Система управления виртуальными рабочими местами «РЕД ВРМ»

Руководство администратора

Оглавление

1 Введение

1.1 Назначение и состав системы

1.1.1. Система управления виртуальными рабочими местами «РЕД ВРМ» (далее – РЕД ВРМ) является программным продуктом, разработанным компанией «РЕД СОФТ».

РЕД ВРМ обеспечивает централизованное управление инфраструктурой виртуальных рабочих мест (далее – ВРМ).

> **Важно!** Текущая версия предназначена для ознакомительных целей и не предназначена для коммерческого использования, поэтому для нее обновление на будущие версии с сохранением настроек не гарантируется. ■

1.1.2. В настоящем документе описана процедура настройки РЕД ВРМ для администраторов, которые будут непосредственно использовать данную систему. Процесс установки описан в Руководстве по установке.

1.1.3. Развернутая система РЕД ВРМ предоставляет:

- страницу администратора для настройки подключений и создания пулов ВРМ на платформе виртуализации РЕД Виртуализация с использованием механизма связанных клонов;
- страницу пользователя с витриной ресурсов для доступа и подключения к опубликованным ВРМ.

1.1.4. Для аутентификации и закрепления ВРМ за пользователем используется либо встроенная база данных, либо существующая служба каталогов.

1.1.5. РЕД ВРМ имеет модульную структуру и включает в себя следующие компоненты:

- Брокер – основной компонент, отвечающий за централизованное управление и доступ к системе РЕД ВРМ;

– Агент – серверное ПО для управления и организации доступа к BPM;
– Клиент – клиентское ПО для доступа и подключения к BPM;
– База данных – используется для хранения настроек системы РЕД BPM, автоматически устанавливается при развертывании Брокера.

Дополнительно для своей работы РЕД BPM может использовать LDAP-аутентификаторы для интеграции со службами каталога РЕД АДМ и Active Directory, а также поставщиков для подключения к кластерам РЕД Виртуализация при использовании динамических пулов и управления их жизненным циклом.

1.2 Вход в систему

1.2.1. Для входа в систему в адресной строке браузера введите IP-адрес брокера. Откроется окно авторизации (рисунок 1).

1.2.2. Введите логин, пароль и аутентификатор. При первом входе введите логин администратора и пароль, заданные при установке брокера (по умолчанию – `login` и `password`), аутентификатор – `DataBase`.

Нажмите кнопку «Войти», и при правильности введенных данных откроется веб-интерфейс.

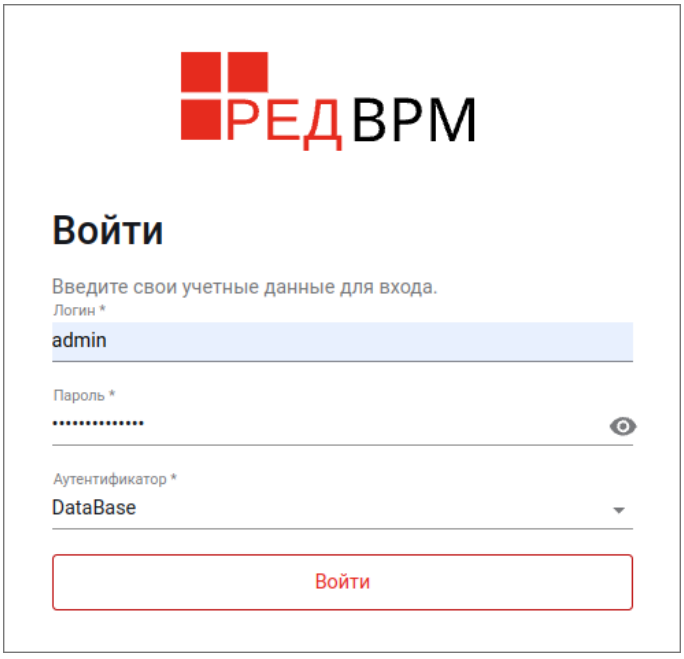

Рисунок 1 – Авторизация

1.3 Страница администратора и страница пользователя

1.3.1. При входе в систему, в зависимости от роли авторизующегося пользователя системы («Администратор» или «Пользователь») откроется либо страница администратора (рисунок 2), либо витрина ресурсов (страница пользователя).

1.3.2. Страница администратора позволяет администрировать BPM и сопутствующую инфраструктуру.

В главном меню панели администратора, расположенном слева, отображены следующие разделы (вкладки) и кнопки:

- Учётные записи:
  - Аутентификаторы,
  - Группы,
  - Пользователи;
- Ресурсы:
  - Агенты,
  - Поставщики,
  - Пулы;
- Рабочие места;
- Настройки:
  - Разрешения,
  - Группы доступа;
- Страница пользователя;
- смена темы;
- информация о программе.

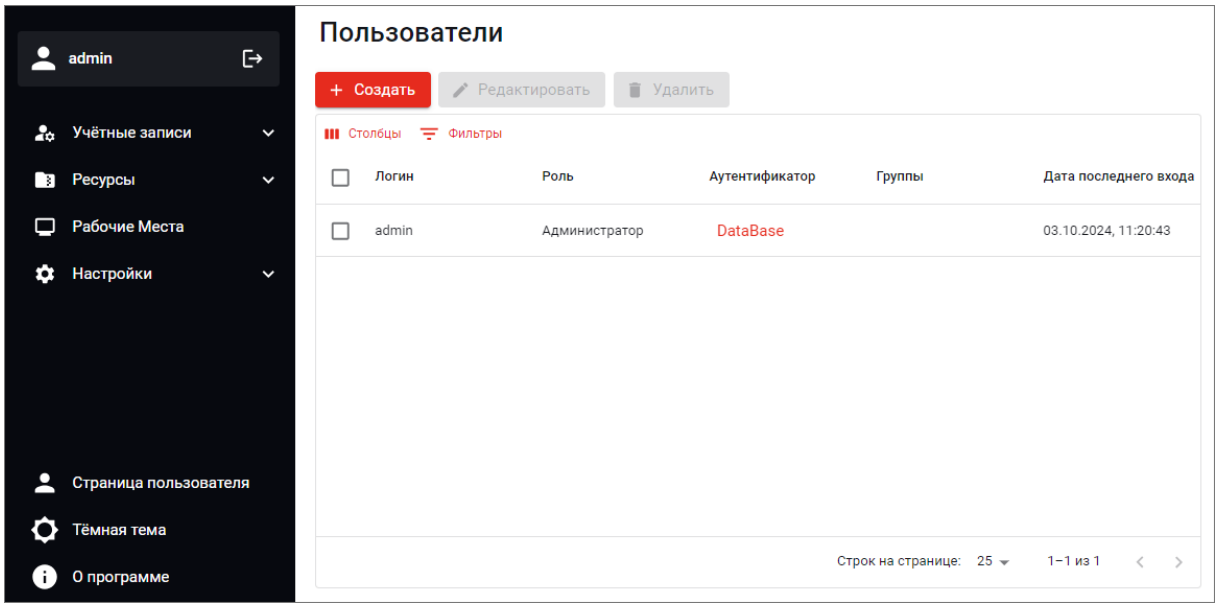

Рисунок 2 – Страница администратора

Примечание. Текущая версия использует soft-delete модель для создаваемых объектов, поэтому в случае невозможности повторного добавления объектов убедитесь в том, что они действительно удалены.

Для этого на странице администратора выберите соответствующий раздел, далее нажмите «Фильтры» и для столбца «Удален» установите значение «Все».

1.3.3. При желании, можно выбрать тему – тёмную или светлую. Для этого нужно нажать соответствующую кнопку, расположенную в левом нижнем углу (рисунок 3).

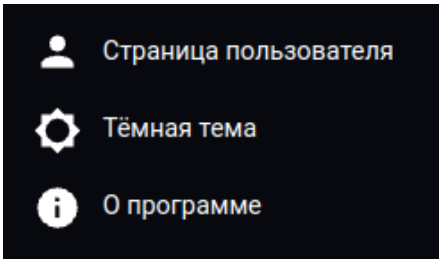

Рисунок 3 – Кнопки, расположенные в левом нижнем углу интерфейса (перечисление сверху-вниз): (а) переход на витрину ресурсов, (б) переключение темы и (в) вывод информации о программе

1.3.4. Страница пользователя даёт доступ к опубликованным BPM. На ней отображается «Витрина ресурсов», которая отображает доступные для данного пользователя BPM.

Обычный пользователь (пользователь системы, которому присвоена роль «Пользователь») при входе в систему попадает именно на витрину доступных для него ресурсов и не имеет доступа к панели администратора

Администратор (пользователь системы, которому присвоена роль «Администратор») при входе в систему попадает на страницу администратора, и может перейти на витрину доступных для него ресурсов, нажав на кнопку «Страница пользователя» в левом нижнем углу (рисунок 3). Для выхода обратно на страницу администратора нужно нажать на самую левую кнопку в правом верхнем углу (при наведении на неё выводится надпись «Страница администратора») (рисунок 4).

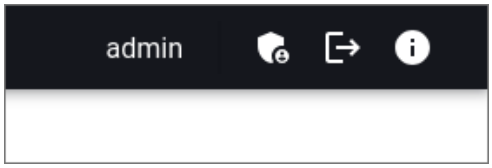

Рисунок 4 – Кнопки, расположенные в правом верхнем углу интерфейса (перечисление слева-направо): (а) переход на страницу администратора (только для пользователя, являющегося администратором системы), (б) выход из системы, (в) вывод информации о программе

2 Работа с учётными записями

Раздел «Учётные записи» включает в себя следующие подразделы (вкладки), в которых производится работа с соответствующими объектами:

– Аутентификаторы,
– Группы,
– Пользователи.

2.1 Аутентификаторы

2.1.1 Раздел «Аутентификаторы»

2.1.1.1. При переходе в раздел «Аутентификаторы» открывается список имеющихся аутентификаторов (рисунок 5).

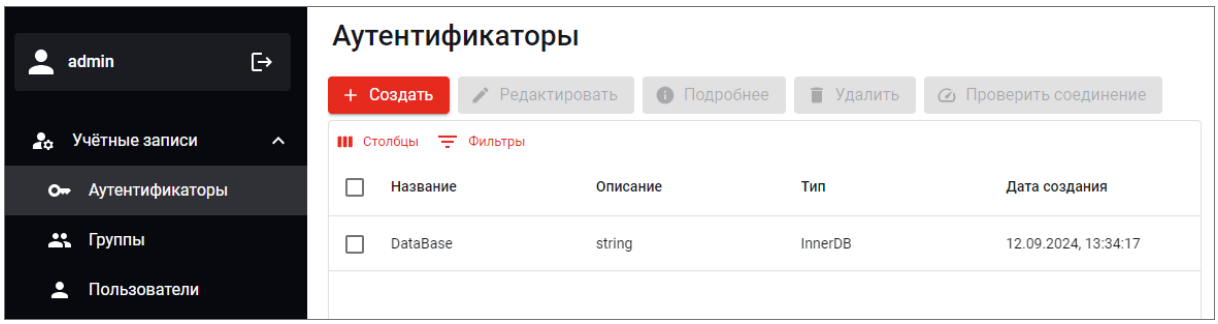

Рисунок 5 – Раздел «Аутентификаторы»

2.1.1.2. Для того, чтобы создать новый аутентификатор, нажмите кнопку «Создать».

В открывшемся окне редактирования свойств нового аутентификатора выберите тип аутентификации и затем введите параметры. Есть два возможных типа аутентификаторов: «Внутренняя БД» и «LDAP» (рисунок 6).

