

RuBackup

Система резервного копирования и восстановления данных

Интеграция RuBackup со средствами управления доменом Microsoft Active Directory



Содержание

| | |
|--|----|
| Введение..... | 3 |
| Предварительные настройки..... | 3 |
| Первичная настройка СРК для работы с MS AD..... | 4 |
| Выбор типа аутентификации по умолчанию..... | 11 |
| Аутентификация пользователя СРК посредством MS AD..... | 13 |
| Аудит аутентификации пользователей..... | 15 |
| Решение проблем..... | 17 |
| Ограничения..... | 17 |

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 разместить 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 CPK (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.

RuBackup Manager

Имя сервера

Имя пользователя

Пароль

3. Активируйте в RBM сервисный режим СРК в разделе настроек в правом верхнем углу экрана.

The screenshot shows the RuBackup management interface. On the left is a dark sidebar with navigation links: Объекты, Стратегии, Глобальное расписание, Удалённая репликация, Репозиторий, Очередь задач, Серверы RuBackup, Журналы, and Администрирование. The main area displays several cards: Task statuses (Success: 0, Processing: 0, Pause: 0, Error: 0), Clients (Connected: 1, Disconnected: 0, Unauthorized: 0), Media servers (Connected: 1, Disconnected: 0, Unauthorized: 0), and Server status (Primary server: 1, Secondary server: 0). A prominent feature is a large circular chart titled 'RPO compiled resources' showing 6 resources in total, with a legend indicating 0 RPO compiled (0.00%) and 6 not RPO compiled (100.00%). Below this are sections for Capacity (Total capacity: 914.87 Gb, used: 770.69 Gb, free: 144.18 Gb) and Storages amount (File storages: 1, Block devices: 0, Clouds: 0, Tape libraries: 0). A line chart titled 'Tasks by day' tracks task progress from December 4 to December 10, showing a flat line at 0.00% completion. In the top right corner, there is a 'Service mode' toggle switch, which is currently turned on. A tooltip for this switch includes links to 'Глобальная конфигурация...', 'Настройки интерфейса...', 'Поддержка...', and 'О RuBackup...'.

4. Перейдите в раздел «Администрирование».

The screenshot shows the 'Administration' section of the RuBackup interface. It includes a sidebar with the same navigation links as the main dashboard. The main area is divided into several sections: 'Пользователи' (Users), 'Объекты' (Objects), 'Хранилища' (Storage), 'Очереди' (Queues), 'Планы' (Plans), and 'Отчеты' (Reports). Each section contains icons and descriptive text for its respective management functions. The 'Пользователи' section includes links for Пользователи, Группы для уведомлений, Супервайзеры, and Сопровождающие. The 'Объекты' section includes links for Клиенты, Группы клиентов, Медиасерверы, Пулы, Группы пулов, Подмена пулов, Локальные файловые хранилища, Блочные устройства, Облачa, Ленточные картриджи, and Ленточные библиотеки. The 'Хранилища' section includes links for Очередь задач, Очередь задач ленточных библиотек, Очередь задач взаимодействия с облачами, and Очередь уведомлений. The 'Планы' section includes links for План аварийного восстановления and План регламентного обслуживания. The 'Отчеты' section is currently empty. A small icon of a toucan is visible in the top right corner of the main content area.

5. Перейдите в подраздел «Настройки соединения с MS Active Directory».

