Интеграция с Active Directory в платформе виртуализации РУСТЭК

2022

Содержание

ВВЕДЕНИЕ

В платформе РУСТЭК есть возможность использовать Active Directory (далее AD) как внешний сервер аутентификации. Пользователи, находящиеся в AD и помещенные в определенную группу, могут аутентифицироваться на платформе РУСТЭК для управления инфраструктурой.

1 Настройка сервера AD

Для интеграции с AD сначала необходимо выполнить соответствующую настройку.

В первую очередь следует создать пользователя с правами вывода списка остальных пользователей РУСТЭК и установить для него пароль (рисунок 1).

⚠ Данного пользователя, как и других пользователей для РУСТЭК, необходимо создавать только в контейнере, который создан по умолчанию AD – "Users".

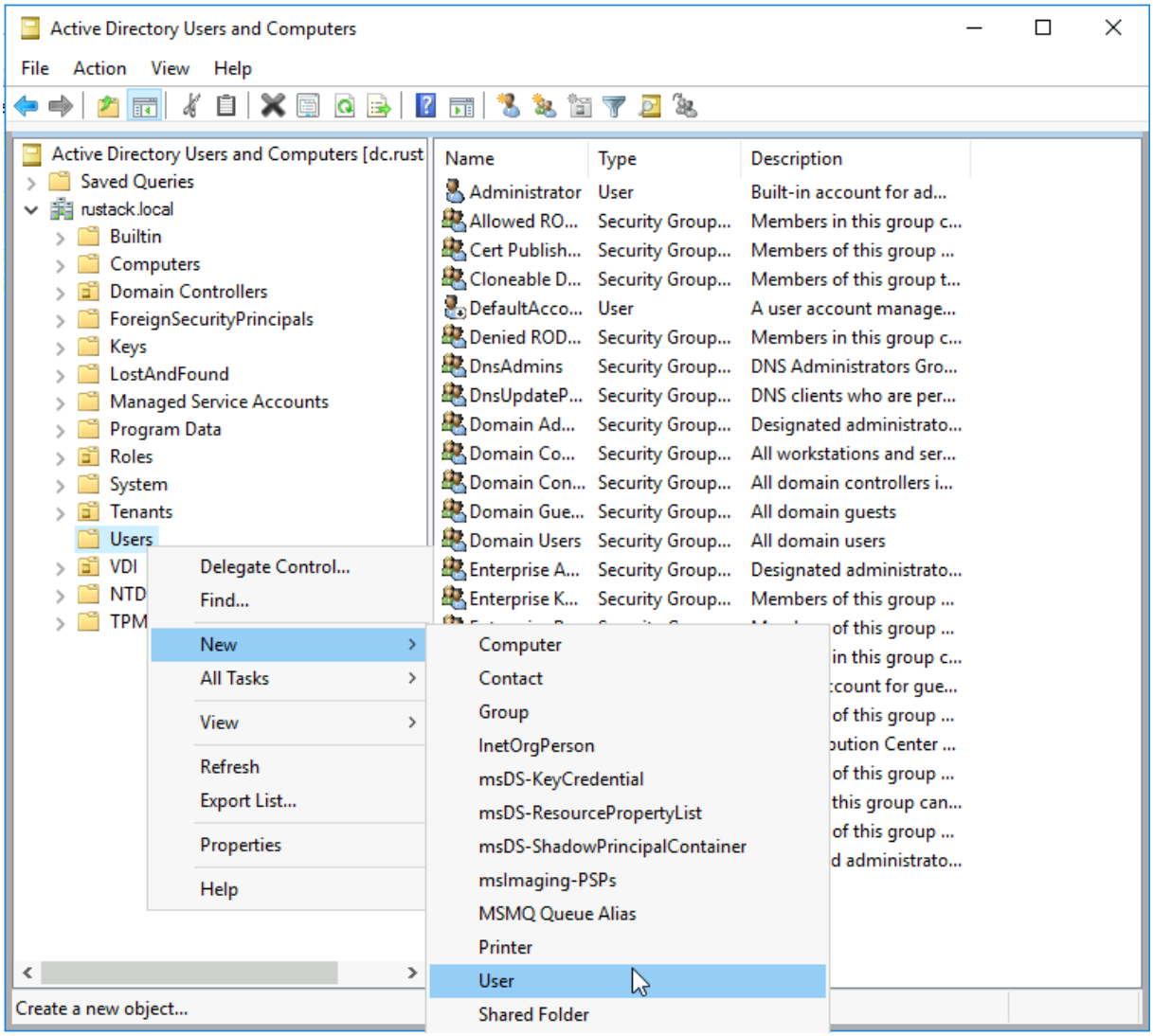

Рисунок 1. Создание нового пользователя

Затем необходимо создать группу, позволяющую добавлять (создавать) в неё других пользователей РУСТЭК (рисунок 2).

