Руководство по администрированию

Red Hat Virtualization 4.3

**Аннотация**

В данном руководстве содержатся сведения и инструкции для администраторов системы виртуализации Red Hat Virtualization.

# Часть I. Администрирование и обслуживание среды виртуализации Red Hat

Для своей работы, среда виртуализации требует администратора. В обязанности администратора входят следующие задачи:

* Управление физическими и виртуальными ресурсами, такими, как хосты и виртуальные машины. Сюда входит добавление хостов и обновление версий ПО на хостах, импорт доменов, преобразование виртуальных машин, созданных на чужих гипервизорах, а также управление пулами виртуальных машин.
* Мониторинг всех системных ресурсов на предмет потенциальных проблем, таких, как чрезмерная нагрузка на один из хостов, недостаток памяти или места на диске, а также выполнение любых необходимых задач (например, миграция ВМ на другие хосты для снижения нагрузки или высвобождение ресурсов путём выключения машин).
* Своевременное реагирование на изменяющиеся требования ВМ (например, обновление версии ОС или выделение большего объёма памяти).
* Управление собственными свойствами объектов с помощью тегов
* Работа с результатами поиска, сохранёнными как общедоступные закладки (<https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.3/html-single/introduction_to_the_administration_portal/index#chap-Bookmarks> )
* Управление параметрами пользователей и настройка уровней полномочий
* Диагностика и решение проблем конкретных пользователей или виртуальных машин в масштабе общих функциональных возможностей системы
* Создание общих и частных отчётов

# Глава 1. Конфигурация глобальных ресурсов

Окно **Параметры** можно открыть из меню Администрирование → Параметры. В этом окне можно настроить такие глобальные ресурсы среды виртуализации Red Hat, как пользователи, роли, системные полномочия, политики планирования задач, типы экземпляров и пулы адресов MAC. Кроме того, в этом окне можно настроить способы взаимодействия пользователей с ресурсами в окружении, также здесь располагается центральная локация для настройки параметров, которые можно применять к нескольким кластерам.

## Роли

Роли — это предварительно настроенный набор привилегий, настройку которых можно выполнить в виртуализированном центре управления. Роли предоставляют доступ и управленческие полномочия к разным уровням ресурсов в дата-центре, а также к конкретным физическим и виртуальным ресурсам.

В условиях многоуровневого администрирования, любые полномочия, применяемые к контейнерному объекту, также применяются ко всем отдельным объектам в этом контейнере. Если, например, роль администратора хоста присвоена пользователю на конкретном хосте, то этот пользователь получает полномочия на выполнение любых доступных действий с хостом, но только на присвоенном хосте. Но если роль администратора хоста будет присвоена пользователю в дата-центре, то этот пользователь получает полномочия на выполнение действий для всех хостов в рамках кластера дата-центра.

### Создание новой роли

Если требуемая роль отсутствует в изначальном списке ролей системы виртуализации Red Hat, то можно создать новую роль и настроить её согласно целевому назначению.

**Добавление роли**

1. Чтобы открыть окно **Параметры**, нажмите Администрирование → Параметры. Вкладка **Роли** выбрана по умолчанию, и здесь показывается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Нажмите **Добавить**.
3. Введите **Имя** и **Описание** новой роли.
4. Для параметра **Тип учётной записи** выберите **Администратор** или **Пользователь**.
5. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть больше или меньше подробностей для полномочий объектов, присутствующих в списке **Чтобы разрешить действие, поставьте галочки**. Также можно развернуть или свернуть параметры для каждого объекта.
6. Для каждого объекта выберите или очистите действия, которые нужно разрешить или запретить в настраиваемой роли.
7. Для применения изменений нажмите **OK**. Новая роль будет показана в списке ролей.

### Изменение или копирование роли

Можно изменять параметры созданной администратором роли, но нельзя изменять роли по умолчанию. Чтобы изменить роль по умолчанию, клонируйте и измените копию роли согласно своим нуждам.