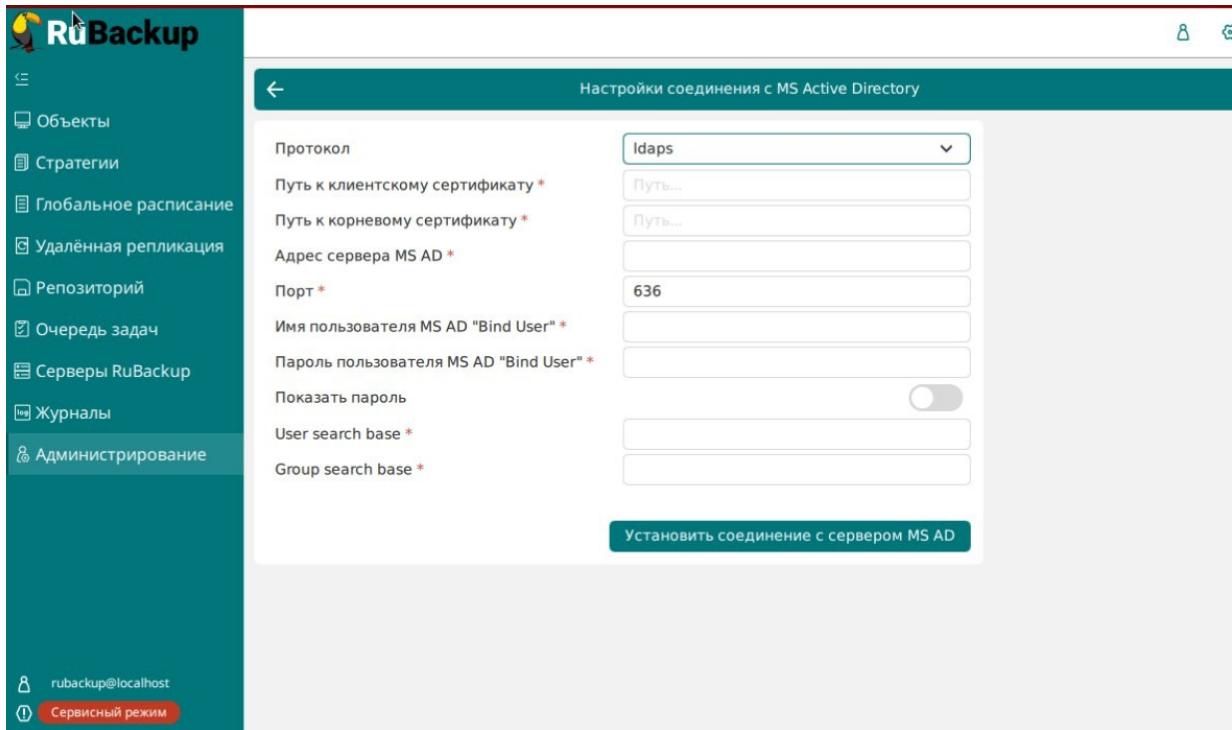
The screenshot shows the RuBackup application interface. On the left is a dark sidebar with navigation items: Объекты, Стратегии, Глобальное расписание, Удалённая репликация, Репозиторий, Очередь задач, Серверы RuBackup, Журналы, and Администрирование. Under Администрирование, there are two buttons: rubackup@localhost and Сервисный режим. The main panel has several sections: 'Планы' (Plans) with 'План аварийного восстановления' (Emergency Recovery Plan) and 'План регламентного обслуживания' (Planned Maintenance Plan); 'Отчеты' (Reports) with 'Отчеты' (Reports); 'Запросы клиентов' (Client Requests) with 'Запросы на добавление правил' (Requests for rule addition) and 'Запросы на удаление правил' (Requests for rule deletion); and 'MS Active Directory' with 'Настройки соединения с MS Active Directory' (Connection settings for MS Active Directory) highlighted in a green box, and 'Ассоциации групп MS AD и ролей RuBackup' (Associations between MS AD groups and RuBackup roles).

6. Укажите следующие настройки для подключения к MS AD:

The screenshot shows the 'Настройки соединения с MS Active Directory' (Connection settings for MS Active Directory) configuration page. It includes fields for: Протокол (Protocol) set to 'ldap'; Путь к клиентскому сертификату (Path to client certificate) and Путь к корневому сертификату (Path to root certificate), both with 'Путь...' (Path...) buttons; Адрес сервера MS AD * (Address of MS AD server *); Порт * (Port *); Имя пользователя MS AD "Bind User" * (Name of MS AD "Bind User" *); Пароль пользователя MS AD "Bind User" * (Password of MS AD "Bind User" *); Показать пароль (Show password) with a toggle switch; User search base * (User search base *); Group search base * (Group search base *); and a large 'Установить соединение с сервером MS AD' (Establish connection with MS AD server) button at the bottom.

- Протокол (LDAP/LDAPS);

