RuBackup
Система резервного копирования и восстановления данных

Интеграция RuBackup со средствами управления доменом Microsoft Active Directory

Версия 2.2.0

18.09.2024 г.

Содержание

Введение

Система резервного копирования и восстановления данных RuBackup (далее — СРК, Система) предоставляет возможность использовать ролевую модель MS AD для аутентификации в СРК и ассоциировать группы MS AD с ролями СРК. Данный функционал позволяет использовать имеющиеся учетные данные MS AD для доступа и работы в RuBackup.

Предварительные настройки

СРК поддерживает интеграцию с Microsoft Active Directory версий 2012 R2 или 2016, развернутой на Microsoft Windows Server 2016.

1. Установите и настройте MS AD. Для этого:

- Скачайте корневой сертификат в Службе сертификации и разместите его на основном сервере RuBackup в формате PEM. Для конвертации сертификата в формат PEM выполните команду:

```
openssl x509 -inform der -in <имя_сертификата>.cer -out <имя_сертификата>.pem
```

Внимание! Имя хоста в сертификате должно совпадать с именем хоста, на котором запущен Microsoft Windows Server 2016 с настроенным на нем сервисом MS AD и к которому будет осуществляться подключение по протоколу LDAP/LDAPS.

- Сконфигурируйте сервис MS AD;
- Создайте необходимые группы пользователей в MS AD;
- Создайте пользователя MS AD, который будет использоваться в качестве служебного (Bind User). Пользователь Bind User должен иметь права на просмотр общей информации о конфигурации: список существующих групп, список существующих пользователей, общая информация о пользователях;
- С помощью стандартных средств Microsoft Windows убедитесь, что MS AD доступна через LDAP/LDAPS-протоколы. Это можно сделать с помощью стандартной утилиты ldp.exe;
- Скачайте клиентский сертификат и разместите его на основном сервере RuBackup в формате PEM. Для конвертации сертификата в формат PEM выполните команду:

openssl x509 -inform der -in <имя_сертификата>.cer -out <имя_сертификата>.pem

2. Обеспечьте возможность подключения MS AD по протоколам LDAP/LDAPS с хоста, на котором установлен сервер СРК (как основной, так и резервный). Для этого нужно, чтобы:

- Хост, на котором запущен Microsoft Windows Server 2016, был доступен по имени с хоста, на котором установлен основной сервер RuBackup;
- Были доступны порты 389 (LDAP) и 636 (LDAPS) с сервера RuBackup.

Первичная настройка CPK для работы с MS AD

1. Запросите у Администратора MS AD наименования созданных групп пользователей, которые будут ассоциированы с ролями CPK, а также аутентификационную информацию служебной учетной записи Bind User, обладающей правами на получение данных о пользователях и группах из дерева LDAP, для последующей аутентификации.
2. Войдите в RBM посредством существующего механизма аутентификации, основанного на СУБД PostgreSQL (Рисунок 1).

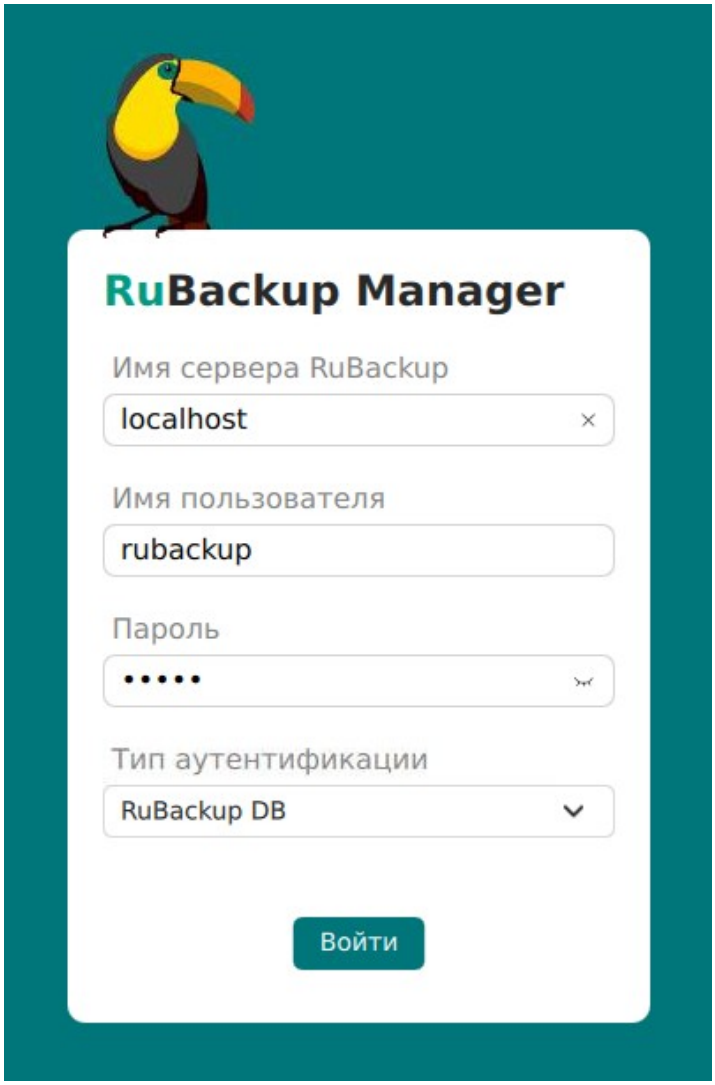

Рисунок 1

3. Активируйте в RBM сервисный режим CPK в разделе настроек в правом верхнем углу экрана (Рисунок 2).

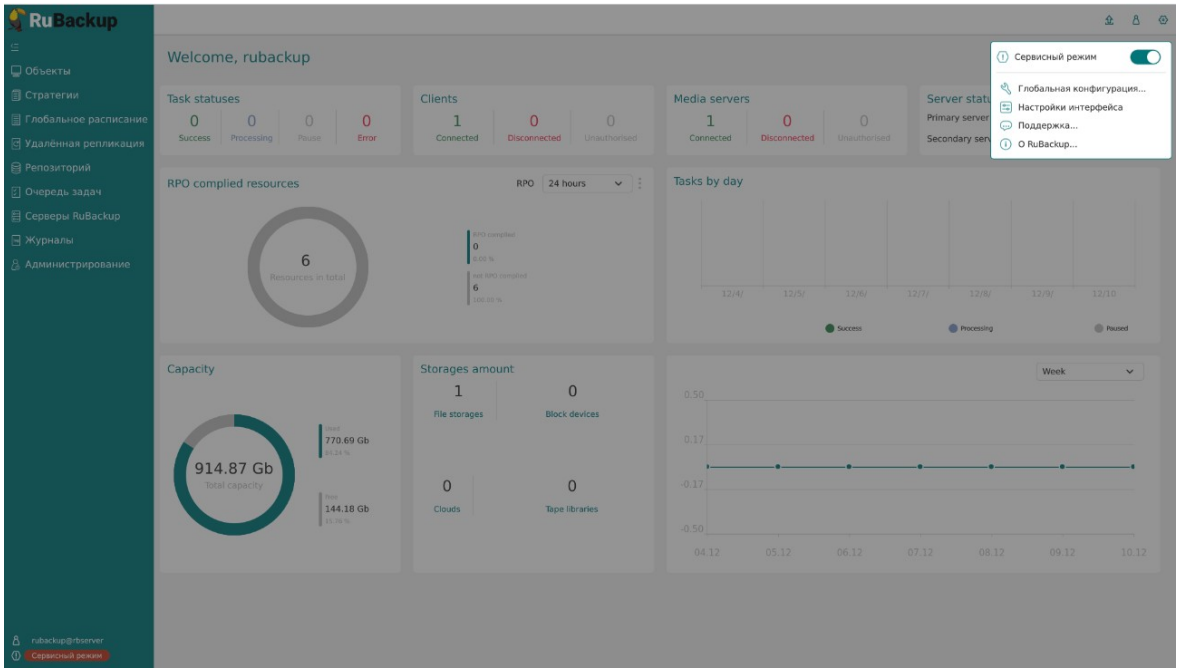

Рисунок 2

4. Перейдите в раздел «Администрирование» (Рисунок 3).