**Изменение или копирование роли**

1. Чтобы открыть окно **Параметры**, нажмите Администрирование → Параметры. В окне показывается список изначальных ролей **Пользователя** и **Администратора**, а также все частные роли.
2. Выберите роль, которую нужно изменить. Чтобы открыть окно **Параметры роли**, нажмите **Изменить**, или же, чтобы открыть окно **Копировать роль**, нажмите **Копировать**.
3. При необходимости, измените **Имя** и **Описание** роли.
4. С помощью кнопок **Развернуть всё** или **Свернуть всё** можно увидеть больше или меньше подробностей для полномочий объектов, присутствующих в списке. Также можно развернуть или свернуть параметры для каждого объекта.
5. Для каждого объекта выберите или очистите действия, которые нужно разрешить или запретить в настраиваемой роли.
6. Для применения внесённых изменений нажмите **OK**.

### Роль «Пользователь» и примеры авторизации

В примерах ниже демонстрируется применение контроля авторизации в различных сценариях с использованием различных возможностей системы авторизации, описываемой в данной главе.

**Пример 1.1. Полномочия для кластера**

Светлана – системный администратор отдела бухгалтерии в своей организации. Все виртуальные ресурсы её отдела организованы в кластер системы виртуализации Red Hat под названием Accounts. В кластере бухгалтерии Светлане присвоена роль **ClusterAdmin**. Это даёт ей возможность администрирования всех виртуальных машин в кластере, поскольку виртуальные машин являются дочерними объектами кластера. Администрирование ВМ включает в себя изменение, добавление или удаление таких виртуальных ресурсов, как диски, а также создание снимков. Её роль не позволяет администрировать никакие ресурсы за пределами кластера. Поскольку **ClusterAdmin** является ролью администратора, то Светлане позволено работать на «Портале администрирования» или на «Портале виртуализированного ЦУ» для управления этими ресурсами.

**Пример 1.2. Полномочия PowerUser на ВМ**

Иван — программист в отделе бухгалтерии. Для сборки и тестирования своих программ он использует виртуальные машины. Светлана создала для него виртуальный рабочий стол с названием ivandesktop. На ВМ со столом ivandesktop Ивану присвоена роль **UserVmManager**, дающая ему доступ с Портала виртуальных машин к этой единственной ВМ. Поскольку Иван обладает полномочиями **UserVmManager, то он может вносить изменения в параметры своей виртуальной машины. А поскольку UserVmManager** является ролью пользователя, то она не даёт ему возможности использовать Портал администрирования.

**Пример 1.3. Полномочия роли PowerUser дата-центра**

Дарья — руководитель отдела. В дополнение к её собственным обязанностям она время от времени помогает менеджеру по персоналу в задачах найма работников, планируя интервью и проверяя рекомендации. Согласно корпоративной политике, для задач найма персонала Дарья должна использовать определённое приложение.

Хотя у Дарьи есть своя собственная машина для задач управления отделом, ей нужно создать отдельную ВМ для запуска приложения с задачами работы по подбору персонала. Ей присвоены полномочия **PowerUserRole** для дата-центра, в котором будет располагаться её новая ВМ, потому что для создания новой виртуальной машины ей нужно внести изменения в некоторые компоненты в границах дата-центра, включая создание виртуального диска в домене хранилища.

Обратите внимание, что это не то же самое, что и присвоение Дарье привилегий **DataCenterAdmin**. В качестве пользователя PowerUser дата-центра, Дарья может входить на Портал ВМ и выполнять действия с виртуальными машинами в границах дата-центра. Но она не может выполнять такие действия на уровне дата-центра, как прикрепление к дата-центру хостов или хранилищ.

**Пример 1.4. Полномочия сетевого администратора**

Наташа работает сетевым администратором в отделе IT. В её ежедневные обязанности входит создание, управление и удаление сетей в окружении виртуализации Red Hat её отдела. Для её роли ей нужны административные привилегии на ресурсы и на сети каждого ресурса. Если, например, у Наташи будут привилегии **NetworkAdmin в дата-центре отдела IT**, то она сможет добавлять и удалять сети в дата-центре, а также присоединять и отсоединять сети для всех ВМ, принадлежащих дата-центру.