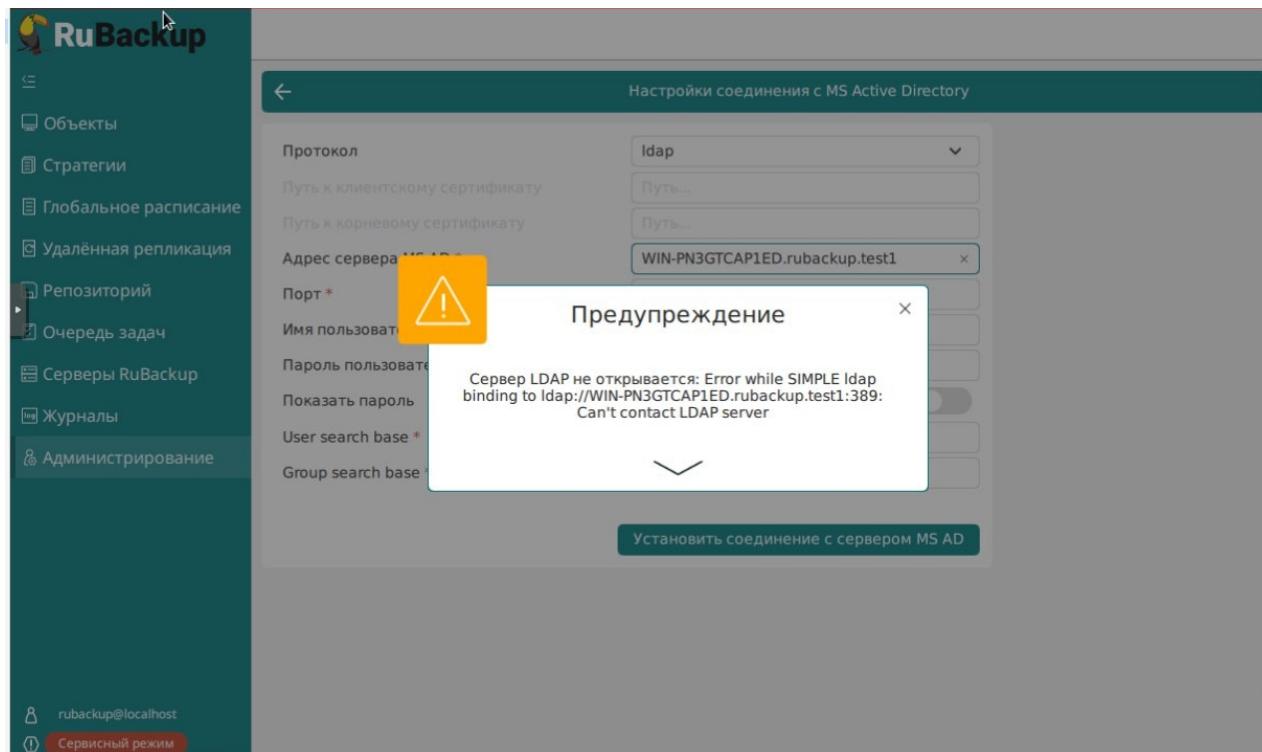
При выборе LDAPS указывается путь к клиентскому и корневому сертификатам Службы сертификации, выдающей сертификаты контроллерам домена.



Сертификаты должны находиться на основном сервере СРК. Проверкой сертификатов будет служить первое подключение к серверу MS AD;

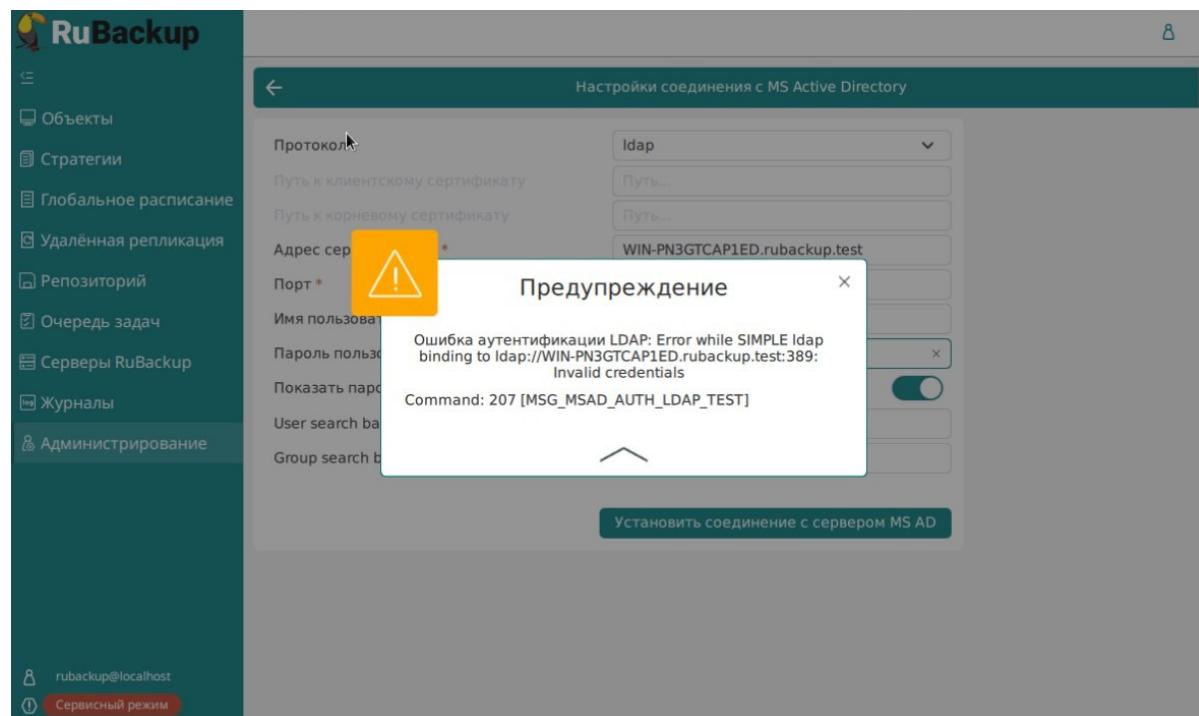
- Адрес сервера MS AD - hostname или ip-адрес для LDAP-протокола, для LDAPS — только hostname.