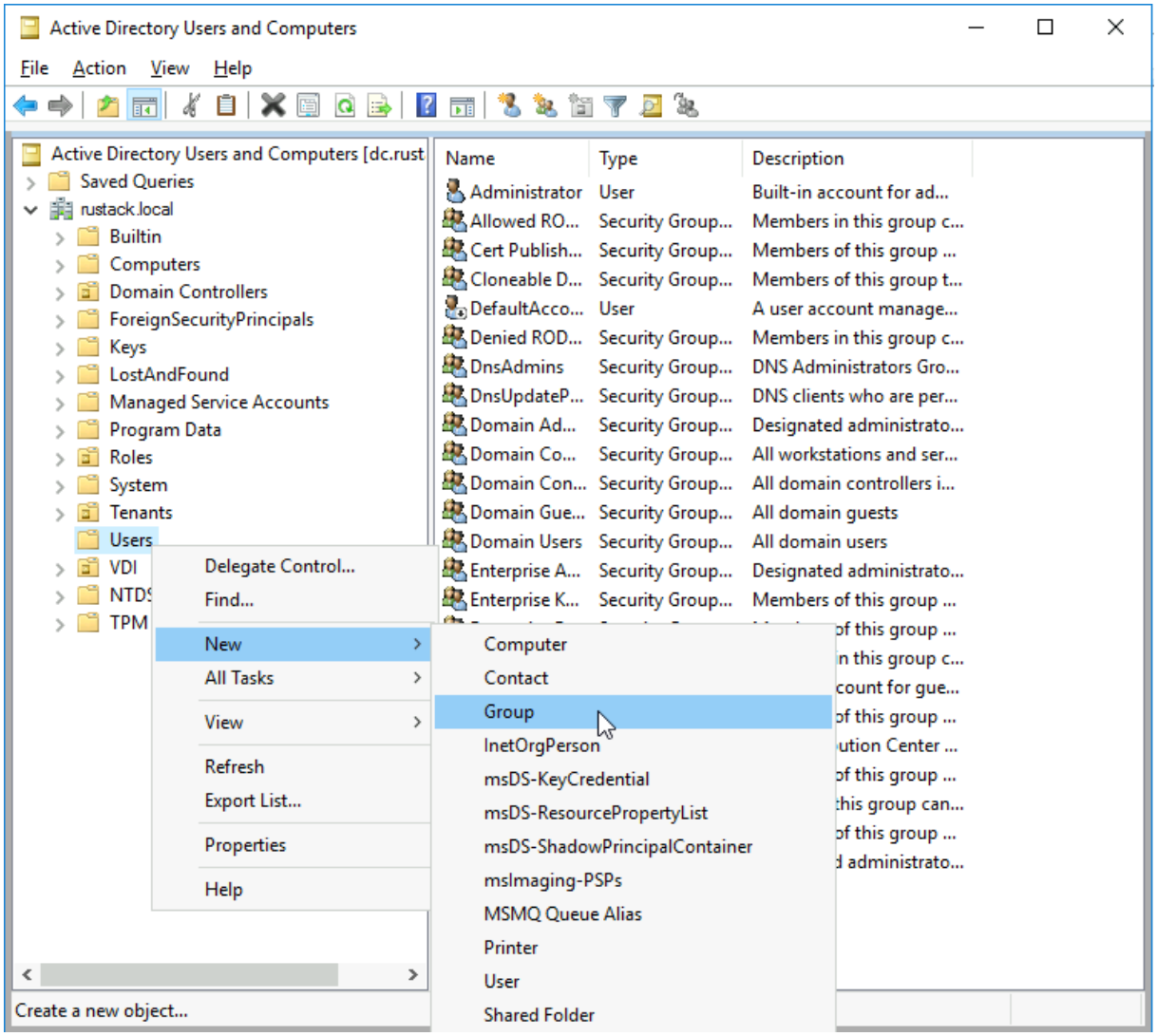

Рисунок 2. Создание новой группы

⚠ Все пользователи должны находиться в контейнере "Users".

Теперь можно создавать других пользователей, задавать им пароль, либо добавлять существующих из AD в созданную группу (рисунок 3).