**Пример 1.5. Полномочия частной роли**

Раиса работает в отделе IT и отвечает за управление учётными записями пользователей в системе виртуализации Red Hat. Ей нужны полномочия для добавления учётных записей пользователей и для присвоения им соответствующих ролей и полномочий. Сама она не использует никаких виртуальных машин, и не должна иметь доступа к администрированию хостов, ВМ, кластеров или дата-центров. Такой встроенной роли, которая предоставляла бы ей этот конкретный набор полномочий, не существует. Для настройки набора полномочий, соответствующих рабочими обязанностям Раисы, нужно создать частную роль.

**Рисунок 1.1. Частная роль UserManager**

****

Частная роль **UserManager** на иллюстрации выше разрешает управление пользователями, полномочия и ролями. Эти действия собраны в разделе **Система**, являющимся самым верхним объектом иерархии, показанной на Рисунке 1.3, что означает, что эти действия применимы ко всем другим объектам в системе. **Тип учётной записи**, указанной для этой роли — **Администратор**, а это означает, что после присвоения ей этой роли, Раиса сможет использовать как Портал администрирования, так и Портал ВМ.

# 1.2. Системные полномочия

Полномочия дают пользователям возможность выполнять действия с объектами, где объекты — это либо отдельные объекты, либо контейнерные. Любые полномочия, применяющиеся к контейнерному объекту, также применимы ко всем членам этого контейнера.

**Рисунок 1.2. Полномочия и роли**

****

**Рисунок 1.3. Иерархия объектов системы виртуализации Red Hat**

****

### 1.2.1. Свойства пользователя

Роли и полномочия являются свойствами пользователя. Роли — это предварительно настроенные наборы привилегий, предоставляющих доступ к разным уровням физических и виртуальных ресурсов. Многоуровневое администрирование предоставляет тонко настроенную иерархию полномочий. У администратора дата-центра, например, есть полномочия на управление всеми объектами в дата-центре, в то время как у администратора хоста есть полномочия на управление одним физическим хостом. Один пользователь может иметь полномочия на использование одной ВМ и не иметь полномочий на внесение изменений в параметры ВМ, в то время как у другого пользователя могут иметься системные полномочия на ВМ.

### 1.2.2. Роли пользователей и администраторов

Система виртуализации Red Hat предоставляет широкий диапазон предварительно настроенных ролей, от администратора с системными полномочиями до конечного пользователя с доступом только к одной ВМ. Хотя роли по умолчанию нельзя изменять или удалять, их можно клонировать и редактировать, а также можно создавать новые роли согласно необходимым требованиям. Сущеcтвует два типа ролей:

* Роль **Администратор**: предоставляет доступ к **Порталу администрирования** для управления физическими и виртуальными ресурсами. Роль администратора присваивает права на выполнение действий на Портале ВМ; тем не менее, она никак не влияет на то, что доступно к просмотру для пользователя на Портале ВМ.
* Роль **Пользователь**: предоставляет доступ к Порталу ВМ для доступа к ВМ и шаблонами и для управления ими. Роль пользователя определяет, что доступно к просмотру для пользователя на Портале ВМ. Полномочия, выданные пользователю с ролью администратора, отражаются на том, какие действия доступны этому пользователю на Портале ВМ.

### 1.2.3. Объяснение ролей пользователей

В таблице ниже описываются базовые роли пользователей, предоставляющие полномочия на доступ к виртуальным машинам и их параметрам на Портале ВМ.