При установке соединения с неправильным адресом сервера появится предупреждение:

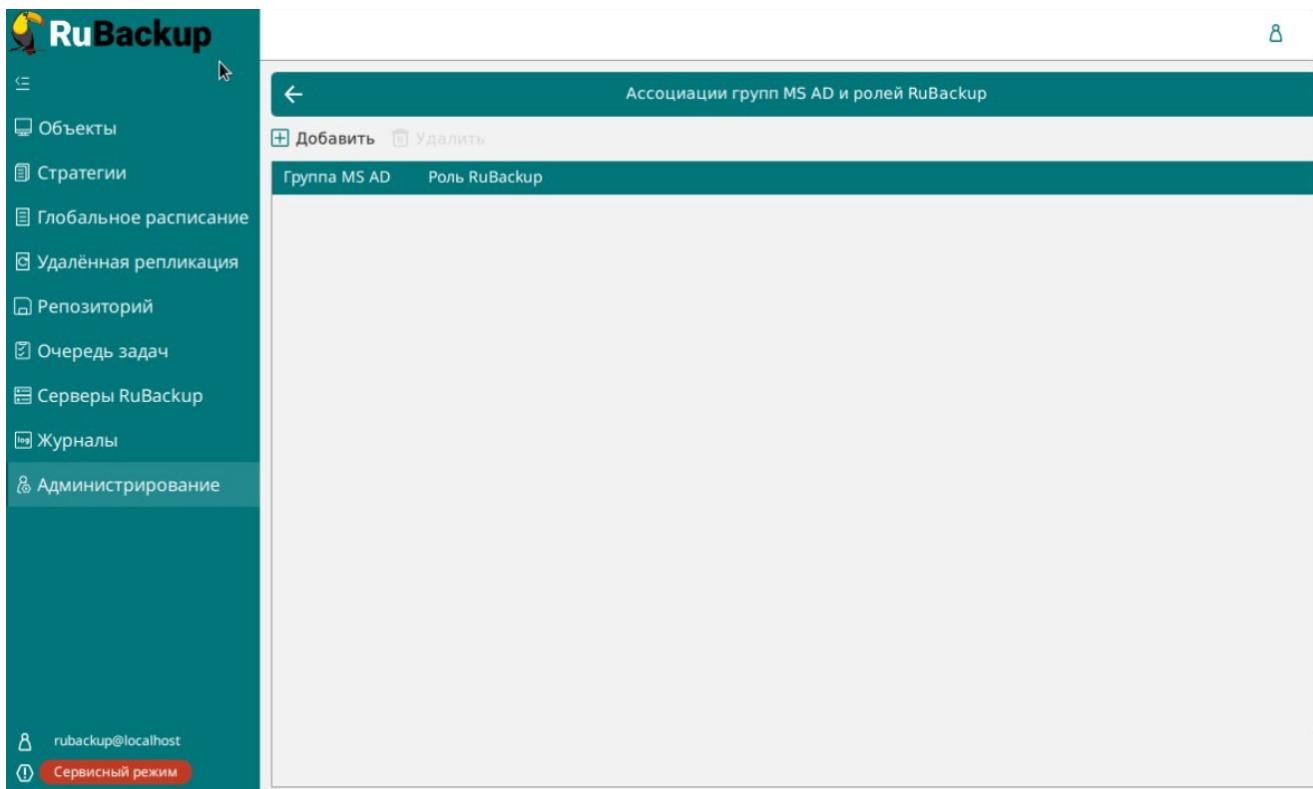


- Порт:
 - Значениями по умолчанию являются — 389 для LDAP, для LDAPS — 636;
- Учетные данные для служебного пользователя Bind User: домен и логин в формате <домен>\<логин>, а также пароль;

При установке соединения с неправильным логином и паролем появится предупреждение:



- 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»:



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

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.

10. Сохраните информацию в RBM, нажав на кнопку «Применить».
11. Деактивируйте сервисный режим.
12. Настройка СРК для работы с MS AD успешно завершена.

Выбор типа аутентификации по умолчанию

1. Активируйте в RBM сервисный режим СРК.