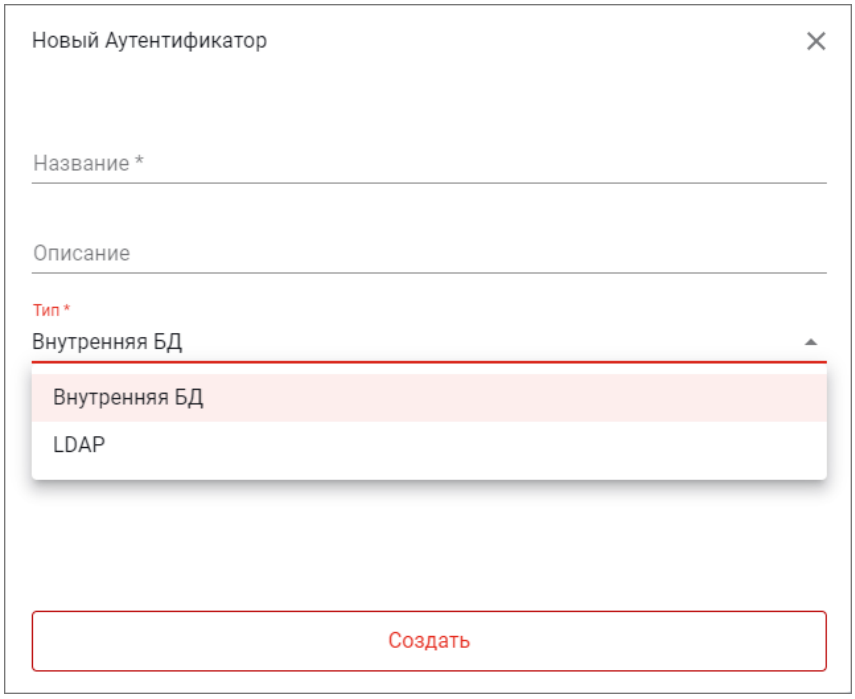

Рисунок 6 – Выбор типа создаваемого аутентификатора

2.1.2 Внутренняя база данных

2.1.2.1. Для создания аутентификатора типа «Внутренняя БД» достаточно ввести имя в поле «Название». Введя название и, при необходимости, описание, нажмите расположенную в этом же окне внизу кнопку «Создать» (рисунок 6).

2.1.2.2. Созданный аутентификатор появится в списке аутентификаторов. Выделив его нажатием, с ним можно будет выполнять следующие операции (рисунок 7) – активными станут соответствующие кнопки:

– «Редактировать» – отредактировать параметры, заданные при создании;
– «Подробнее» – просмотреть информацию о аутентификаторе;
– «Удалить» – удалить аутентификатор.

2.1.3 Аутентификатор типа LDAP

2.1.3.1. РЕД BPM поддерживает добавление аутентификаторов типа LDAP для служб каталогов на основе Microsoft Active Directory и РЕД АДМ.

При создании аутентификатора «LDAP» для подключения к службе каталогов нужно указать параметры в секции «Настройки» (рисунок 8):

– название нового аутентификатора;
– IP-адрес LDAP-сервера;
– порт LDAP-сервера (по умолчанию – 389);
– логин администратора LDAP-сервера (обязательно в формате `domain\login`) и его пароль.

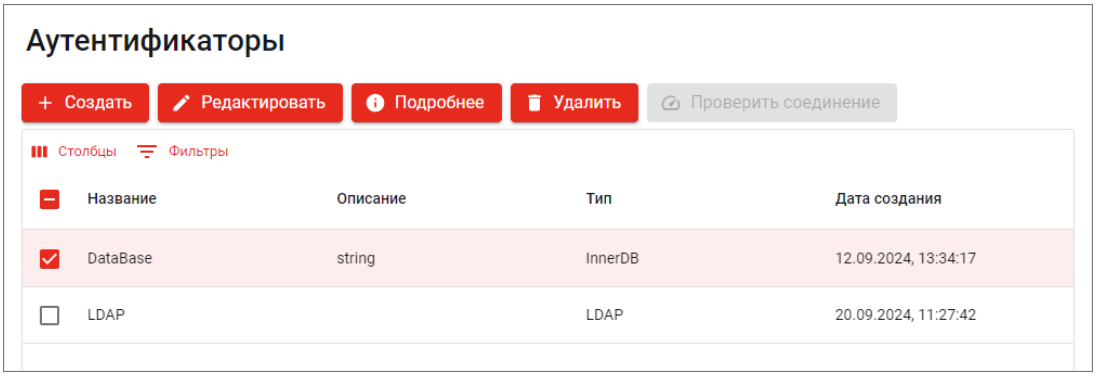

Рисунок 7 – Выбор аутентификатора типа «Внутренняя БД» для работы с ним

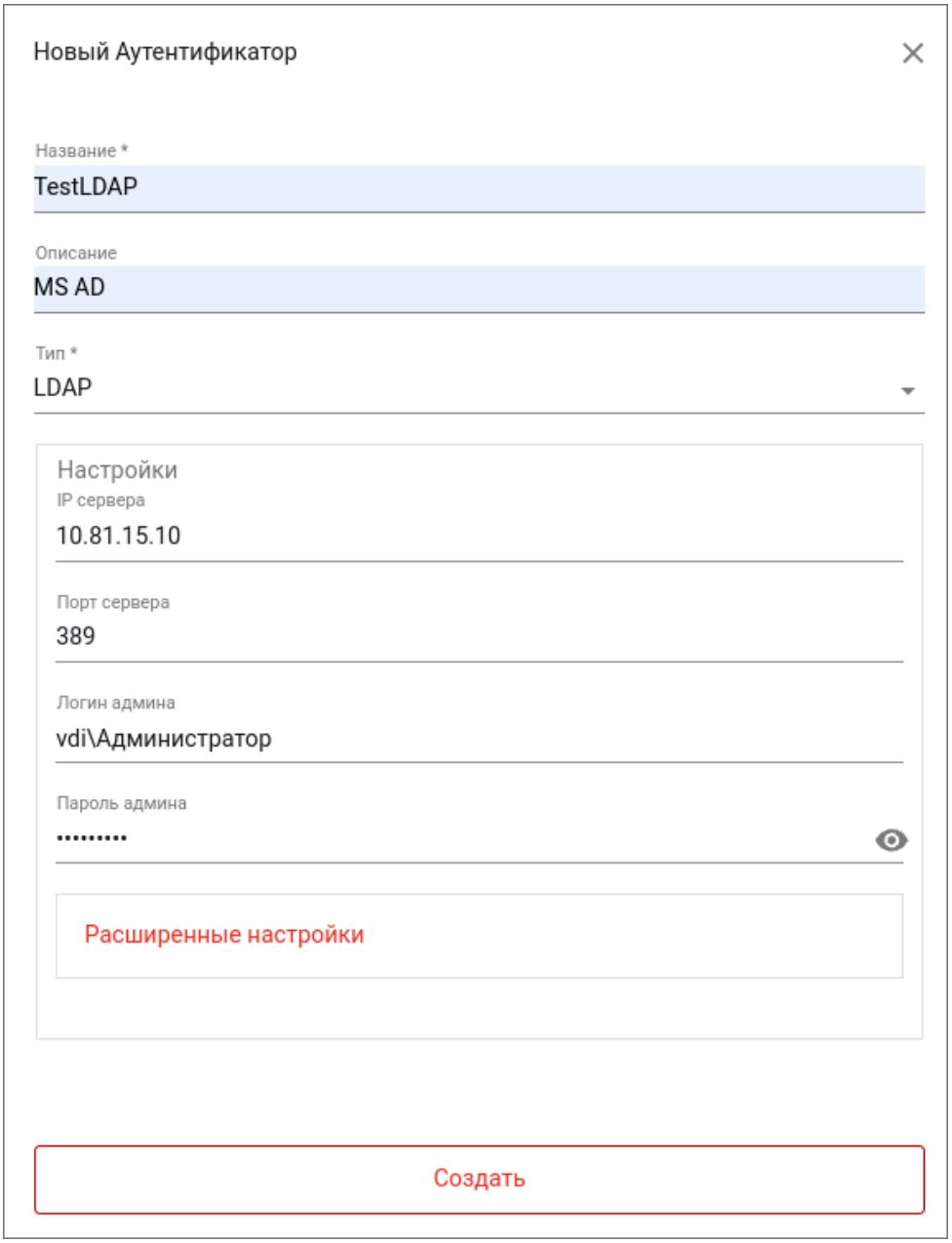

Рисунок 8 – Основные параметры создаваемого аутентификатора типа «LDAP»

Примечание. В текущей версии РЕД ВРМ для корректной работы со службой каталогов РЕД АДМ необходимо на сервере `reddc` в файле `/opt/reddc/etc/smb.conf` в разделе `[global]` указать значение параметра:

```
ldap server require strong auth = no
```

Дополнительные параметры можно задать в подсекции «Расширенные настройки» (рисунок 9), которая раскроется, если нажать на её наименование. В число этих параметров входят такие служебные параметры для работы с пользователями и группами в службах каталогов, как: *ID атрибут*, *пользовательский класс*, *атрибут пользователя*, *атрибут группы*, *альтернативный класс*. Рекомендуется использовать значения по-умолчанию, или использовать те параметры, что указаны в каталоге вашего предприятия.

Перечень дополнительных параметров:

- зона видимости – при необходимости ограничить зону видимости службы каталога определённым организационным подразделением (OU) укажите его в формате `distinguishedName` (например, `CN=Users,DC=vdi,DC=demo`);
- таймаут – время ожидания ответа от сервера LDAP (в секундах);
- пользовательский класс (по умолчанию – `person`);
- ID атрибут – атрибут именования пользователя (по умолчанию – `sAMAccountName`);
- атрибут пользователя (по умолчанию – `member`);
- атрибут группы (по умолчанию – `group`);
- альтернативный класс.

Закончив ввод значений параметров, нажмите расположенную в этом же окне в самом низу кнопку «Создать».

2.1.3.2. После создания аутентификатора он появится в списке аутентификаторов (рисунок 10).

Аналогично аутентификатору типа «Внутренняя БД», для выделенного аутентификатора можно:

- с помощью кнопки «Редактировать» – отредактировать параметры, заданные ранее при создании аутентификатора;
- с помощью кнопки «Подробнее» – перейти в окно, где можно просмотреть расширенный набор параметров аутентификатора или работать с пользователями, группами и логами;
- с помощью кнопки «Удалить» – удалить объект.

Также для выделенного аутентификатора типа «LDAP» с помощью кнопки «Проверить соединение» можно проверить соединение и корректность заданных параметров.

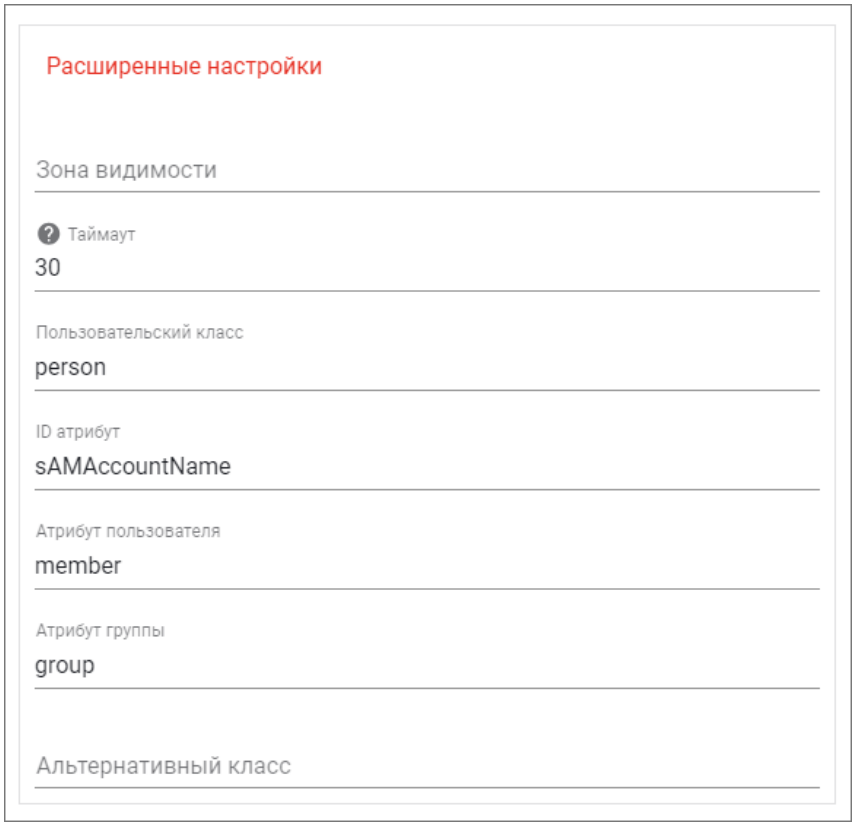

Рисунок 9 – Расширенные настройки создаваемого аутентификатора типа «LDAP»

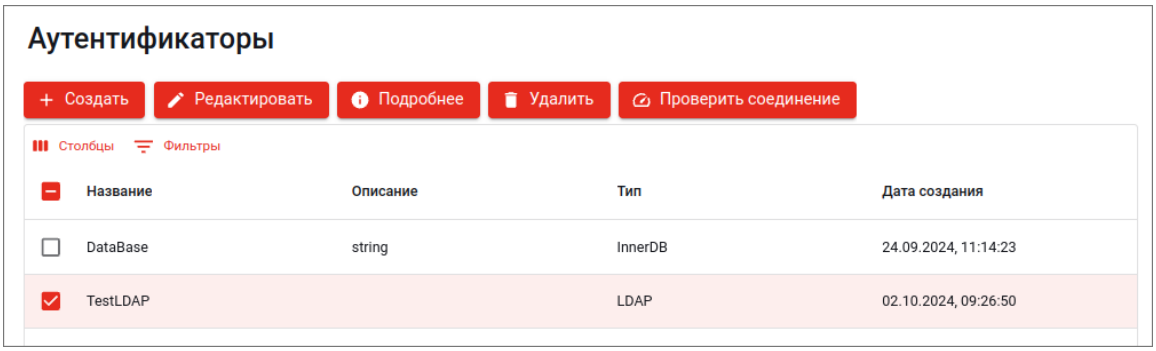

Рисунок 10 – Выбор аутентификатора типа «LDAP» для работы с ним

2.2 Группы

2.2.1. Для работы с группами предназначен подраздел «Группы», расположенный в разделе «Учётные записи» (рисунок 11).