**Таблица 1.1. Базовые роли пользователей в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| UserRole | Доступ и использование ВМ и пулов | Может выполнять вход на Портал ВМ, использовать привязанные к нему виртуальные машины, просматривать статус ВМ и подробные сведения о неё. |
| PowerUserRole | Может создавать ВМ и шаблоны, а также управлять ими. | Присваивайте эту роль пользователю для доступа ко всему окружению в окне Параметры или для доступа к конкретным дата-центрам или кластерам. Если, например, роль PowerUserRole применяется на уровне дата-центра, то пользователь PowerUser может создавать ВМ и шаблоны в дата-центре. |
| UserVmManager | Системный администратор виртуальной машины | Может администрировать ВМ, а также создавать и использовать снимки. Пользователю, создавшему машину на Портале ВМ, автоматически присваивается роль UserVmManager на этой машине. |

В таблице ниже описываются продвинутые роли пользователей, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале ВМ.

**Таблица 1.2. Продвинутые роли пользователей в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| UserTemplateBasedVm | **Привилегии, ограниченные только использованием шаблонов.** | **Может использовать шаблоны для создания виртуальных машин** |
| DiskOperator | **Пользователь виртуального диска** | **Может использовать, просматривать и изменять виртуальные диски. Наследует полномочия на использование ВМ, к которой присоединён виртуальный диск.** |
| VmCreator | **Может создавать виртуальные машины на Портале ВМ** | **Эта роль не применяется конкретной ВМ; присваивайте эту роль пользователю на всё окружение в окне Параметры. Или же присваивайте эту роль для конкретных дата-центров или кластеров. Присваивая роль для кластера, также нужно присваивать роль** DiskCreator для всего дата-центра или для конкретных доменов хранилищ. |
| TemplateCreator | **Может создавать, редактировать и удалять шаблоны ВМ в рамках присвоенных ресурсов.** | **Эта роль не присваивается к конкретному шаблону; присваивайте эту роль пользователю для всего окружения с окном Параметры. Или же присваивайте эту роль для конкретных дата-центров, кластеров или доменов хранилищ.** |
| **DiskCreator** | **Может создавать, редактировать, управлять и удалять виртуальные диски рамках присвоенных кластеров или дата-центров** | **Эта роль не присваивается конкретному виртуальному диску; присваивайте эту роль пользователю для всего окружения с окном Параметры. Или же присваивайте эту роль для конкретных дата-центров, кластеров или доменов хранилищ.** |
| TemplateOwner | **Может изменять и удалять шаблоны, присваивать и управлять полномочиями пользователей на шаблон.** | **Эта роль автоматически присваивается пользователю, создающему шаблон. Другие пользователи, не имеющие полномочий TemplateOwner для шаблона, не могут просматривать или использовать этот шаблон.** |
| VnicProfileUser | **Пользователь логических сетей и сетевых интерфейсов виртуальной машины и шаблона.** | **Может присоединять или отсоединять сетевые интерфейсы конкретных логических сетей.** |

### 1.2.4. Объяснение ролей администратора

В таблице ниже описываются базовые роли администратора, дающие полномочия на доступ и настройку ресурсов на Портале администрирования.

**Таблица 1.3. Базовые роли администраторов в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| SuperUser | **Системный администратор среды виртуализации red hat** | **Полные полномочия на все объекты и уровни, администрирует всеми объектами во всех дата-центрах** |
| ClusterAdmin | **Администратор кластера** | **Обладает административными полномочиями на все объекты в рамках конкретного кластера.** |
| DataCenterAdmin | Администратора дата-центра | **Обладает административными полномочиями на все объекты в рамках конкретного дата-центра, за исключением хранилища.** |

ВАЖНО

Не используйте пользователя-администратора сервера каталогов в качестве пользователя-администратора системы виртуализации red hat. Создайте на сервере каталогов пользователя специально для использования в качестве пользователя-администратора системы виртуализации.

В таблице ниже описываются продвинутые роли администраторов, позволяющие выполнять более тонкую настройку полномочий на ресурсы на Портале администрирования.