The screenshot shows the RuBackup management interface. On the right side, there is a sidebar with various configuration options. One of the items is 'Сервисный режим' (Service mode), which is currently turned on, indicated by a green switch icon. Other options in the sidebar include 'Глобальная конфигурация...' (Global configuration...), 'Настройки интерфейса' (Interface settings...), 'Поддержка...' (Support...), and 'О RuBackup...' (About RuBackup...). The main dashboard area displays various metrics and charts related to backup tasks, storage capacity, and server status.

2. Перейдите во вкладку «Глобальная конфигурация».

The screenshot shows the RuBackup web interface. On the left is a sidebar with navigation items: Объекты, Стратегии, Глобальное расписание, Удалённая репликация, Репозиторий, Очередь задач, Серверы RuBackup, Журналы, and Администрирование. The Администрирование item is selected. In the main area, a sub-menu titled 'Общее' is open, showing various global configuration settings. A large 'Применить' (Apply) button is visible in the top right corner of the configuration panel.

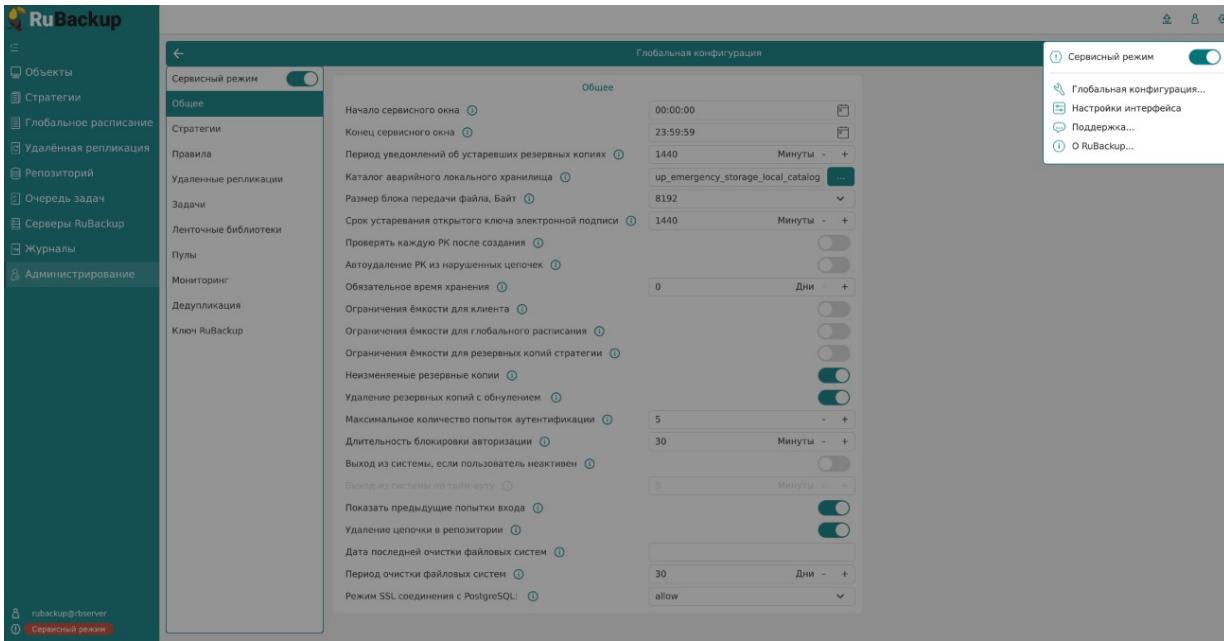
3. Перейдите в раздел с настройками аутентификации.

The screenshot shows the 'Аутентификация' (Authentication) section. It includes fields for 'Максимальное количество попыток аутентификации' (5), 'Длительность блокировки аутентификации' (30 минут), 'Показать предыдущие попытки входа' (enabled), 'Тип аутентификации по умолчанию' (set to 'MS Active Directory'), 'Выход из системы, если пользователь неактивен' (disabled), and 'Выход из системы по тайм-ауту' (5 минут). A 'Сохранить' (Save) button is located at the bottom right of the form.

4. Выберите тип аутентификации по умолчанию - MS Active Directory;.

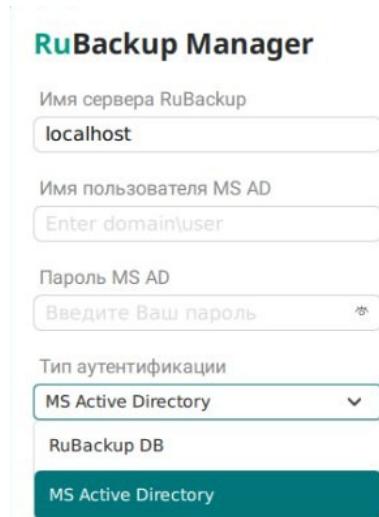
5. Сохраните настройки в RBM нажатием кнопки «Применить».

