Ролевая система

Окружение

- **Версия ПО:** redadm-2.0.0

В РЕД АДМ контроль доступа реализован с помощью ролевой системы (Role Based Access Control, RBAC), что позволяет гибко настраивать права на любой объект системы: можно не настраивать права для каждого пользователя отдельно, а создать роли с нужными правами и добавлять в них пользователей.

Субъекты доступа

По умолчанию администратор домена является главным администратором в РЕД АДМ. Не рекомендуется использовать эту учётную запись для повседневной эксплуатации, предпочтительным вариантом является назначение необходимых ролей другим доменным пользователям.

Ролевая система в РЕД АДМ назначает права только на собственный функционал. Таким образом, если администратору РЕД АДМ не назначать права на редактирование объектов в домене, то он не сможет редактировать учётные записи пользователей.

Примечание.

Права на объекты в домене управляются контроллером домена.

ВАЖНО!

После первого входа администратором домена или служебным доменным пользователем -- все учётные записи домена, которые имеют атрибут adminCount, будут по умолчанию являться администраторами РЕД АДМ.

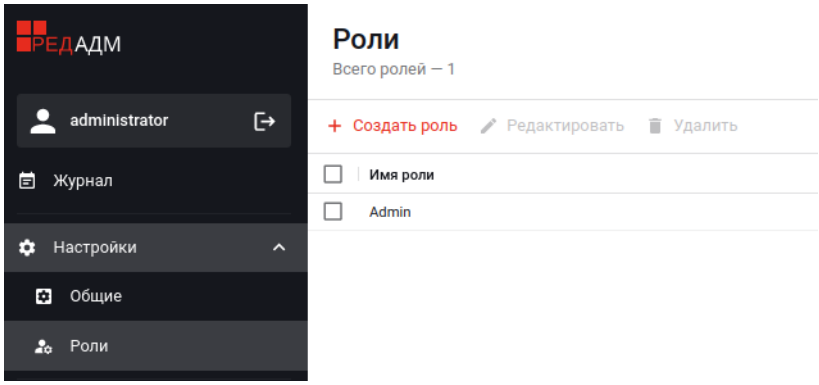
По умолчанию существует группа Administrators. Её членам будет доступен весь функционал РЕД АДМ.

Вы можете добавлять пользователей в стандартную роль Admin, им будут доступны все привилегии. Роль Admin нельзя удалить.

Для ограниченного функционала необходимо создать отдельную роль.

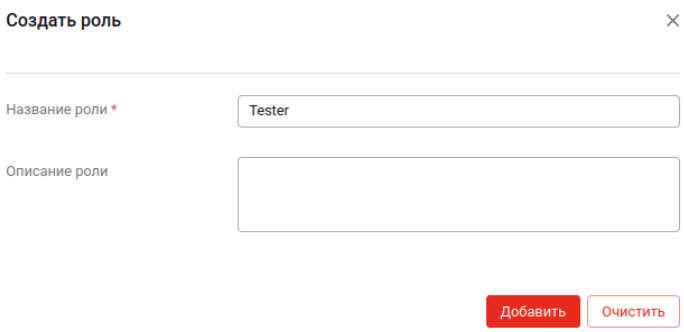
Если в РЕД АДМ необходимо наличие нескольких администраторов с различными привилегиями, создайте требуемое количество учётных записей для таких администраторов в домене или используйте существующие. Затем назначьте им роли в интерфейсе РЕД АДМ на странице «Роли», переход на которую осуществляется нажатием на вкладку «Роли» в раскрывающемся меню «Настройки» основного (бокового) меню (см. рисунок ниже).

Если пользователю запрещен какой-либо модуль, такой модуль пропадет из главного меню и к нему будет запрещено совершать запросы.



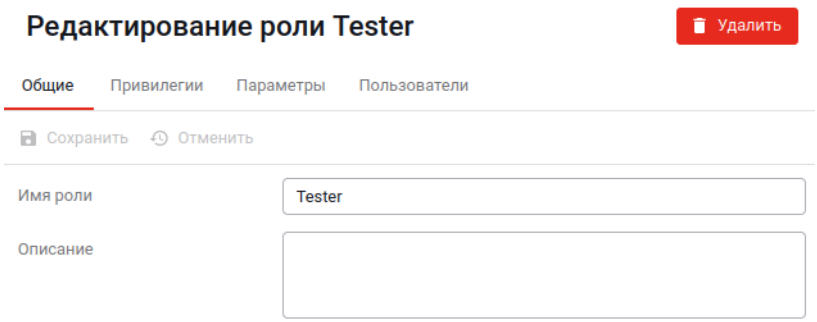
Работа с ролями

Для создания роли нажмите на кнопку «Создать роль». В открывшемся диалоговом окне укажите название роли (обязательное поле) и описание (необязательно поле) и нажмите на кнопку «Добавить» (см. рисунок ниже).