**Таблица 1.4. Продвинутые роли администраторов в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| TemplateAdmin | Администратор шаблона ВМ | Может создавать, удалять и настраивать домены хранилищ и сетевые параметры шаблонов, а также перемещать шаблоны между доменами. |
| StorageAdmin | Администратор хранилища | Может создавать, удалять, настраивать и управлять присвоенным доменом хранилищ. |
| HostAdmin | Администратор хоста | Может присоединять, удалять, настраивать и управлять конкретным хостом. |
| NetworkAdmin | Сетевой администратор | Может настраивать и управлять сетью конкретного дата-центра или кластера. Сетевой администратор дата-центра или кластера наследует сетевые полномочия на виртуальные пулы в рамках кластера. |
| VmPoolAdmin | Системный администратор виртуального пула | Может создавать, удалять и настраивать виртуальный пул; присваивать и удалять пользователей виртуального пула; а также выполнять базовые операции на ВМ в пуле. |
| GlusterAdmin | Администратор хранилища Gluster | Может создавать, удалять, настраивать и управлять томами хранилища Gluster. |
| VmImporterExporter | Администратор импорта и экспорта виртуальных машин | Может импортировать и экспортировать ВМ. Имеет возможность посматривать все ВМ и шаблоны, экспортированные другими пользователями. |

### 1.2.5. Присвоение ресурсу роли администратора или пользователя

Присвоение роли администратора или пользователя ресурсу, чтобы дать возможность доступа или управления этим ресурсом.

**Присвоение роли ресурсу**

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Полномочия**, чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.
3. Нажмите **Добавить**.
4. Укажите имя или пользовательское имя существующего пользователя в поле **Поиск** и нажмите **Выполнить**. Из полученного списка возможных совпадений выберите пользователя.
5. В выпадающем списке **Присвоить роль** выберите нужную роль.
6. Нажмите **OK**.

Теперь на указанном ресурсе действуют наследуемые полномочия этой роли для указанного пользователя.

### 1.2.6. Удаление роли администратора или пользователя с ресурса

Удаление роли администратора или пользователя с ресурса; на этом ресурсе пользователь теряет наследуемые полномочия, связанные с ролью.

**Удаление роли с ресурса**

1. Найдите название нужного ресурса и нажмите на него, чтобы просмотреть детали.
2. Перейдите на вкладку **Полномочия**, чтобы указать присвоенных пользователей, роль пользователя и наследуемые полномочия для выбранного ресурса.
3. Выберите пользователя, удаляемого с ресурса.
4. Нажмите **Удалить**.
5. Нажмите **OK**.

### 1.2.7.  Администрирование системных полномочий в дата-центре

В качестве пользователя **SuperUser** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор дата-центра — это роль системного администратора только для конкретного дата-центра. Она удобна в среде виртуализации с несколькими дата-центрами, где каждому дата-центру требуется администратор. Роль **DataCenterAdmin** является иерархической моделью; пользователь, которому назначена роль администратора дата-центра, может управлять всеми объектами в дата-центре за исключением хранилища этого дата-центра. С помощью кнопки **Параметры** на панели заголовков назначайте администраторов дата-центров для всех дата-центров в окружении.

Роль администратора дата-центра разрешает выполнять следующие действия:

* Создание и удаление кластеров, связанных с дата-центром.
* Добавление и удаление хостов, ВМ и пулов, связанных с дата-центром.
* Изменение пользовательских полномочий на виртуальных машинах, связанных с дата-центром.

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

Сменить администратора дата-центра можно, удалив существующего системного администратора и добавив нового.

### 1.2.8. Объяснение роли администратора дата-центра

**Роли с полномочиями в дата-центре**

В таблице ниже описываются административные роли и привилегии, применимые в администрировании дата-центров.

