.attachment.directory (поле ввода)

Максимальный размер файла для загрузок (в байтах) / org.unidata.mdm.core.upload.attachment.max.size (поле ввода): по умолчанию = 5242880

Максимальный объем памяти для загрузок (в байтах) / org.unidata.mdm.core.upload.attachment.memory.threshold (поле ввода)

11.1.10. Служебные задачи модуля черновиков

CRON выражение для задачи 'Удалить неиспользуемые черновики' / org.unidata.mdm.draft.job.clean.drafts.cronex (поле ввода): 0 0 0/1 * * ?

Задача 'Удалить неиспользуемые черновики' отключена, если true / org.unidata.mdm.draft.job.clean.drafts.disabled (флаг): да / нет

Время жизни неиспользуемого черновика, до того, как его соберет задача 'Удалить неиспользуемые черновики' (в минутах) / org.unidata.mdm.draft.job.clean.drafts.lifetime (поле ввода): 10080. Определяет период времени, в течение которого на сервере будут храниться неиспользуемые черновики. Максимальное значение - число минут от -1000000000-01-01T00:00Z до текущего момента.

11.1.11. Настройки хранилища данных

Узлы хранения / org.unidata.mdm.data.nodes (поле ввода): 0:node0:postgres@postgres:postgres@postgres-mdm:5432

Шарды хранения / org.unidata.mdm.data.shards (поле ввода): 32

11.1.12. Индексы

Количество реплик по умолчанию / org.unidata.mdm.core.indexing.replicas.number (поле ввода): 0

Количество шард по умолчанию / org.unidata.mdm.core.indexing.shards.number (поле ввода): 1

11.1.13. Настройки индексирования данных

Формат атрибута типа 'Дата' / org.unidata.mdm.data.index.date.display.format (поле ввода): yyyy-MM-dd

Прямая связь / org.unidata.mdm.data.index.relations.straight (флаг):

Формат атрибута типа 'Время' / org.unidata.mdm.data.index.time.display.format

(поле ввода): HH:mm:ss

Формат атрибута типа 'Дата/Время' / org.unidata.mdm.data.index.timestamp.display.format (поле ввода): yyyy-MM-dd'T'HH:mm:ss

11.1.14. Настройки индексирования модели данных

> Примечание:
> Параметры являются разметкой для будущей функциональности. В настоящее время эти значения не учитываются и могут быть любыми.

Репликация реестров / org.unidata.mdm.data.indexing.entity.replicas (поле ввода): 0

Шардирование реестров / org.unidata.mdm.data.indexing.entity.shards (поле ввода): 1

Репликация справочников / org.unidata.mdm.data.indexing.lookup.replicas (поле ввода): 0

Шардирование справочников / org.unidata.mdm.data.indexing.lookup.shards (поле ввода): 1

11.1.15. Настройки кэширования

Секция параметров отвечает за настройки кластерной конфигурации системы. Настройка кластеров должна выполняться специалистом.

Автоопределение стратегии обнаружения / org.unidata.mdm.system.cache.auto-detection.enabled (флаг): да / нет

Если включен, то производится автоматический поиск среды выполнения кэширования. Это могут быть AWS, Azure, GCP или Kubernetes

Автопоиск нод кластера включен / org.unidata.mdm.system.cache.multicast.enabled (флаг): да / нет

С помощью автоматического обнаружения многоадресной рассылки Hazelcast позволяет членам кластера находить друг друга с помощью многоадресной связи. Членам кластера не нужно знать конкретные адреса других участников, поскольку они просто передают многоадресную рассылку всем остальным участникам для прослушивания. Возможна или разрешена многоадресная рассылка, зависит от вашей среды

Маска подсети для отправки мультикаст-запросов / org.unidata.mdm.system.cache.multicast.group (поле ввода): 224.2.2.3

Порт, куда будут отправляться мультикаст-запросы / org.unidata.mdm.system.cache.multicast.port (поле ввода): 54327

Таймаут отправки сообщений / org.unidata.mdm.system.cache.multicast.timeout (поле ввода): 2

Время жизни мультикаст-запросов / org.unidata.mdm.system.cache.multicast.ttl (поле ввода): 32

Порт / org.unidata.mdm.system.cache.port (поле ввода): 5701

Автоинкремент порта кэша системы / org.unidata.mdm.system.cache.port.autoincrement (флаг): да / нет

Включение автоматического поиска свободного порта

Поиск нод по заданному списку включен / org.unidata.mdm.system.cache.tcp-ip.enabled (флаг): да / нет

Поиск узлов для кластера. Связь между узлами осуществляется через TCP/IP

IP-адреса нод кластера / org.unidata.mdm.system.cache.tcp-ip.members (поле ввода): 127.0.0.1

11.1.16. Конфигурация стандартных операций

Минимальное количество потоков / org.unidata.mdm.core.job.pool.min.size (поле ввода): 4

Максимальное количество потоков / org.unidata.mdm.core.job.pool.max.size (поле ввода): 24

Значение максимального количества потоков зависит от нескольких факторов: от сложности самих операций, от объема данных в системе, и от количества ядер процессора на сервере. Как правило, задается значение в 2 раза больше, чем ядер процессора. Рекомендуется настраивать количество экспериментальным путем, опираясь на данные в системе. Параметр определяет количество потоков Java, которое выделяется на все операции сразу.

Размер очереди / org.unidata.mdm.core.job.queue.size (поле ввода): 100

Объем очереди потоков. Очередь выстраивает порядок запуска операций, т.к. одновременно все операции обработать невозможно. Размер очереди зависит от характеристик сервера и его работоспособности, размер устанавливается экспериментальным путем.

11.1.17. Настройки аудита системы

> Примечание:
>
> Параметры являются разметкой для будущей функциональности. В настоящее время эти значения не учитываются и могут быть любыми.

Включить аудит / org.unidata.mdm.core.audit.enabled (флаг)

Хранилище журнала аудита / org.unidata.mdm.core.audit.enabled.storages (поле ввода): os

Сообщать о событиях чтения? / org.unidata.mdm.core.audit.read.events (флаг)

Глубина стектрейса в сообщениях об ошибках / org.unidata.mdm.core.audit.stacktrace.depth (поле ввода): 32

Размер пула потоков диспетчера аудита / org.unidata.mdm.core.audit.writer.pool.size (поле ввода): 4

11.1.18. Фоновая операция очистки данных журнала аудита системы

Время жизни записей логов в базе данных / com.universe.mdm.core.audit.ttl.db (поле ввода): значение по умолчанию не ограничено. Формат значения: число + m | h | d | M | y (*minutes* | *hours* | *days* | *months* | *years* соответственно).

Расписание старта операции очистки логов в базе данных / com.universe.mdm.core.audit.ttl.db.job.cron (поле ввода): Cron-выражение для старта операции, запуск по умолчанию раз в сутки в 1:00 ночи

Время жизни записей аудита в индексе / com.universe.mdm.core.audit.ttl.index (поле ввода): значение по умолчанию не ограничено. Формат значения: число + m | h | d | M | y (*minutes* | *hours* | *days* | *months* | *years* соответственно).

Расписание старта операции очистки логов в индексе / com.universe.mdm.core.audit.ttl.index.job.cron (поле ввода): Cron-выражение для старта операции, запуск по умолчанию раз в сутки в 1:00 ночи

11.1.19. Исполнение асинхронных задач

Размер пула потоков / org.unidata.mdm.core.async.task.executor.pool.size (поле ввода): 4

Применяется для регуляции асинхронных (отложенных) действий. Например: выгрузка в эксель, пакетные операции с записями, кастомные операции. Всегда должен быть пул задач, поэтому не рекомендуется ставить 1 (в таком случае

очереди не будет, и задачи будут выдавать ошибку).

11.1.20. Настройки подсистемы сообщений

Маршруты сообщений модуля Commercial Core / org.unidata.mdm.system.messaging.domains.commercial-core-messaging (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://camel.apache.org/schema/spring
http://camel.apache.org/schema/spring/camel-spring.xsd">
    <route id="commercial-core">
        <from uri="direct:commercial-core-messaging"/>
        <to uri="vm:commercial-core"/>
    </route>

    <route id="commercial_core_vm">
        <from uri="vm:commercial-core"/>
        <to uri="direct:audit"/>
    </route>
</routes>
```

Маршруты сообщений модуля Core / org.unidata.mdm.system.messaging.domains.core-messaging (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://camel.apache.org/schema/spring
     http://camel.apache.org/schema/spring/camel-spring.xsd">
     <route id="core"> <from uri="direct:core-messaging"/> <to uri="vm:core"/>
</route> <route id="core_vm"> <from uri="vm:core"/> <choice> <when>
<header>type</header> <toD uri="direct:${header.type}"/> </when> <otherwise> <to
uri="direct:withoutType"/> </otherwise> </choice> </route> <route id="login">
<from uri="direct:login"/> <to uri="direct:audit"/> </route> <route id="logout">
<from uri="direct:logout"/> <to uri="direct:audit"/> </route> <route
id="audit_xlsx_export"> <from uri="direct:audit_xlsx_export"/> <to
uri="direct:audit"/> </route> <route id="role_create"> <from
uri="direct:role_create"/> <to uri="direct:audit"/> </route> <route
id="role_delete"> <from uri="direct:role_delete"/> <to uri="direct:audit"/>
</route> <route id="role_update"> <from uri="direct:role_update"/> <to
uri="direct:audit"/> </route> <route id="role_label_attach"> <from
uri="direct:role_label_attach"/> <to uri="direct:audit"/> </route> <route
id="label_create"> <from uri="direct:label_create"/> <to uri="direct:audit"/>
</route> <route id="label_update"> <from uri="direct:label_update"/> <to
uri="direct:audit"/> </route> <route id="label_delete"> <from
uri="direct:label_delete"/> <to uri="direct:audit"/> </route> <route
id="password_reset"> <from uri="direct:password_reset"/> <to
uri="direct:email.password_reset"/> </route> <route id="audit"> <from
uri="direct:audit"/> <bean
beanType="org.unidata.mdm.core.service.impl.CoreAuditEventContextBuilder"
method="build"/> <aggregate strategyRef="groupedBodyAggregationStrategy"
completionInterval="60000" completionSize="1000"> <correlationExpression>
<constant>true</constant> </correlationExpression> <multicast> <to
uri="bean:indexAuditStorageService?method=write"/> <to
uri="bean:databaseAuditStorageService?method=write"/> </multicast>
</aggregate> </route> <route id="email.password_reset"> <from
uri="direct:email.password_reset"/> <setHeader
name="CamelVelocityResourceUri">
<simple>${header.email_args.get(templates_folder)}/email_password_reset.vm</s
imple> </setHeader> <setHeader name="Subject"> <constant>Unidata notification:
Password reset</constant> </setHeader> <setHeader name="Content-Type">
<simple>text/html</simple> </setHeader> <setHeader name="temp_password">
<simple>${header.email_args.get(temp_password)}</simple> </setHeader>
<setHeader name="password_reset_link">
<simple>${header.email_args.get(password_reset_link)}</simple> </setHeader>
<to uri="velocity:email_password_reset.vm"/> <to uri="direct:email.send"/>
</route> <route id="email.send"> <from uri="direct:email.send"/> <setHeader
name="from"> <constant>{{org.unidata.mdm.core.email.username}}</constant>
</setHeader> <setHeader name="to">
<simple>${header.email_args.get(email)}</simple> </setHeader> <to
uri="smtps://{{org.unidata.mdm.core.email.server_host}}:{{org.unidata.mdm.cor
e.email.server_port}}?username={{org.unidata.mdm.core.email.username}}&amp;pa
ssword={{org.unidata.mdm.core.email.password}}"/> </route> </routes>
```

Маршруты сообщений модуля Data /
org.unidata.mdm.system.messaging.domains.data-messaging (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://camel.apache.org/schema/spring
http://camel.apache.org/schema/spring/camel-spring.xsd"> <route id="data">
<from uri="direct:data-messaging"/> <to uri="vm:data"/> </route> <route
id="data_vm"> <from uri="vm:data"/> <to uri="direct:audit"/> </route> </routes>
```

Маршруты сообщений модуля Meta /
org.unidata.mdm.system.messaging.domains.meta-messaging (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://camel.apache.org/schema/spring
http://camel.apache.org/schema/spring/camel-spring.xsd"> <route id="meta">
<from uri="direct:meta-messaging"/> <to uri="vm:meta"/> </route> <route
id="meta_vm"> <from uri="vm:meta"/> <to uri="direct:audit"/> </route> </routes>
```

Настройка маршрутизации импорта данных /
org.unidata.mdm.system.messaging.domains.smart-etl-data-recipient-messaging (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://camel.apache.org/schema/spring
http://camel.apache.org/schema/spring/camel-spring.xsd">

    <route id="smart_etl_mdm_recipient_kafka">
        <from uri="direct:recipientQueueConnection"/>
        <process ref="dataRecordMessageConverter"/>
        <aggregate strategyRef="dataRecordMessageAggregation"
                completionSize="500"
                completionTimeout="1000">
            <correlationExpression>
                <constant>true</constant>
            </correlationExpression>
            <threads maxPoolSize="16"/>
            <process ref="dataRecordMessageProcessor"/>
            <split>
                <simple>${body.records}</simple>
                <process ref="toJsonMessageConverter"/>
                <split>
                    <simple>${body.records}</simple>
                    <process ref="toJsonMessageConverter"/>
                    <to uri="log:foo"/>
                </split>
            </split>
        </aggregate>
    </route>
</routes>
```

Маршруты сообщений нотификации ETL /
org.unidata.mdm.system.messaging.domains.smart_etl_notification (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://camel.apache.org/schema/spring
http://camel.apache.org/schema/spring/camel-spring.xsd">

<route id="smart_etl_notification">
    <from uri="direct:smart_etl_notification"/>
    <to uri="vm:smart_etl_notification_wm"/>
</route>

<route id="smart_etl_notification_wm">
    <from uri="vm:smart_etl_notification_wm"/>
    <setHeader name="CamelHttpMethod">
        <constant>POST</constant>
    </setHeader>
    <setHeader name="Content-Type">
        <constant>application/json</constant>
    </setHeader>
    <to
uri="http://{{com.unidata.smartetl.mdm.notifications.messaging.endpoint}}"/>
</route> </routes>
```

Маршруты сообщений модуля Workflow /
org.unidata.mdm.system.messaging.domains.workflow-messaging (поле ввода):

```
<routes xmlns="http://camel.apache.org/schema/spring"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://camel.apache.org/schema/spring
http://camel.apache.org/schema/spring/camel-spring.xsd"> <route id="workflow">
<from uri="direct:workflow-messaging"/> <to uri="vm:workflow"/> </route> <route
id="workflow_vm"> <from uri="vm:workflow"/> <choice> <when>
<simple>${header.type} == 'start-workflow'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.StartWorkflowAudit
EventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'complete-task'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.CompleteTaskAuditE
ventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'assign-task'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.AssignTaskAuditEve
ntBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'add-comment'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.UpsertCommentAudit
EventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'edit-comment'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.UpsertCommentAudit
EventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'delete-comment'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.DeleteCommentAudit
EventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'add-attachment'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.UpsertAttachmentAu
ditEventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'edit-attachment'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.UpsertAttachmentAu
ditEventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'delete-attachment'</simple> <bean
beanType="com.unidata.mdm.workflow.core.service.impl.audit.DeleteAttachmentAu
ditEventBuilder" method="build"/> </when> <when> <simple>${header.type} ==
'email-notification'</simple> <to uri="direct:email-notification"/> </when>
</choice> <to uri="direct:audit"/> </route> <route id="email-notification">
<from uri="direct:email-notification"/> <to
uri="direct:email.email-notification"/> </route> <route
id="email.email-notification"> <from uri="direct:email.email-notification"/>
<setHeader name="CamelVelocityResourceUri">
<simple>${header.email_args.get(templates_folder)}/mail_workflow_notification
.vm</simple> </setHeader> <setHeader name="Subject">
<simple>${header.email_args.get(subject)}</simple> </setHeader> <setHeader
name="Content-Type"> <simple>text/html; charset="UTF-8"</simple> </setHeader>
<setHeader name="task_id"> <simple>${header.email_args.get(task_id)}</simple>
</setHeader> <setHeader name="result">
<simple>${header.email_args.get(result)}</simple> </setHeader> <setHeader
name="comment"> <simple>${header.email_args.get(comment)}</simple>
</setHeader> <setHeader name="task_link">
<simple>${header.email_args.get(task_link)}</simple> </setHeader> <to
uri="velocity:mail_workflow_notification.vm?encoding=UTF-8"/> <to
uri="direct:email.send"/> </route> </routes>
```

Включить трассировку / org.unidata.mdm.system.messaging.trace.enabled (флаг):

11.1.21. Настройки поиска

Время ожидания ответа от сервера для запросов управления (в миллисекундах). Значения <= 0 подразумевают "ждать бесконечно" / org.unidata.mdm.search.admin.action.timeout (поле ввода): 5000

Логин суперпользователя, используется продуктами Юниверс для доступа к узлам поисковой системы / org.unidata.mdm.search.admin.login: admin

Пароль суперпользователя / org.unidata.mdm.search.admin.password: admin

Имя кластера / org.unidata.mdm.search.cluster.name (поле ввода): docker-cluster

Узлы кластера / org.unidata.mdm.search.cluster.nodes (поле ввода): opensearch-mdm:9200

Лимит полей поиска / org.unidata.mdm.search.fields.limit (поле ввода): 10000

Объем маппинга для поиска в Opensearch. Определяет, насколько много атрибутов и других полей может быть в реестре при поиске.