РЕД BPM использует следующие типы групп:

– Пльзовательские группы. Расположены в разделе «Учётные записи» и могут содержать учетные записи из разных аутентификаторов. Далее под группами подразумеваются пользовательские группы, если не указано иное.

– LDAP-группы. Управляются через службу каталога и для LDAP-групп поддерживается выгрузка в соответствующую пользовательскую группу.

– Группы доступа. Включают набор разрешений и пользовательских групп для публикации BPM. При использовании нескольких групп доступа порядок их применения определяется значением поля «Приоритет». Чем ниже значение, тем выше приоритет.

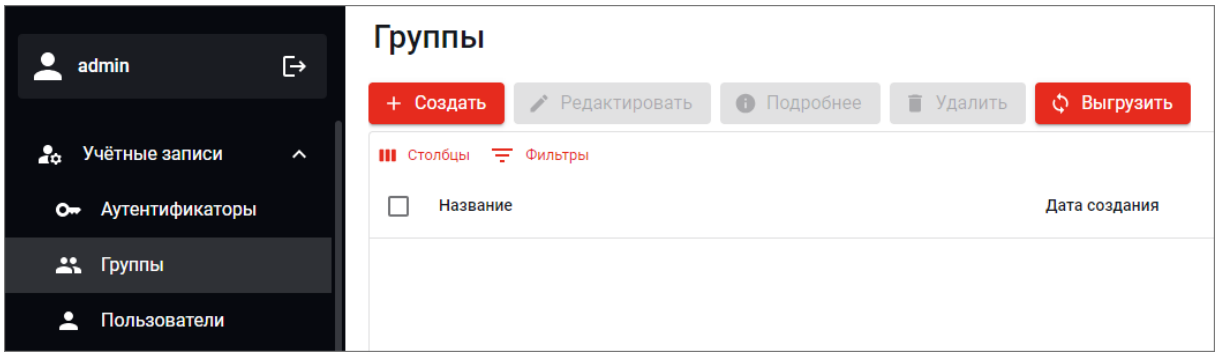

Рисунок 11 – Страница «Группы»

2.2.2. Для добавления новой группы нажмите кнопку «Создать». В открывшемся модальном окне введите имя новой группы и нажмите кнопку «Создать», расположенную в самом низу модального окна (рисунок 12).

2.2.3. Созданная группа появится в списке групп. Выделив её нажатием, с ней можно будет выполнять следующие операции (рисунок 13) – активными станут соответствующие кнопки:

– «Редактировать» – отредактировать параметры, заданные ранее при создании группы;
– «Подробнее» – просмотреть входящих в группу пользователей, удалить их из группы или добавить новых (рисунок 14); также в данную группу можно выгрузить список пользователей LDAP-группы;
– «Удалить» – удалить группу.

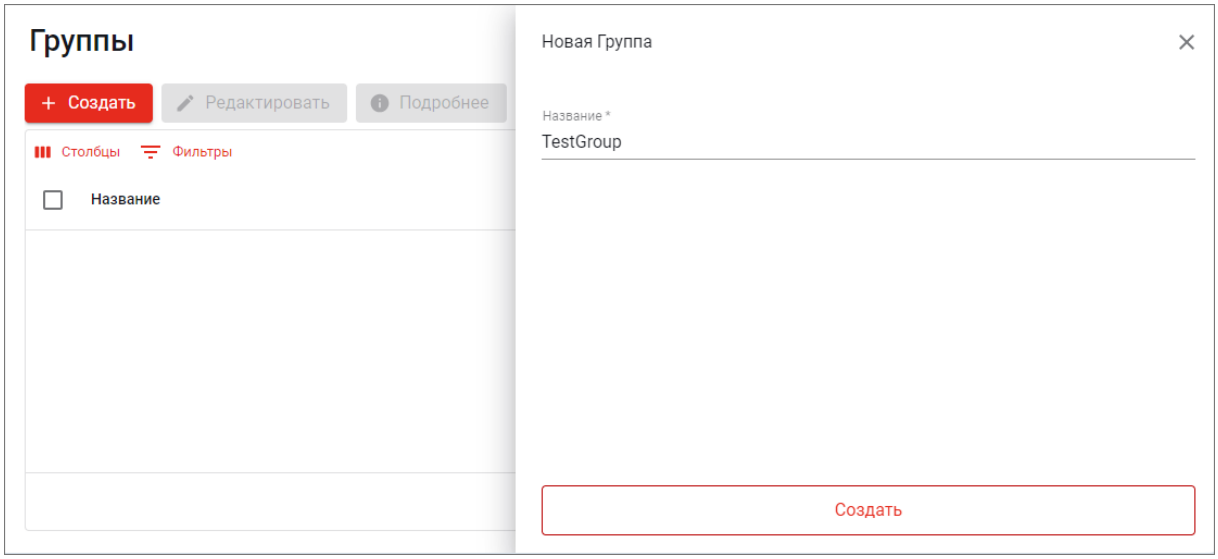

Рисунок 12 – Добавление группы

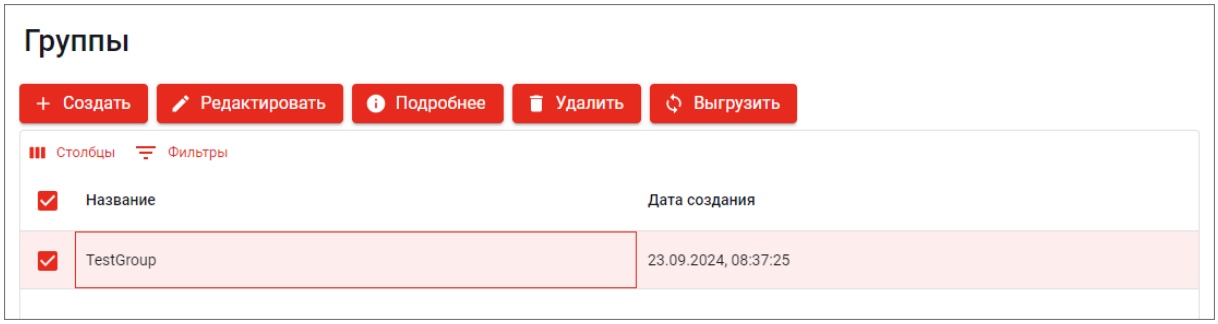

Рисунок 13 – Доступные действия с выбранной группой

Рисунок 14 – Пользователи данной группы

2.2.4. Для того чтобы выгрузить список пользователей LDAP-группы нажмите кнопку «Выгрузить» (пользовательские группы могут содержать пользователей из разных аутентификаторов).

При нажатии кнопки «Выгрузить» пользователи из указанной LDAP-группы выгрузятся в указанную пользовательскую группу.

Важно! Для успешной выгрузки LDAP-группа не должна содержать вложенных групп (т. е. может содержать только пользователей). ■

Примечание. В текущей версии не поддерживается подключение по LDAPS (TCP/636).

В открывшемся модальном окне (рисунок 15) установите значения параметров:
– выберите из имеющихся нужный аутентификатор типа LDAP;
– название группы LDAP в «кратком» формате (например, `vdi_test`);
– название группы пользователя.

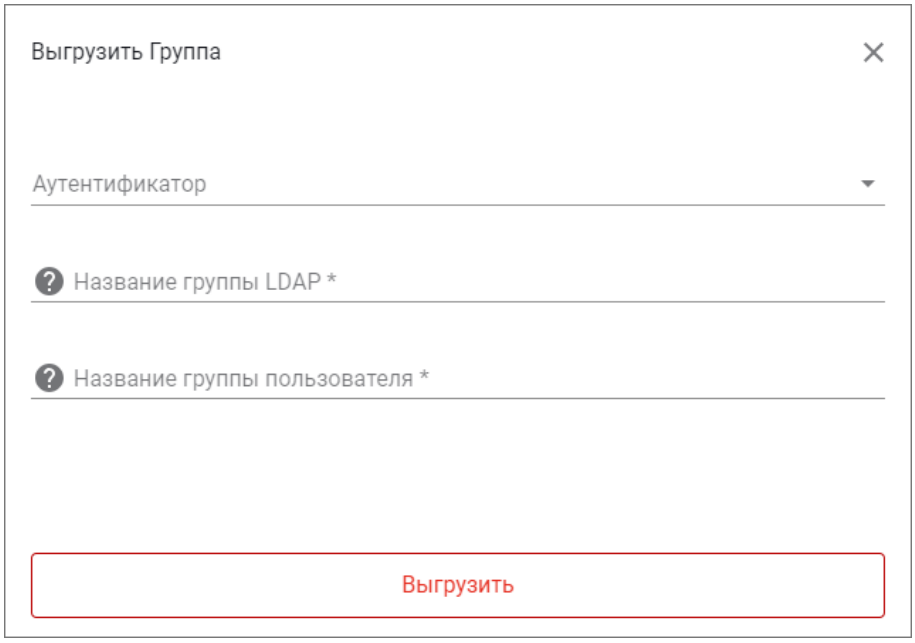

Рисунок 15 – Выгрузка группы в LDAP

Если всё сделано верно, то при нажатии кнопки «Выгрузить», пользователи из указанной группы AD выгрузятся в аутентификатор в группу с указанным именем.

При изменении LDAP-групп в службе каталогов, из которых была произведена выгрузка (например, путём добавления новых пользователей или удаления существующих) для их актуализации в разделе «Учетные записи», требуется повторная выгрузка.

2.3 Пользователи

2.3.1. Для работы с пользователями предназначен подраздел «Пользователи», расположенный в разделе «Учётные записи» (рисунок 16).

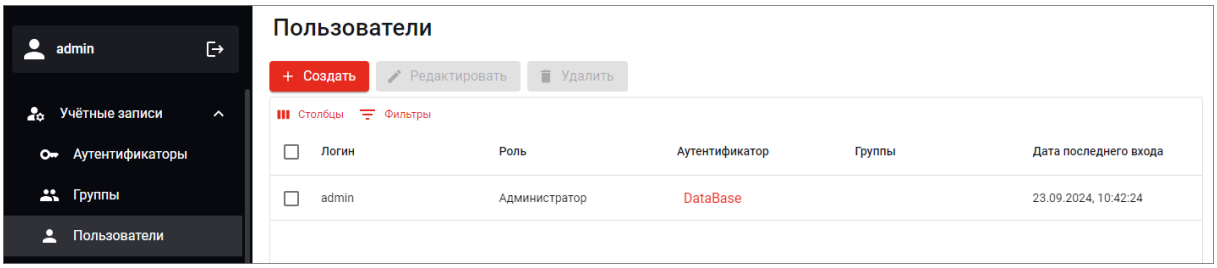

Рисунок 16 – Страница «Пользователи»

2.3.2. Для аутентификаторов типа «Внутренняя БД» учётные записи должны быть созданы в явном виде на странице администратора.