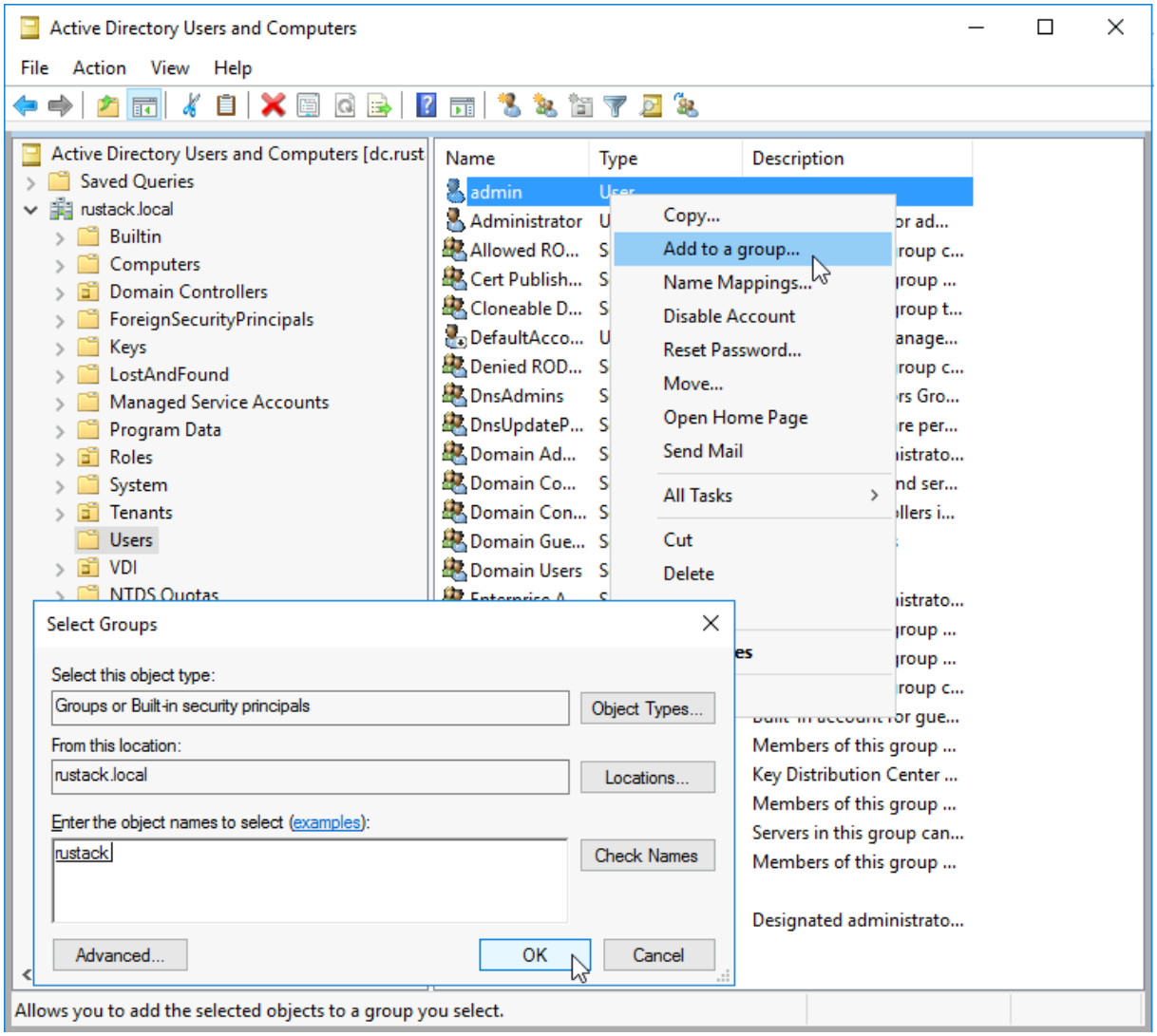

Рисунок 3. Добавление в группу

После выполнения указанных выше действий настройка со стороны AD считается завершённой. Далее необходимо выполнить настройку в конфигураторе РУСТЭК.

2 Настройка конфигуратора РУСТЭК

Для настройки AD в конфигураторе РУСТЭК необходимо перейти в раздел «Интеграция с Active Directory», заполнить все необходимые поля и поставить флажок X в поле «Интеграция с AD» (рисунок 4).