Лимит результатов поиска / org.unidata.mdm.search.hits.limit (поле ввода): 200000

Количество выдаваемых результатов поиска.

Префикс для имен поисковых индексов / org.unidata.mdm.search.index.prefix (поле ввода): default

Пароль к keystore / org.unidata.mdm.search.keystore.password: password

Путь к keystore формата JKS, хранящему .p12 сертификат открытого и закрытого ключа продуктов Юниверс для установки защищенного соединения / org.unidata.mdm.search.keystore.path: path

Максимальное количество запросов в балк запросе / org.unidata.mdm.search.max.bulk.size (поле ввода): 8192

Максимальное количество условий в запросе в поисковую систему / org.unidata.mdm.search.query.bool.max_clause_count (поле ввода): 1024

Незамедлительно обновлять состояние записи в поисковой системе / org.unidata.mdm.search.refresh.immediate (флаг):

Если флаг включен, то все изменения записей моментально отображаются. Если флаг выключен, то изменения отображаются после следующей переиндексации Opensearch. Функция влияет на производительность.

Количество реплик по умолчанию для справочников / org.unidata.mdm.search.replicas.number (поле ввода): 0

Включены меры безопасности поисковой системы (аутентификация, шифрование) / org.unidata.mdm.search.security.enabled (флаг):

Количество шард по умолчанию / org.unidata.mdm.search.shards.number (поле ввода): 1

Время таймаута соединения (в миллисекундах). Значения < 0 подразумевают "использовать стандартное системное", значение = 0 подразумевает "ждать бесконечно" (для применения требуется перезапуск) / org.unidata.mdm.search.socket.timeout.milliseconds (поле ввода): 30000

Пароль к truststore / org.unidata.mdm.search.truststore.password: password

Путь к truststore формата JKS, хранящему сертификаты открытого ключа узлов поисковой системы, верифицируемые продуктами Юниверс / org.unidata.mdm.search.truststore.path: path

11.1.22. Операция выгрузки аудита

Заголовок файла выгрузки по умолчанию / com.universe.mdm.core.audit.export.job.result.header:

Содержит настройки для генерации заголовка .xlsx-файла с аудитом.

11.1.23. Настройки нечеткого поиска

Max отличий символов для поиска по сходству / org.unidata.mdm.search.fuzziness (поле ввода): 1

Параметр ищет совпадения с учетом указанного количества возможных ошибок в части запроса, оставшейся после org.unidata.mdm.search.fuzziness.prefix.length. Чем число выше, тем это больше замедляет работу поиска.

Min совпадений символов в начале запроса / org.unidata.mdm.search.fuzziness.prefix.length (поле ввода): 4

Количество символов в начале запроса, после которого начинается часть нечеткого поиска. Например, если указано 4, то первые 4 символа в слове будут найдены по точному совпадению, среди оставшихся символов слова будет производиться нечеткий поиск. Если org.unidata.mdm.search.fuzziness было указано как 1, то в оставшейся части допустима 1 ошибка.

Совпадения по маске / org.unidata.mdm.search.fuzziness.with.wildcard (флаг):

Не рекомендуется использовать. Если включено, то в поиске записей может применяться поиск по шаблонам (маске).

11.1.24. Настройки скоринга при поиске

Вычисление score / org.unidata.mdm.search.calculate.score (флаг):

Используется для поиска наиболее релевантных результатов, а также для сортировки результатов поиска. Не рекомендуется отключать, так как не будет работать сортировка записей в таблицах результатов.

Min записей для повышения релевантности выдачи / org.unidata.mdm.search.default.min.score (поле ввода): 0.0

Отсеивание в результатах поиска записей, которые ниже указанной релевантности. В релизе 6.11 не применяется.

11.1.25. Настройки сопоставления данных

Real-time сопоставление данных / org.unidata.mdm.matching.data.real.time.matching.enabled (флаг):

Если параметр включен, то он влияет на производительность. Если выключен, то сопоставление данных будет производиться при переиндексации Opensearch. Не влияет на проверку дублей.

11.1.26. Настройки периодов актуальности

Режим периода актуальности / org.unidata.mdm.data.validity.period.mode (поле ввода): DATE. Параметр определяет глобальный режим гранулярности для периодов актуальности, если он не задан напрямую для конкретного реестра/справочника. Возможные значения: DATE - показывается только дата, DATETIME - дата и время, DATETIMEMILLIS - дата, время и миллисекунды (в интерфейсе пользователя не отображается).

Конец периода актуальности / org.unidata.mdm.data.validity.period.end (поле ввода): 2500-12-31T23:59:59.999Z

Начало периода актуальности / org.unidata.mdm.data.validity.period.start (поле ввода): 1900-01-01T00:00:00Z

> Предупреждение:
>
> Параметры ...start и ...end должны иметь одинаковый формат даты, иначе система не запустится

В Юниверс MDM 6.x принимаются периоды актуальности в форматах:

- yyyy-MM-dd'T'HH:mm:ss.SSS
- yyyy-MM-dd'T'HH:mm:ss.SSS'Z'

- yyyy-MM-dd'T'HH:mm:ss.SSS+00:00

11.1.27. Настройки применения правил качества при публикации

Фаза проверки данных для запуска при публикации / com.universe.mdm.dqw.quality.publishing.phase (поле ввода): системное имя фазы выполнения - по умолчанию DRAFT. Фаза запускает правила качества при публикации черновика записи. Если фаза не определена, то проверки не запускаются.

11.1.28. Применение правил качества перед закрытием процесса согласования

Фаза проверки данных перед закрытием процесса согласования / com.universe.mdm.dqw.quality.workflow.phase (поле ввода): системное имя фазы выполнения - по умолчанию PROCESS. Фаза запускает правила качества перед закрытием процесса согласования. Если фаза не определена, то проверки не запускаются.

11.1.29. Настройки применения правил качества при прямой вставке

Фаза для проверок при прямой вставке / org.unidata.mdm.dq.data.quality.upsert.phase (поле ввода): системное имя фазы выполнения - по умолчанию DEFAULT. Фаза запускает правила качества при загрузке данных в систему с помощью пакетных операций или внешних систем. Если фаза не определена, то проверки не запускаются.

Подробнее о фазах выполнения и их настройке см. в статье.

> Предупреждение:
>
> В версии 6.10.2 реализована работа правил качества для атрибутов связи и классификатора.

11.1.30. Настройки системного источника данных

Имя системного источника данных / org.unidata.mdm.meta.admin.source.system.name (поле ввода): по умолчанию - universe.

11.1.31. Свойства классификаторов

Максимально допустимая длина описания объекта / com.unidata.mdm.classifiers.model.description.length (поле ввода): по умолчанию - 255

Максимально допустимая длина отображаемого имени объекта / com.unidata.mdm.classifiers.model.display.name.length (поле ввода): по умолчанию - 255

Максимально допустимая длина имени объекта / com.unidata.mdm.classifiers.model.name.length (поле ввода): по умолчанию - 255

Размер блока переидексации классификатора / com.unidata.mdm.classifiers.model.reindex.batch.size (поле ввода): по умолчанию - 1024

Размер блока загружаемых из БД узлов для переидексации классификатора / com.unidata.mdm.classifiers.model.reindex.load.size (поле ввода): по умолчанию - 65536

11.1.32. Настройки экспорта XLSX

Максимальное количество экспортируемых записей / com.unidata.mdm.bulk.export.records.max.count (поле ввода) : по умолчанию - 50000

11.1.33. Настройки бизнес-процессов

Включить job executor в Camunda / com.unidata.mdm.workflow.core.job.executor.activate (флаг). При запуске через Docker передать настройку можно через переменную `WORKFLOW_JOB_EXECUTOR_ACTIVATE`

Максимальное время ожидания job executor в Camunda (в миллисекундах) / com.unidata.mdm.workflow.core.job.executor.maxWait (поле ввода): по умолчанию = 60000. Позволяет настроить таймер бизнес-процесса. При запуске через Docker передать настройку можно через переменную среды `WORKFLOW_JOB_EXECUTOR_MAX_WAIT`

11.1.34. Импорт данных из очередей

Включить загрузку объекта результата / com.universe.mdm.data.recipient.recipient.resolveResult (флаг). Если параметр

включен, то в ответе на импорт данных из очереди сообщений будет отправляться вставленная запись.

11.1.35. ETL. Реестр обработки записей

Тип файлового хранилища / com.unidata.smartetl.dpr.fileStorage.storageType (поле ввода): local

Тип хранилища процессов и истории / com.unidata.smartetl.dpr.process.storageType (поле ввода): default

11.1.36. Настройка ETL. нотификаций

Адрес получателя / com.universe.mdm.notifications.messaging.endpoint (поле ввода):

Отправлять список изменений при обновлении / com.universe.mdm.notifications.notifications.changes (флаг):

Загружать запись события / com.universe.mdm.notifications.notifications.fetchResult (флаг):

Отправлять нотификацию сохранения черновика / com.universe.mdm.notifications.notifications.sendDraftEvent (флаг):

Версия сегмента нотификации вставки записи / com.universe.mdm.notifications.notifications.upsert.version (поле ввода): по умолчанию = 3. Значение не может быть пустым и должно содержаться в списке версий сегмента SmartEtlSendUpsertNotification.VERSIONS (значения: 1 - старая версия и 2 - новая версия).

Отправлять атрибуты типа "Ссылка на справочник" с ключами записи справочника / com.universe.mdm.notifications.notifications.fetchLookupLinkAttributesLookupKeys (флаг): устанавливает, заполнять ли поле lookupLinkAttributes в уведомлении. По умолчанию выключен.

Отправлять объекты незаполненных атрибутов типа "Ссылка на справочник" как null / com.universe.mdm.notifications.notifications.showAbsentLookupLinkAttributes (флаг): устанавливает, вносить ли в lookupLinkAttributes отсутствующие атрибуты как null (в ChangeDiffResult не вносится). По умолчанию выключен.

Отправлять ключи записей справочников, на которые ссылается запись /

com.universe.mdm.notifications.notifications.fetchRecordKeys (флаг): устанавливает, заполнять ли в атрибутах поля lookupLinkAttributes поля recordKeys. По умолчанию выключен.

11.1.37. Настройки модуля правил сопоставления

Количество кластеров в пакете, удаляемых за раз при редактировании назначений в модели сопоставления / org.unidata.mdm.matching.core.remove.cluster.record.from.index.bulk.size (поле ввода): 10000

11.2. Доступные действия с параметрами

11.2.1. Редактирование параметров

Большинство параметров доступны только для чтения и отмечены серым цветом.

При необходимости отредактируйте доступные параметры и нажмите кнопку *Сохранить*, расположенную в правом верхнем углу экрана, чтобы внести изменения.

Перед редактированием рекомендуется создать резервную копию параметров при помощи экспорта (см. ниже).

11.2.2. Фоновые операции

Некоторые наборы параметров описывают настройки фоновых операций в системе. Фоновые операции запускаются и выполняются самостоятельно, и используются для обслуживания отдельных частей системы. Например для удаления заброшенных черновиков.

Перечень операций и соответствующих групп параметров:

- Очистка файлов-вложений, которые были добавлены в систему, но не подтверждены. Например, файл был добавлен к атрибуту, но перед сохранением записи был заменен на другой файл. *Группа параметров*: Параметры системных операций модуля Core.
- Удаление неиспользуемых черновиков. *Группа параметров*: Служебные задачи модуля черновиков.

11.2.3. Импорт и экспорт параметров

> Примечание:
>
> Экспортируется весь набор параметров. Импортируются только параметры, доступные для редактирования.

Чтобы импортировать или экспортировать набор параметров, необходимо воспользоваться соответствующим мастером. Для этого нажмите кнопку "Импорт/экспорт", расположенную в правом верхнем углу экрана.

1. Выберите требуемое действие (Рисунок 2). Экспорт выполняется в 2 шага. Импорт в 3 шага.
2. **Для экспорта**: на 2 шаге нажмите *Подтвердить*. В результате начнется экспорт, результаты которого можно скачать в уведомлениях.
3. **Для импорта**: на 2 шаге выберите файл с набором параметров (расширение .properties) и нажмите *Следующий шаг*. На 3 шаге нажмите *Подтвердить*. Сообщение о результатах импорта отобразится в уведомлениях.

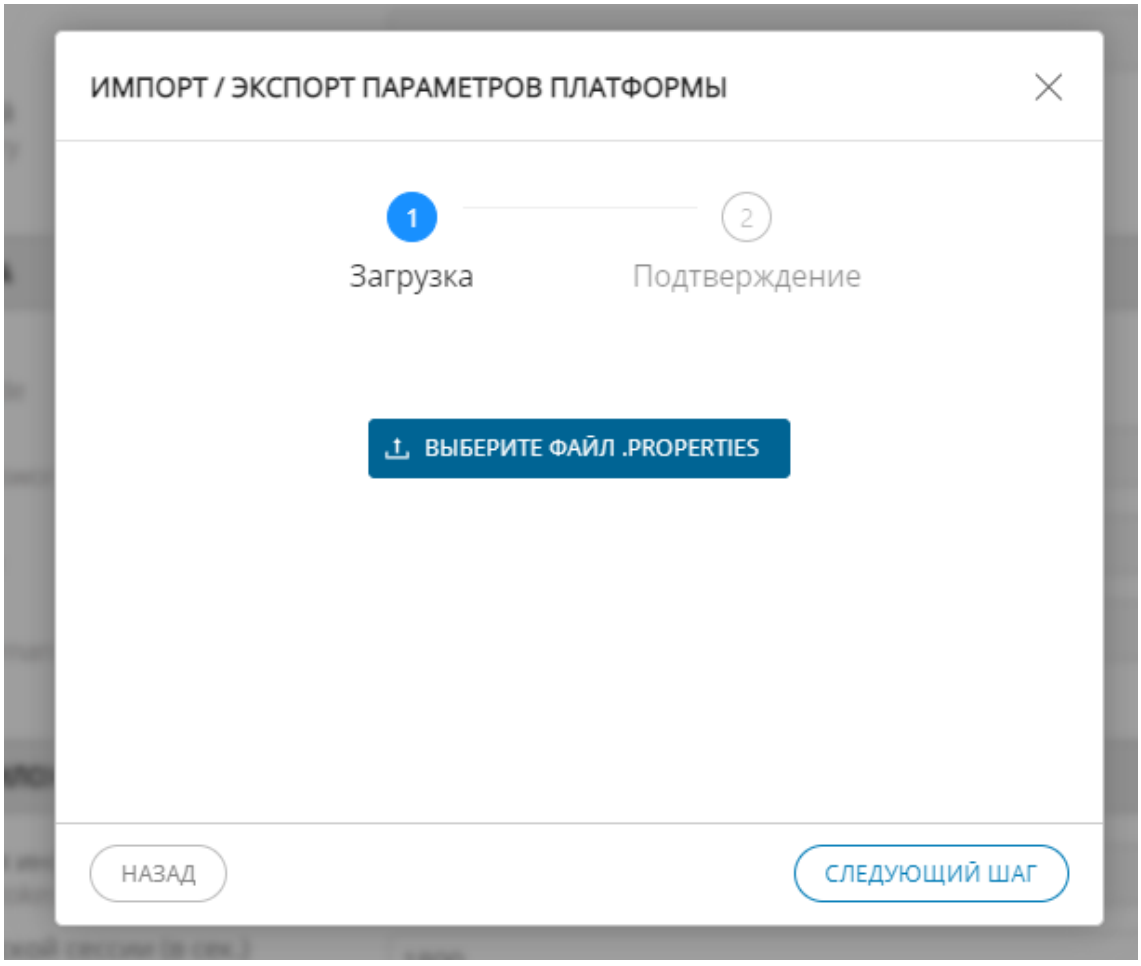


Рисунок 2 - Мастер импорта/экспорта параметров

11.3. Настройки паролей

Параметры настроек паролей хранятся в файле backend.properties. Некоторые параметры доступны для редактирования через интерфейс раздела "Параметры системы" в одноименной секции.

11.3.1. Очистка неиспользуемых паролей

Задача по очистке неиспользуемых паролей удаляет из БД все неактивные пароли, которые старше времени жизни на момент очистки. Если время жизни равно или меньше нуля, то пароли не удаляются.

Задача запускается по Cron-выражению, которое редактируется только через backend.properties, после чего требуется перезапуск системы.

Параметр, определяющий время жизни неактивных паролей, доступен для редактирования через интерфейс системы - параметр "Время жизни записей неактивных паролей".