Для аутентификаторов типа LDAP учётные записи пользователей создаются автоматически после первой успешной аутентификации, а также могут быть добавлены вручную, например когда пользователю необходимо назначить роль «Администратор» либо добавить его в пользовательскую группу.

2.3.3. Для добавления пользователя нажмите кнопку «Создать» и в открывшемя модальном окне введите параметры нового пользователя (рисунок 17):

– имеющийся аутентификатор (любого типа – «Внутренняя БД» или «LDAP»);
– логин пользователя;
– пароль пользователя – для аутентификатора типа «Внутренняя БД»;
– выбрать роль – «Пользователь» (по умолчанию) или «Администратор»;
– выбрать группы (из имеющихся), в которые будет входить данный пользователь.

2.3.4. Созданный пользователь появится в списке пользователей. Если его выбрать, нажав на него, то станут активными кнопки «Редактировать» и «Удалить».

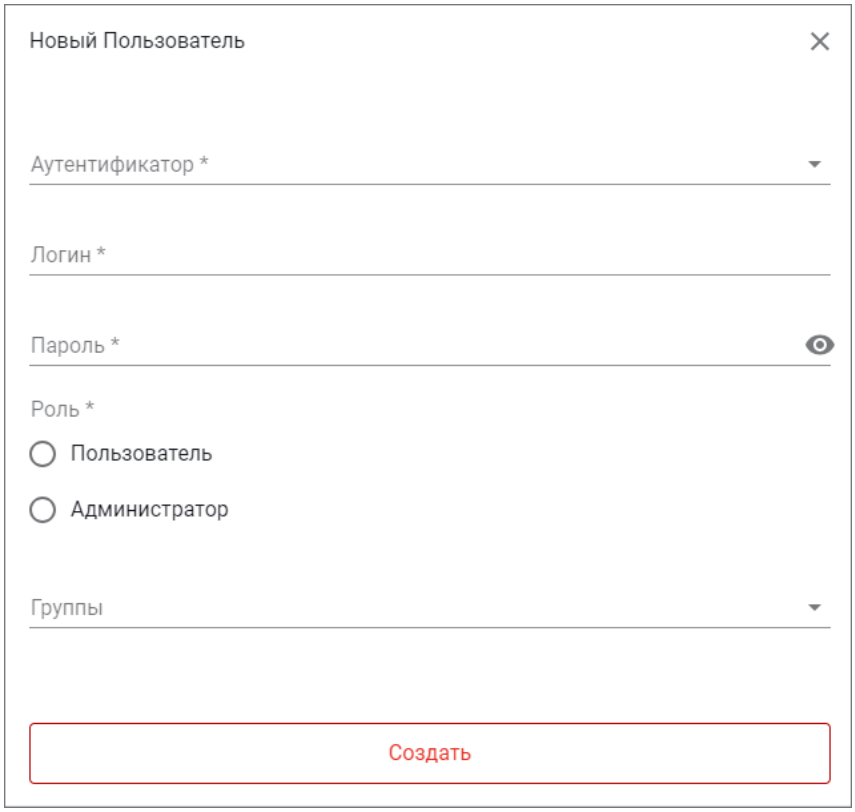

Рисунок 17 – Создание нового пользователя

Вхождение пользователя в группы можно отредактировать либо в ходе его редактирования и выбора групп в выпадающем меню, либо при переходе в подраздел «Группы» и редактирования состава нужных групп (см. подраздел 2.2).

3 Работа с ресурсами

3.1 Агенты

3.1.1. Агент служит для инициализации виртуальной машины на брокере, устанавливается на физической или виртуальной машине, к которой будет вестись подключение клиента.

Страница «Агенты» расположена в разделе «Ресурсы» (рисунок 18).

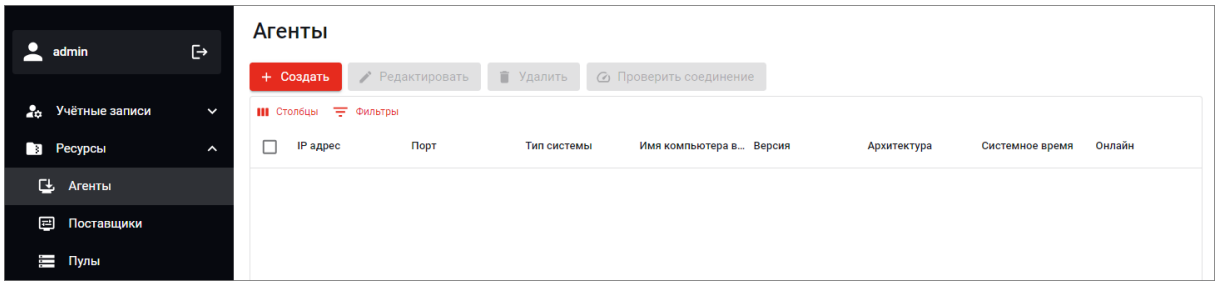

Рисунок 18 – Страница «Агенты»

3.1.2. Для создания нового агента нажмите кнопку «Создать». В открывшемся модальном окне укажите IP-адрес машины, на которой развёрнут агент, и порт (по умолчанию – 8010). Нажмите кнопку «Создать» (рисунок 19).

3.1.3. Созданный агент появится в списке. Если после добавления агента помимо IP и порта не отображается инаф информация – это значит, что валидация проведена неудачно из-за того, что машина выключена, не доступен IP-адрес или закрыт порт 8010.

Выделив его нажатием, с ним можно будет выполнять следующие операции (активными станут соответствующие кнопки) рисунок 20):

– редактирование параметров, заданных ранее при создании агента;

– удаление агента;
– проверка соединения.

Рисунок 19 – Добавление нового агента

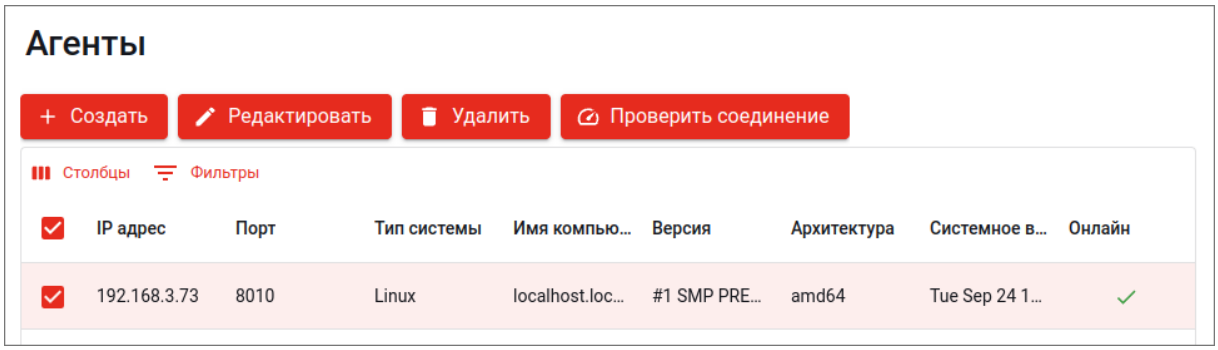

Рисунок 20 – Действия, доступные для выбранного агента

3.2 Поставщики

3.2.1. Поставщик – это внешняя система виртуализации РЕД Виртуализация, на которой будет создаваться динамический пул.

Страница «Поставщики» расположена в разделе «Ресурсы» (рисунок 21).

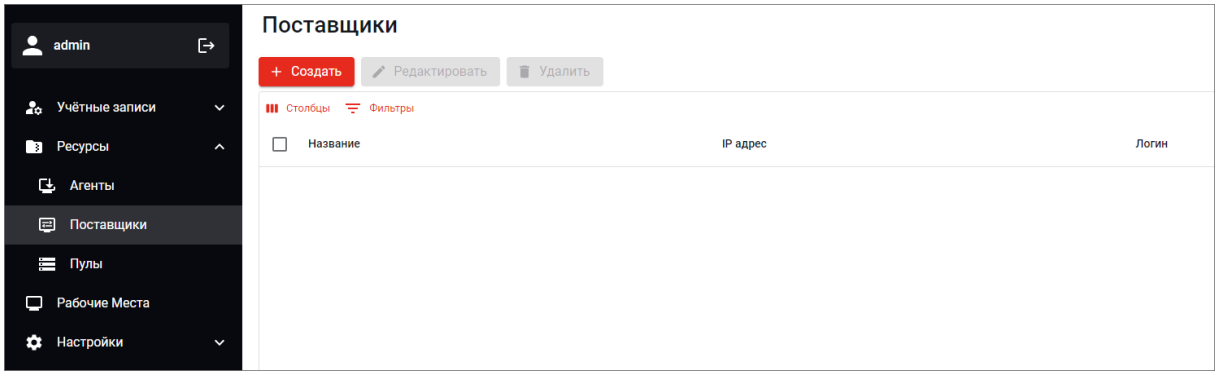

Рисунок 21 – Страница «Поставщики»

3.2.2. Для создания нового поставщика нажмите кнопку «Создать» и в открывшемся модальном окне введите параметры (рисунок 22):

– название нового поставщика;
– IP-адрес – адрес менеджера системы виртуализации РЕД Виртуализация;
– логин и пароль учётной записи от системы виртуализации;
– тайм-аут – максимальное время ожидания ответа от системы виртуализации (в секундах);
– чек-бокс «SSL» – по какому из протоколов будет идти связь (HTTP или HTTPS).

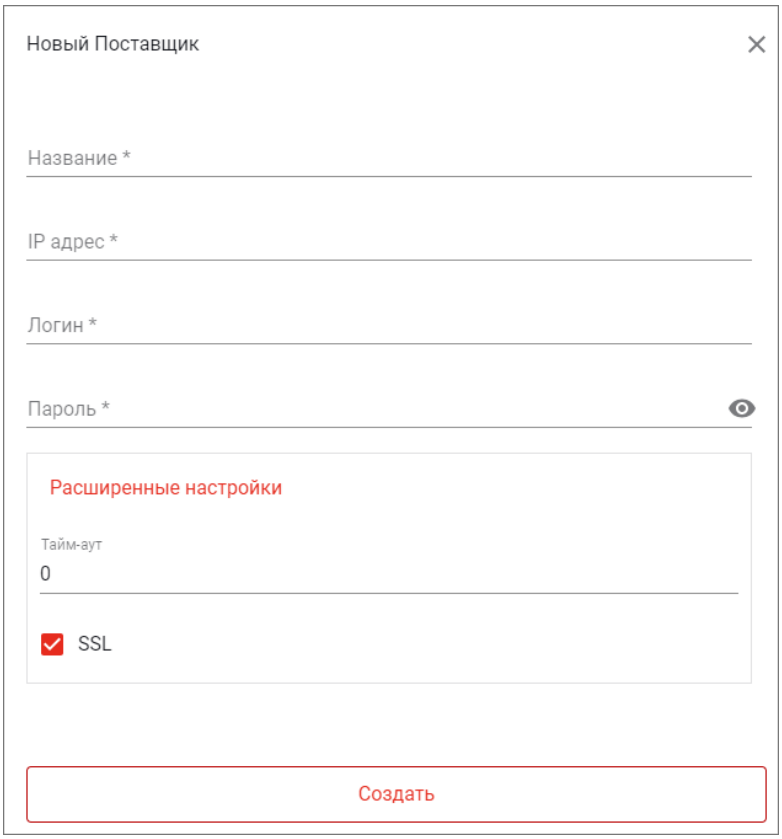

Рисунок 22 – Создание нового поставщика

По окончанию ввода параметров нажмите кнопку «Создать» в самом низу модального окна.

3.2.3. Созданный поставщик появится в списке. Выделив его нажатием, с ним можно будет выполнять операции редактирования и удаления (активными станут соответствующие кнопки) (рисунок 23).