6. Деактивируйте сервисный режим.



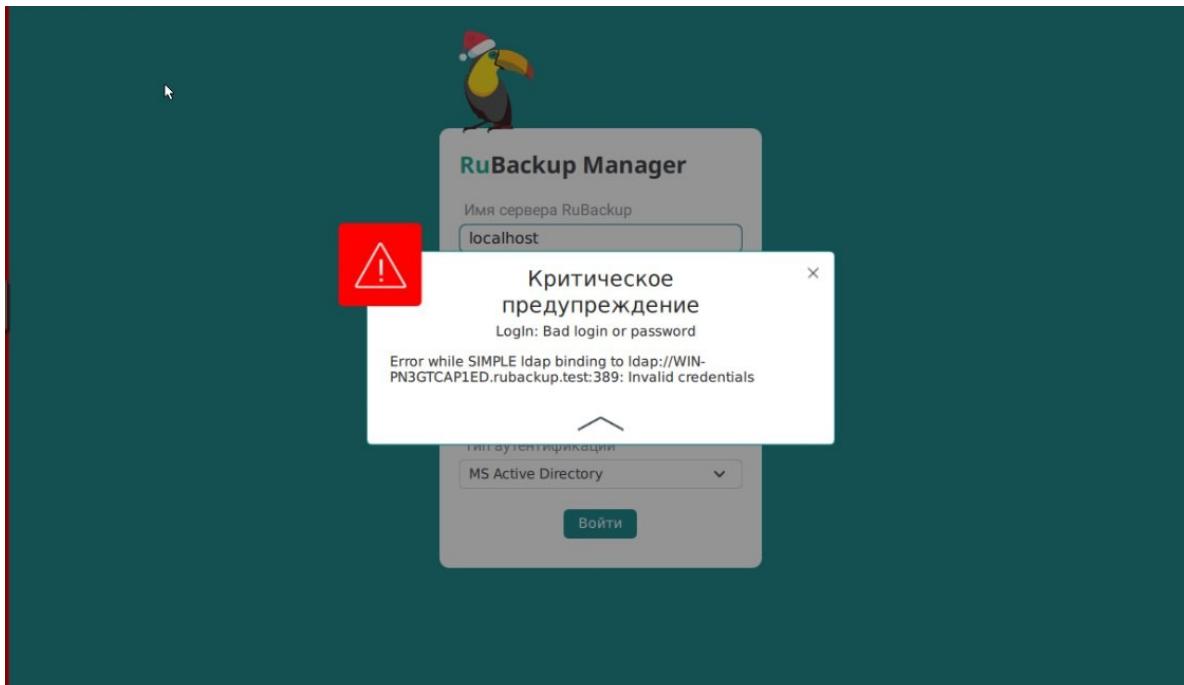
Аутентификация пользователя СРК посредством MS AD

1. Запустите RBM.
2. Появится окно для ввода логина и пароля с выпадающим списком, в котором Вы можете выбрать тип аутентификации.