Примечания:

- Из-за относительно частых событий аутентификации запуск очистки не должен производиться часто во избежание блокировки в БД и долгого ожидания аутентификации. Зависит от настроек блокировки при DELETE в БД.
- Запуск рекомендуется ставить в нерабочее время (по возможности) или в часы наименьшей нагрузки.
- Время жизни старого пароля определяется днями, поэтому запуск операции не рекомендуется производить чаще одного раза в сутки.

11.3.2. Проверки аутентификации по имени пользователя и IP-адресу

В текущей реализации проверка по имени пользователя не фиксирует попытки аутентификации по пустому имени пользователя (пустая строка, null, пробелы, табуляции и т.д.).

При попытке аутентификации берется контекст AuthenticationRequestContext, который содержит имя пользователя, IP-адрес клиента, время получения запроса, язык и другие параметры.

Перед проверкой введенных данных проверяется возможность аутентификации под введенным логином или IP-адресом:

- Если аутентификация невозможна, то счетчик неудачных попыток увеличивается, возвращается ошибка о превышении лимита, таймер таймаута запускается заново.
- Если аутентификация возможна, то идет обычная проверка правильности введенных данных.
- Если данные верны, то аутентификация успешна, а счетчики неудачных попыток обнуляются.
- Если данные неверные, то счетчик увеличивается, и в случае достижения или превышения лимита неверных попыток возвращается ошибка о превышении лимита.

Ошибка вида "*Превышен лимит ошибок аутентификации {limit}. {timeout} секунд до следующей попытки*" появляется на UI при превышении лимита ошибок аутентификации.

- limit и timeout настраиваются в параметрах системы.
- limit - Лимит ошибок аутентификации по имени пользователя или Лимит ошибок аутентификации по IP-адресу клиента.
- timeout - Время ожидания после превышения лимита ошибок аутентификации по имени пользователя или Время ожидания после превышения лимита ошибок аутентификации по IP-адресу клиента.

Пример:

Каждая повторная неудачная аутентификация продлевает время жизни записи.

Заданные параметры: Лимит - 3 попытки; Таймаут - 30 секунд; Время жизни записи - 30 минут.

1. При первой неудачной попытке в 15:00:00, введенные данные проверяются, в счетчике создается запись.
   - Неудачных попыток - 1, время последней неудачной попытки - 15:00:00, время жизни записи - 30 минут.
2. Вторая неудачная попытка в 15:01:00, введенные данные проверяются, в счетчике запись обновляется.
   - Неудачных попыток - 2, время последней неудачной попытки - 15:01:00, время жизни записи - 30 минут (время жизни обновилось).
3. Третья неудачная попытка в 15:02:00, введенные данные проверяются, в счетчике запись обновляется.
   - Неудачных попыток - 3, время последней неудачной попытки - 15:02:00,

время жизни записи - 30 минут (время жизни обновилось), таймаут - 30 секунд, лимит достигнут, следующие попытки будут блокироваться до истечения таймаута.

4. Четвертая неудачная попытка в 15:02:15 - таймаут не истек, попытка по умолчанию не удачна, введенные данные не проверяются, в счетчике запись обновляется.
    - Неудачных попыток - 4, время последней неудачной попытки - 15:02:15, время жизни записи - 30 минут (время жизни обновилось), таймаут - 30 секунд (таймаут обновился), лимит превышен, следующие попытки будут блокироваться до истечения таймаута.
5. Пятая неудачная в 15:15:00 - таймаут истек, но время жизни записи еще не истекло, в счетчике запись обновляется.
    - Неудачных попыток - 5, время последней неудачной попытки - 15:15:00, время жизни записи - 30 минут (время жизни обновилось), таймаут - 30 секунд (таймаут обновился), лимит превышен, следующие попытки будут блокироваться до истечения таймаута.

Неверный ввод может осуществляться 3 раза без таймаута, после этого (до истечения времени жизни записи) таймаут будет выводиться после каждого неверного ввода.

Успешная аутентификация удаляет запись, после чего будут доступны все 3 попытки без таймаута.

11.3.2.1. Известные проблемы

1. При превышении лимита по обеим аутентификациям - ошибка будет приходить только от одной, заранее неизвестно от какой.
    - **Возможное решение**: включайте счетчики через Параметры системы в несколько шагов. Сначала (при выключенных компонентах проверки) включите проверку по имени пользователя и сохраните изменения. Далее включите проверку по IP-адресу и сохраните изменения.
2. Некорректная работа при использовании общего прокси для доступа к системе. У всех пользователей будет один и тот же IP-адрес, вследствие чего счетчик будет увеличиваться от разных людей, и заблокированы будут все пользователи на этом IP-адресе.
    - **Возможное решение**: отключите компонент проверки по IP-адресу.

11.4. Описание файла backend.properties

Файл **backend.properties** содержит перечень конфигурационных параметров системы:

- Одна часть параметров доступна для просмотра и редактирования через интерфейс системы - см. описание по ссылке;
- Вторая часть параметров не отображается в интерфейсе системы и является скрытой от пользователя - описание некоторых см. ниже.

Файл *backend.properties* разделен на различные секции, каждая из которых отвечает за определенные функции системы.

11.4.1. Параметры файла, недоступные на UI

11.4.1.1. Секция System

Блок #DB

SystemDataSource является пулом подключений, что позволяет переподключаться при потере соединения.

- `org.unidata.mdm.system.datasource.url` - url адрес БД.
- `org.unidata.mdm.system.datasource.minPoolSize` - Кол-во минимальных подключений в пуле (по умолчанию 1). *pool* - это список подключений к БД, т.е. кол-во токенов для подключения.
- `org.unidata.mdm.system.datasource.maxPoolSize` - Кол-во максимальных подключений в пуле (по умолчанию 3).
- `org.unidata.mdm.system.datasource.testOnBorrow` - Валидация объекта перед взятием (по умолчанию *true*).
- `org.unidata.mdm.system.datasource.removeAbandoned` - Флаг для удаления заброшенного подключения (по умолчанию *true*).
- `org.unidata.mdm.system.datasource.validationQuery` - Запрос для валидации подключения к БД (по умолчанию *SELECT 1*).
- `org.unidata.mdm.system.datasource.validationInterval` - Минимальная частота валидации (по умолчанию *30000*).

11.4.1.2. Секция Core

Блок #Jobs

Параметры, доступные для редактирования через интерфейс (см. описание по ссылке):

- org.unidata.mdm.core.job.pool.min.size = 4
- org.unidata.mdm.core.job.pool.max.size = 24
- org.unidata.mdm.core.job.queue.size = 100

Блок #Job DS

Конфигурации стандартных операций.

- org.unidata.mdm.core.job.datasource.url - url адрес БД.
- org.unidata.mdm.core.job.datasource.minPoolSize - Кол-во минимальных подключений в пуле (по умолчанию 3).
- org.unidata.mdm.core.job.datasource.maxPoolSize - Кол-во максимальных подключений в пуле (по умолчанию 10).

Параметры для создания nonXA dataSource для переподключения к БД (**изменения не рекомендуются**).

- org.unidata.mdm.core.job.datasource.testOnBorrow - Валидация объекта перед взятием (по умолчанию *true*).
- org.unidata.mdm.core.job.datasource.removeAbandoned - Флаг для удаления заброшенного подключения (по умолчанию *true*).
- org.unidata.mdm.core.job.datasource.validationQuery - Запрос для валидации подключения к БД (по умолчанию *SELECT 1*).
- org.unidata.mdm.core.job.datasource.validationInterval - Минимальная частота валидации (по умолчанию *30000*).

Параметры, отвечающие за настройки таймаута заброшенных подключений к БД.

- org.unidata.mdm.core.job.datasource.removeAbandonedTimeout - таймаут отключения соединения в секундах (по умолчанию 60).
- org.unidata.mdm.core.job.datasource.suspectTimeout - аналогичен removeAbandonedTimeout, только вместо закрытия соединений, пишет лог о возможном таймауте (по умолчанию 0, не пишет лог).

11.4.1.3. Секция ldap Integration

- com.universe.mdm.ldap.integration.ldap.full.name.source = ${LDAP_INTEGRATION_LDAP_FULL_NAME_FORMAT_SOURCE:-sgi} - задает источник для чтения полного имени, указывается для всех ldap-соединений. Допустимые значения displayName - чтение из атрибута displayName; sgi - чтение из атрибутов sn, given_name, initials (текущее поведение). Значение по умолчанию = sgi.

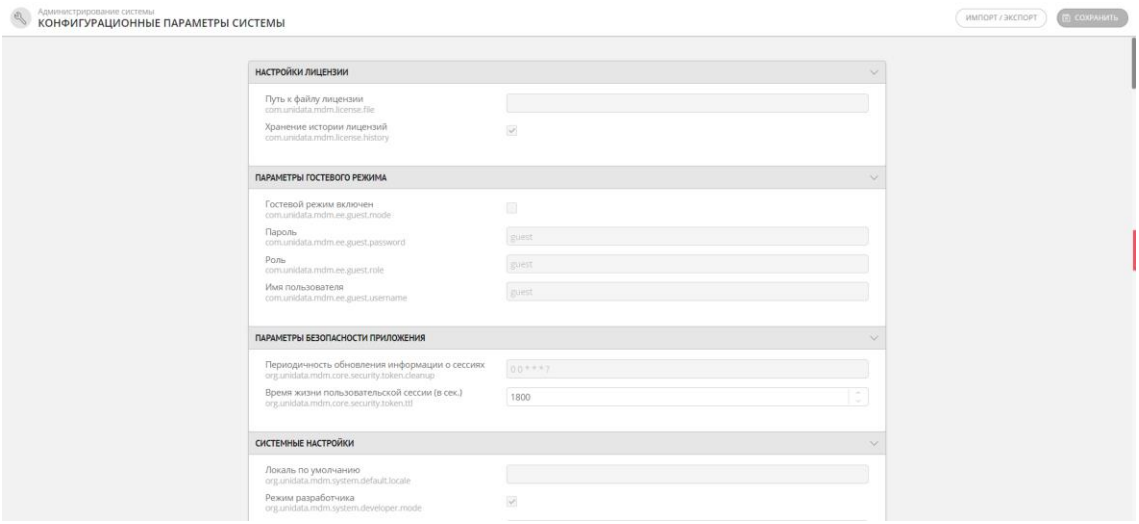


Рисунок 1 - Раздел "Параметры системы"

Руководство интегратора

12.Настройка системы

Также смотрите Руководство администратора системы: Раздел Параметры системы

Содержание:

12.1. Конфигурация и Логи

12.1.1. Конфигурация в Docker

Относительный путь к конфигурациям в Docker: */usr/share/tomcat/conf/universe*.

Каталог содержит:

- **backend.properties** - Системные параметры (раздел "Параметры системы").
- **templates** - Каталог шаблонов электронной почты.
- **enterprise-pipelines.json** - Потоки выполнения.
- **logback.xml** - Параметры логирования.

12.1.2. Конфигурация Backend

Система использует единственный конфигурационный файл **backend.properties** (имя предопределено). Содержимое файла смотрите в сборке системы, а также в интерфейсе пользователя (раздел "Параметры системы"). Описание некоторых параметров доступно в статье.

Если система устанавливается вручную, расположение файла может быть указано через флаги JVM: `-Duniverse.conf="<path>/universe-conf"`

12.1.3. Конфигурация Frontend

Используйте файл *customer.json* для настройки параметров пользовательского интерфейса. Он отображается как путь: */usr/share/nginx/html/customer.json* при запуске приложения в Docker. Изменение файла в контейнере может привести к

потере конфигурации после следующего запуска.

Для сохранения изменений:

- Если вы запускаете приложение из репозитория, то поместите файл с изменениями (с другим именем, например: "my_customer.json") в каталог json_configs, а затем перезапустите приложение с помощью docker-compose:

```
docker-compose -f docker-compose.yml -f docker-compose-json-generate.yml up -d
```

- Если вы локально создаете пользовательский интерфейс, то необходимо просто изменить файл *customer.json* перед сборкой кода или образа docker (в этом случае измените файл *customer.json* в папке "Build").

12.1.4. Логи

Продукты Юниверс используют slf4j и logback classic для ведения общих логов системы.

Параметры логирования настраиваются в файле *logback.xml*.

Описание логгеров:

- **<logger name="org.apache.cxf" level="INFO"/>** - вывод логов типа INFO + WARNING + ERROR для пакета CXF.
- **<logger name="org.universe" level="INFO"/>** - вывод логов от модулей CE (модулей ядра системы).
- **<logger name="com.universe" level="INFO"/>** и **<logger name="com.universe" level="INFO"/>** - вывод логов от модулей EE / SE.

12.2. Аутентификация через SSO

В этой статье:

Примечание:

Функционал SSO реализован в виде модуля `com.universe.mdm.sso.kerberos`, который является примером использования SSO. Некоторые шаги могут

отличаться в зависимости от используемой инфраструктуры.

Модуль `com.universe.mdm.sso.kerberos` поставляется отдельно в виде собранных jar-файлов. Для включения функционала SSO необходимо добавить 4 jar-файла в папку *./universe-integration*. См. подробнее о добавлении кастомных модулей.

Исходники SSO:

Скачать `com.universe.mdm.sso.kerberos-6.9.0-SNAPSHOT-sources.jar`

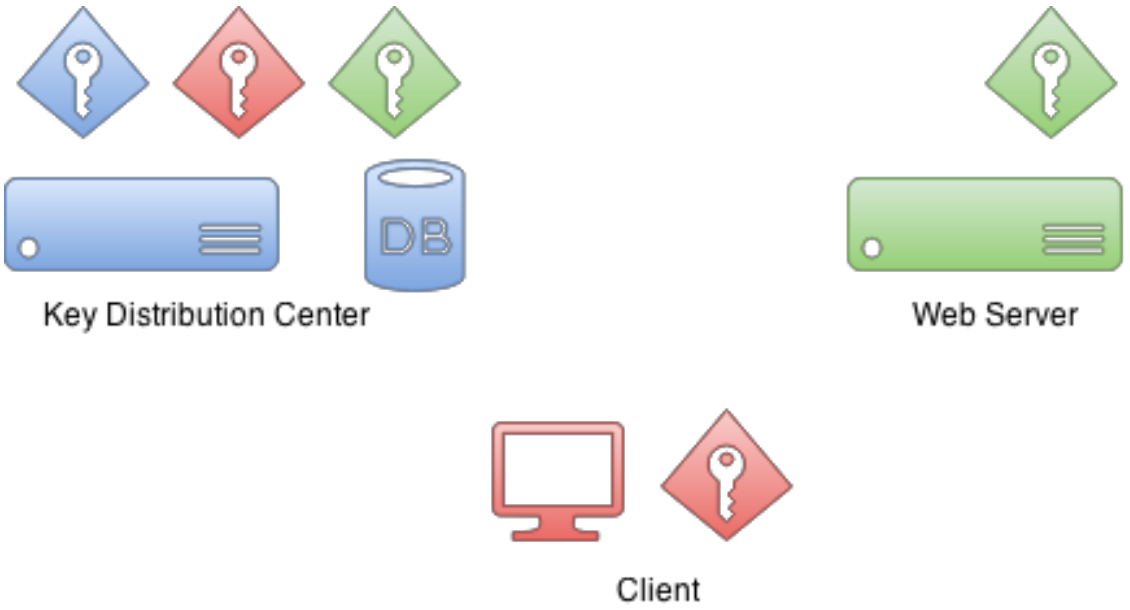
Скачать `com.universe.mdm.sso.kerberos-6.9.0-SNAPSHOT.jar`

Зависимости для Spring:

Скачать `spring-security-kerberos-core-1.0.1.RELEASE.jar`

Скачать `spring-security-kerberos-client-1.0.1.RELEASE.jar`

12.2.1. Общие сведения



Основные участники:

- Client - клиентский компьютер, который хочет пройти аутентификацию на сервере (Web Server).
- Web Server - сервер, который предоставляет сервис клиенту, в данном случае сервер с universe web app.
- KDC - Key Distribution Center - центральный узел Kerberos (в случае Windows Server - Domain Controller), который состоит из двух компонентов:
    - Authentication Server - сервер аутентификации.
    - Ticket Granting Server (TGT) - сервер выдачи тикетов

пользователю.