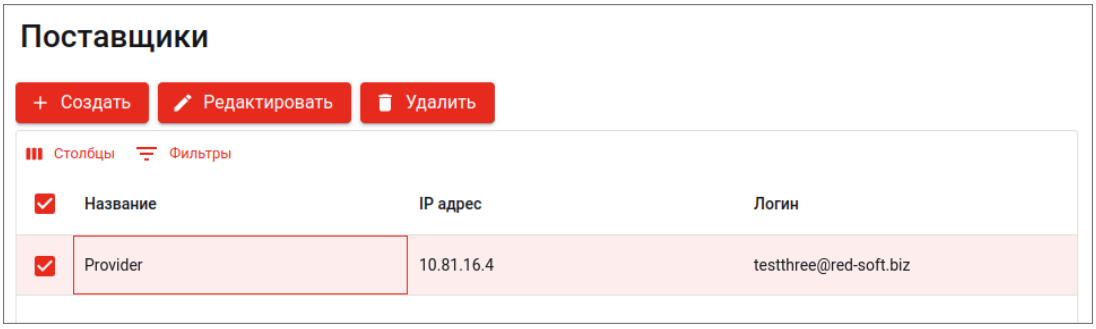

Рисунок 23 – Действия, доступные для выделенного в списке поставщика

3.3 Пулы

На странице «Пулы», расположенной в разделе «Ресурсы» (рисунок 24), можно создать два вида варианта пулов:

- статичный – включает набор установленных агентов на физических узлах либо виртуальных машинах, жизненным циклом которых РЕД ВРМ не управляет;
- динамичный – включает набор агентов, жизненным циклом которых управляет РЕД ВРМ. Агенты создаются путем клонирования шаблона базового образа с использованием механизма связанных клонов на поставщике виртуализации. Также при удалении динамического пула виртуальные машины агентов удаляются вместе с шаблоном.

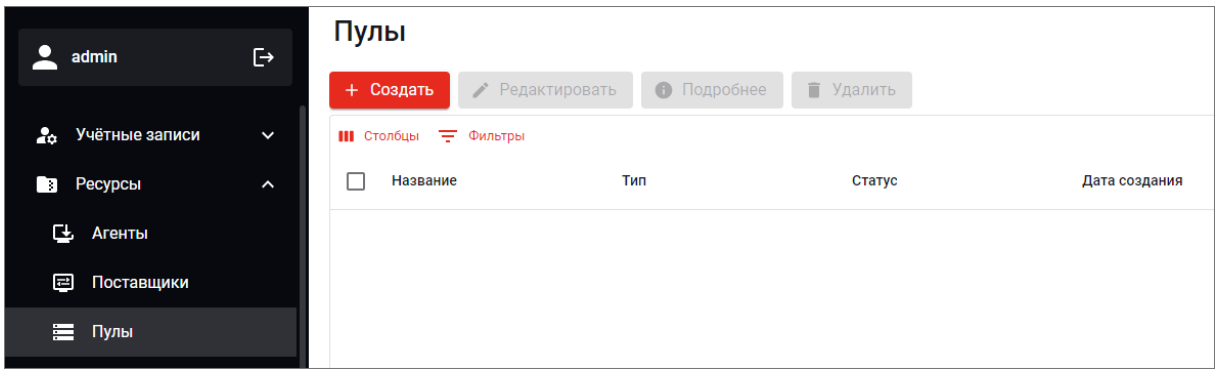

Рисунок 24 – Страница «Пулы»

3.3.1 Статичный пул

3.3.1.1. Для создания нового статичного пула нажмите кнопку «Создать» и в открывшемся модальном окне выберите статичный тип пула (рисунок 25).

3.3.1.2. Созданный пул появится в списке пулов.

Важно! После добавления агентов в статичный пул они переходят в этот пул и перестают отображаться во вкладке «Агенты». ■

Выделив его нажатием, с ним можно будет выполнять следующие операции (рисунок 26) – активными станут соответствующие кнопки:

– «Редактировать» – отредактировать параметры, заданные ранее при создании пула;
– «Подробнее» – откроются расширенные настройки пула в части работы с агентами;
– «Удалить» – удалить пул.

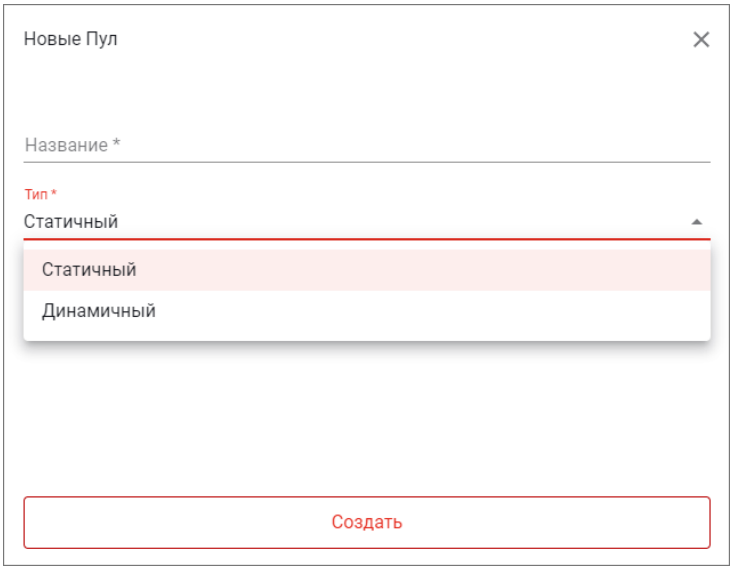

Рисунок 25 – Выбор типа пула и создание статичного пула

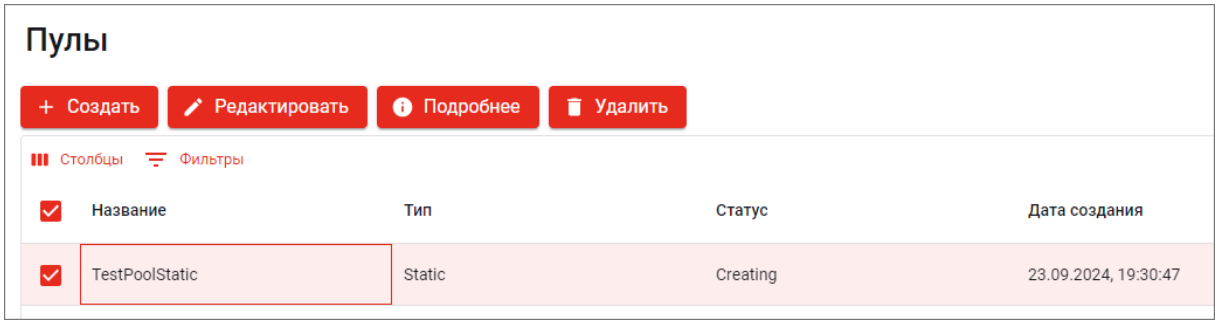

Рисунок 26 – Действия с выбранным пулом

При нажатии кнопки «Подробнее» откроется окно свойств пула, вкладка «Агенты» (рисунок 27).

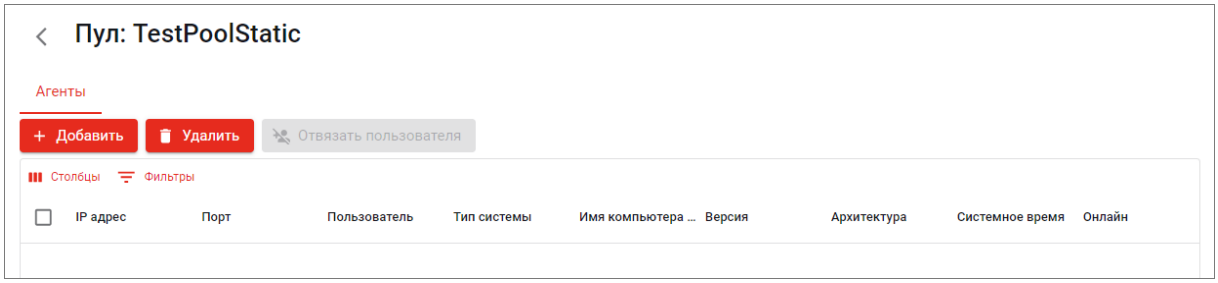

Рисунок 27 – Вкладка «Агенты»

3.3.1.3. Для добавления в пул агентов нажмите на кнопку «Добавить», в открывшемся модальном окне в выпадающем списке выберите с помощью чек-боксов нужных агентов и нажмите кнопку «Добавить» (рисунок 28).

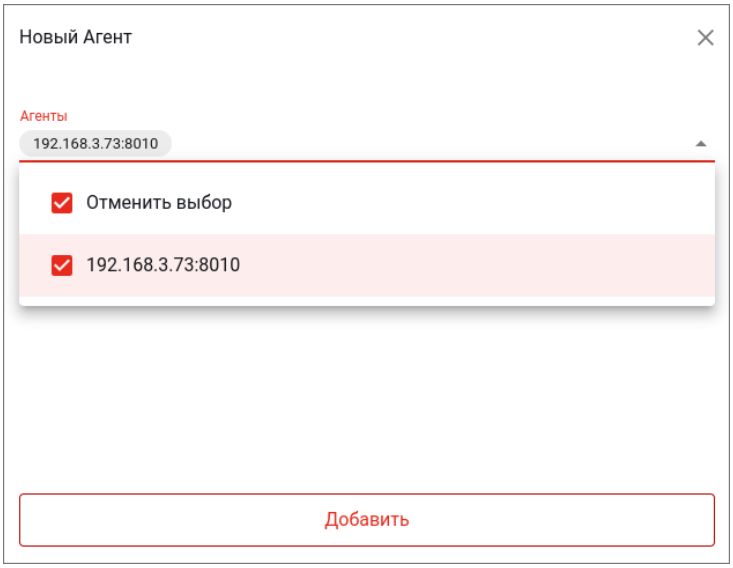

Рисунок 28 – Выбор агентов для добавления в статичный пул

Добавленный агент появится в списке. При необходимости можно его удалить, выделив в списке и нажав соответствующую кнопку.

3.3.2 Динамичный пул

3.3.2.1. Динамичный пул можно создать только при наличии поставщика. Для создания такого пула нажмите кнопку «Создать» и в открывшемся модальном окне выберите динамичный тип пула и укажите значения параметров (рисунок 29):

- название пула;
- в поле «Максимальное количество агентов» – количество виртуальных рабочих мест (машин), которые при создании пула создаются и настраиваются;
- в поле «Количество активных агентов» – количество доступных виртуальных рабочих мест. Они всегда будут настроены и готовы к назначению пользователю;
- в поле «Количество агентов в ожидании» – количество виртуальных рабочих мест в спящем режиме;
- в выпадающем меню «Поставщик» – выбрать Поставщика;

– в выпадающем меню «Дата центр» – выбрать датацентр на Поставщике;
– в выпадающем меню «Кластер» – выбрать кластер на Поставщике;
– в выпадающем меню «Хранилище» – выбрать хранилище на поставщике;
– в выпадающем меню «Образ» – указать машину в системе виртуализации, которая будет использована как шаблон для агентов в пуле. На машение должен быть установлен агент и она должна быть выключена.

Нажмите кнопку «Создать», расположенную в самом низу этого окна.