Сразу после этого откроется окно редактирования свойств роли, где можно настроить следующие семейства параметров (для каждого из которых есть соответствующая вкладка):

- привилегии,
- параметры,
- пользователи.



Если вам нужно отредактировать ранее созданную роль, то в меню «Настройки» на вкладке «Роли» выделите нужную роль и нажмите кнопку «Редактировать».

Привилегии подробно описаны в следующем подразделе.

Во вкладке «Параметры конфигурации» можно определить для данной роли то, к каким параметрам конфигурации может быть доступ у данной роли. Доступ разделяется по категориям:

- «Показать настройки»,
- «Создать настройки»,
- «Удалить настройки».

Вкладка «Пользователи» предназначена для изменения области применения роли (списка пользователей, которым эта роль назначена) -- в ней можно добавить или удалить необходимых пользователей (из числа имеющихся).

Объекты доступа и привилегии

Назначать привилегии (права) возможно на следующие основные объекты:

- конфигурации,
- авторизация,
- журнал,
- дашборд,
- контроллер LDAP,
- внедоменные узлы,
- ролевая система,
- справка.

Ролевая система в РЕД АДМ назначает права только на собственный функционал.

Конфигурации

Вы можете разграничить права на любые действия с конфигурациями (задайте в параметрах конфигурации необходимые разрешения):

-- «Просмотр списка конфигураций»;

-- «Просмотр конфигурации»;

-- «Создание конфигурации»;

-- «Обновление конфигурации»;

-- «Принудительный запуск конфигурации»;

-- «Экспорт конфигурации»;

-- «Импорт конфигурации»;

-- «Удаление конфигурации» -- позволяет удалять конфигурации;

-- «Создание области применения»;

-- «Обновление области применения»;

-- «Удаление области применения»;

-- «Создание планировщика» -- позволяет создать планировщик в конфигурации;

-- «Просмотр интервала обновления в области применения»;

-- «Обновление интервала обновления области применения»;

-- «Просмотр настроек кэша»;

-- «Обновление настроек кэша»;

-- «Просмотр планировщика»;

-- «Обновление планировщика»;

-- «Удаление планировщика».

Авторизация

К авторизации относятся следующие права:

-- «Получение jwt токена» -- позволяет получить права на использование

функционала РЕД АДМ. Необходимы права «Авторизация»;

-- «UserAuthorization» -- позволяет пользователю авторизоваться в веб-интерфейсе РЕД АДМ.

Журнал

К действиям с журналом относятся следующие права:

-- «Просмотр всех записей задач» -- позволяет увидеть и фильтровать задачи;

-- «Подробный просмотр задачи» -- позволяет увидеть подробную информацию о задаче. Необходимы права «Просмотр всех записей задач»;

-- «Просмотр всех записей событий» -- позволяет увидеть и фильтровать события;

-- «Подробный просмотр события» -- позволяет увидеть подробную информацию о событии. Необходимы права «Просмотр всех записей событий»;

-- «Экспорт событий в файл»;

-- «Экспорт задач в файл».

Дашбоард

К дашборду относятся следующие права:

-- «Просмотр количества настроек» -- позволяет увидеть, сколько всего настроек конфигураций было создано;

-- «Просмотр графика выполнения задач» -- позволяет просматривать статус выполнения задач в графике;

-- «Просмотр количества успешно распространенных клиентских приложений» -- количество подключенных компьютеров;

-- «Просмотр количества пользователей, на которых применялась конфигурация» -- количество авторизовавшихся пользователей;

-- «Просмотр количества конфигураций».

Контроллер LDAP

К правам данной категории относятся:

-- «Просмотр LDAP каталога» -- позволяет просматривать LDAP каталог (Подразделения, Пользователи, Компьютеры, Группы). Необходимы права: «Расширенный просмотр LDAP объектов», «Получение схемы LDAP»;

-- «Создание объекта в LDAP каталоге» -- позволяет создавать объекты (Подразделения, Пользователи, Компьютеры, Группы). Необходимы права «Просмотр LDAP каталога», «Изменение LDAP объекта», «Получение схемы LDAP»;

-- «Удаление объекта в LDAP каталоге» -- позволяет удалять объекты (Подразделения, Пользователи, Компьютеры, Группы). Необходимы права «Просмотр LDAP каталога»;