Основные понятия:

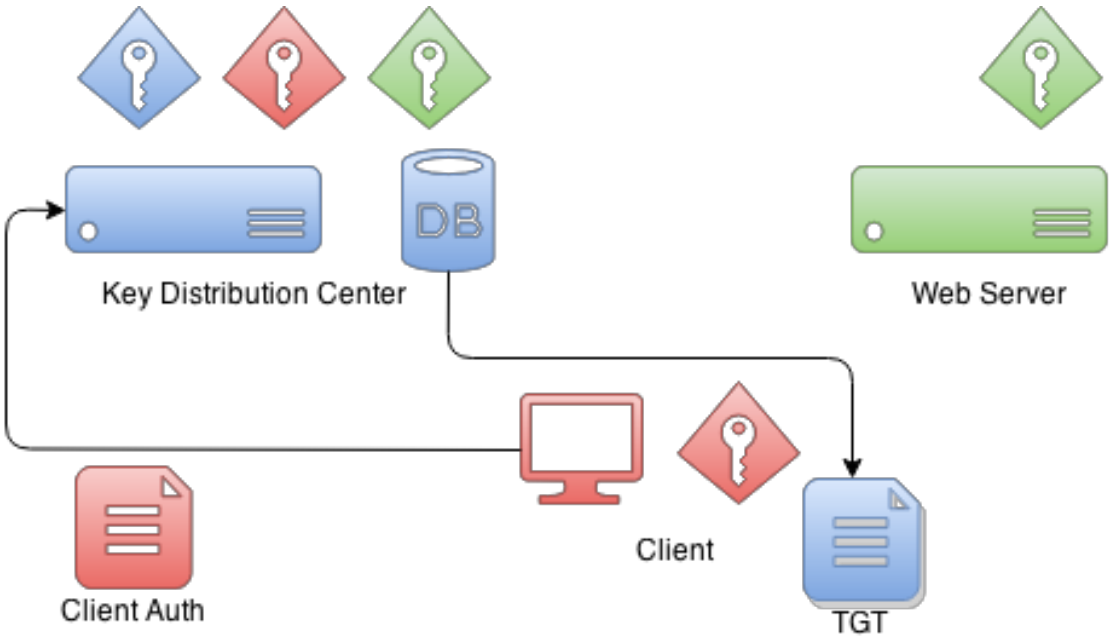
- Key Distribution Center (KDC) - хранилище информации о паролях пользователей.
- Admin server - основной сервер kerberos. У нас KDC и admin server находятся на одной машине
- Realm - домен, в котором производится аутентификация.
- Principal - пользователь, участвующий в механизме аутентификации.
- Keytab - файл таблицы ключей, содержащий пары имен субъектов Kerberos и зашифрованные ключи, полученные из пароля Kerberos.
- krb5.conf - настройки KDC в Universe web app.

Ускоренный курс по Kerberos:

Первоначально, когда среда Kerberos настроена и участники домена создаются в базе данных, также создаются ключи шифрования, основанные на общих секретах (например, пароле пользователя), а фактические пароли никогда не хранятся в виде открытого текста.

Фактически KDC имеет свой собственный ключ и другие ключи для пользователей домена.

В процессе аутентификации пользователя в web-сервере нет взаимодействия между web-сервером и KDC в Windows Domain Controller.

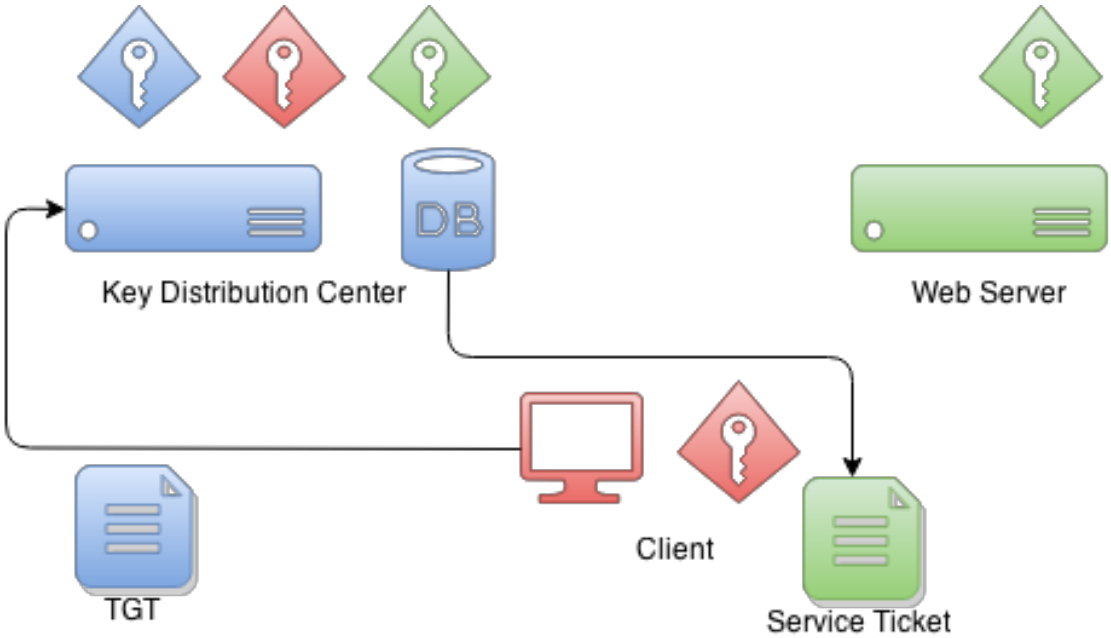


Когда клиент пытается аутентифицировать себя на веб-сервере, ему сначала

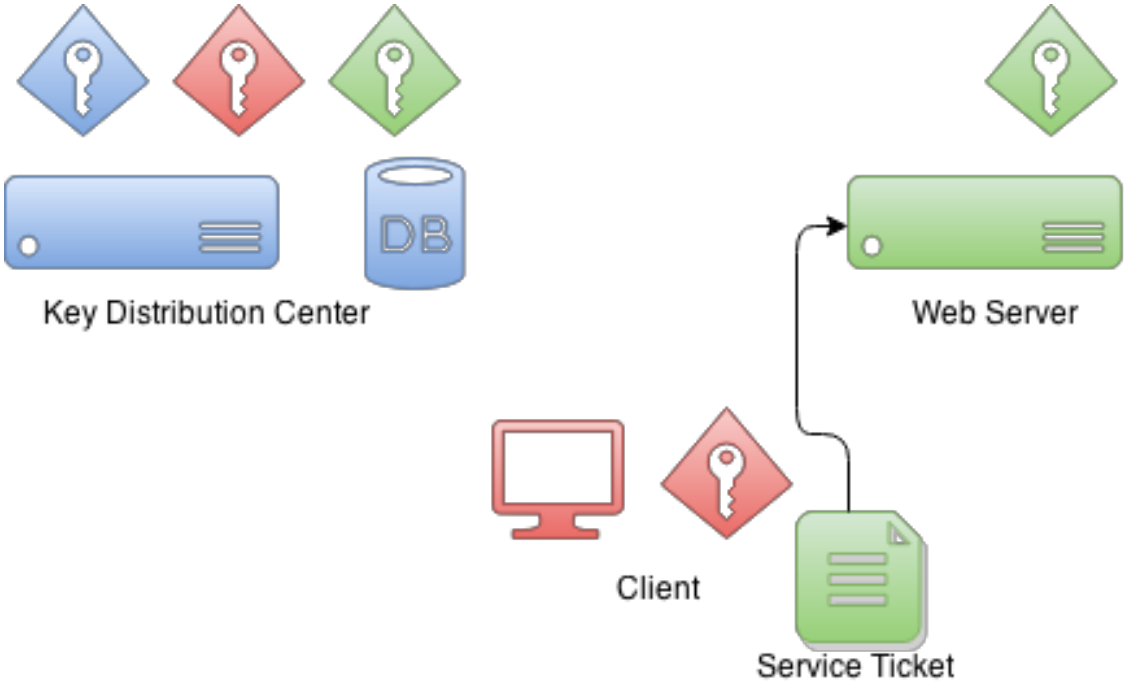
необходимо связаться с KDC. Клиент создаст специальный пакет, содержащий зашифрованные и незашифрованные части. Незашифрованная часть содержит, например, информацию о пользователе, а зашифрованная часть — другую информацию, которая является частью протокола. Клиент будет шифровать данные пакета своим ключом.

Когда KDC получает этот пакет от клиента, он проверяет, кем этот клиент называет себя из незашифрованной части, и на основе этой информации использует ключ дешифрования клиента, который уже есть в его базе данных. Если эта расшифровка прошла успешно, KDC знает, что этот клиент является тем, за кого он себя выдает.

То, что KDC возвращает клиенту, — это тикет под названием Ticket Granting Ticket, который подписан собственным закрытым ключом KDC. Позже, когда клиент отправляет обратно этот тикет, он может попытаться расшифровать его, и если эта операция прошла успешно, он знает, что это был тикет, который он сам изначально подписал и передал клиенту.



Когда клиент хочет получить тикет, который он может использовать для аутентификации на веб-сервере, TGT отправляется в KDC и там подписывается с помощью ключа веб-сервера. Этот тикет содержит данные, которые может расшифровать только сам веб-сервер.

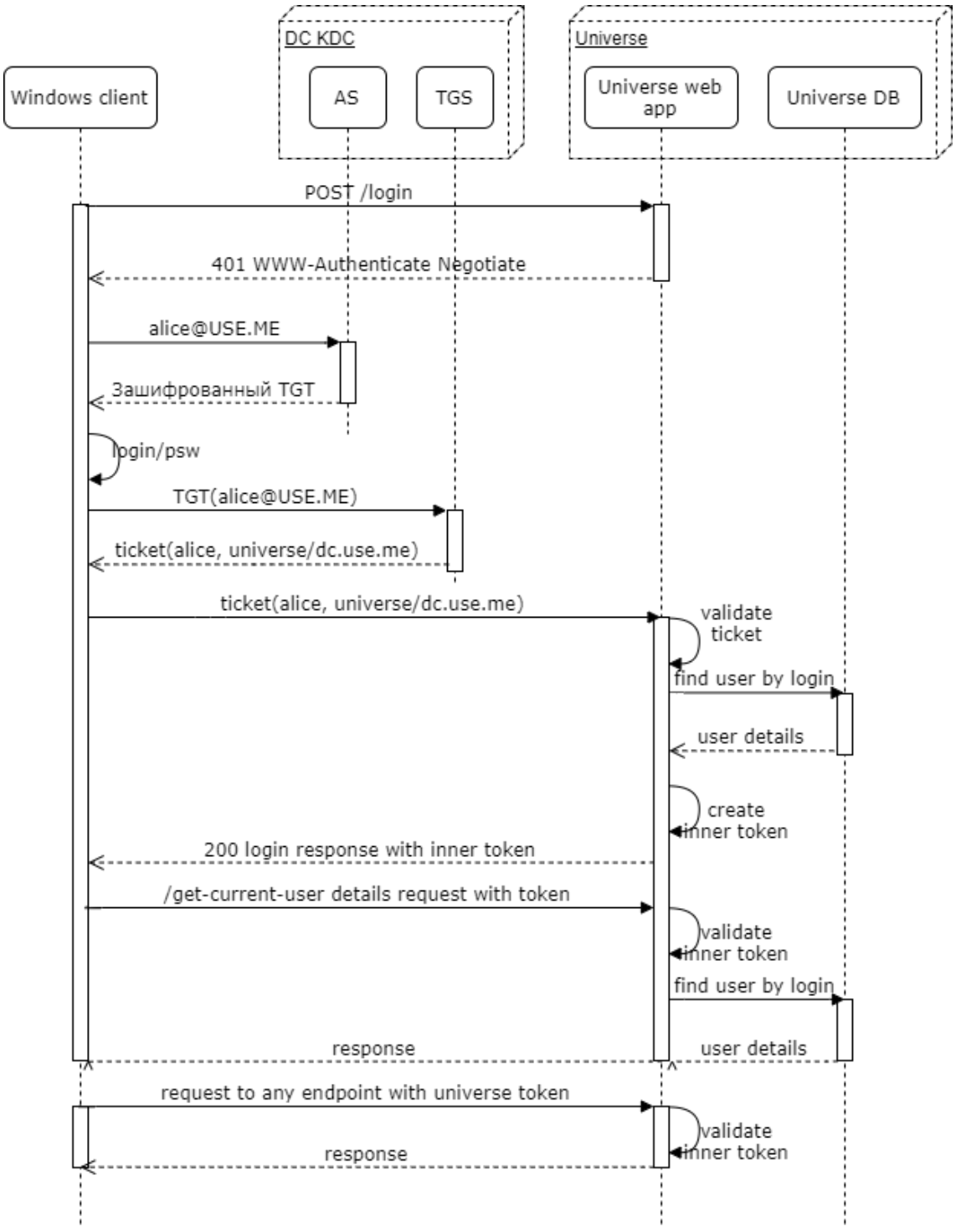


Когда клиент проходит аутентификацию на веб-сервере, он отправляет полученный из KDC тикет подписанный ключом веб-сервера (ключ есть в KDC). Веб-сервер пытается расшифровать тикет (с помощью *keytab*), и если эта операция будет успешной, веб-сервер полагается на то, что другой стороной, которая знает учетные данные веб-сервера является KDC, поэтому клиент является тем, за кого себя выдает.

Полезные ссылки:

- Spring Security Kerberos - Reference Documentation
- LDAP search user by username with server Kerberos authentication
- Настройка Kerberos аудита в AD

12.2.2. Механизм аутентификации



Предусловия:

- Пользователь успешно аутентифицирован на машине под управлением Windows.
- Ссылка на ресурсы universe (Url) не может быть в виде ip:port, а только с

указанием DNS-имени (связано с регистрацией Web-сервиса в AD).

Предупреждение:

БД Universe должна быть синхронизирована с AD через LDAP

Шаги аутентификации:

1. Пользователь открывает ссылку на ресурс universe с указанием get параметра sso со значением on или true (например, universe-ea?sso=true).
2. Сервер universe возвращает HTTP-код 401 "Not Authorized".
3. Браузер пользователя запрашивает токен в KDC.
4. AD возвращает токен.
5. Браузер отправляет запрос на аутентификацию пользователя в universe, в запросе присутствует полученный токен.
6. Сервер валидирует токен в KDC. В случае успеха сервер получает имя пользователя в AD.
7. Сервер получает доп. данные (например, группы/роли, в которых он состоит) по имени пользователя в локальной бд.

12.2.3. Настройка окружения

12.2.3.1. Имена хостов

Каждый сервер внутри Kerberos realm должен иметь FQDN (Fully Qualified Domain Name).

Kerberos так же ожидает, что FQDN сервера является reverse-resolvable. Если выяснение доменного имени по IP недоступно, то установите значение переменной `rdns` в значение false на клиентах в файле krb5.conf.

Если сервер уже имеет назначенное FQDN, проверьте корректность обнаружения `forward` и `reverse`, выполнив на клиенте следующие команды:

```
$ nslookup dc.use.me
$ nslookup "Ваш IP"
```

12.2.3.2. Наличие соединения

Для проверки соединения между хостами, выполните `ping` для каждого хоста по его FQDN:

```
$ ping dc.use.me
PING dc.use.me (10.0.0.1) 56(84) bytes of data.
64 bytes from dc.use.me (10.0.0.1): icmp_seq=1 ttl=128 time=0.176ms
```

Вывод команды `ping` показывает успешное определение IP-адреса по FQDN, и простой ответ от сервера. Ответ от сервера является подтверждением того, что между хостом и сервером есть соединение.

Проблемы при работе `ping` указывают на проблемы настройки сервера или клиента.

12.2.3.3. Синхронизация времени

Протокол Kerberos требует синхронизации времени сервера и клиента: если системные часы клиентов и сервера расходятся, то аутентификация не будет выполнена. Простейший способ синхронизировать системные часы - использование Network Time Protocol (NTP) сервера.

Для настройки допустимого расхождения времени в *krb5.conf* предусмотрен параметр clockskew.