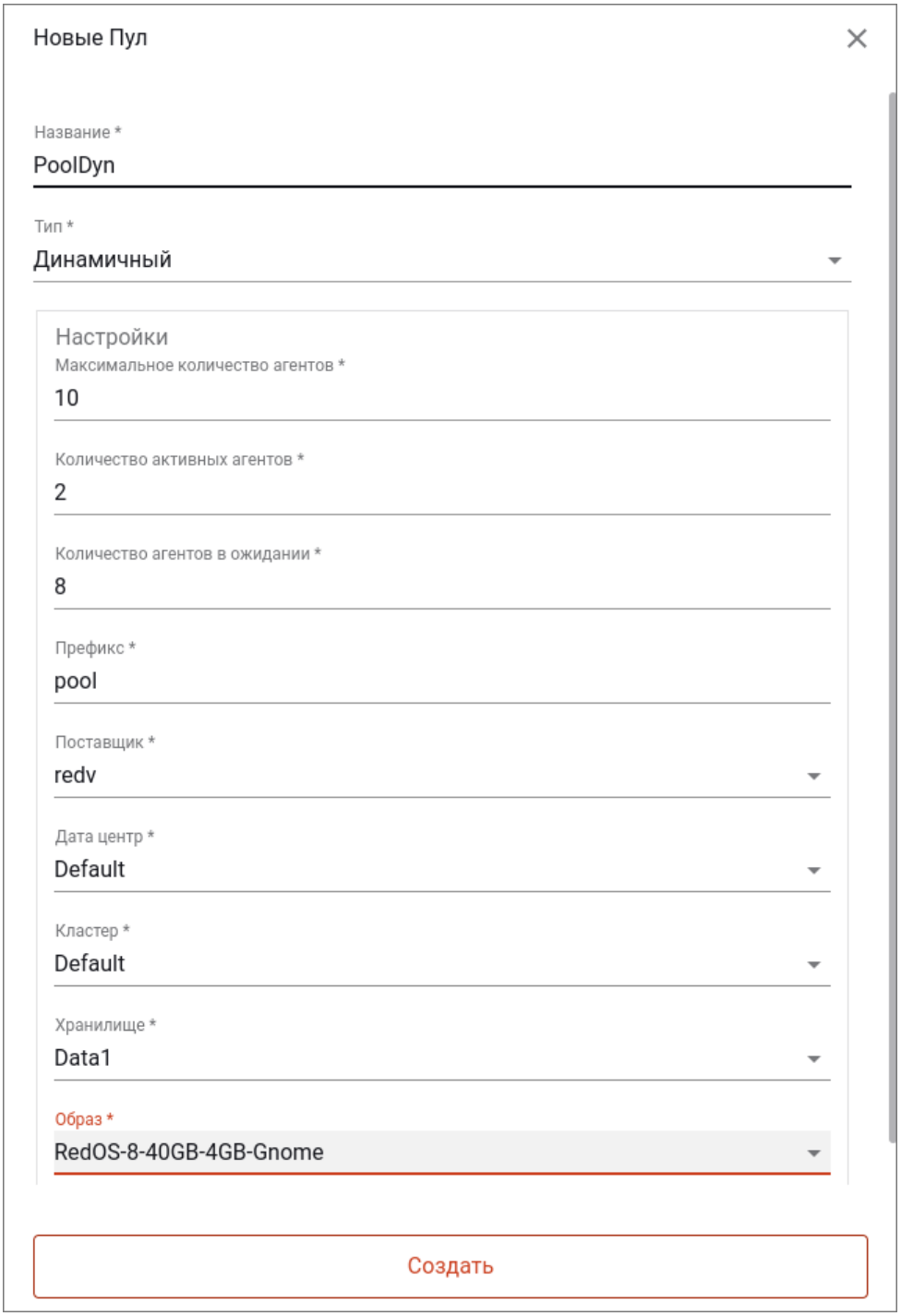

Рисунок 29 – Создание динамичного пула

3.3.2.2. После создания пула он появится в списке. Выделив его нажатием, с ним можно будет выполнять следующие операции – активными станут соответствующие кнопки (аналогично статичному пулу):

– «Редактировать» – отредактировать параметры, заданные ранее при создании пула;
– «Подробнее» – откроются расширенные настройки пула в части работы с агентами;
– «Удалить» – удалить пул.

При нажатии кнопки «Подробнее» откроется окно свойств пула, вкладка «Агенты» (рисунок 30).

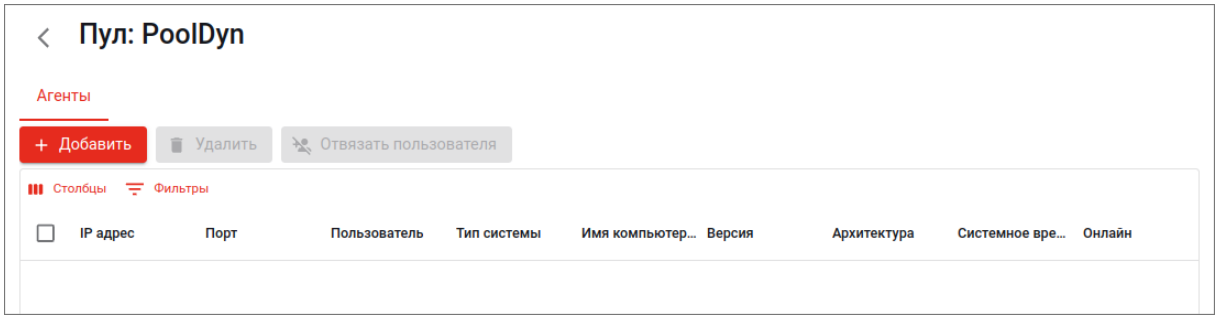

Рисунок 30 – Вкладка «Агенты»

3.3.2.3. Для указания количества агентов в пуле нажмите на кнопку «Добавить», в открывшемся модальном окне укажите необходимое максимальное количество агентов и нажмите кнопку «Добавить» (рисунок 31).

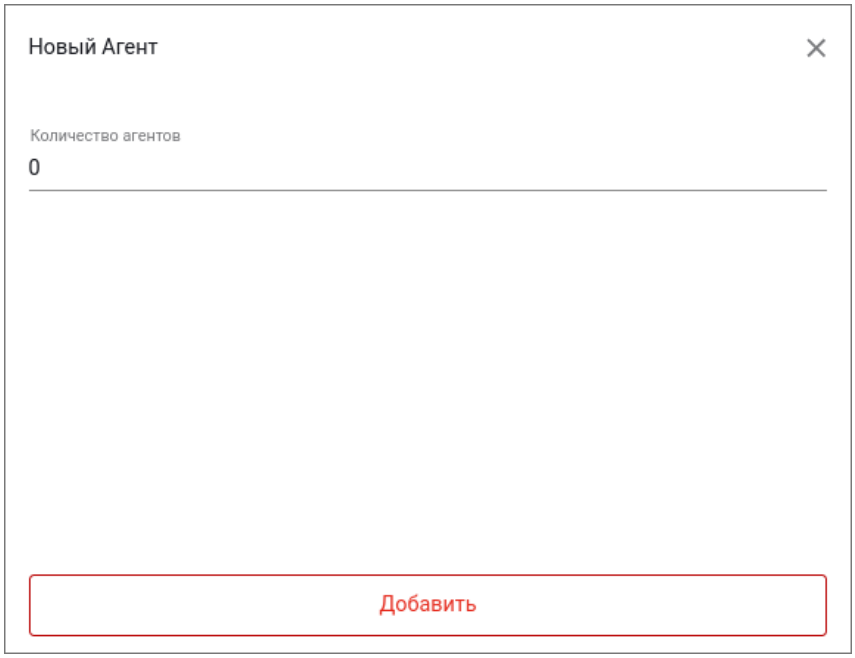

Рисунок 31 – Добавление агентов в динамичный пул

Если количество существующих агентов в пуле меньше, чем значение параметра «Максимальное количество агентов», и при этом ко всем агентам прикреплены пользователи, то при обращении к пулу нового пользователя, который имеет доступ, для него в системе виртуализации будет создан новый агент.

4 Настройки

4.1 Разрешения

4.1.1. Разрешение – это набор параметров протокола удаленного доступа при подключении к BPM. Для работы с разрешениями используется подраздел «Разрешения» раздела «Настройки» (рисунок 32).

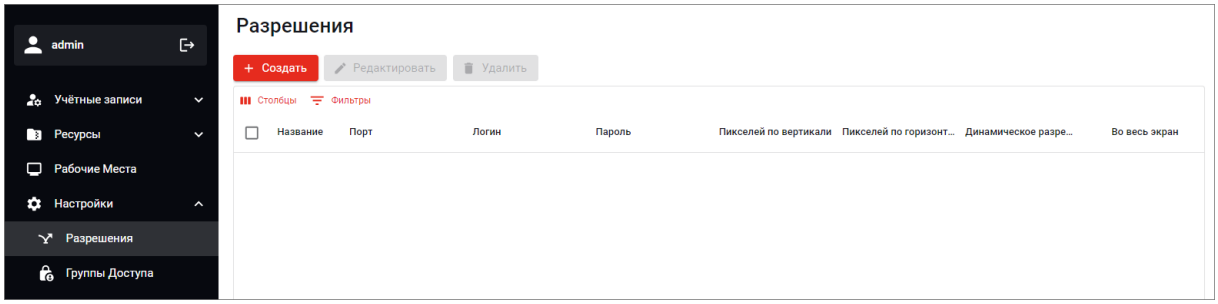

Рисунок 32 – Страница «Разрешения»

4.1.2. Для создания нового разрешения нажмите кнопку «Создать» и установите параметры (рисунок 33):

- название (обязательный параметр);
- порт подключения (по умолчанию – 3389);
- должно ли BPM отображаться в полноэкранном режиме;
- (опционально) логин и пароль учётной записи для пользовательской сессии на BPM;
- разрешение экрана по вертикали и горизонтали;
- допускается ли динамическое разрешение.

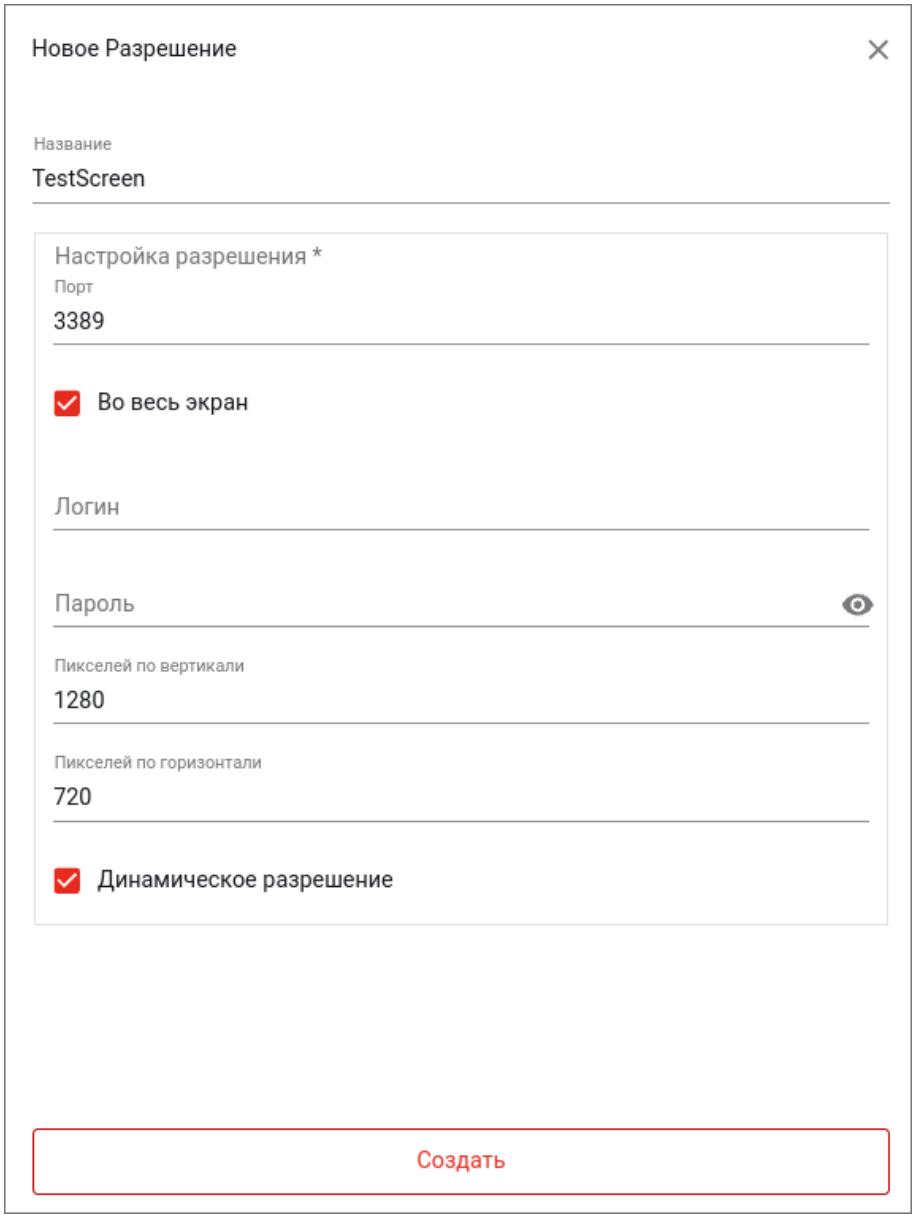

Рисунок 33 – Создание нового разрешения

4.1.3. Созданное разрешение появится в списке. Выделив его нажатием, с ним можно будет выполнять следующие операции (активными станут соответствующие кнопки) рисунок 34):

– редактирование параметров, заданных ранее при создании разрешения;
– удаление разрешения.