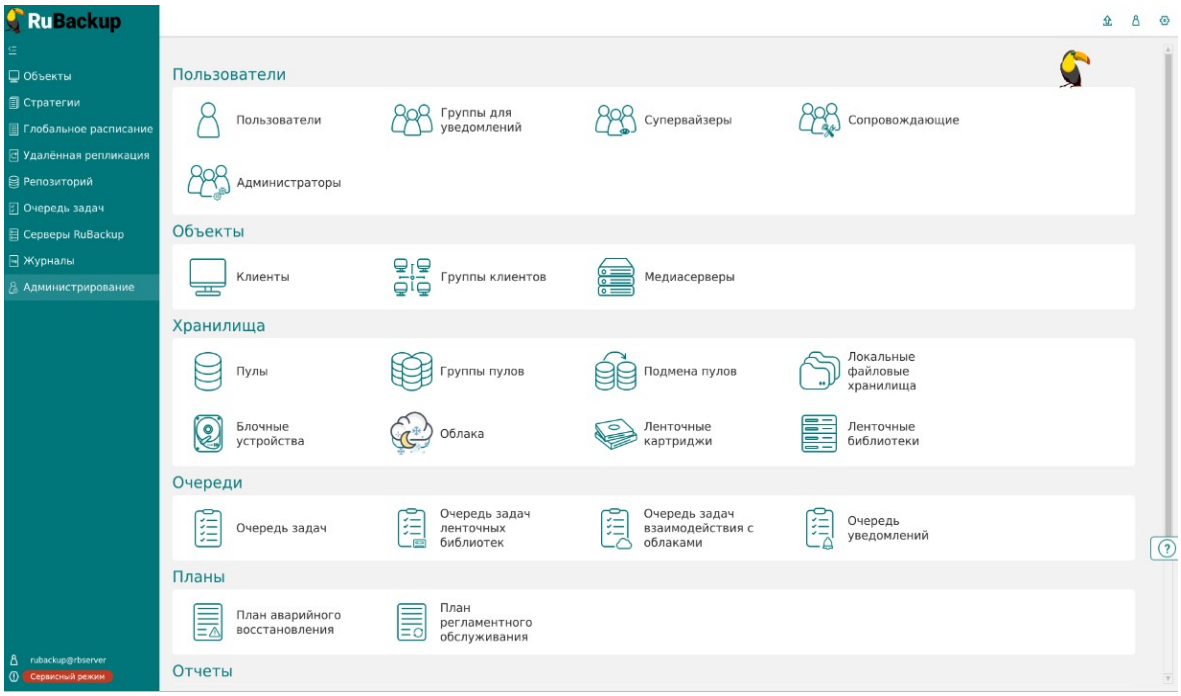

Рисунок 3

5. Перейдите в подраздел «Настройки соединения с MS Active Directory» (Рисунок 4).

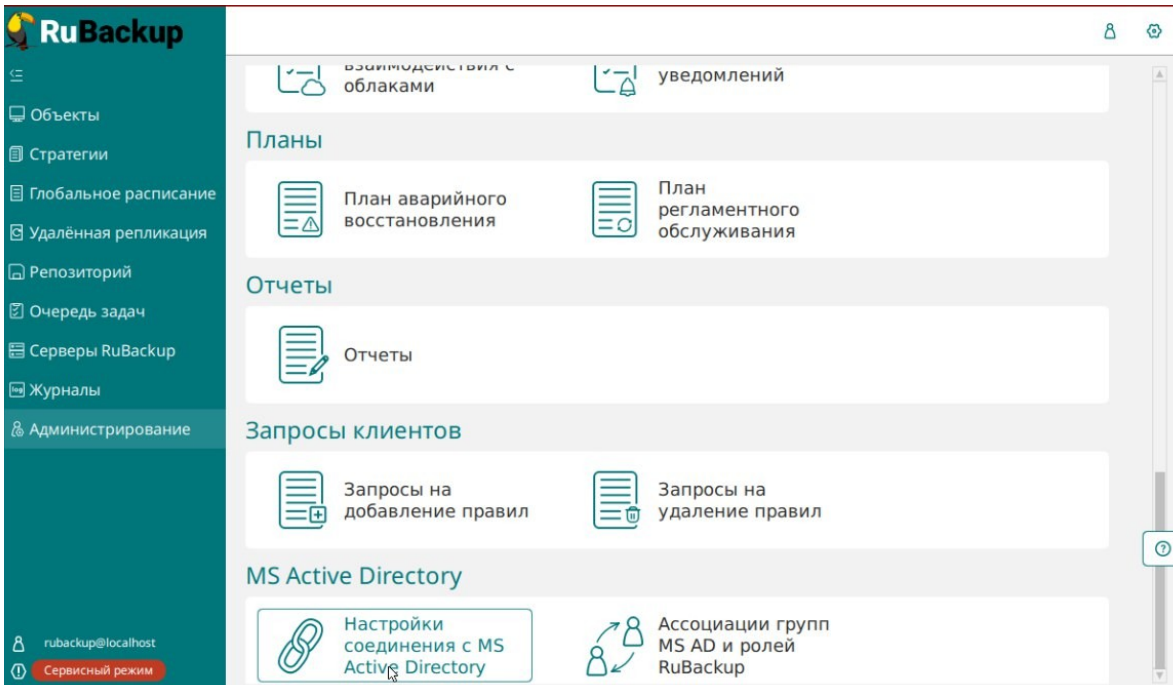

Рисунок 4

6. Укажите следующие настройки для подключения к MS AD (Рисунок 5):