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

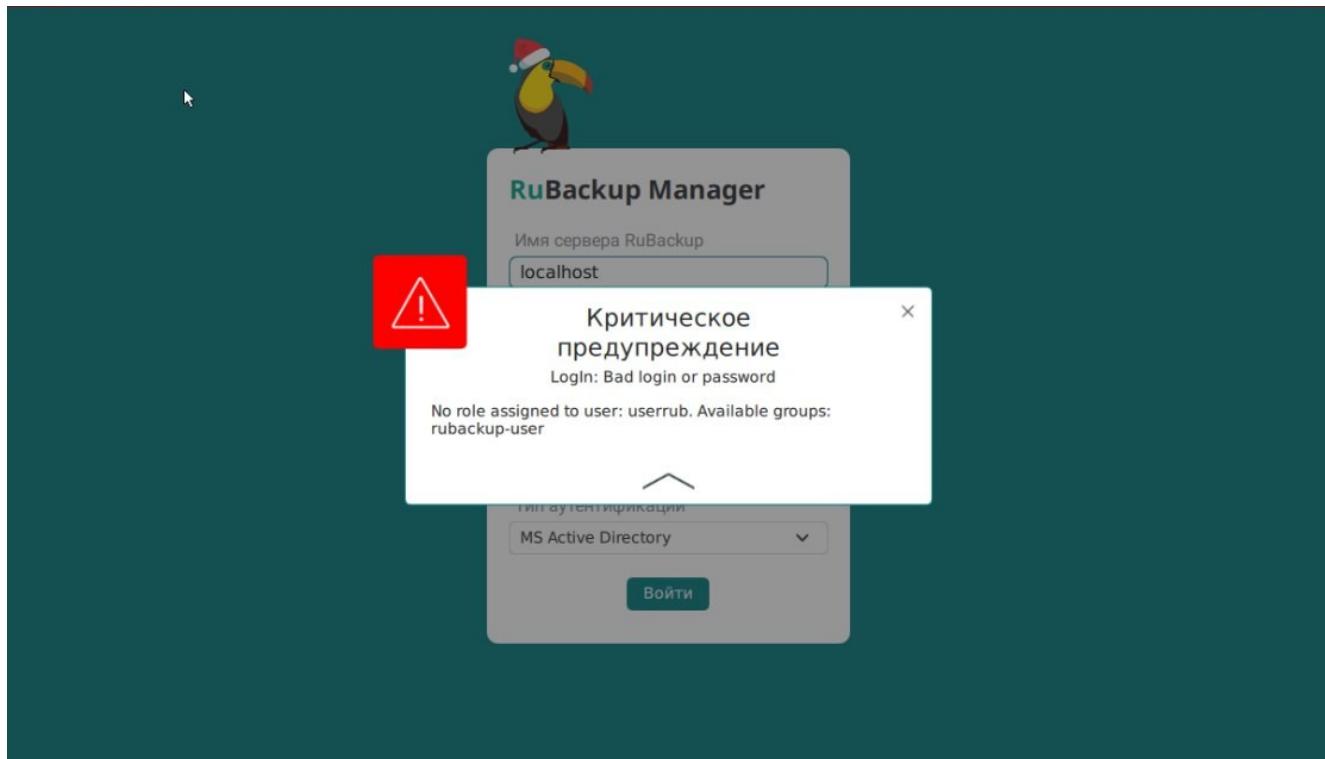
- 2.1. Выберите в выпадающем списке «MS Active Directory».
3. Введите в RBM:
 - 3.1. Домен и логин от учетной записи MS AD в формате <домен>\<пароль>.
 - 3.2. Пароль от учетной записи MS AD.
4. Войдите в СРК нажатием на кнопку «Войти»
5. Если аутентификационные данные введены неверно, RBM выводит сообщение об ошибке с текстом: «Неверно введены логин или пароль»:



В этом случае:

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

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

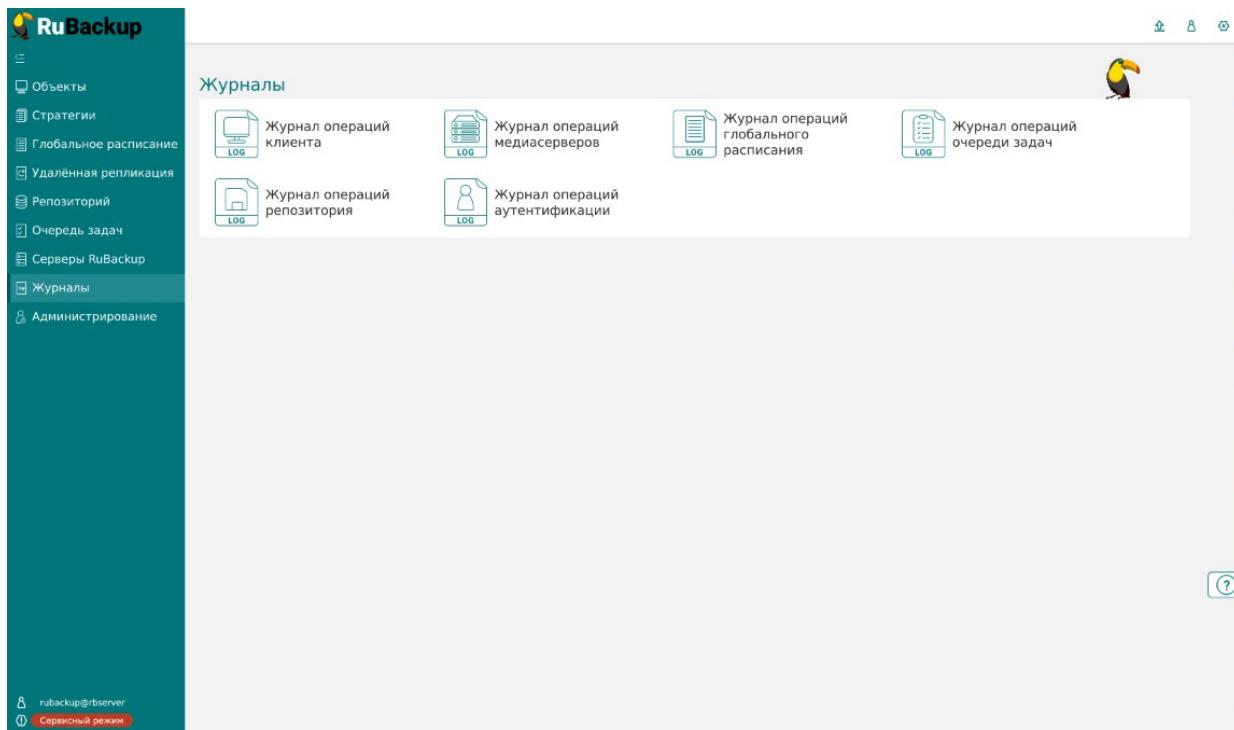


- 7.1. Обратитесь к администратору MS AD для добавления данного пользователя средствами MS AD в необходимую группу MS AD, соответствующую его роли доступа в СРК.
- 7.2. Выполните шаги из данного раздела с начала.

Аудит аутентификации пользователей

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

1. Перейдите в пункт меню «Журналы», выберите «Журнал операций аутентификации».



2. В данном разделе Вы можете проанализировать успешные и неудачные попытки аутентификации, а также их количество.

| Страна | Имя пользователя | Действие | Успешно | Удалённый IP | Дата/Время |
|--------|------------------|-------------|---------|--------------|----------------|
| 94 | rubackup | Connected | true | 172.18.0.1 | 2023.12.11 11: |
| 93 | rubackup | Connected | true | 172.18.0.1 | 2023.12.10 22: |
| 92 | rubackup | Disconnecte | true | 172.18.0.1 | 2023.12.10 22: |
| 91 | rubackup | Connected | true | 172.18.0.1 | 2023.12.10 22: |
| 90 | rubackup | Connected | true | 172.18.0.1 | 2023.12.09 11: |
| 89 | rubackup | Connected | true | 172.18.0.1 | 2023.12.08 15: |
| 88 | rubackup | Connected | false | 172.18.0.1 | 2023.12.08 14: |
| 87 | rubackup | Connected | false | 172.18.0.1 | 2023.12.08 14: |
| 86 | rubackup | Disconnecte | true | 172.18.0.1 | 2023.12.08 14: |
| 85 | rubackup | Connected | true | 172.18.0.1 | 2023.12.08 14: |
| 84 | rubackup | Disconnecte | true | 172.18.0.1 | 2023.12.08 14: |
| 83 | rubackup | Connected | true | 172.18.0.1 | 2023.12.08 13: |
| 82 | rubackup | Connected | true | 172.18.0.1 | 2023.12.06 21: |
| 81 | rubackup | Connected | true | 172.18.0.1 | 2023.12.06 09: |
| 80 | rubackup | Connected | true | 172.18.0.1 | 2023.12.05 17: |
| 79 | rubackup | Connected | true | 172.18.0.1 | 2023.12.05 15: |
| 78 | rubackup | Connected | true | 172.18.0.1 | 2023.12.05 14: |
| 77 | rubackup | Disconnecte | true | 172.18.0.1 | 2023.12.05 09: |
| 76 | rubackup | Connected | true | 172.18.0.1 | 2023.12.05 09: |
| 75 | rubackup | Connected | true | 172.18.0.1 | 2023.12.04 18: |
| 74 | rubackup | Connected | true | 172.18.0.1 | 2023.12.04 17: |
| 73 | rubackup | Connected | true | 172.18.0.1 | 2023.12.01 17: |
| 72 | rubackup | Connected | false | 172.18.0.1 | 2023.12.01 17: |
| 71 | rubackup | Connected | true | 172.18.0.1 | 2023.12.01 10: |
| 70 | rubackup | Connected | true | 172.18.0.1 | 2023.12.01 10: |
| 69 | rubackup | Connected | true | 172.18.0.1 | 2023.11.29 15: |
| 68 | rubackup | Connected | true | 172.18.0.1 | 2023.11.27 17: |
| 67 | rubackup | Connected | true | 172.18.0.1 | 2023.11.15 10: |

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 CPK 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 CPK, 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 CPK к группам MS AD, использующимся для аутентификации в CPK RuBackup.
 - 2.4. Если найденная ошибка связана с внутренней ошибкой CPK, обратитесь в службу технической поддержки продукта CPK, предоставив информацию о выполненных шагах и журнал логов.
3. Проверьте доступность сервера MS AD, валидность наименований групп доступа и учетных записей, устранитте 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 РК. Аутентификация клиентов РК 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 СРК для изменения настроек аутентификации, а также для решения других внештатных ситуаций.

- Аутентификация с использованием MS AD не распространяется на утилиты командной строки (CLI).