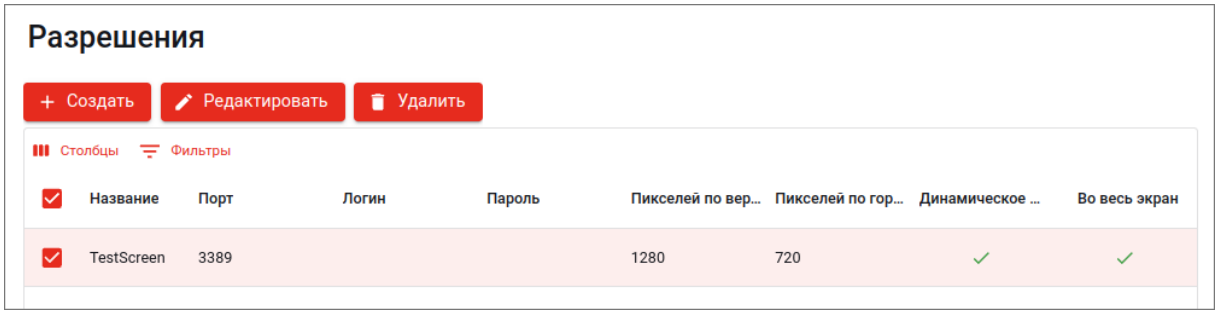

Рисунок 34 – Действия, доступные для выбранного разрешения

4.2 Группы доступа

4.2.1. Для настройки доступа к виртуальным рабочим местам используются группы доступа, расположенные в подразделе «Группы доступа» раздела «Настройки» (рисунок 35).

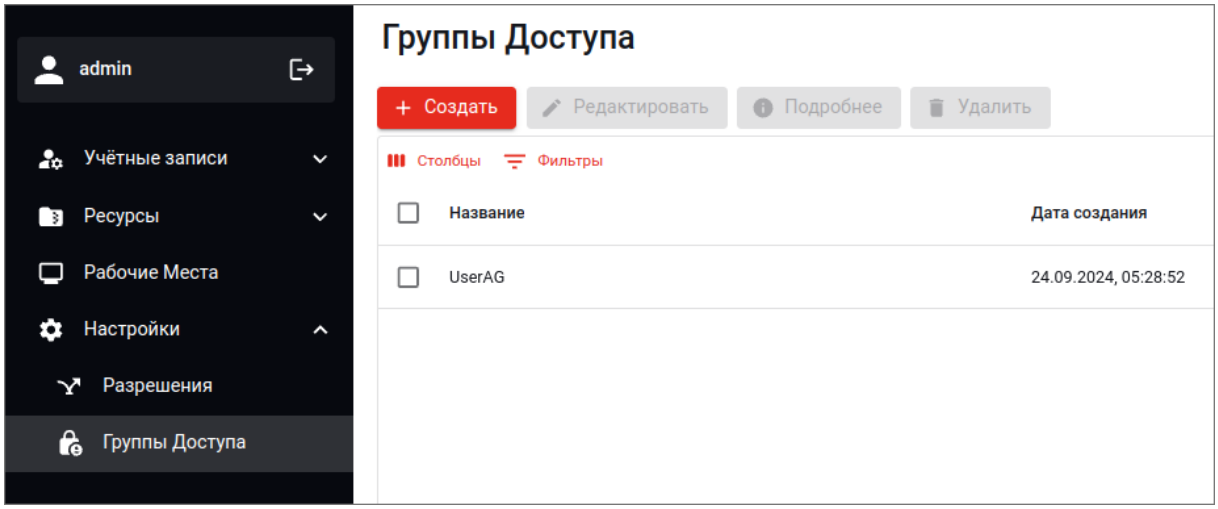

Рисунок 35 – Страница «Группы доступа»

4.2.2. Для создания новой группы доступа нажмите кнопку «Создать» и установите параметры (рисунок 36):

– название (обязательный параметр);
– в выпадающем меню «Группы» – с помощью чек-бокса выберите одну или несколько групп из имеющихся (необязательно);
– в выпадающем меню «Разрешения» – выберите имеющееся разрешение, которое будет использовано в качестве шаблона (необязательно);
– приоритет разрешений.

Если вы выберете разрешение, то появится секция с настройкой параметров разрешения, где в качестве параметров по умолчанию будут указаны параметры выбранного разрешения (рисунок 36).

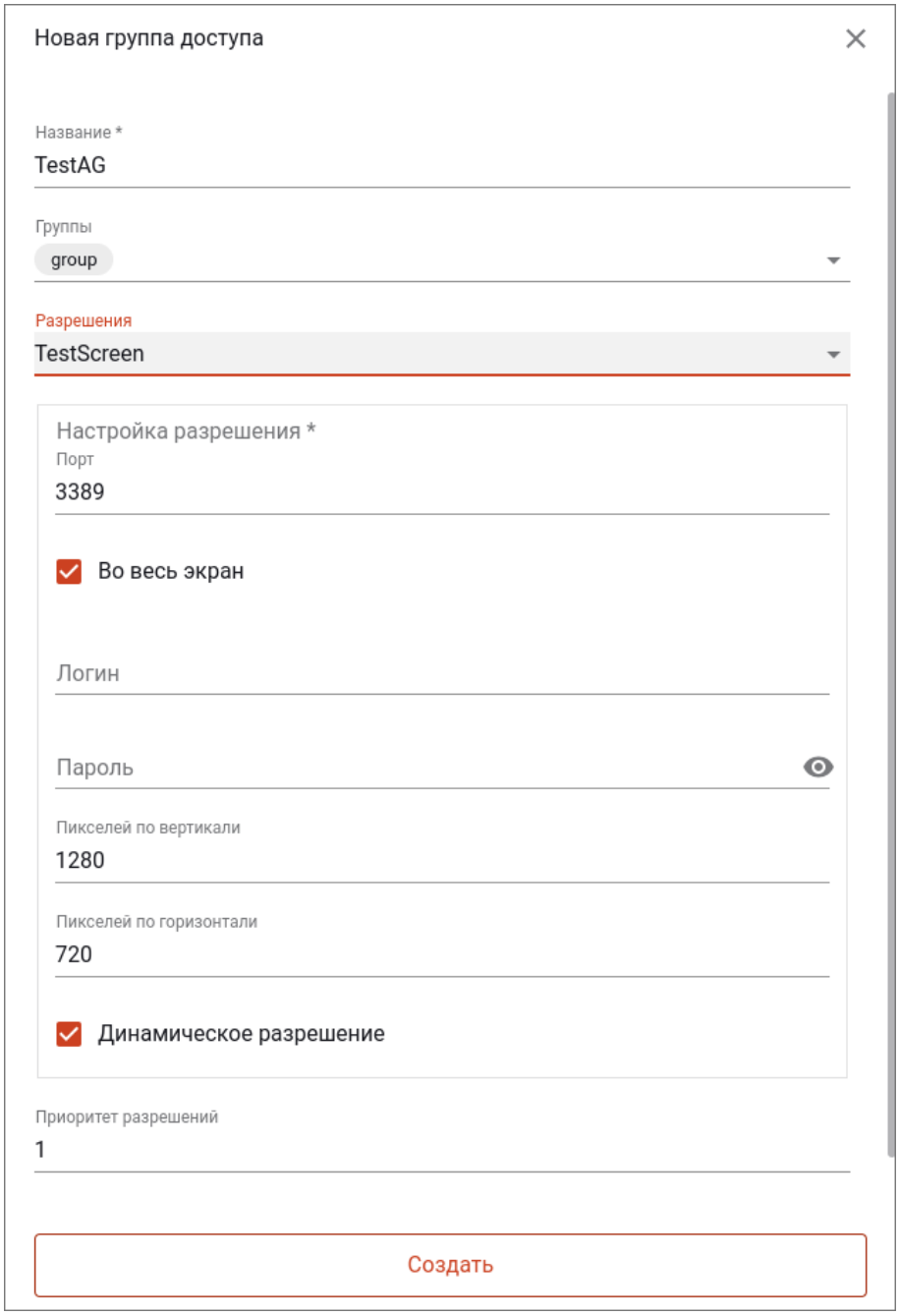

Рисунок 36 – Создание новой группы доступа

4.2.3. Созданная группа доступа появится в списке. Выделив его нажатием, с ним можно будет выполнять следующие операции (активными станут соответствующие кнопки) рисунок 37):

– «Редактировать» – редактирование параметров, заданных ранее при создании группы доступа;
– «Подробнее» – откроются расширенные настройки в части работы с пользователями в составе группы доступа;
– «Удалить» – удаление группы доступа.

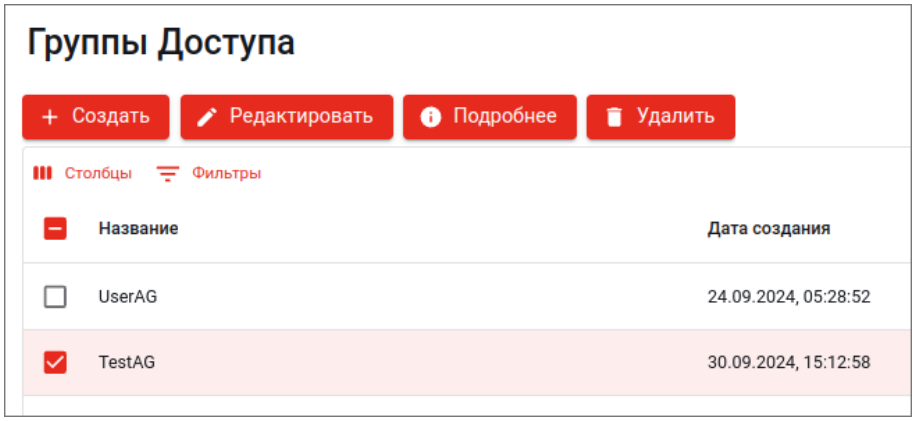

Рисунок 37 – Действия, доступные для выбранной группы доступа

При нажатии кнопки «Подробнее» откроется окно свойств группы доступа, вкладка «Пользователи» (рисунок 38).

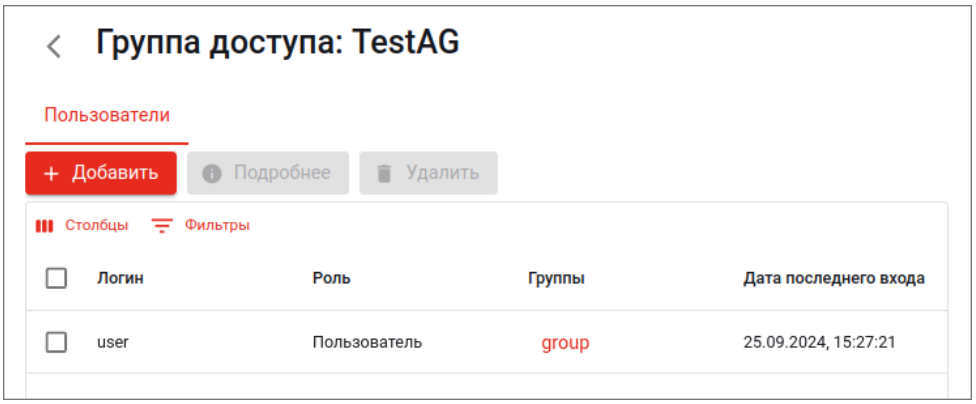

Рисунок 38 – Страница «Пользователи» выбранной для группы доступа

4.2.4. Для добавления в данную группу доступа пользователей нажмите кнопку «Добавить» и в открывшемся модальном окне в выпадающем списке с помощью чекбоксов выберите нужных пользователей. Закончив выбор, нажмите кнопку «Добавить» (рисунок 39).