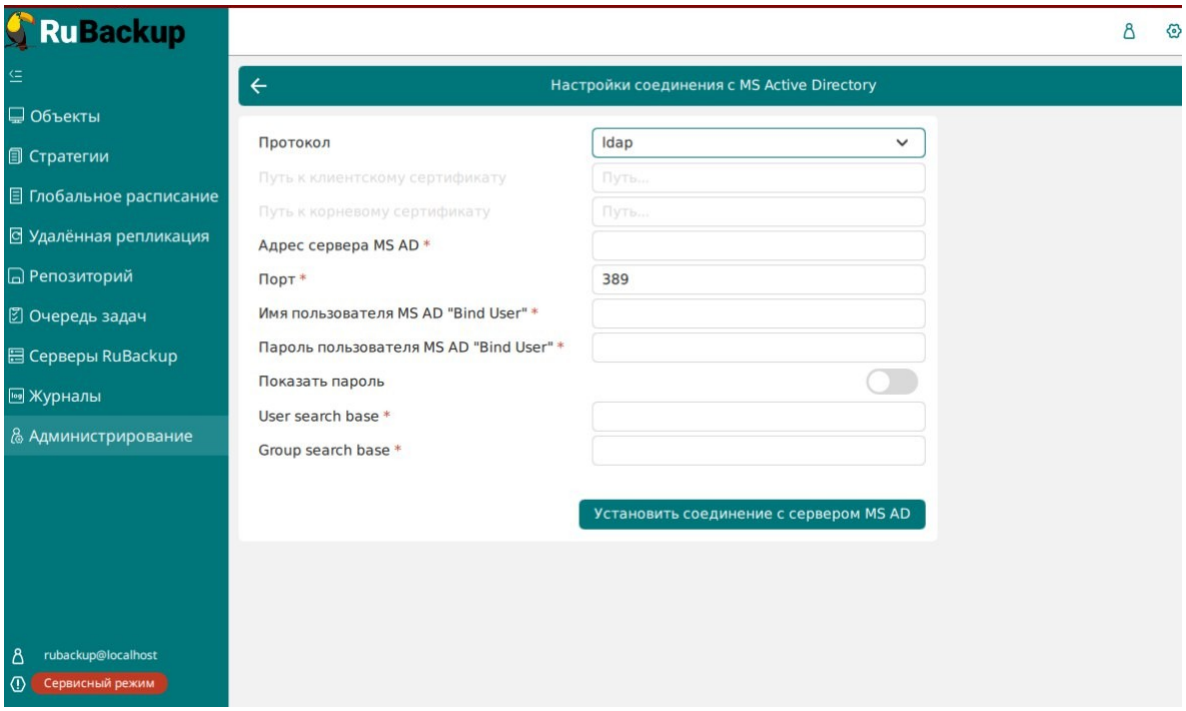

Рисунок 5

- Протокол (LDAP/LDAPS);

При выборе LDAPS указывается путь к клиентскому и корневому сертификатам Службы сертификации, выдающей сертификаты контроллерам домена (Рисунок 6).

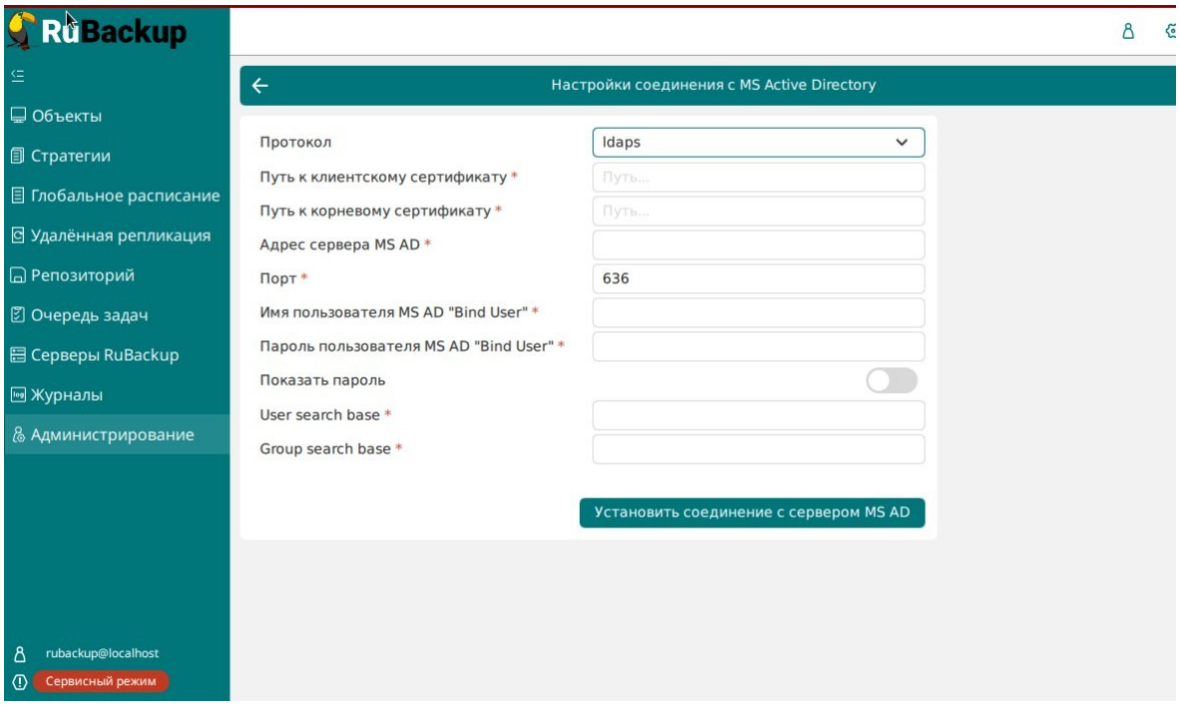

Рисунок 6

- Сертификаты должны находиться на основном сервере СРК. Проверкой сертификатов будет служить первое подключение к серверу MS AD;
- Адрес сервера MS AD - hostname или ip-адрес для LDAP-протокола, для LDAPS — только hostname.

При установке соединения с неправильным адресом сервера появится предупреждение (Рисунок 7):