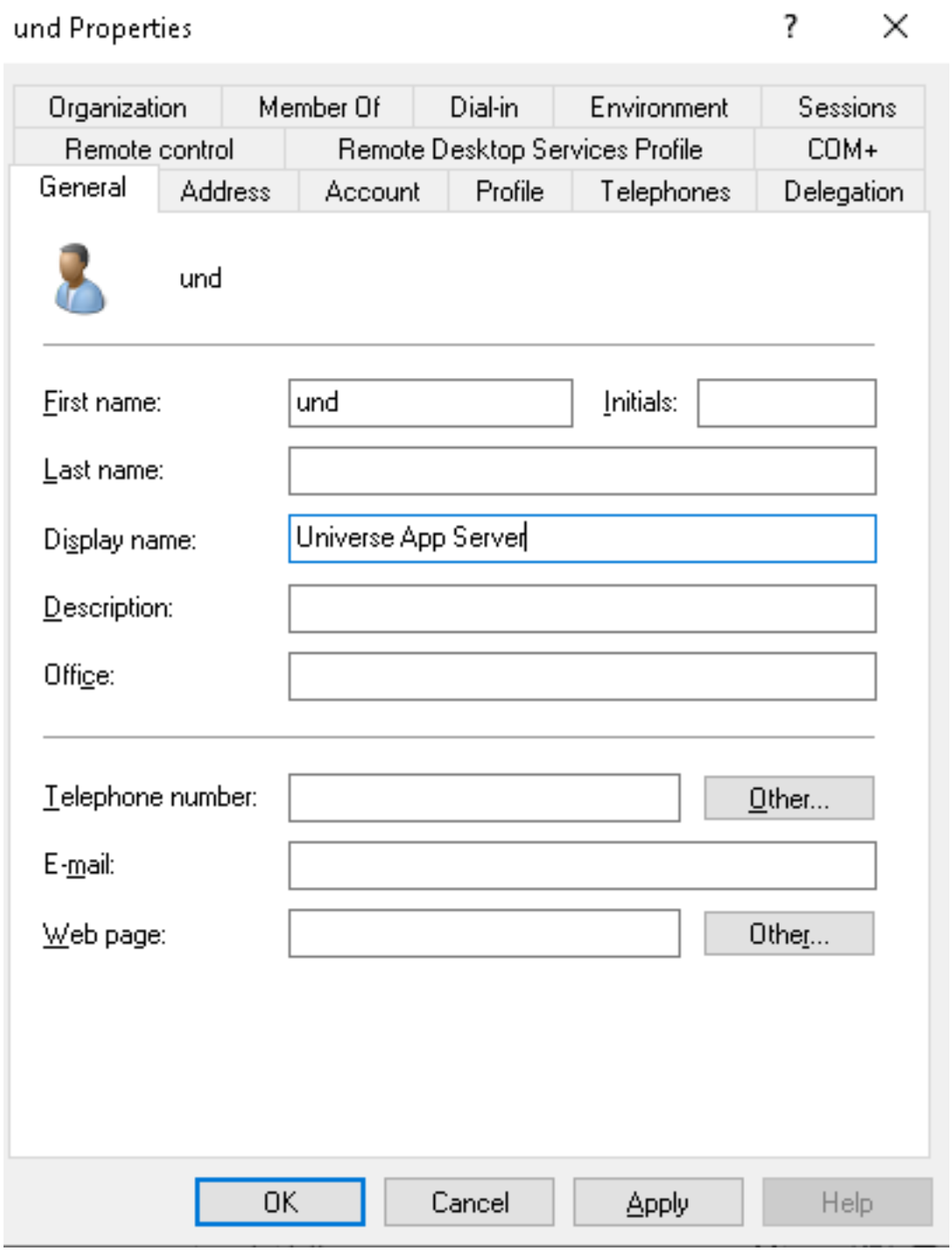
12.2.3.4. Брандмауэры

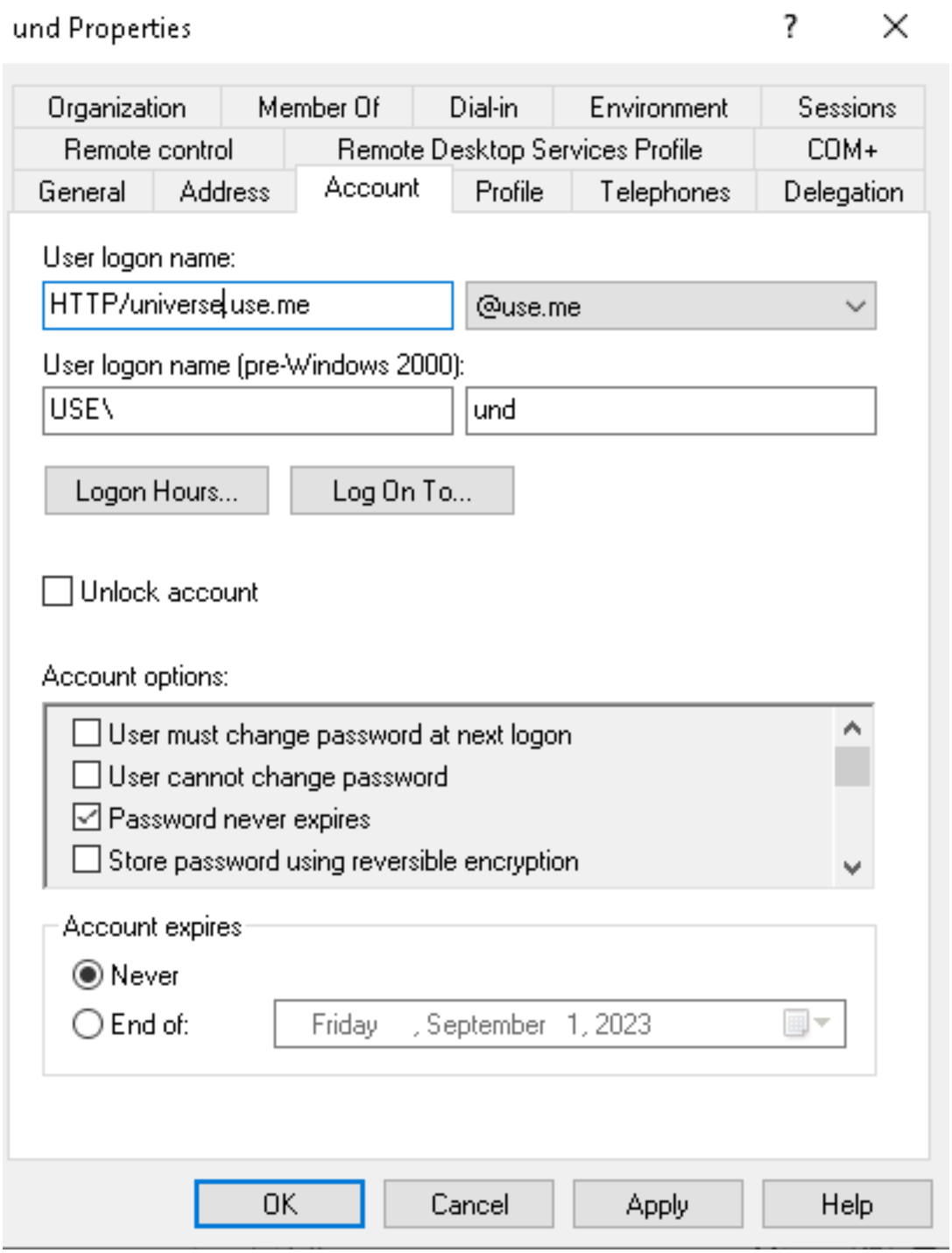
Так же как и все остальные сетевые службы, Kerberos должен иметь возможность проходить через любые брандмауэры между хостами. Инструкция Kerberos System Administration Manual имеет детальное описание портов, которые необходимо открыть при настройке брандмауэров.

12.2.3.5. Настройка Windows Domain Controller with KDC

Шаг 1. Создать пользователя для сервера приложений, который будет выполнять роль ServicePrincipal.

Первоначально пользователь создается с логином und, логин меняется на *HTTP/universe.use.me@USE.ME* после создания.


und Properties
Organization
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Delegation
und
First name:
und
Initials:
Last name:
Display name:
Universe App Server
Description:
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help



Шаг 2. Создать маппинг пользователя на сервис командой `setspn`в cmd в режиме Администратора:

```
$ setspn -A HTTP/universe.use.me und
```

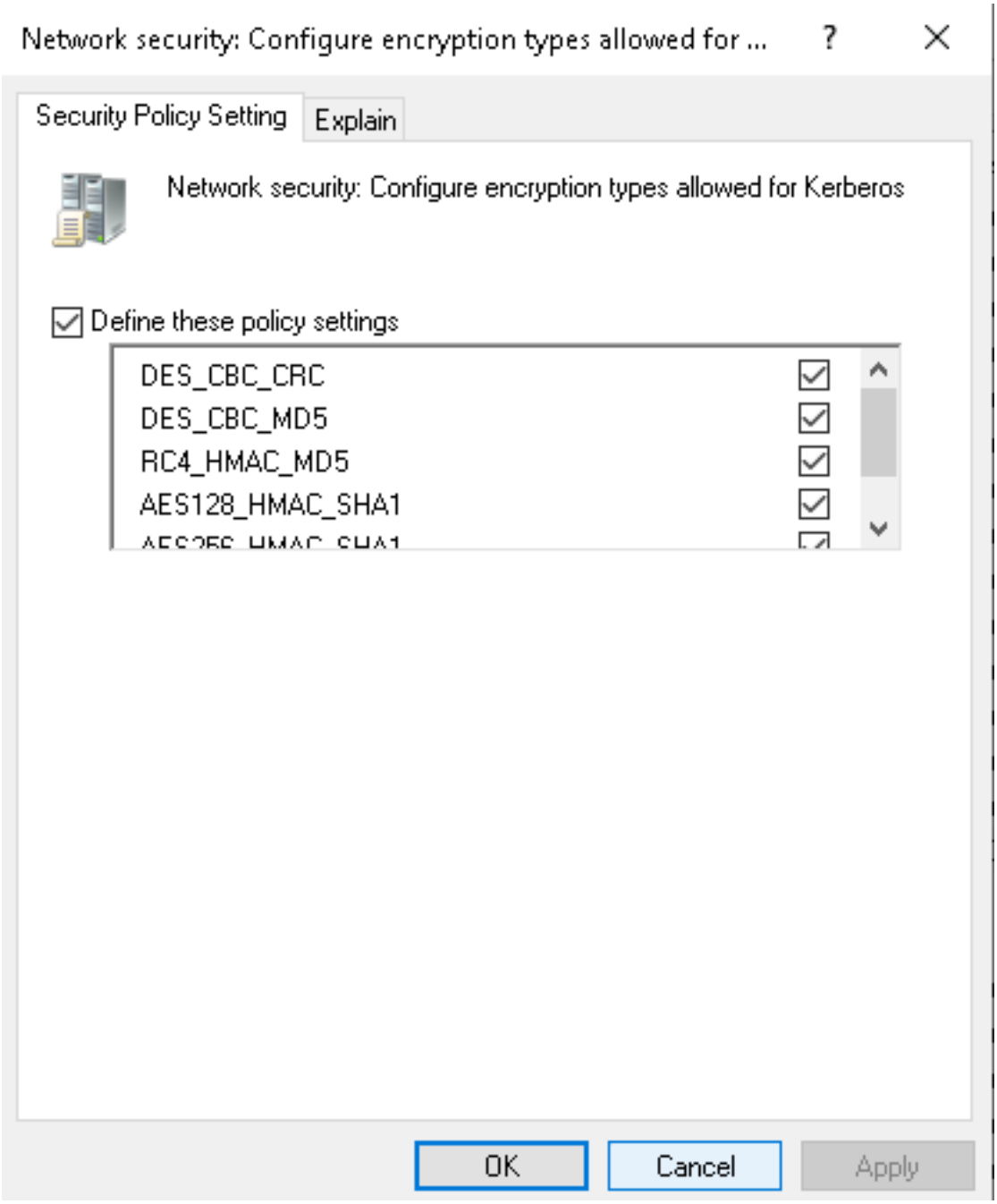
Шаг 3. Сгенерировать *.keytab* файл и поместить его на сервер приложений (Universe):

```
$ ktpass /out c:¥tomcat.keytab /mapuser und@USE.ME /princ
HTTP/universe.use.me@USE.ME /pass Qwerty123 /ptype KRB5_NT_PRINCIPAL /crypto All
```

Предупреждение:

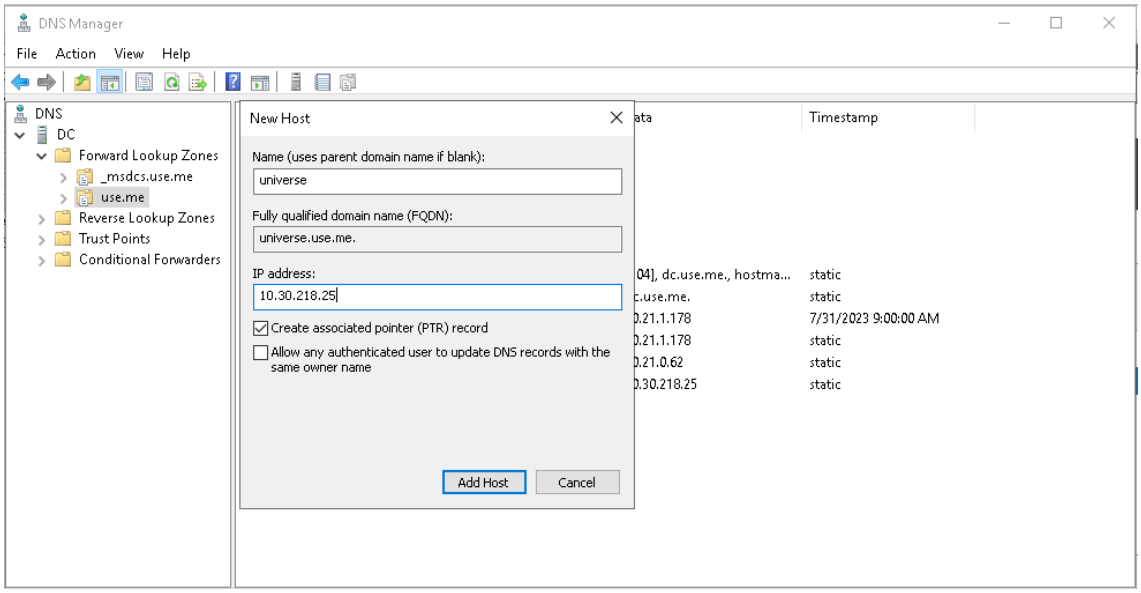
@USE.MEпрописывается в верхнем регистре даже если при конфигурировании указывался нижний регистр

Шаг 4. Настроить допустимые encryption types: Group Policy Management → Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options → Network security: Configure encryption types allowed for Kerberos.



Шаг 5. Hostname сервера universe должен быть reverse-resolvable для Windows AD Server. Проверяется с помощью команды `nslookup`

Если это не так, должна быть создана запись Host A в DNS → Forward Lookup Zones и pointer в Reverse Lookup Zones.

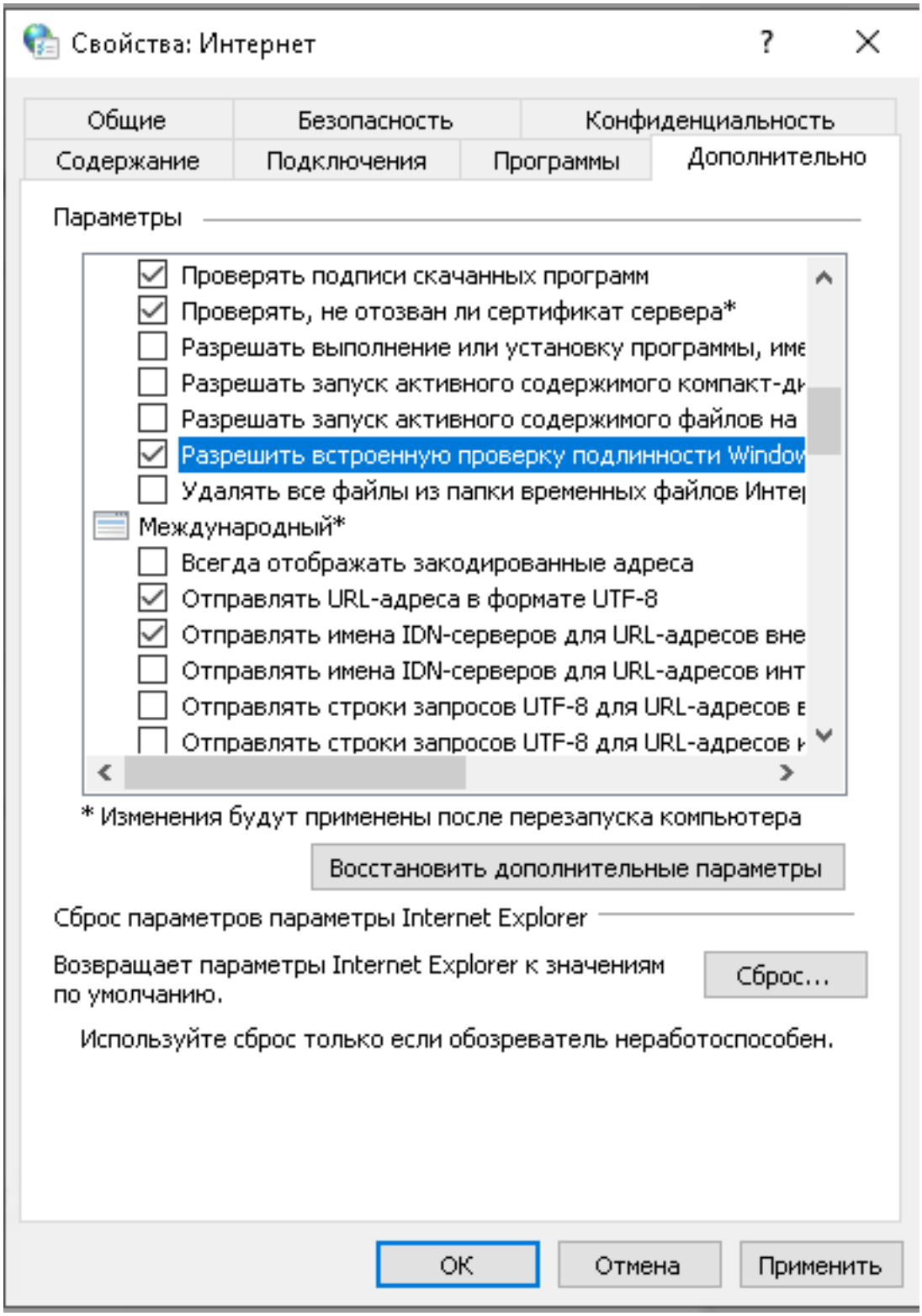


В Windows AD Server можно настроить аудит для Kerberos (Настройка Kerberos аудита в AD).