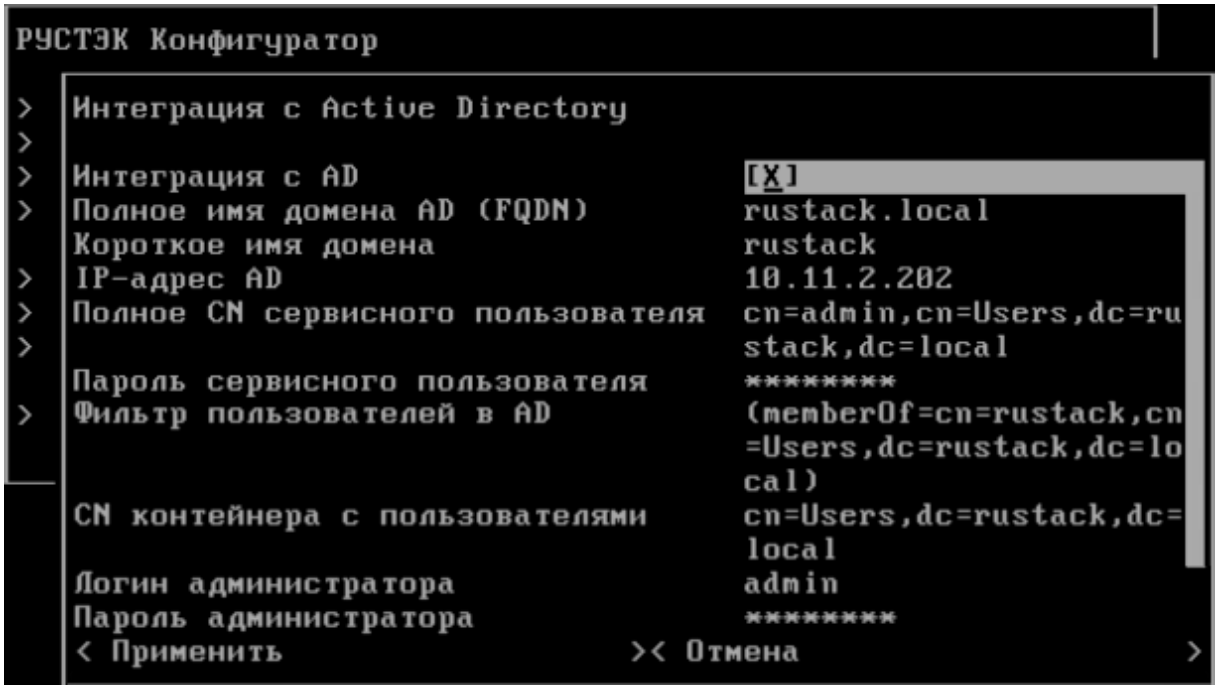

Рисунок 4. РУСТЭК Конфигуратор. Интеграция с AD

В таблице 1 представлено описание полей для заполнения.

Таблица 1. Поля для заполнения в окне **Интеграция с AD** в РУСТЭК Конфигураторе

Параметр	**Описание**
Полное имя домена AD (FQDN)	Полное имя домена, использующееся в AD, без точки в конце
Короткое имя домена	Имя, получаемое с сервера AD, указано в свойствах домена (рисунок 5)
IP-адрес AD	IP-адрес сервера AD
Полное CN сервисного пользователя	Имя пользователя в формате distinguishedName
Пароль сервисного пользователя	Пароль сервисного пользователя, который задавался при его создании в AD
Фильтр пользователей в AD	Фильтр, по которому будет происходит поиск пользователей, указанных в группе (создана ранее в AD)
CN контейнер с пользователями	Контейнер, в котором находятся пользователи для интеграции с РУСТЭК (только созданный по умолчанию - "Users")
Логин администратора	Пользователь (только admin), который будет создан в РУСТЭК для управления пользователями из AD (также пользователями из AD может управлять администратор РУСТЭК)
Пароль администратора	Пароль администратора, который будет создан в РУСТЭК