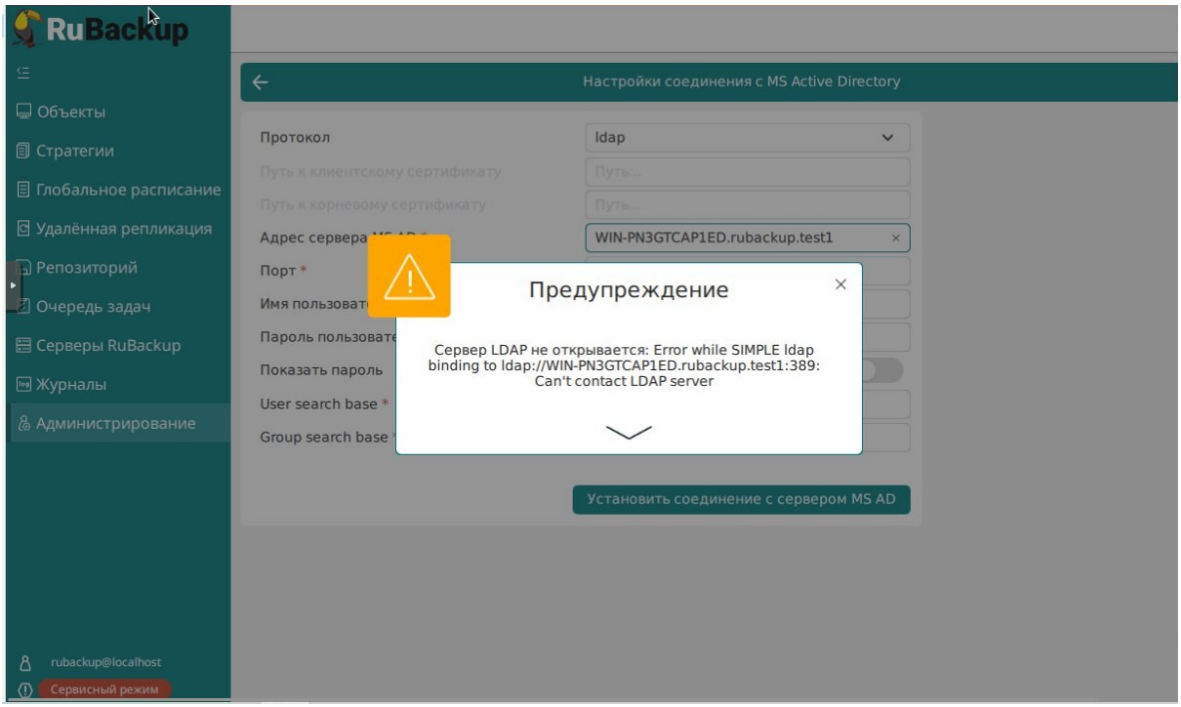

Рисунок 7

- Порт:
  - Значениями по умолчанию являются — 389 для LDAP, для LDAPS — 636;
- Учетные данные для служебного пользователя Bind User: домен и логин в формате <домен>\<логин>, а также пароль;

  При установке соединения с неправильным логином и паролем появится предупреждение (Рисунок 8):

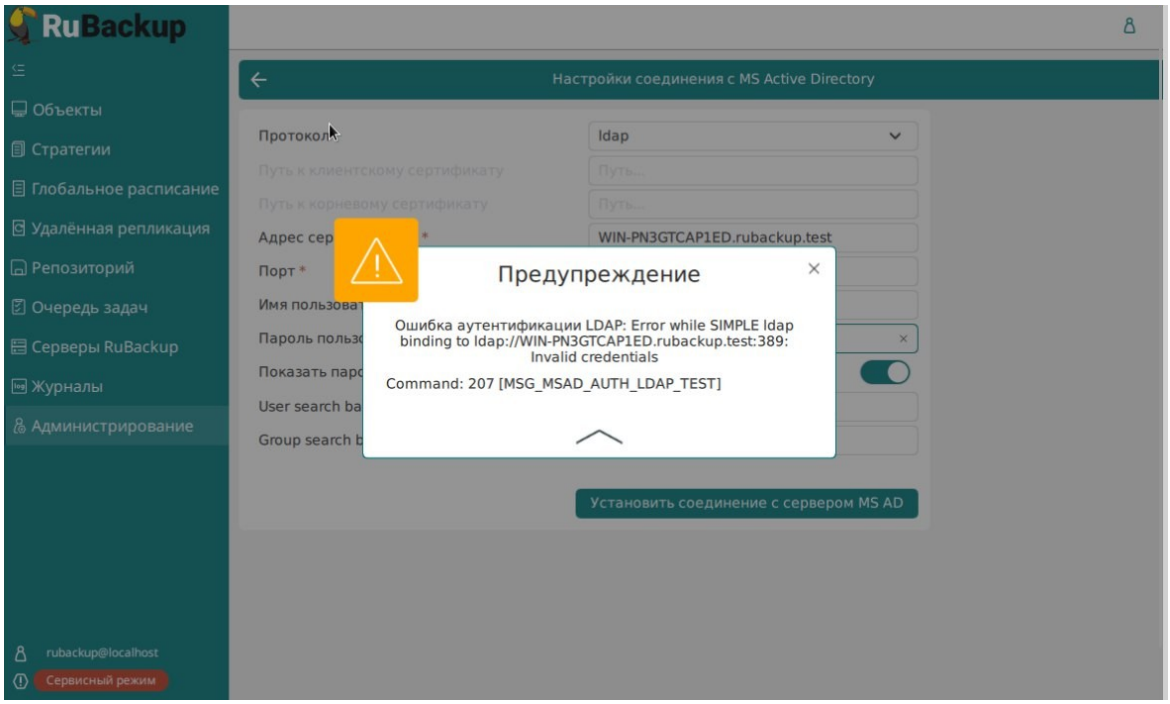

Рисунок 8

- User search base — указывает, от какого объекта в иерархии Active Directory начинать поиск пользователей;
- Group search base — указывает, от какого объекта в иерархии Active Directory начинать поиск групп.

5. Нажмите на кнопку «Установить соединение с сервером MS AD», чтобы произвести тестовый запрос и проверить:
   - Возможность подключения к указанному серверу MS AD, используя предоставленные параметры для подключения;
   - Возможность получения списка информации о пользователях и группах из дерева LDAP.

6. Если вы успешно прошли шаги из п. 5, предварительная настройка СРК для работы с MS AD успешно завершена — открывается окно «Ассоциация групп MS AD и ролей RuBackup» (Рисунок 9):

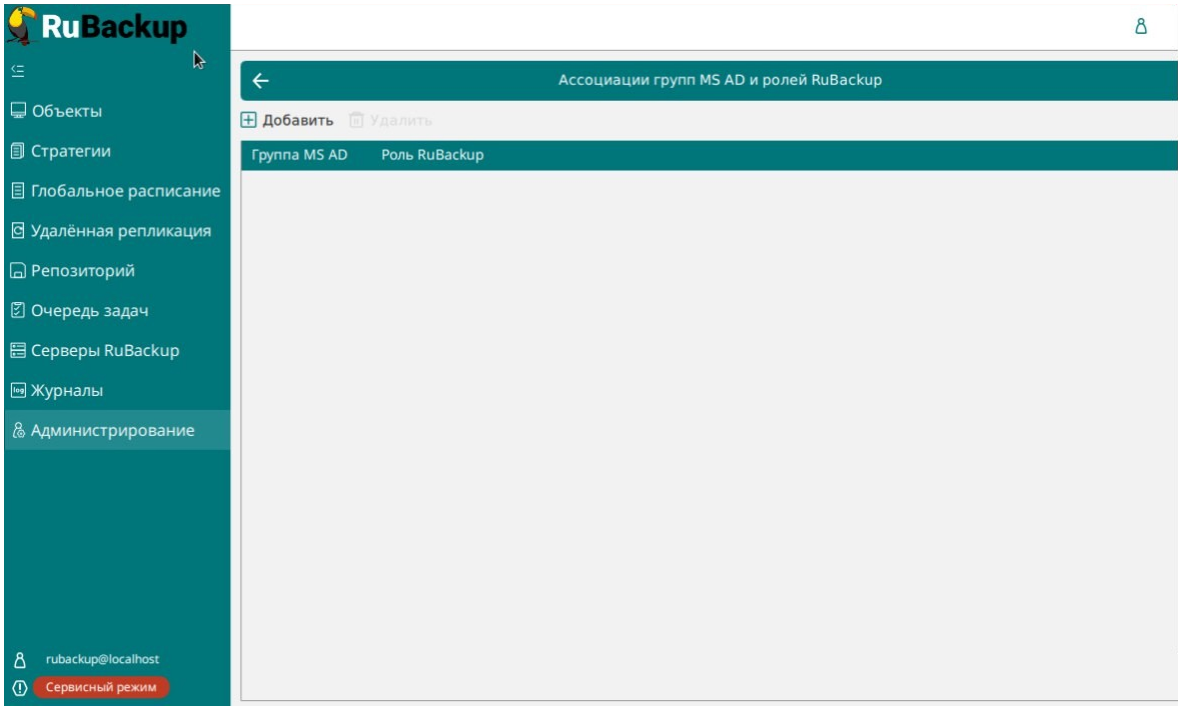

Рисунок 9

7. Если Вам не удалось успешно пройти шаги из п. 5, RBM отображает сообщение о невозможности подключения к серверу MS AD.
   7.1. Выполните шаги из раздела "Решение проблем" для устранения сложностей, а затем повторите шаги раздела «Первичная настройка СРК для работы с MS AD», начиная с 4.
8. СРК сохраняет указанную конфигурационную информацию в БД RuBackup. Пароль от пользователя Bind User сохраняется в БД RuBackup в зашифрованном средствами PostgreSQL виде.