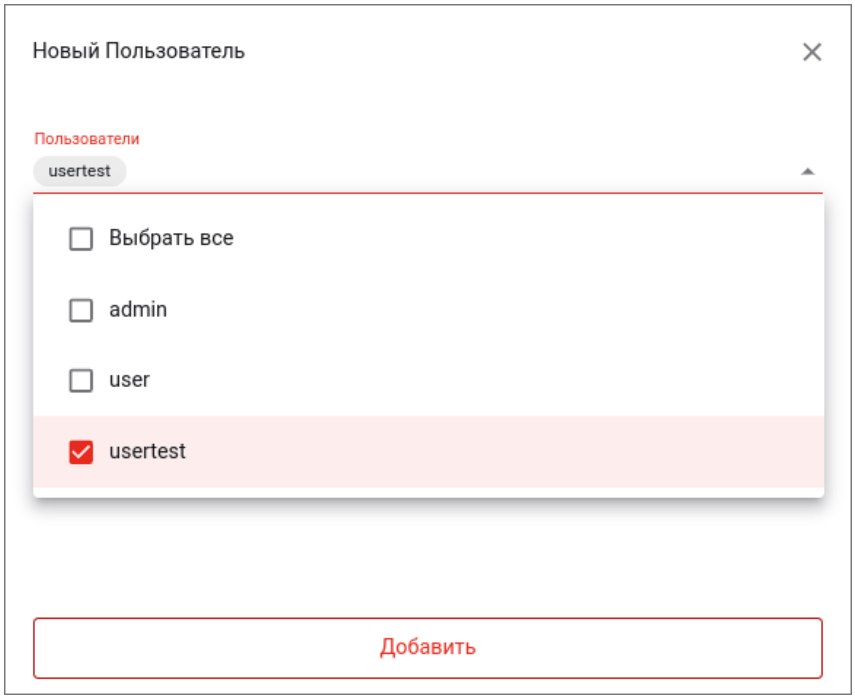

Рисунок 39 – Добавление пользователей в группу доступа

Выделив пользователя, можно будет посмотреть его свойства, нажав кнопку «Подробнее», или удалить, нажав кнопку «Удалить» (рисунок 40).

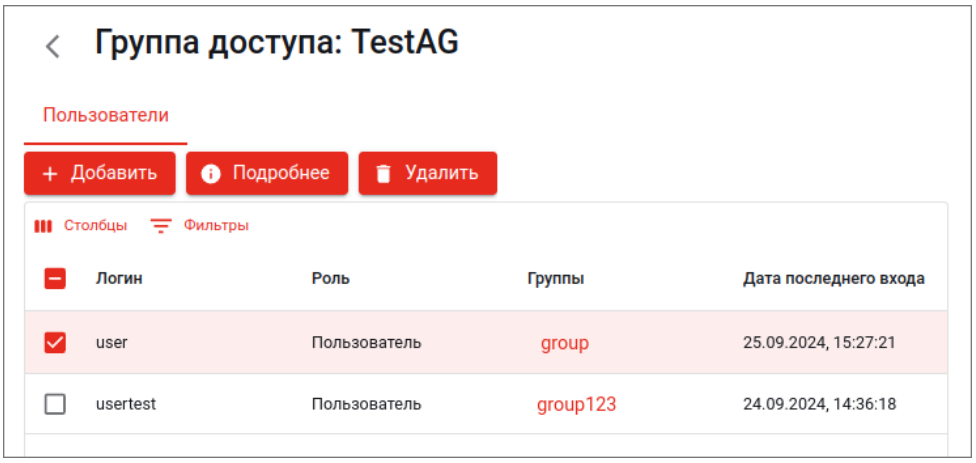

Рисунок 40 – Действия, доступные для выбранного пользователя в составе группы доступа

5 Рабочие места

5.1. Управление виртуальными рабочими местами осуществляется в разделе «Рабочие места» (рисунок 41).

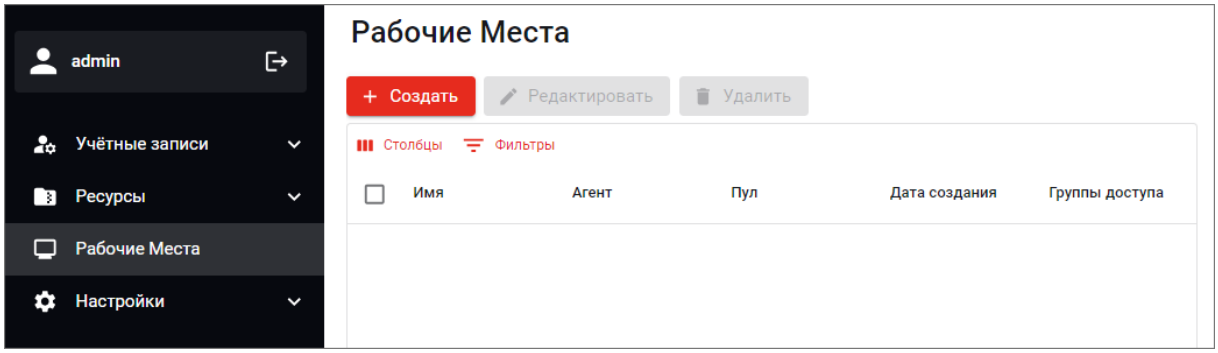

Рисунок 41 – Страница «Рабочие места»

5.2. Для создания нового рабочего места нажмите кнопку «Создать» и в открывшемся модальном окне укажите значения параметров (рисунок 42):

– имя рабочего места (обязательный параметр);
– в выпадающем меню «Агент» – выбрать имеющегося агента, который будет предоставлять клиенту доступ к ресурсам;
– в выпадающем меню «Группы доступа» – выбрать группы доступа, которые определяют пользователей, имеющих доступ к данному BPM;
– в выпадающем меню «Пул» – выбрать пул.

Нажмите кнопку «Создать», расположенную в самом низу этого окна.

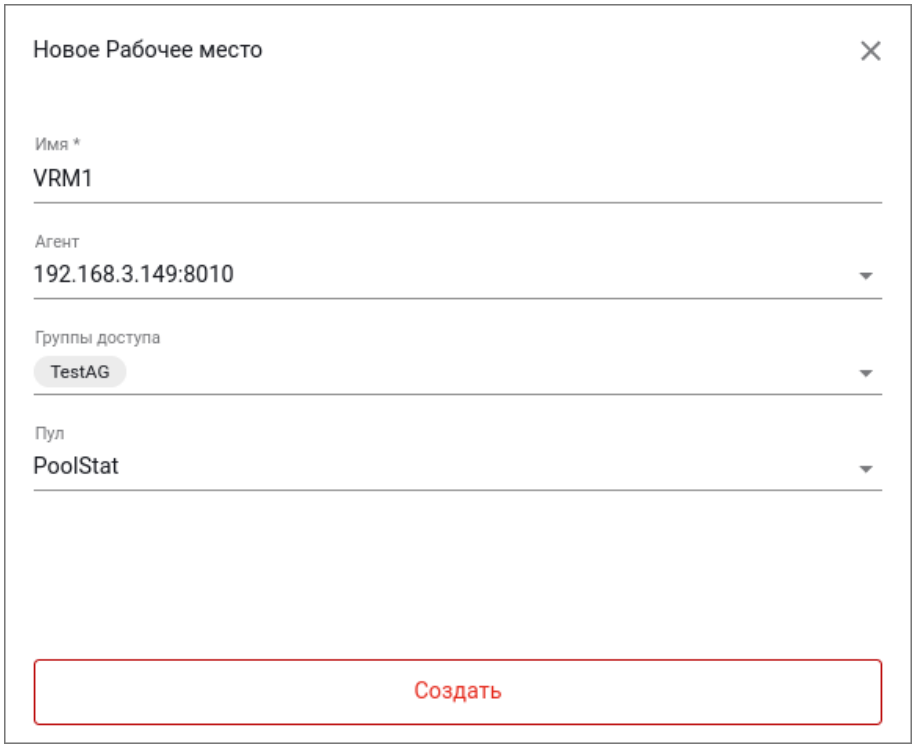

Рисунок 42 – Создание нового рабочего места

5.3. После создания рабочего места оно появится в списке. Выделив его нажатием, можно отредактировать параметры, заданные ранее при его создании, либо удалить его (активными станут соответствующие кнопки) (рисунок 43).

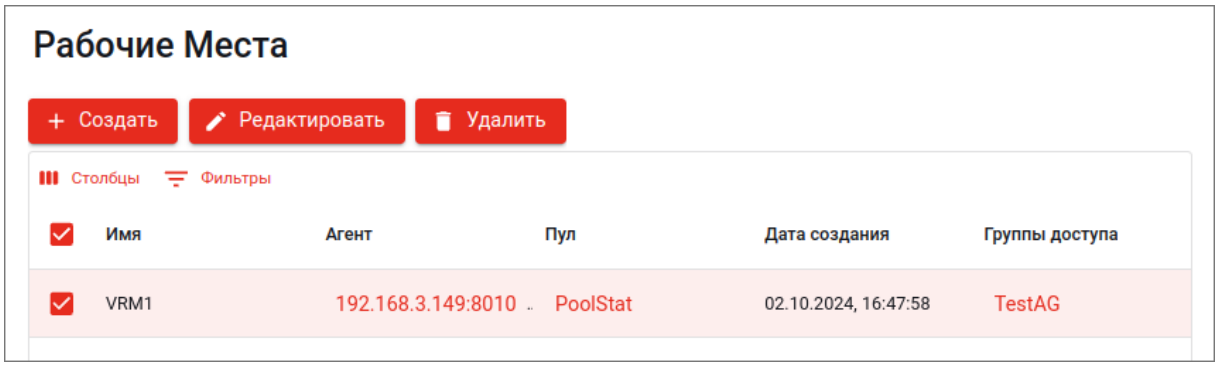

Рисунок 43 – Действия, доступные для выбранного рабочего места

6 Конфигурационные файлы

В данном разделе рассмотрены важные моменты для конфигурационных файлов Брокера.

Изменение значений указанных ниже параметров приведёт к изменению поведения программного обеспечения, но не выведет его из строя. Изменение остальных значений параметров в этих файлах конфигурации или файлах конфигурации, которые в данном разделе не указаны, могут привести к выходу программного обеспечения из строя.

6.1 Сервис администратора

6.1.1. Полный путь к конфигурационному файлу:
`/opt/redvrm/broker_admin/config/server.conf`.

6.1.2. Параметры секции `[VIRT]`:
`AWAIT_TIMEOUT_SECONDS` – время ожидания операции на каждом шагу при создание пула (в секундах). Стоит изменить, если шаблон для пула создаётся более 300 с.

6.1.3. Параметры секции `[AGENTS]`:
`IS_ALIVE_CHECK_INTERVAL_SECONDS` – время между проверками агентов на статус онлайн (в секундах).

6.2 Сервис аутентификации

6.2.1. Полный путь к конфигурационному файлу:
`/opt/redvrm/broker_auth/config/server.conf`.

6.2.2. Параметры секции `[jwt]`:

`access_token_expire_minutes` – время действия токена доступа (в секундах).

`refresh_token_expire_minutes` – время действия токена обновления (в секундах).

7 Просмотр логов

Здесь рассмотрены логи на Брокере.

Рекомедуем смотреть логи через инструмент `journalctl` для каждого из сервисов отдельно.

7.1. Сервис администратора:

```
journalctl -u broker_admin
```

```
journalctl -u broker_admin_worker
```

```
journalctl -u broker_admin_scheduler
```

7.2. Сервис аутентификации:

```
journalctl -u broker_auth
```

7.3. Сервис пулов:

```
journalctl -u broker_pool_provider
```

7.4. Клиентский сервис:

```
journalctl -u broker_client_api
```