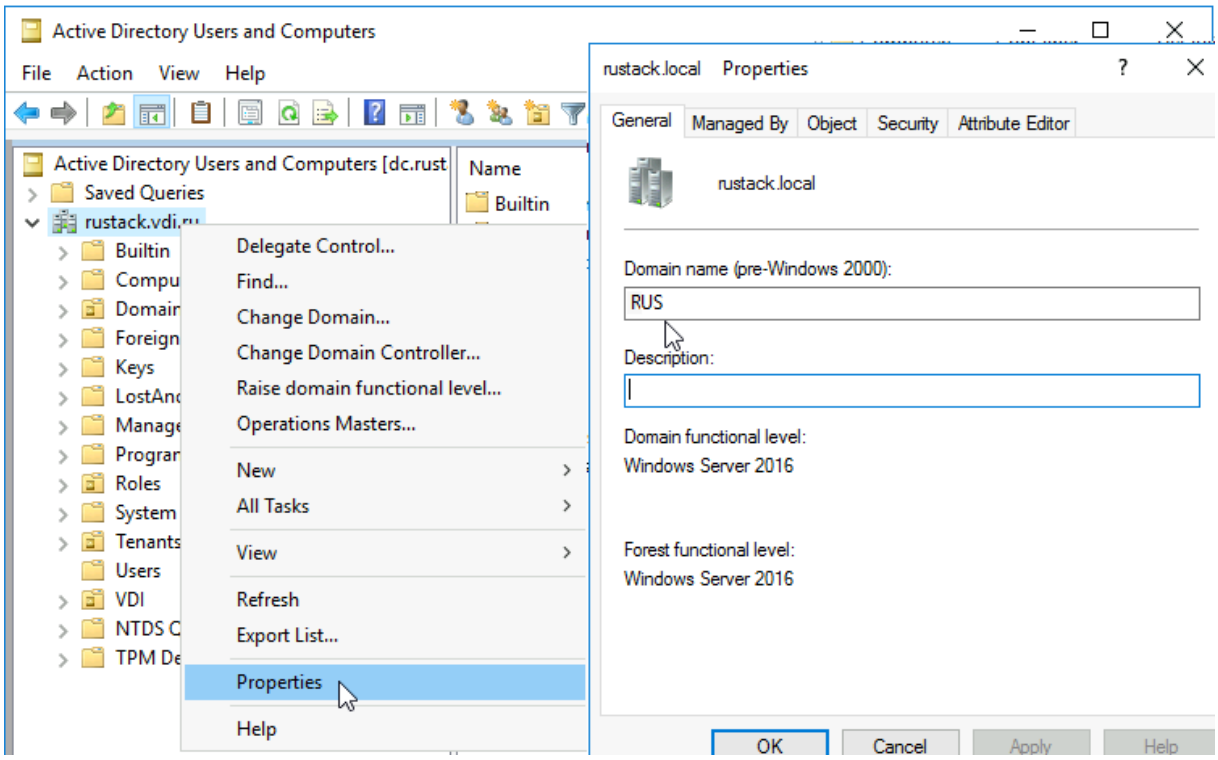

Рисунок 5. Имя домена, получаемое с сервера AD

После полной настройки конфигуратора РУСТЭК (см. документы «Установка РУСТЭК. Быстрый старт» и «Описание конфигуратора РУСТЭК») и применения конфигурации РУСТЭК можно управлять пользователями AD в портале РУСТЭК.

3 Управление пользователями AD в портале РУСТЭК

Для авторизации пользователя в портале необходимо ввести имя пользователя AD в формате: <имя@полное имя домена>.

При блокировке пользователя в AD он также блокируется в РУСТЭК.

При удалении пользователя из группы ему запрещена авторизация в РУСТЭК.

4 Варианты поломок и методы их устранения

1. **Выполнена настройка в AD и в конфигураторе, но пользователь не смог зайти в портал**.

   Возможные причины:

   - Пользователь AD не добавлен в соответствующую группу;
   - Пользователь не находится в контейнере по умолчанию «Users»;
   - Неправильно выполнена настройка. Для этого можно проверить доступность AD и список пользователей командой на рисунке 6.

```
ldapsearch -b 'cn=Users,dc=rustack,dc=local' -H ldap://<IP> -w <PASSWORD>  -D cn=admin,cn=Users,dc=rustack,dc=local  '(&(memberOf=cn=rustack,cn=Users,dc=rustack,dc=local)(objectClass=person)(cn=*))'
```

Рисунок 6. Команда для просмотра доступности AD и списка пользователей

Переменные указанные в команде на рисунке 6:

- b – место, где происходит поиск;
- H – URL AD;
- D – указанное в binddn уникальное имя Distinguished Name при подсоединении к каталогу LDAP;
- memberOf... – фильтр для поиска.

2. **При работе в интерфейсе командной строки РУСТЭК некоторые команды Openstack выдают ошибку.**

   На рисунке 7 представлен вид ошибки.

```
You are not authorized to perform the requested action: identity:list_users. (HTTP 403) (Request-ID: req-0c1178ee-8e11-4cd1-98c3-6dcddefc3641)
```

Рисунок 7. Вид ошибки

При работе в интерфейсе командной строки в командах Openstack необходимо указывать параметр *os-cloud*. В качестве примера команда представлена на рисунке 8.

```
openstack --os-cloud rustack_system <команда>
```

Рисунок 8. Команда для параметра *os-cloud*