-- «Изменение LDAP объекта» -- позволяет изменять объекты LDAP каталога. Необходимы права «Просмотр LDAP каталога» и «Подробный просмотр объекта LDAP»;

-- «Добавление объекта в группу LDAP» -- позволяет добавлять объекты в группы. Необходимы права:

- «Просмотр LDAP каталога»,
- «Изменение LDAP объекта»,
- «Добавление объекта в группу LDAP»,
- «Подробный просмотр объекта LDAP»,
- «Просмотр объектов, входящих в группу LDAP»

-- «Удаление объекта в группе LDAP» -- позволяет удалять объекты из группы. Необходимы права:

- «Просмотр LDAP каталога»,
- «Изменение LDAP объекта»,
- «Добавление объекта в группу LDAP»,
- «Подробный просмотр объекта LDAP»,
- «Просмотр объектов, входящих в группу LDAP»

-- «Перемещение объекта LDAP». Необходимы права «Просмотр LDAP каталога»;

-- «Подробный просмотр объекта LDAP» -- позвляет просматривать общую информацию об объекте. Необходимы права «Просмотр LDAP каталога». При необходимости просмотра результирующей конфигурации и членства в группах необходимо выдать соответствующие права;

-- «Просмотр объектов, входящих в группу LDAP» -- позволяет увидеть объекты в группе. Необходимы права «Просмотр LDAP каталога» и «Подробный просмотр объекта LDAP»;

-- «Расширенный просмотр LDAP объектов» -- позволяет просматривать подробную информацию об объекте. Необходимы права: «Просмотр LDAP каталога», «Подробный просмотр объекта LDAP», «Получение схемы LDAP ». При необходимости просмотра результирующей конфигурации и членства в группах необходимо выдать соответствующие права;

-- «Расширенное создание объектов LDAP»;

-- «Получение схемы LDAP» -- позволяет предоставить пользователю перечень LDAP объектов. Необходимы права «Расширенный просмотр LDAP объектов»;

-- «Удаление вложенных объектов LDAP»;

-- «Перемещение/переименование объектов LDAP».

Для того чтобы пользоваться этими правами, у пользователя должны быть права на управление доменом.

Внедоменные узлы

К работе с внедоменными узлами относятся следующие права:

-- «Создание группы для внедоменных конфигураций» -- позволяет создать группы для внедоменных конфигураций. Необходимы права «Просмотр всех групп для внедоменных конфигураций»;

-- «Удаление группы для внедоменных конфигураций» -- позволяет удалять группы для внедоменных конфигураций. Необходимы права «Просмотр всех групп для внедоменных конфигураций»;

-- «Просмотр всех групп для внедоменных конфигураций» -- позволяет просматривать все группы для внедоменных конфигураций;

-- «Подробный просмотр группы для внедоменных конфигураций» -- позволяет увидеть название группы, её описание и внедоменные узлы, входящие в эту группу. Необходимы права «Просмотр всех групп для внедоменных конфигураций». Для просмотра результирующей конфигурации необходимы права «Просмотр

результирующей конфигурации для внедоменых узлов»;

-- «Изменение группы для внедоменных конфигураций» -- позволяет изменять состав группы для внедоменных конфигураций. Необходимые права:

- «Просмотр всех групп для внедоменных конфигураций»,
- «Просмотр всех узлов для внедоменных конфигураций»,
- «Подробный просмотр группы для внедоменных конфигураций»;

-- «Создание узла для внедоменных конфигураций» -- позволяет добавлять внедоменные узлы. Необходимы права «Просмотр всех узлов для внедоменных конфигураций»;

-- «Удаление узла для внедоменных конфигураций» -- позволяет удалять внедоменные узлы. Необходимы права «Просмотр всех узлов для внедоменных конфигураций»;

-- «Просмотр всех узлов для внедоменных конфигураций» -- позволяет просматривать все подключенные внедоменные узлы;

-- «Подробный просмотр узла для внедоменных конфигураций» -- позволяет просматривать подробную информацию узла -- в какой группе состоит, результирующая конфигурация. Должны быть права:

- «Просмотр всех узлов для внедоменных конфигураций»,
- «Просмотр результирующей конфигурации для внедоменных узлов»,
- «Просмотр настроек и конфигурации для внедоменных узлов»,
- «Просмотр настроек конфигурации для внедоменных узлов»;

-- «Изменение узла для внедоменных конфигураций» -- позволяет изменить настройки внедоменнного узла, такие как «Активность», «Описание» и «Членство в группе». Должны быть права:

- «Просмотр всех групп для внедоменных конфигураций»,
- «Изменение группы для внедоменных конфигураций»,

- «Просмотр всех узлов для внедоменных конфигураций»,
- «Подробный просмотр узла для внедоменных конфигураций»;

-- «Просмотр результирующей конфигурации для внедоменных узлов» -- позволяет просматривать результирующую конфигурацию внедоменных узлов. Необходимы права:

- «Просмотр всех узлов для внедоменных конфигураций»,
- «Подробный просмотр узла для внедоменных конфигураций»,
- «Просмотр настроек конфигураций для внедоменных узлов»,
- «Просмотр конфигурации для внедоменных узлов»,
- «Подробный просмотр конфигурации для внедоменных узлов»;

-- «Просмотр настроек конфигураций для внедоменных узлов» -- позволяет просматривать созданные конфигурации с настройками. Необходимы права:

- «Просмотр настроек и конфигурации для внедоменных узлов»,
- «Просмотр конфигурации для внедоменных узлов»,
- «Подробный просмотр конфигурации для внедоменных узлов»;

-- «Создание настроек конфигураций для внедоменных узлов» -- позволяет создавать настройки для конфигураций. Необходимы права:

- «Просмотр настроек конфигураций для внедоменных узлов»,
- «Просмотр настроек и конфигурации для внедоменных узлов»,
- «Подробный просмотр конфигурации для внедоменных узлов»;

-- «Создание конфигурации для внедоменных узлов» -- позволяет создать конфигурацию для внедоменных узлов, без настроек. Необходимы права

«Просмотр конфигурации для внедоменных узлов»;

-- «Просмотр конфигурации для внедоменных узлов» -- позволяет просматривать список созданных конфигураций без настроек;

-- «Подробный просмотр конфигурации для внедоменных узлов»;

-- «Просмотр настроек и конфигурации для внедоменных узлов» -- просматривать список конфигураций для внедоменных узлов и их настройки. Должны быть выданы права: «Просмотр конфигурации для внедоменных узлов» и «Подробный просмотр конфигурации для внедоменных узлов»;

-- «Удаление конфигурации для внедоменных узлов» -- позволяет удалять конфигурацию. Необходимы права «Просмотр конфигурации для внедоменных узлов»;

-- «Запуск плейбука в режиме push для внедоменных узлов» -- позволяет запускать плейбуки из конфигурации. Необходимы права «Просмотр конфигурации для внедоменных узлов»;

-- «Удаление настройки»;

-- «Изменение конфигурации для внедоменных узлов» -- позволяет изменять конфигурацию. Необходимы права: «Просмотр конфигурации для внедоменных узлов»;

-- «Изменение области применения для внедоменных узлов» -- позволяет изменять область применения. Необходимы права: «Просмотр конфигурации для внедоменных узлов» и «Подробный просмотр конфигурации для внедоменных узлов»;

-- «Распространение SSH-ключа» -- позволяет распространить SSH-ключ на внедоменнные узлы. Необходимы права «Проверка SSH-ключа» и «Получение списка узлов»;

-- «Получение статуса внедоменных узлов» -- позволяет пользователю просмотреть статусы существующих внедоменных узлов;

-- «Обновление статуса внедоменных узлов» -- позволяет пользователю осуществлять обновление статусов существующих внедоменных узлов. Необходимы права «Получение статуса внедоменных узлов».

-- «Добавление внедоменных компьютеров».

Ролевая система

К правам данной категории относятся:

-- «Просмотр всех записей ролей» -- позволяет увидеть все созданные в системе роли;

-- «Подробный просмотр роли» -- позволяет увидеть все выданные привилегии и пользователей, входящих в роль. Должны быть выданы права «Просмотр всех записей ролей»;

-- «Изменение роли» -- позволяет редактировать роль. Должны быть выданы права «Просмотр всех записей» и «Подробный просмотр роли»;

-- «Создание роли» -- позволяет создавать новые роли и добавлять туда пользователей. Должный быть выданы права:

- «Просмотр всех записей»,
- «Подробный просмотр роли»,
- «Изменение роли»;

-- «Удаление роли» -- позволяет удалять роль. Должны быть выданы права «Просмотр всех записей»;

-- «Копирование роли РЕД АДМ».

Справка

-- «Просмотр справки»;

-- «Просмотр содержания документов в справке»;

-- «Поиск по справке».

Источник: https://redadm.red-soft.ru/base/red-adm/ra-admin/ra-2-0-0-admin/ra-2-0-0-rolevaya-sistema/