9. Находясь в подразделе «Ассоциация групп MS AD и ролей RuBackup», добавьте ассоциации групп MS AD с ролями СРК (Рисунок 10):

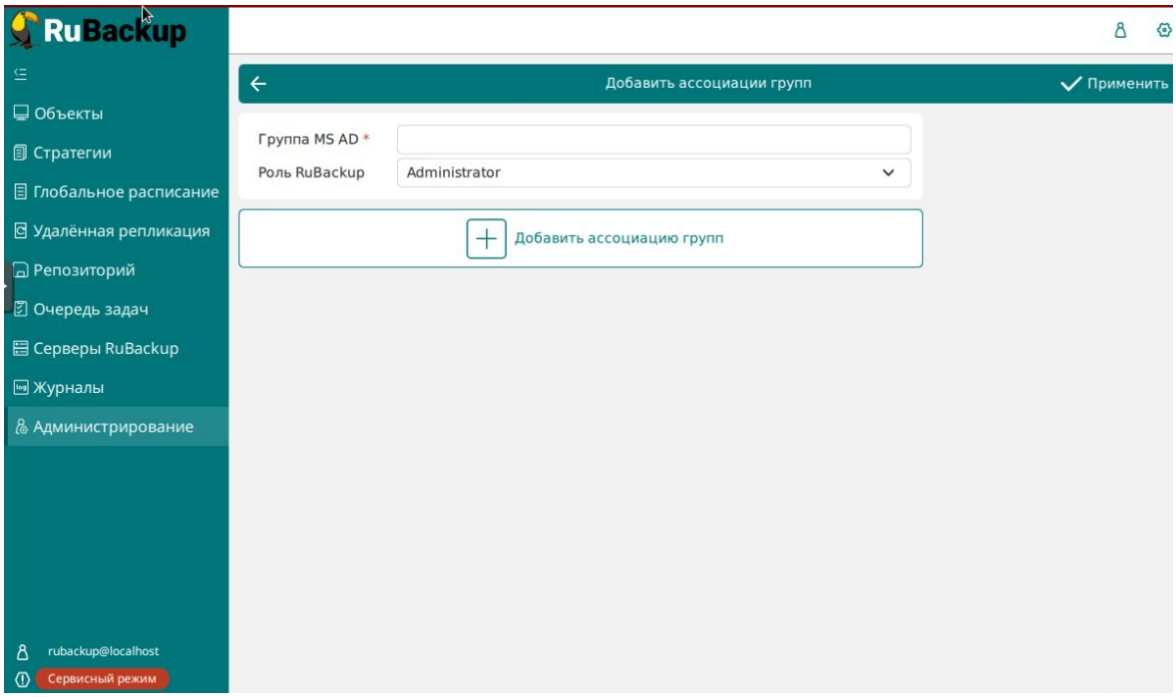

Рисунок 10

Одну роль доступа RuBackup вы можете связать с одной или несколькими группами MS AD. Связать одну группу MS AD с несколькими ролями СРК нельзя: учетная запись MS AD не может принадлежать нескольким ролям RuBackup.

Внимание! Информация о пользователях, входящих в группу MS AD, есть только у администратора MS AD и не отображается в СРК RuBackup.

10. Сохраните информацию в RBM, нажав на кнопку «Применить».
11. Деактивируйте сервисный режим.

Настройка СРК для работы с MS AD успешно завершена.

Выбор типа аутентификации по умолчанию

1. Активируйте в RBM сервисный режим СРК (Рисунок 11).

Рисунок 11

2. Перейдите во вкладку «Глобальная конфигурация» (Рисунок 12).

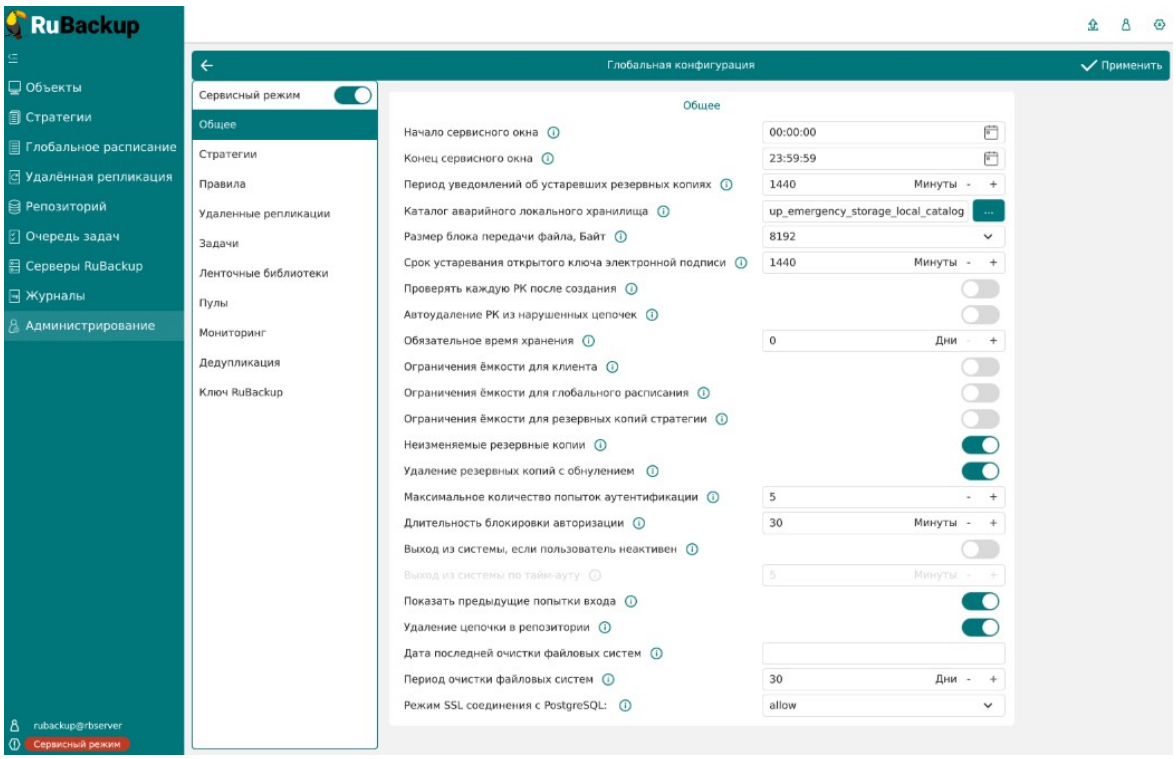

Рисунок 12

3. Перейдите в раздел с настройками аутентификации (Рисунок 13).