**Таблица 1.5. Административные роли в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| DataCenterAdmin | Администратор дата-центра | Может использовать, создавать, удалять и управлять всеми физическими и виртуальными ресурсами в рамках указанного дата-центра, за исключением хранилища, и включая кластеры, хосты, шаблоны и виртуальные машины. |
| NetworkAdmin | Администратор сети | Может настраивать и управлять сетью конкретного дата-центра. Сетевой администратор дата-центра также наследует сетевые полномочия на виртуальные машины в рамках дата-центра. |

### 1.2.9. Управление системными полномочиями в кластере

В качестве пользователя **SuperUser** системный администратор управляет всеми аспектами Портала администрирования. Другим пользователям можно присваивать более конкретные административные роли. Эти узкоспециализированные административные роли удобны для присвоения пользователю административных привилегий, ограниченных конкретным ресурсом. У роли **DataCenterAdmin**, например, есть административные привилегии только для присвоенного дата-центра, за исключением хранилища этого дата-центра, а у роли **ClusterAdmin** есть административные привилегии только для назначенного кластера.

Администратор кластера — это роль системного администратора только для конкретного кластера. Она удобна в среде виртуализации с несколькими кластерами, где каждому кластеру требуется администратор. Роль **ClusterAdmin** является иерархической моделью; пользователь, которому назначена роль администратора кластера, может управлять всеми объектами в кластере. С помощью кнопки **Параметры** на панели заголовков назначайте администраторов кластеров для всех кластеров в окружении.

Роль администратора кластера разрешает выполнять следующие действия:

* Создание и удаление ассоциированных кластеров.
* Добавление и удаление хостов, ВМ и пулов, связанных с кластером.
* Изменение пользовательских полномочий на виртуальных машинах, связанных с кластером.

ВНИМАНИЕ

Присваивать роли и полномочия можно только существующим пользователям.

Также сменить администратора кластера можно, удалив существующего системного администратора и добавив нового.

### 1.2.10. Объяснение роли администратора кластера

**Роли с полномочиями в кластере**

В таблице ниже описываются административные роли и привилегии, применимые в администрировании кластеров.

**Таблица 1.6. Административные роли в системе виртуализации Red Hat**

|  |  |  |
| --- | --- | --- |
| **Роль** | **Привилегии** | **Примечания** |
| ClusterAdmin | Администратор кластера | Может использовать, создавать и управлять всеми физичсекими и виртуальными ресурсами в конкртеном кластере, включая хосты, аблоны и виртуальные машины. Может настраивать свсойтва сети в рамках калстера, такие, как выделение сетей визуализации или назначение сети как требуемая или не требуемая.  Тем не менее, у **ClusterAdmin** нет полномочий на присоединение или отсоединение сетей от кластера, для этого требуются полномочия **NetworkAdmin.** |
| NetworkAdmin | Администратор сети | Может настраивать и управлять сетью конкретного кластера. Сетевой администратор кластера также наследует сетевые полномочия на виртуальные машины в рамках кластера. |

### 1.2.11. Managing System Permissions for a Network

As the **SuperUser**, the system administrator manages all aspects of the Administration Portal. More specific administrative roles can be assigned to other users. These restricted administrator roles are useful for granting a user administrative privileges that limit them to a specific resource. For example, a **DataCenterAdmin** role has administrator privileges only for the assigned data center with the exception of the storage for that data center, and a **ClusterAdmin** has administrator privileges only for the assigned cluster.

A network administrator is a system administration role that can be applied for a specific network, or for all networks on a data center, cluster, host, virtual machine, or template. A network user can perform limited administration roles, such as viewing and attaching networks on a specific virtual machine or template. You can use the **Configure** button in the header bar to assign a network administrator for all networks in the environment.

The network administrator role permits the following actions:

* Create, edit and remove networks.
* Edit the configuration of the network, including configuring port mirroring.
* Attach and detach networks from resources including clusters and virtual machines.

The user who creates a network is automatically assigned **NetworkAdmin** permissions on the created network. You can also change the administrator of a network by removing the existing administrator and adding the new administrator.

### 1.2.12. Network Administrator and User Roles Explained

**Network Permission Roles**

The table below describes the administrator and user roles and privileges applicable to network administration.

**Table 1.7. Red Hat Virtualization Network Administrator and User Roles**