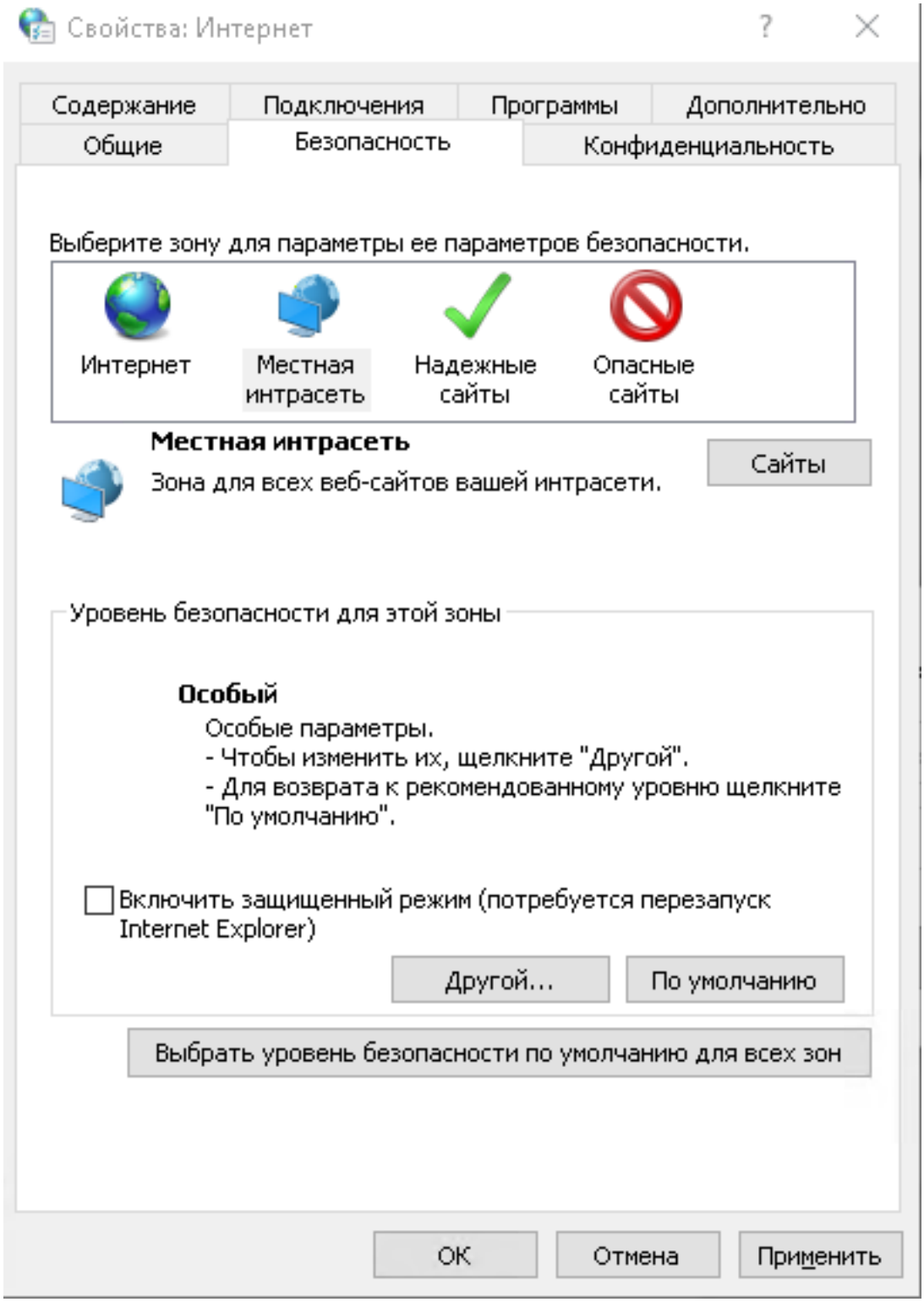
12.2.3.6. Настройка Windows клиентов

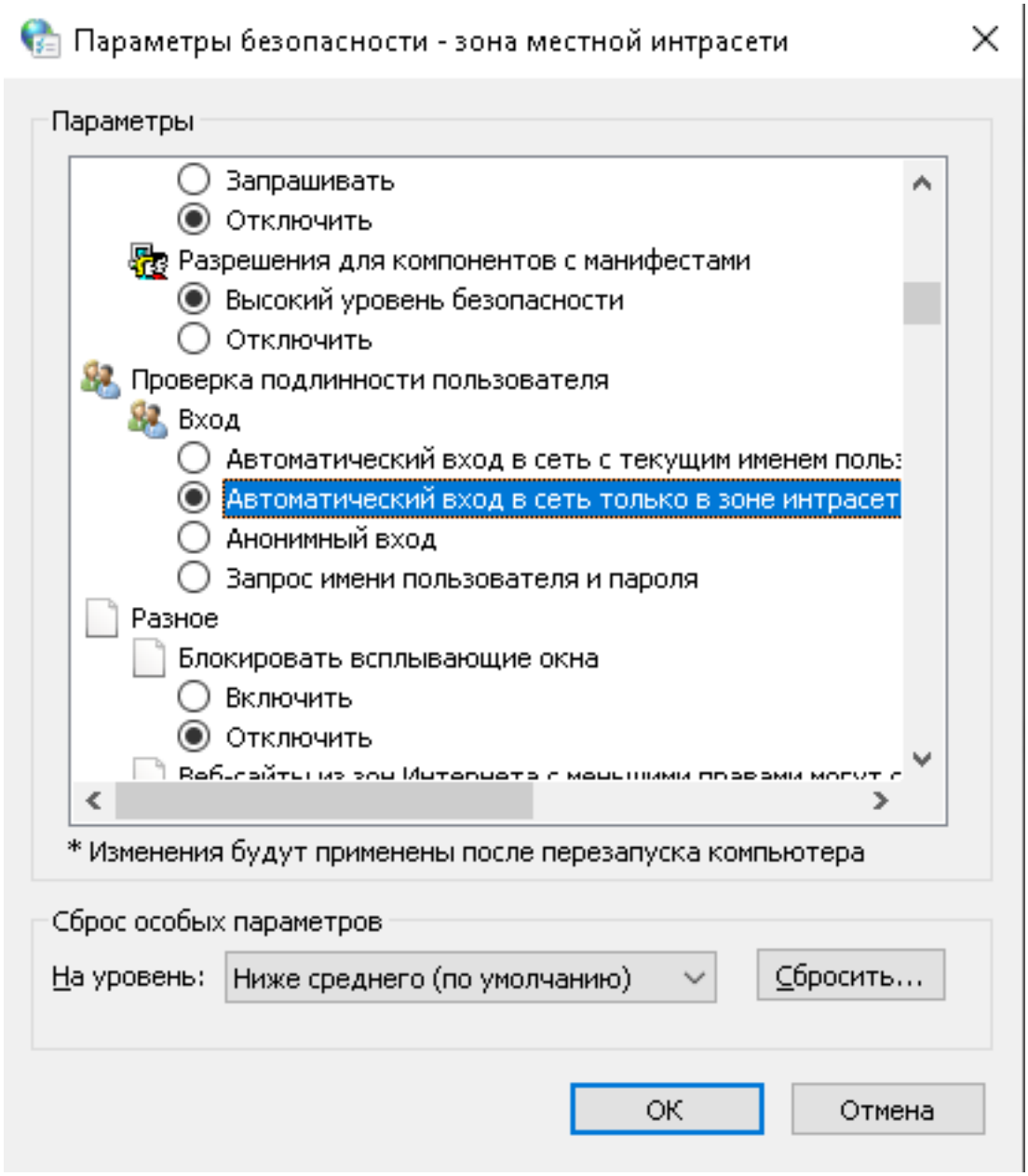
Необходимо настроить браузер IE/MS Edge на каждом клиенте в Свойствах Браузера.

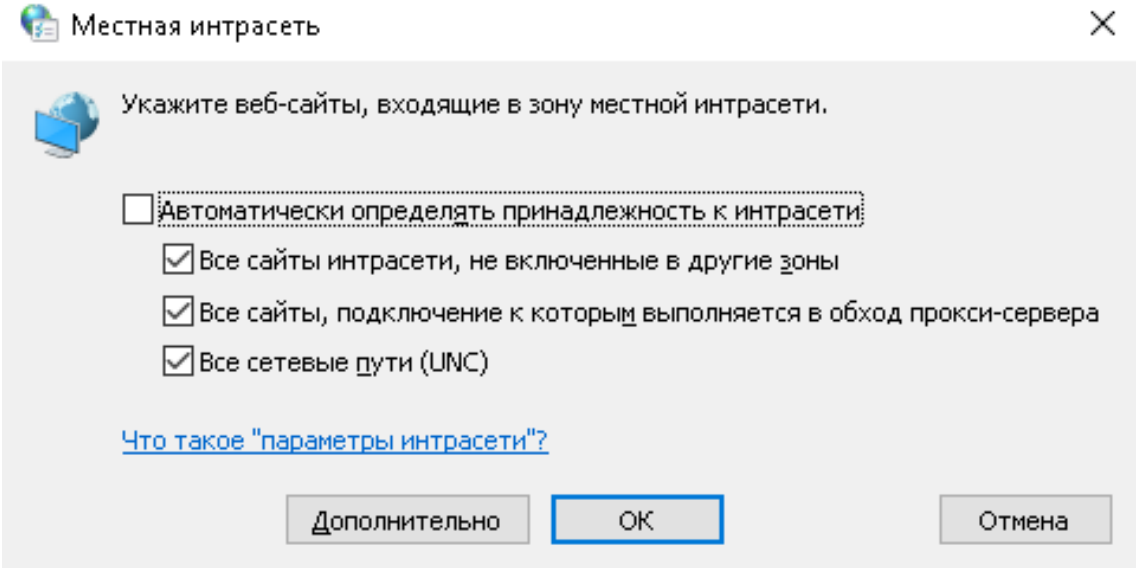
Шаг 1. Разрешить встроенную проверку подлинности Windows.



Шаг 2. Настроить местную интрасеть.


Свойства: Интернет
Содержание
Подключения
Программы
Дополнительно
Общие
Безопасность
Конфиденциальность
Выберите зону для параметры ее параметров безопасности.
Интернет
Местная интрасеть
Надежные сайты
Опасные сайты
Местная интрасеть
Зона для всех веб-сайтов вашей интрасети.
Сайты
Уровень безопасности для этой зоны
Особый
Особые параметры.
- Чтобы изменить их, щелкните "Другой".
- Для возврата к рекомендованному уровню щелкните "По умолчанию".
Включить защищенный режим (потребуется перезапуск Internet Explorer)
Другой...
По умолчанию
Выбрать уровень безопасности по умолчанию для всех зон
ОК
Отмена
Применить


Параметры безопасности - зона местной интрасети
Параметры
Запрашивать
Отключить
Разрешения для компонентов с манифестами
Высокий уровень безопасности
Отключить
Проверка подлинности пользователя
Вход
Автоматический вход в сеть с текущим именем польз
Автоматический вход в сеть только в зоне интрасет
Анонимный вход
Запрос имени пользователя и пароля
Разное
Блокировать всплывающие окна
Включить
Отключить
* Изменения будут применены после перезапуска компьютера
Сброс особых параметров
На уровень:
Ниже среднего (по умолчанию)
Сбросить...
OK
Отмена



Шаг 3. Ссылка на ресурсы universe (Url) не может быть в виде *ip:port*, а только с указанием DNS-имени (связано с регистрацией Web-сервиса в AD). При невозможности использовать DNS, маппинг должно быть прописан в файле *C:WindowsSystem32driversetchosts*.

Пример:

```
10.30.218.25 universe.use.me
```

Шаг 4. Время должно быть должно быть синхронизировано с AD и веб-сервером universe. Настройка браузеров для использования с Kerberos.

12.2.3.7. Настройка Universe web app

1. Время должно быть синхронизировано с Windows AD Server.
2. Скопируйте *keytab* сгенерированный во время настройки Windows AD Server на сервер с tomcat.
3. Скопируйте *krb5.conf* на сервер с tomcat.
   - Realm - доменное имя большими буквами.
   - Дополнительно см. в файле *krb5.conf*

Пример krb5.conf:

```
[libdefaults]
      default_realm = USE.ME

[realms]
      USE.ME = {
               kdc = dc.use.me
      }

[domain_realm]
      use.me=USE.ME
      .use.me=USE.ME
```

4. В universe должно быть реализован модуль со следующими сущностями:
   - Interceptor запросов, который перехватывает запросы пользователя и отвечает схемой "401 Negotiate" для получения KDC тикета от пользователя и валидирует пришедший тикет.
   - *KerberosSecurityDataSource* реализует *SecurityDataSource*, *AfterModuleStartup*, который регистрирует провайдеры аутентификации, авторизации и получения профиля для SSO через Kerberos, либо делегирует дефолтному компоненту.
   - Необходимые провайдеры для SSO через Kerberos, зарегистрированные в *KerberosSecurityDataSource*, например *LoginProvider*.
   - Сервис, осуществляющий поиск пользовательских атрибутов по имени пользователя (через LDAP или в локальной бд, если она синхронизирована с AD).
5. Tomcat должно быть запущен с опциями.

Пример:

```
-Djava.security.krb5.conf=/path/to/krb5.conf
-Dsun.security.krb5.debug=true //for debug only, remove when all works
```

6. Должны быть предоставлены необходимые свойства для валидации пришедшего тикета.

Пример свойств в *backend.properties*:

```
security.kerberos.realm=USE.ME //edit with correct domain name
security.kerberos.keytab.file=/path/to/tomcat.keytab
security.kerberos.service.principal=HTTP/universe.use.me@USE.ME
```

7. FQDN должно быть reverse-resolvable. Если выяснение доменного имени по IP недоступно, то установите значение переменной `rdns` в значение false в файле параметров *krb5.conf*.

Если сервер KDC уже имеет назначенное FQDN, проверьте корректность

обнаружения forward и reverse выполнив на клиенте следующие команды:

```
$ nslookup dc.use.me
$ nslookup "Ваш IP"
```

Вывод первой команды должен содержать IP-адрес сервера. Вывод второй команды должен содержать FQDN сервера.

Если у сервера нет назначенного FQDN и сервис DNS не доступен, то вы можете отредактировать локальные файлы hosts (обычно они находятся в /etc) на сервере.

> **Предупреждение:**
> После ip сначала должно быть fqdn.

Пример:

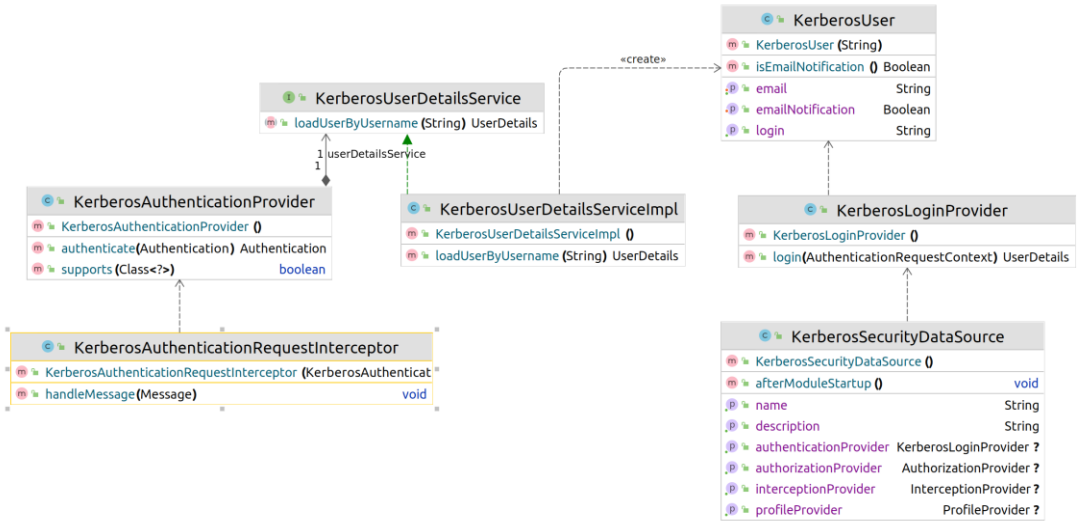
```
#Правильно
10.21.1.178    dc.use.me    use.me

#Неправильно
10.21.1.178    use.me       dc.use.me
```

После этого проверьте работу локальных DNS имен используя команду nslookup.

12.2.3.8. Поиск неисправностей

См. документацию по исправлению возможных проблем

12.2.4. Пример реализации Kerberos SSO модуля



Процесс авторизации:

- Запросы на сервер universe перехватывается

KerberosAuthenticationRequestInterceptor.

- Если запрос на */login* и есть header ("Single-Sign-On", true), в ответ отправляется 401 с header (""WWW-Authenticate", "Negotiate").
- Если пришедший ответ или один из запросов присылает header ("Authorization", "Negotiate"), *KerberosServiceAuthenticationProvider*:
    - Проверяет тикет;
    - Ищет пользователя в локальной БД по username с помощью *KerberosUserDetailsService*;
    - Устанавливает аутентификацию в контекст.
- Запрос отправляется на endpoint */login*.
- Приложение пытается залогинить пользователя используя Authentication провайдеры из имеющихся *SecurityDataSource*.
- KerberosLoginProvider проверяет контекст аутентификации.
- В приложении создается внутренний токен для пользователя.
- При последующих запросах авторизованного пользователя на другие endpoint'ы проверяется внутренний токен.