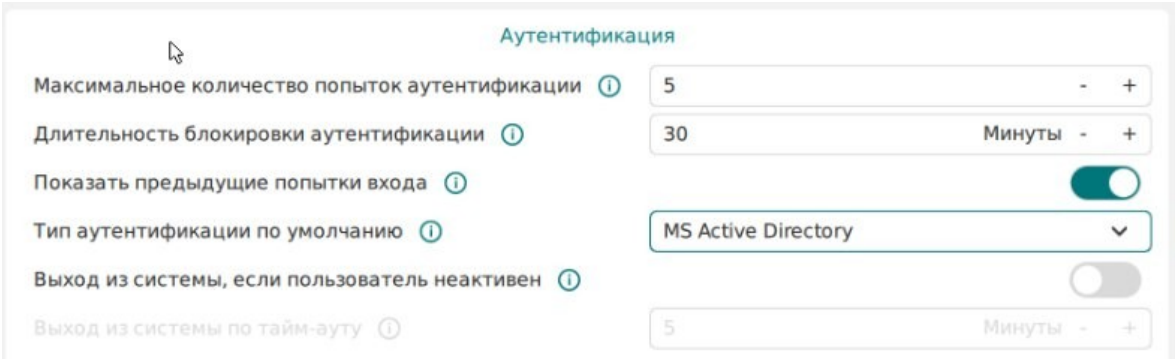

Рисунок 13

4. Выберите тип аутентификации по умолчанию - MS Active Directory.
5. Сохраните настройки в RBM нажатием кнопки «Применить».
6. Деактивируйте сервисный режим (Рисунок 14).

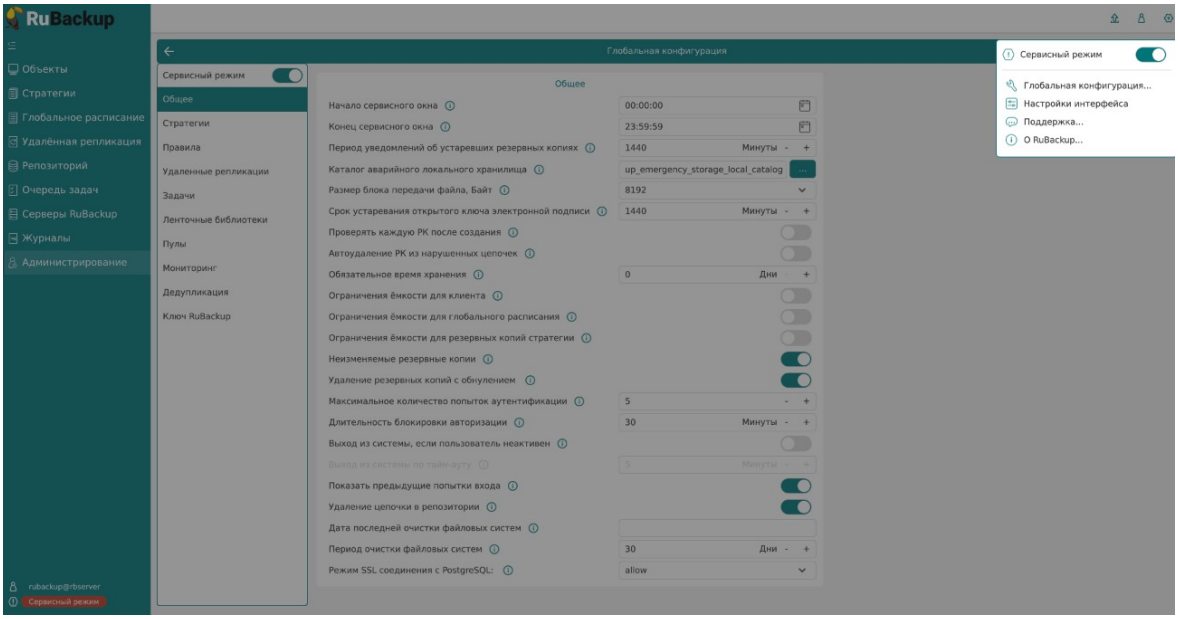

Рисунок 14

Аутентификация пользователя СРК посредством MS AD

1. Запустите RBM.
2. Появится окно для ввода логина и пароля с выпадающим списком, в котором вы можете выбрать тип аутентификации (Рисунок 15).

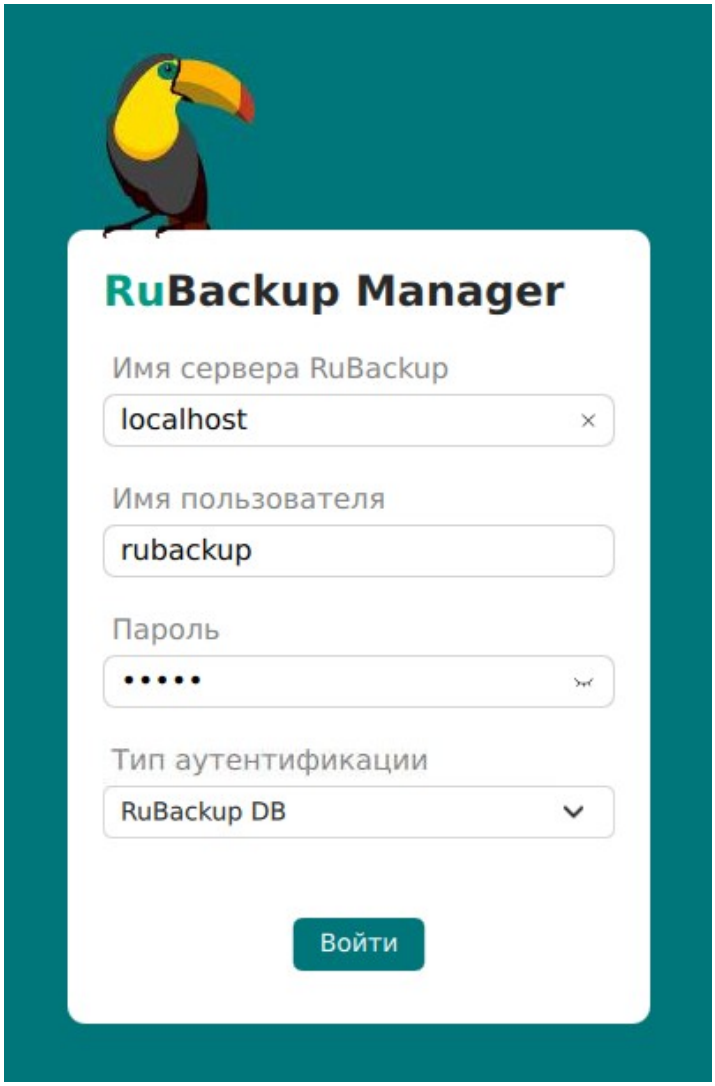

Рисунок 15

При этом по умолчанию выбран тип аутентификации, установленный в глобальной конфигурации СРК (раздел «Выбор типа аутентификации по умолчанию»).

2.1. Выберите в выпадающем списке «MS Active Directory».

3. Введите в RBM:
   3.1. Домен и логин от учетной записи MS AD в формате <домен>\<пароль>.
   3.2. Пароль от учетной записи MS AD.
4. Войдите в СРК нажатием на кнопку «Войти»

5. Если аутентификационные данные введены неверно, RBM выводит сообщение об ошибке с текстом: «Неверно введены логин или пароль» (Рисунок 16):

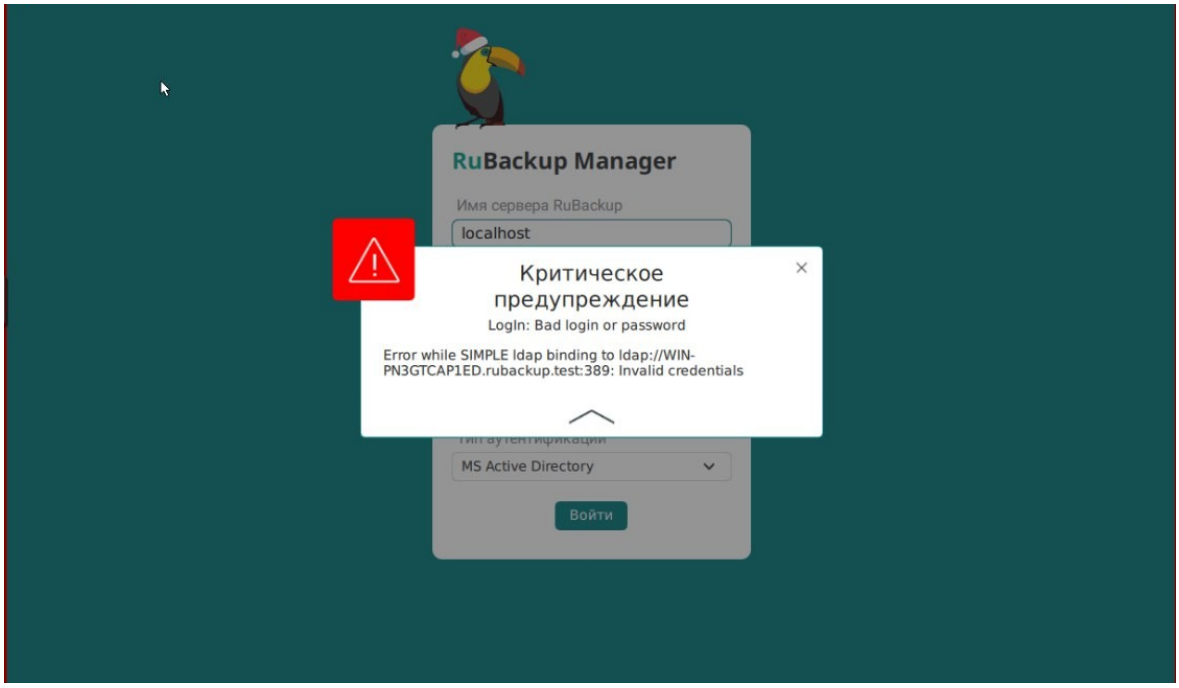

Рисунок 16

6. В этом случае:
   6.1. Введите корректные логин и пароль.
   6.2. В случае возникновения проблем обратитесь к Администратору СРК. Администратор СРК выполняет шаги из раздела «Решение проблем».
7. Если пользователь СРК находится в одной или нескольких группах MS AD, которым соответствует одна роль СРК, то он видит главное меню RBM.

   Если пользователь не находится ни в одной группе, соответствующей роли СРК, RBM выводит сообщение об ошибке: «Данному пользователю не назначена роль СРК (Рисунок 17). Обратитесь к Администратору СРК.».

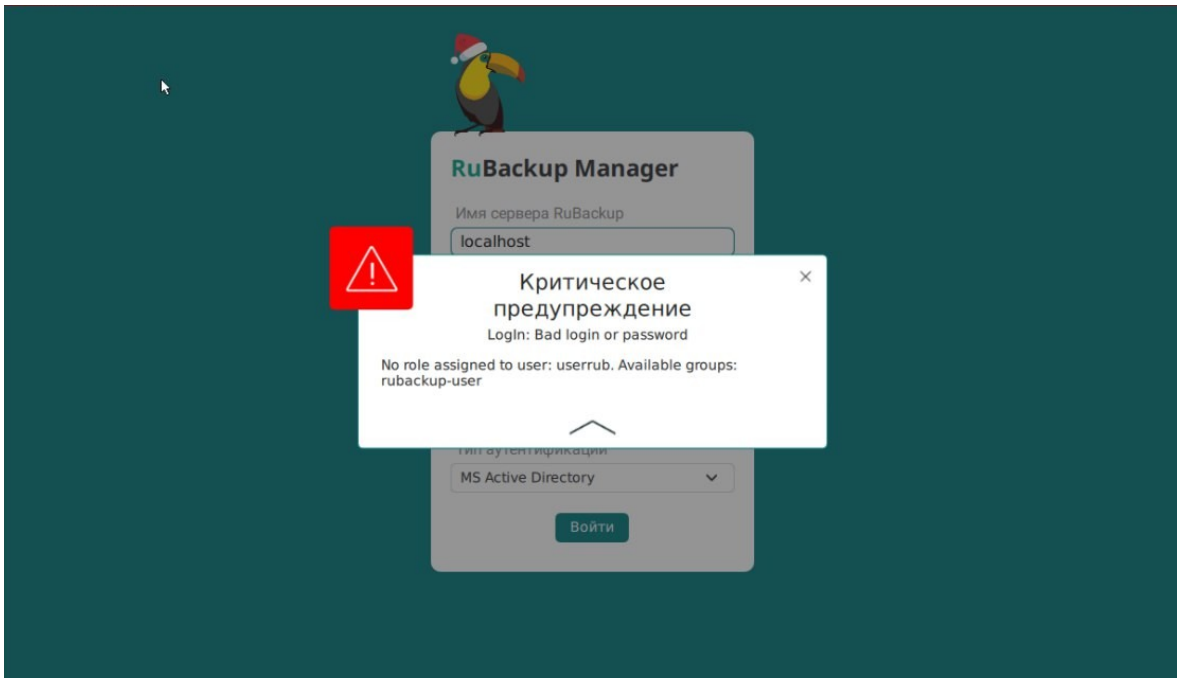

Рисунок 17

6.1. Обратитесь к администратору MS AD для добавления данного пользователя средствами MS AD в необходимую группу MS AD, соответствующую его роли доступа в СРК.

6.2. Выполните шаги из данного раздела с начала.

Аудит аутентификации пользователей

СРК RuBackup предоставляет возможность просмотра операций аутентификации пользователей. Для этого:

1. Перейдите в пункт меню «Журналы», выберите «Журнал операций аутентификации» (Рисунок 18).