Тикет KDC проверяется только при запросе на endpoint */login*.

Ограничения:

1. В текущей имплементации пользователи подтягиваются из локальной БД, поэтому приложение должно быть синхронизировано с AD.
    - Пользователь не сможет залогиниться, если после его создания не была синхронизирована локальная БД приложения и AD. *Error response: Пользователь не найден. Требуется синхронизация с Active Directory.*
    - Если после синхронизации данные изменились, пользователь войдет в систему с устаревшими данными.

Возможные решения:

- Синхронизировать локального пользователя с AD через LDAP Rest Template при логине.
- Синхронизировать локального пользователя с AD используя имеющийся модуль для синхронизации через LDAP.
- Синхронизировать локального пользователя с AD через LDAP с аутентификацией через Kerberos (LDAP search user by username with server Kerberos authentication).

2. Если деактивировать пользователя в AD, пользователь не сможет войти в приложение, т.к. KDC не выдаст тикет. Однако, если пользователь уже

авторизован в приложении автоматического логаута не произойдет.

3. Логаут приводит к автоматической авторизации пользователя, т.к. наличие в пути */sso=true* или */sso=on* перенаправляет на endpoint */login*.

12.2.4.1. Примеры конфигурации

krb5.conf и *keytab* должны быть скопированы в universe web server.

Пример конфигурации KDC:

```
[libdefaults]
      default_realm = USE.ME

[realms]
      USE.ME = {
               kdc = dc.use.me
      }

[domain_realm]
      use.me=USE.ME
      .use.me=USE.ME
```

Пример настройки в *backend.properties*:

```
security.kerberos.realm=USE.ME //edit with correct domain name
security.kerberos.keytab.file=/path/to/tomcat.keytab
security.kerberos.service.principal=HTTP/universe.use.me@USE.ME
```

Параметры Java:

```
-Djava.security.krb5.conf=/path/to/krb5.conf
-Dsun.security.krb5.debug=true //for debug only, remove when all works
```

12.2.5. Полезные команды

Команды для Windows:

- #setspn - добавляет/проверяет связки principal name - domain name; сопоставляет внешние адреса с пользователем (Principal user HTTP/@).
  - `setspn -L accountname` - отображает текущий зарегистрированный SPN для учетной записи.
  - `setspn -F -Q HTTP/*@*` показать созданные связки, где `-F` - фильтр на уровень леса (не используется, если лес из одного домена), `-Q HTTP/*@*` - фильтр на созданные principal name.
- #klist
  - `klist tickets` - проверяет получение кешированных билетов kerberos.

- `klist get http/universe132.use.me` - информация о хранимых в кэше krbTicket.
- `klist.exe -K -e -t -k c:¥tomcat132.keytab` - анализ файла с ключами. На основе этого ключа получаем krbTicket, продлеваемый после использования.
- `klist tgt` - информация о текущем тикете из кэша учетных данных Kerberos.
- `klist purge` - очищает ключи из кэша.

- #ktpass - генерирует связку principal name - domain name - key.
  - `ktpass /out c:¥tomcat132.keytab /mapuser und2@UNI.ME /princ HTTP/universe132.use.me@UNI.ME /pass q1w2e3r4Q /ptype KRB5_NT_PRINCIPAL /crypto All`

Команды для Linux:

- #klist - проверяет получение кешированных билетов kerberos.
  - `klist -k -t tomcat132.keytab -K -e`
- #kinit - получает тикет */etc/krb5.conf*.
  - `kinit girl@USE.ME`

kinit для principal требует сертификат - см. официальную документацию.

12.2.6. Возможные ошибки

Если параметры учетной записи при настройке Windows Domain Controller with KDC не сработали корректно (Рисунок 1), и нет возможности внести исправления в домен - добавьте параметры понижения безопасности в файл *krb5.conf*:

```
[libdefaults]
clockskew = 200000
allow_weak_crypto = TRUE
```

В логе будет ошибка вида:

```
2024-02-16 11:40:24,529 [http-nio-8080-exec-1] [-] [-] WARN
org.apache.cxf.phase.PhaseInterceptorChain.doLog:465 - Interceptor for
{http://service.core.v2.rest.mdm.unidata.org/}LoginRestService has thrown
exception, unwinding now
org.springframework.security.authentication.BadCredentialsException: Kerberos
validation not successful
Caused by: sun.security.krb5.KrbException: Encryption type RC4 with HMAC is not
supported/enabled
```

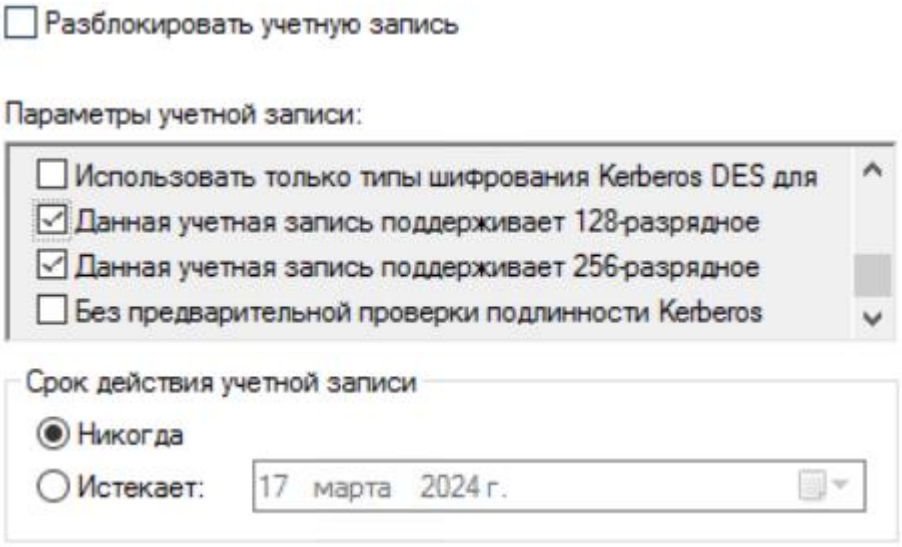


Рисунок 1 – Настройка параметров учетной записи

12.3. Рассылка по электронной почте

Возможна настройка других почтовых сервисов. Для настройки необходимо в параметре `unidata.activiti.task.mailServerHost=smtp.yande` указать другой хост, в `unidata.activiti.task.mailServerPassword` указать пароль почты, и выполнить настройки сервиса, аналогичные шагам 2 и 3 из инструкции по настройке "Яндекс Почты".

12.3.1. Настройка Яндекс Почты

Чтобы настроить рассылку для Яндекс Почты:

1. Воспользуйтесь "Яндекс Справкой". Перейдите в раздел "Настройка почтовых программ" > "Другие программы".
2. Выполните действия:
   - Откройте раздел "Почтовые программы" в настройках "Яндекс Почты".
   - Выберите опции "С сервера imap.yandex.ru по протоколу IMAP" и "Пароли приложений и OAuth-токены".
   - Сохраните изменения.
3. Необходима генерация нового пароля, так как в целях безопасности сервис требует различные пароли:
   - Откройте страницу "Пароли приложений" вашего аккаунта Яндекс ID и нажмите "Создать новый пароль".
   - Выберите тип приложения "Почта".

- Придумайте название пароля, например укажите название приложения, для которого вы создаете пароль. С этим названием пароль будет отображаться в списке.
- Нажмите кнопку *Создать*. Пароль приложения отобразится во всплывающем окне. Созданный пароль можно увидеть только один раз. Если вы ввели его неправильно и закрыли окно, удалите текущий пароль и создайте новый.

4. Полученный пароль используйте далее при настройке конфигурации.
5. Если система устанавливалась через Docker, то оптимальный способ конфигурирования - через файл *.env*. Пример:

```
RESTORE_EMAIL_FRONTEND_URL=http://localhost:8082/
RESTORE_EMAIL_ENABLED=true
RESTORE_EMAIL_SERVER_HOST=smtp.yandex.ru
RESTORE_EMAIL_SERVER_PORT=465
RESTORE_EMAIL_SSL_ENABLE=true
RESTORE_EMAIL_STARTTLS_ENABLE=false
RESTORE_EMAIL_USERNAME=<Почта>
RESTORE_EMAIL_PASSWORD=<Сгенерированный пароль>
```

6. Если система устанавливалась вручную из дистрибутива, то измените параметры в файле *<UNIVERSE_CONF_DIR>/backend.properties*. Пример:

```
# Email notifications
org.unidata.mdm.core.email.enabled=true
org.unidata.mdm.core.email.templates_folder=file://${universe.conf}/temp
lates
org.unidata.mdm.core.email.server_host=smtp.yandex.ru
org.unidata.mdm.core.email.server_port=465
org.unidata.mdm.core.email.username=<Почта>
org.unidata.mdm.core.email.password=<Сгенерированный пароль сервиса>
org.unidata.mdm.core.email.frontend_url=http://localhost:8080/
```

- Используйте один из способов сохранения параметров *backend.properties*:
  - Сохраните изменения в *backend.properties* и перезагрузите контейнер, не перезапуская сборку.
  - Или подложите через docker-compose уже настроенный *backend.properties* в запускающийся контейнер.

Шаблоны писем расположены в каталоге *<TOMCAT_HOME>/conf/universe/templates*. Используется процессор шаблонов Apache Velocity.

12.3.2. Настройка Google почты

Чтобы настроить рассылку для Google почты:

1. Войдите в Google-аккаунт. Включите двухэтапную аутентификацию, если это не было сделано ранее:
   - Откройте страницу "Аккаунт Google".
   - На панели навигации выберите "Безопасность".
   - В разделе "Вход в аккаунт Google" нажмите "Двухэтапная аутентификация" > "Начать".
   - Следуйте инструкциям на экране.
2. После завершения действий станет доступен пункт "Пароли приложений".
   - Если пункт недоступен, то см. "Примечания" в конце статьи.
3. Войдите в "Пароли приложений" и создайте пароль для приложения "Другое", вписав название приложения. Например, Universe. Полученный пароль используйте в следующем шаге.
4. Если система устанавливалась через Docker, то оптимальный способ конфигурирования - через файл *.env*. Пример:

```
RESTORE_EMAIL_FRONTEND_URL=http://localhost:8082/
RESTORE_EMAIL_ENABLED=true
RESTORE_EMAIL_SERVER_HOST=smtp.gmail.com
RESTORE_EMAIL_SERVER_PORT=465
RESTORE_EMAIL_SSL_ENABLE=true
RESTORE_EMAIL_STARTTLS_ENABLE=false
RESTORE_EMAIL_USERNAME=<почта>
RESTORE_EMAIL_PASSWORD=<сгенерированный пароль>
```

5. Если система устанавливалась вручную из дистрибутива, то измените параметры в файле *<UNIVERSE_CONF_DIR>/backend.properties*. Пример:

```
# Email notifications
org.unidata.mdm.core.email.enabled=true
org.unidata.mdm.core.email.templates_folder=file://${universe.conf}/temp
lates
org.unidata.mdm.core.email.server_host=smtp.gmail.com
org.unidata.mdm.core.email.server_port=465
org.unidata.mdm.core.email.username=<почта>
org.unidata.mdm.core.email.password=<сгенерированный пароль>
org.unidata.mdm.core.email.frontend_url=http://localhost:8080/
```

- Используйте один из способов сохранения параметров *backend.properties*:
  - Сохраните изменения в backend.properties и перезагрузите контейнер, не перезапуская сборку.
  - Или подложите через docker-compose уже настроенный *backend.properties* в запускающийся контейнер.

Шаблоны писем расположены в каталоге

<TOMCAT_HOME>/conf/universe/templates. Используется процессор шаблонов Apache Velocity.

Примечания:

Пункт "Пароли приложений" может быть недоступен, если:

- Двухэтапная аутентификация не настроена для вашего аккаунта;
- Двухэтапная аутентификация настроена только для электронных ключей;
- Вы вошли в рабочий, учебный или другой корпоративный аккаунт;
- В аккаунте включена "Дополнительная защита".

12.4. Настройки онлайн-документации

12.4.1. Общая информация

Интеграция с онлайн-справкой доступна в любом продукте по умолчанию, и ведет на общедоступный хостинг *https://doc.ru.universe-data.ru/*. В каждом разделе продуктов доступна контекстная ссылка, которая ведет на инструкции по работе с соответствующим разделом.

Чтобы перейти на сайт документации:

1. Перейдите в требуемый раздел. Например, в раздел "Дубликаты".
2. Наведите курсор на правый край экрана - на красную полоску (Рисунок 1).
3. Дождитесь, пока полоска не сменит вид на кнопку (Рисунок 2).
4. Нажмите кнопку *Справка*.

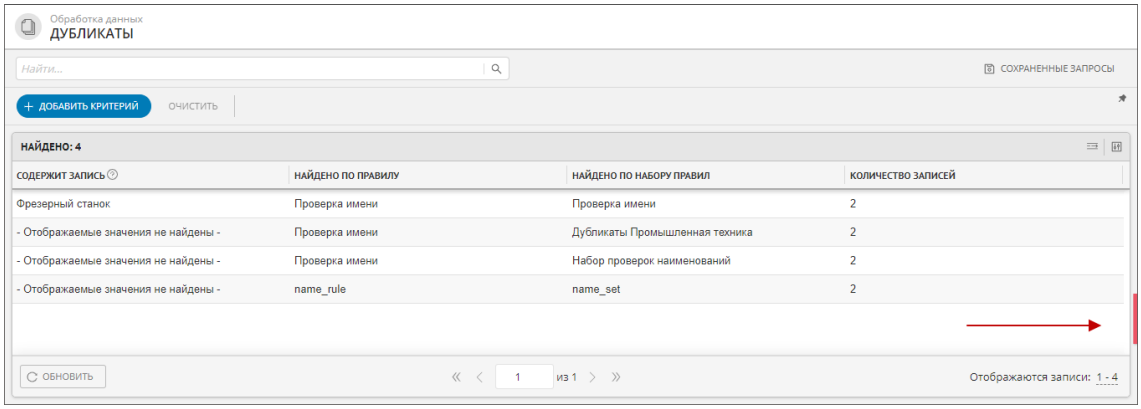


Рисунок 1 – Область для появления кнопки

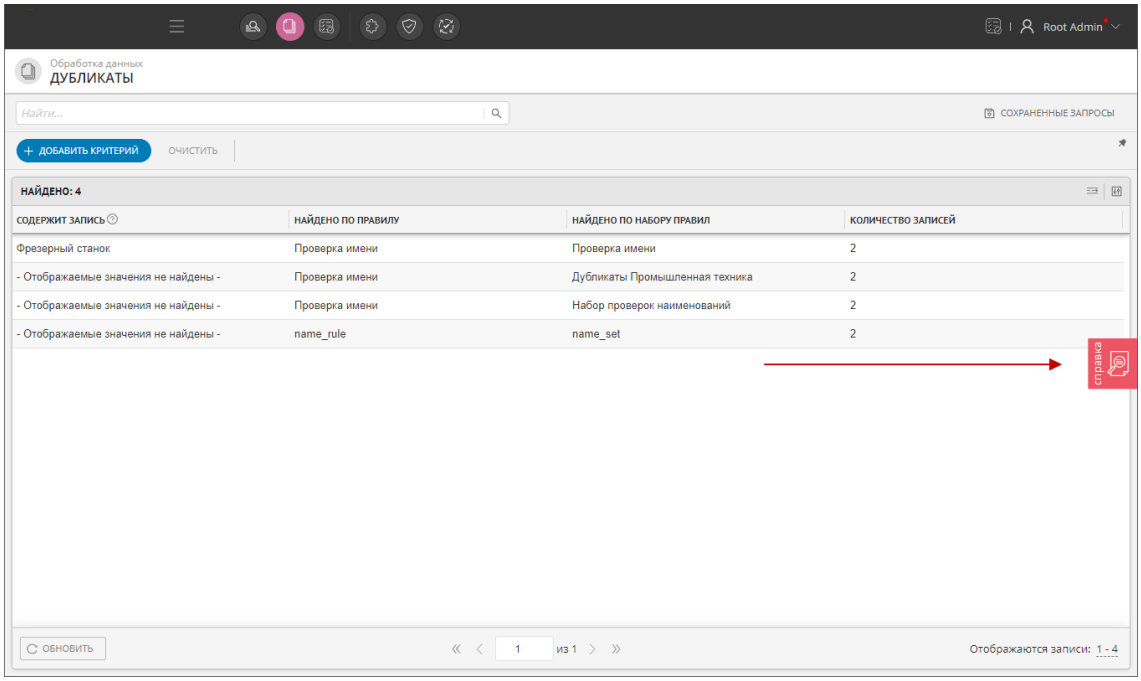


Рисунок 2 – Кнопка перехода в справку

12.4.2. Установка онлайн-справки на собственном сервере

12.4.2.1. Установка на Nginx

Установка Nginx на базе CentOS 7:

1. Добавьте EPEL-репозиторий:

```
# sudo yum install epel-release
```

2. Установите Nginx:

```
# sudo yum install nginx
```

3. Разрешите HTTP и HTTPS-трафик на брандмауэре:

```
# sudo firewall-cmd --permanent --add-service=http
# sudo firewall-cmd --permanent --add-service=https
```

4. Перезагрузите брандмауэр:

```
# sudo firewall-cmd --reload
```

5. Запустите Nginx:

```
# sudo systemctl start nginx
```

6. Настройте автозапуск Nginx при перезагрузке системы:

```
# sudo systemctl enable nginx
```

7. Проверьте статус службы Nginx (он должен быть - active):

```
# sudo systemctl status nginx
```

Настройка Nginx под локальную справку:

1. Настройте конфигурацию Nginx в файле */etc/nginx/nginx.conf*. В блоке server замените часть кода на:

```
server {
listen 80;
server_name localhost;

location / {
root /usr/share/nginx/html/;
index index.html index.htm;
error_page 404 /page404.html;
}
}
```

2. Перезапустите Nginx:

```
# sudo systemctl reload nginx
```

3. Проверьте статус службы Nginx (должен быть - active):

```
#sudo systemctl status nginx
```

4. Полностью очистите каталог */usr/share/nginx/html*.
5. Скопируйте содержимое из каталога *mdm* в каталог */usr/share/nginx/html*.
6. Структура каталогов и файлов должна иметь следующий вид:

```
#ls /usr/share/nginx/html
6.11.0-EE index.html page404.html
```

   - где 6.11.0-EE - версия справки для системы,
   - index.html - страница стартовая (ссылка на url=/6.11.0-EE/index.html),
   - page404.html - страница ошибки 404 (ссылка на url=/6.11.0-EE/content/404.html).

7. Для проверки работоспособности справки зайдите на *localhost:80*.

12.4.2.2. Установка с помощью Docker

Подготовка сервера:

- Установите Docker через официальный репозиторий. Документацию см. по ссылке *https://docs.docker.com/*.

- Установите Docker Compose (версия выше 1.29).

Установка:

1. Для разворачивания справки на локальном сервере клиенту поставляются архивы:
   - Архив с конфигурацией *docs-configs.zip*. Также архив можно скачать ниже.
   - Архив с каталогом справки. Каталог имеет имя, отражающее номер релиза и редакцию. Например, 6.11.0-EE.
2. Создайте в любом удобном месте каталог, где будет храниться справка. Например, *opt/docs/*.
3. Скопируйте содержимое архива *docs-configs.zip* в созданный каталог.
4. Переименуйте каталог *site/[name]* в каталог *site/mdm*.
5. Скопируйте содержимое архива с каталогом справки в каталог *site/mdm*.
6. В *docker-compose.yml* укажите путь к каталогу *site/mdm*. При необходимости, измените порты. Если разворачивается несколько сайтов со справкой, то их порты не должны повторяться.
7. В *site/mdm/index.html* и *site/mdm/page404.html* укажите номер и редакцию релиза чтобы значения соответствовали имени каталога справки. Если устанавливается 6.11.0-EE, то это же название должно быть в файлах.
8. Запустите контейнер. При первом запуске загрузятся все необходимые образы. Команда:

```
docker-compose up -d
```

9. Проверьте статус контейнера. Команда:

```
docker-compose ps
```

10. Сайт со справкой будет доступен по адресу *http://localhost:8090/*.

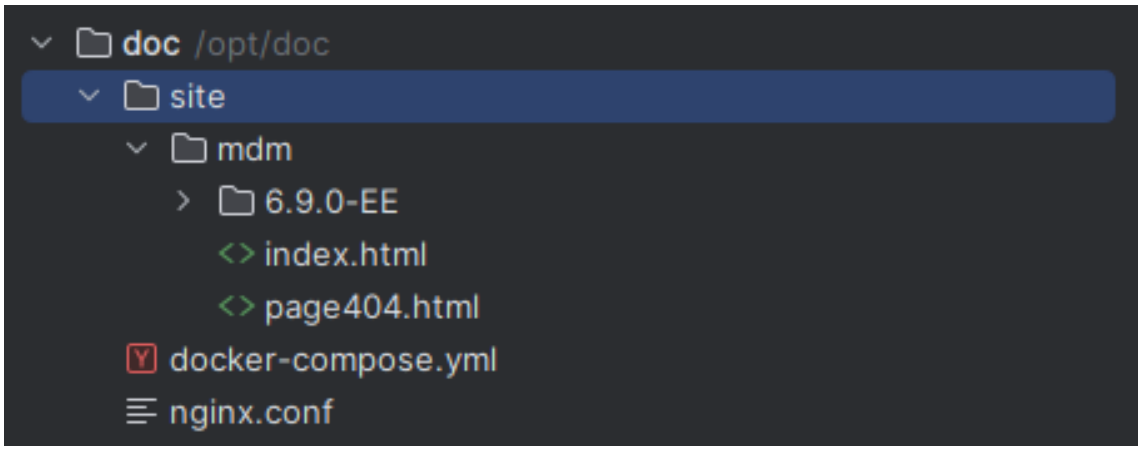


Рисунок 3 – Структура каталогов

Рисунок 4 – Статус контейнера

12.4.2.3. Содержимое основных файлов конфигурации

Скачать архив с конфигурацией `docs-configs.zip`

docker-compose.yml

```
version: '3'

services:
nginx:
   image: nginx:alpine
   container_name: nginx-doc-mdm
   restart: unless-stopped
   ports:
   - "8090:80"

   volumes:
      - /opt/doc/site/mdm:/usr/share/nginx/html
      - /opt/doc/nginx.conf:/etc/nginx/conf.d/default.conf
```

nginx.conf

```
server {
   listen       80;
   server_name  localhost;

   location / {
      root   /usr/share/nginx/html/;
      index  index.html index.htm;
      error_page 404 /page404.html;
   }
}
```

index.html

```
<!DOCTYPE html>
<meta http-equiv="Refresh" content="0; url=/6.11.0-EE/index.html" />
```

page404.html

```
<!DOCTYPE html>
<meta http-equiv="Refresh" content="0; url=/6.11.0-EE/content/404.html" />
```

12.4.3. Смена адреса хоста для интеграции с продуктом

Адрес хоста настраивается в файле *customer.json*.

Для смены хоста укажите в параметре WIKI_HOST адрес, по которому доступна

онлайн-справка. Если в ссылке указывается порт, то его тоже необходимо добавить.

Пример:

```
"WIKI_HOST": "https://yourhost/",
```

В результате будут формироваться ссылки вида *https://yourhost/6.11.0-EE/index.html*.

12.4.4. Включение / отключение интеграции

Интеграция управляется файлом *customer.json*.

Для включения интеграции укажите смены хоста, укажите значение параметра WIKI_ENABLED = true, для отключения = false.

Пример:

```
"WIKI_ENABLED": true,
```

12.5. Шифрование паролей и параметров

Эта статья описывает включение и настройку шифрования стартовых параметров системы, runtime-параметров и настроек подключений краулеров (LDAP).

Шифрование реализуется вспомогательной утилитой *crypt-utils.jar* (входит в дистрибутив системы). Когда система установлена, утилита сразу готова к работе.

Данные, обрабатываемые утилитой, хранятся в системе в зашифрованном виде. В запросах на изменение UI параметров значения передаются на BE в открытом виде.

Настройка состоит из этапов:

- Создание keystore.
- Задание параметров *backend.properties*.

Указанные этапы позволяют шифровать конфигурационные параметры системы и параметры подключения краулеров. Для шифрования остальных данных требуется дополнительная настройка.

При шифровании на кластерных версиях генерацию ключа `application_ks.p12` для кластерной сборки необходимо выполнить один раз, и затем подложить этот ключ на все ноды системы. Если генерировать ключи на всех нодах, то данный ключ будет уникален на всех нодах, вследствие чего появится ошибка

шифрования пароля на всех нодах.

12.5.1. Создание keystore

Создайте keystore с секретным ключом, имеющим название application_secret:

1. Используйте команду утилиты шифрования для создания пароля keystore:

```
java -jar crypt-utils.jar kpwd 'ключ-строка'
'ключ-строка' - строка, на основе который вычисляется пароль для keystore
```

Пример

```
java -jar crypt-utils.jar kpwd 70ac88aa-b90e-11ee-96b7-55a02820ba60
Результат: Yi4MTYMjYTjBwYBi_wiY
```

2. При помощи утилиты *keytool* создайте *keystore* с паролем, полученным из утилиты:

```
keytool -genseckey -alias 'название ключа' -keyalg 'алгоритм' -keysize 'размер
ключа' -keystore 'путь до keystore' -storepass 'пароль' -storetype 'тип keystore'
```

Пример

```
keytool -genseckey -alias application_secret -keyalg AES -keysize 256 -keystore
/application_ks.p12 -storepass Yi4MTYMjYTjBwYBi_wiY -storetype PKCS12
```

12.5.2. Задание параметров backend.properties

1. Если система устанавливалась вручную из дистрибутива, то измените параметры в файле *<UNIVERSE_CONF_DIR>/backend.properties*.

Пример

```
# Шифрование включено/выключено (true/false)
org.unidata.mdm.system.encryption.enabled=true

# Ключ инсталяции. Любая строка, на основе которой вычисляется пароль для
keystore
org.unidata.mdm.system.installation.id=70ac88aa-b90e-11ee-96b7-55a02820ba60

# Путь до keystore
org.unidata.mdm.system.encryption.keystore.path=/application_ks.p12

# Название алгоритма шифрования. Если не задано, то значение AES.
Поддерживаются все алгоритмы Java,алгоритм должен совпадать с алгоритмом,
указанным при создании keystore
org.unidata.mdm.system.encryption.algorithm=
```

2. Если система устанавливалась через Docker, то оптимальный способ конфигурирования - через файл *docker-compose.yaml*.

Пример

```
  environment:
    #Включение в системе механизма шифрования
    ENCRYPTION_ENABLED: true

    #Ключ-строка для вычисления пароля к keystore
    INSTALLATION_ID: 70ac88aa-b90e-11ee-96b7-55a02820ba60

    #Название алгоритма шифрования. Стандартное значение, если переменная не
указана, AES
    ENCRYPTION_ALGORITHM: AES

    #Путь до файла keystoreв контейнере
    ENCRYPTION_KEYSTORE_PATH: /opt/ks/application_ks.p12
```

12.5.3. Шифрование стартовых параметров

Если система только установлена и PostgreSQL, Opensearch, Orientdb еще не запускались, то зашифровать данные подключения этих сервисов стандартными способами невозможно. Для этого необходимо использовать утилиту шифрования.

```
java -jar crypt-utils.jar encпуть к keystore' ключ-строка' 'пароль'
'[алгоритм]'
'[алгоритм]' - опциональный параметр с названием алгоритма шифрования.
Стандартное значение AES
'ключ-строка' - строка, которая использовалась для генерации пароля к keystore
```

Пример

```
java -jar crypt-utils.jar enc /application_ks.p12
70ac88aa-b90e-11ee-96b7-55a02820ba60 postgres
Результат: @ENC(qR14awFmuwgyTNvmG+km5w==)
```

Зашифрованные значения необходимо указать в файле *backend.properties*, *setenv.sh* или *.env*:

setenv.sh

```
export POSTGRES_ADDRESS="localhost:5432"
export DATABASE_NAME="mdm"
export POSTGRES_USERNAME="postgres"
export POSTGRES_PASSWORD="@ENC(qR14awFmuwgyTNvmG+km5w==)"
```

backend.properties

```
com.unidata.mdm.ee.guest.role=guest
com.unidata.mdm.ee.guest.username=guest
com.unidata.mdm.ee.guest.password=@ENC(qR14awFmuwgyTNvmG+km5w==)
```

.env

```
DG_POSTGRES_USER=postgres
DG_POSTGRES_PASSWORD=@ENC(qR14awFmuwgyTNvmG+km5w==)
DG_POSTGRES_DB_NAME=postgres
POSTGRES_OUTER_PORT=15432
```

12.5.3.1. Работа с Docker версией

При работе с версией Docker необходимо генерировать ключи внутри контейнера, т.к. при появлении различий в java локальной ВМ и контейнере возникнет ошибка при пробросе ключей в контейнере.

Шаги настройки:

1. Заведите в docker-compose новый volumes:

```
ks-data:
driver: local
```

2. Пропишите volume к директории в контейнере для хранения keystore volumes:

```
${BACKEND_INTEGRATION:-./universe-integration}:/usr/local/tomcat/univers
e-integration
ks-data:/opt/keys/
```

3. Запустите контейнер.
4. Выполните на хосте команду создания keystore:

```
/opt/keys/application_ks.p12
docker exec -it unidata-mdm-deploy-mdm-1 keytool -genseckey -alias
application_secret -keyalg AES -keysize 256 -keystore
/opt/keys/application_ks.p12 -storepass Yi4MTYMjYTjBwYBi_wiY -storetype
pkcs12
```

5. Выполните на хосте команду шифрования пароля:

```
docker exec -it unidata-mdm-deploy-mdm-1 java -jar
/usr/local/tomcat/webapps/universe-backend/WEB-INF/lib/org.universe.mdm.
crypt-6.11.0-mdm-2-SNAPSHOT.jar enc /opt/keys/application_ks.p12
70ac88aa-b90e-11ee-96b7-55a02820ba60 postgres AES
```

6. Перезапустите контейнер.

12.5.4. Шифрование runtime-параметров

Примечание:
Ниже представлены дополнительные шаги настройки для разработчиков

Дополнительная настройка позволит шифровать строковые параметры, которые помечены как secret.

Пример регистрации шифруемого параметра:

```
ConfigurationProperty<String> EMAIL_PASSWORD = ConfigurationProperty.string()
            .key(CoreConfigurationConstants.PROPERTY_EMAIL_PASSWORD)
            .groupKey(CoreConfigurationConstants.PROPERTY_EMAIL_GROUP)
            .groupId(PROPERTY_EMAIL_GROUP_ID)
            .moduleId(CoreModule.MODULE_ID)
            .required(false)
            .readOnly(true)
            .secret(true)
            .build();
```

Шифрование параметров краулеров:

Для шифрования параметра краулера необходимо объявить его тип как SECRET.

```
CrawlerParameterDescriptor.string()
            .name(PROPERTY_PASSWORD)
            .required(true)
            .type(CrawlerParameterType.SECRET)
            .displayName(() -> TextUtils.getText(CoreModule.MODULE_ID +
".crawler.base.jdbc.param.password"))
            .build()
```

12.6. Производительность системы

12.6.1. Подход к производительности

Продукты Юниверс не имеют специальной оптимизации производительности под ту или иную серверную конфигурацию. Также не выделено отдельных параметров системы, напрямую влияющих на производительность.

По умолчанию для любой конфигурации продукты Юниверс запускаются и работают. Меры по оптимизации производительности рекомендуется предпринимать только если проявляются явные проблемы. При борьбе с проблемами необходимо использовать индивидуальный подход, учитывая особенности конкретного сервера, состава данных, ожидаемых показателей и т.д.

12.6.2. Параметры производительности

Параметры Java Virtual Machine (или Libercat Virtual Machine), которые используются, и которые влияют на производительность:

- `-XX:+UseStringDeduplication` — одинаковые строки не плодят в памяти новых объектов. Категория "Экономия памяти".

- `-XX:+AlwaysPreTouch` – не отдавать операционной системе однажды использованные страницы памяти, держа их в резерве. Категория "быстродействие".
- `-XX:MaxGCPauseMillis=150` - целевое время паузы коллектора. Стандартное время 200 миллисекунд. Если необходимо проходить тесты производительности и стремиться к 99 перцентилю, то значение нужно понижать (уменьшится задержка). Для повышения реальной пропускной способности нужно выделять больше памяти (-Xmx) и увеличенное время. Категория "быстродействие".
- `-XX:+HeapDumpOnOutOfMemoryError -Xlog:gc*:file=/var/log/apache-tomcat-9.0.65/unidata-gc.log` – лог для поверхностного наблюдения за деятельностью коллектора и инструктируем машину создавать heap dump при проблемах Out Of Memory.
- `-Xms == -Xmx` - выделение памяти. Если оба параметра одинаковы, это может улучшить производительность за счет того, что производится меньше действий с выделением памяти (индивидуально в каждом случае). Настраивается опытным путем.

В разных модулях системы:

- `*.shards.number` – количество первичных шард поисковых индексов. Опытным путем подбирается баланс под кластер.
- `*.replicas.number` – количество реплик шард поисковых индексов. Чем выше число, тем медленнее вставка, но при этом выше и устойчивость кластера.

В модулях операций:

- `*.threads` (например, `org.unidata.mdm.job.reindex.data.reindex.threads`) – количество потоков на узле, доступное для операции. Зависит от количества процессоров сервера.
- `*.commit.interval` (например, `org.unidata.mdm.job.reindex.data.commit.interval`) – количество айтемов для обработки операцией за один проход по курсору одним потоком. Для реиндекс операции "чем выше тем быстрее", но нужен баланс, чтобы не получить ошибку Out Of Memory.