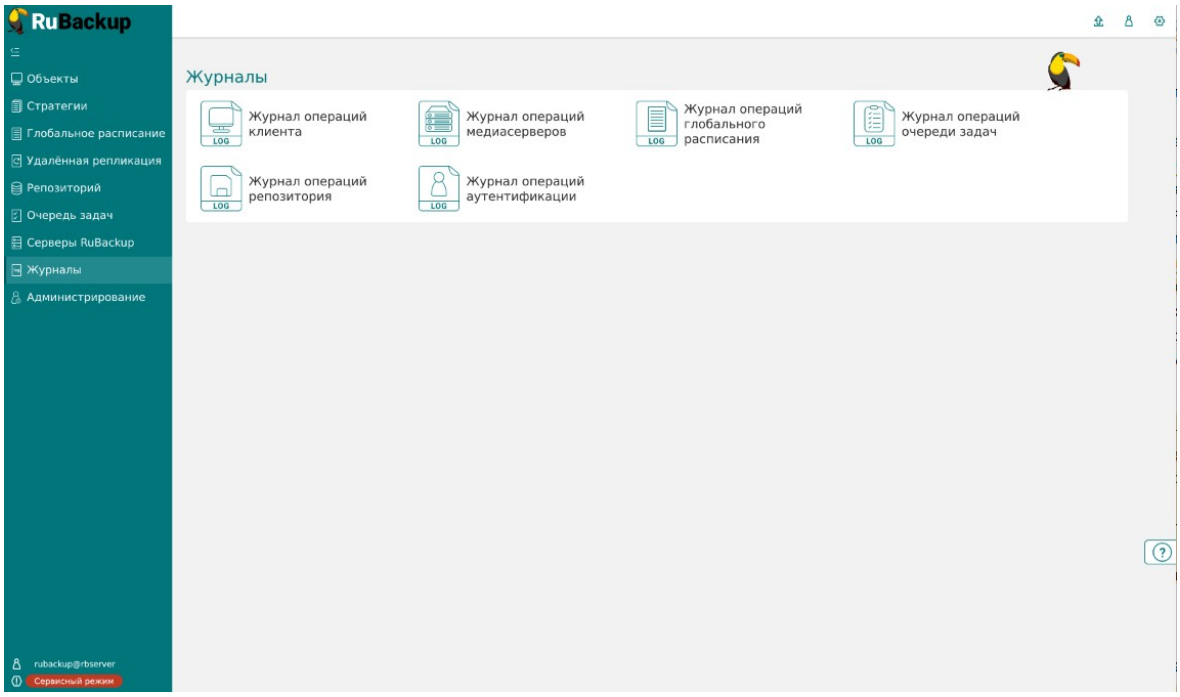

Рисунок 18

2. В данном разделе вы можете проанализировать успешные и неудачные попытки аутентификации, а также их количество (Рисунок 19).

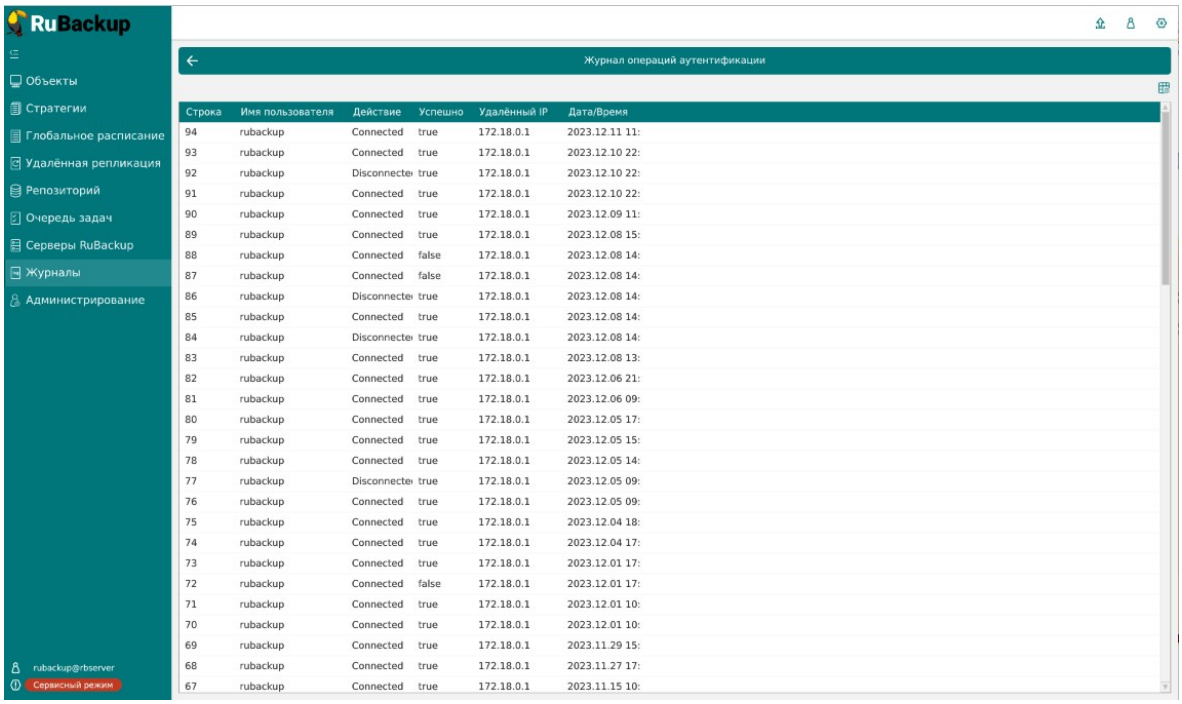

Рисунок 19

Решение проблем

1. Подключитесь к хосту сервера RuBackup, перейдите в директорию /opt/rubackup/log/, откройте файл RuBackup.log, проверьте журнал на наличие ошибок, касающихся взаимодействия СРК с сервером MS AD.
2. Проанализируйте ошибки в файле RuBackup.log:
   2.1. Если найденная ошибка заключается в отсутствии связи с сервером MS AD, то проверьте корректность данных для подключения к серверу MS AD. Проверьте сетевую доступность сервера MS AD с хоста, где в данный момент запущен основной сервер СРК, с помощью команды:

   ```
   ping <hostname>
   ```

   2.2. Если найденная ошибка связана с неверными логином или паролем, проверьте корректность учетных данных для пользователя MS AD «Bind User» в настройках. Если данные учетной записи корректны, то, используя их, подключитесь к серверу MS AD с использованием сторонних инструментов.
   2.3. Если вы нашли несоответствие в правах, проверьте принадлежность пользователя СРК к группам MS AD, использующимся для аутентификации в СРК RuBackup.
   2.4. Если найденная ошибка связана с внутренней ошибкой СРК, обратитесь в службу технической поддержки продукта СРК, предоставив информацию о выполненных шагах и журнал логов.
3. Проверьте доступность сервера MS AD, валидность наименований групп доступа и учетных записей, устраните проблемы.
   3.1. В случае отсутствия явных ошибок на стороне сервера MS AD, откройте запрос в личном кабинете ГК «Астра».

Ограничения

- Аутентификация с использованием MS AD не распространяется на клиенты PK. Аутентификация клиентов PK остается без изменений и осуществляется посредством HWID (подробнее — в документе «Руководство системного администратора RuBackup», раздел «Администрирование»).
- Опцию аутентификации посредством PostgreSQL нельзя отключить, т.к. в случае утери доменного контроллера MS AD вы должны иметь возможность аутентифицироваться в CPK для изменения настроек аутентификации, а также для решения других внештатных ситуаций.
- Аутентификация с использованием MS AD не распространяется на утилиты командной строки (CLI).