



Российская сервисная платформа виртуализации РУСТЭК

Роли узлов

Приложение к Руководству по установке

Релиз 2.6

Оглавление

1	Роли узлов.....	3
1.1	Служебные роли.....	3
1.2	Обязательные роли.....	3
1.3	Дополнительные роли.....	4
2	Ограничения переконфигурации после развертывания	5
2.1.1	Сервис обнаружения	5
2.1.2	Кэш.....	5
2.2	Очередь сообщений	5
2.3	База данных	5
2.4	Кластерное хранилище данных	6
2.5	Удаление узлов.....	6

1 Роли узлов

Роль — совокупность сервисов и их настроек, выполняющих определенную задачу в рамках платформы. Каждый физический узел в составе инсталляции принимает на себя несколько ролей. Роли делятся на служебные, обязательные и дополнительные. Каждая служебная и обязательная роль должны быть назначены хотя бы одному физическому узлу. Дополнительные роли включают расширенный функционал платформы и по умолчанию отключены.

Многие сервисы являются кластерными, значения ролей в РУСТЭК.Конфигураторе являются "начальными настройками кластера" для таких сервисов. Например, текущий «основной» узел может переехать на любой узел с ролью **Кэш «дополнительный»** в результате отказа сети и/или электропитания.

1.1 Служебные роли

- **Сервис обнаружения:** предоставляет функционал обнаружения сервисов на основе DNS, проверки их доступности и балансировки. Используется ролями **Кэш, Очередь сообщений, База данных**;
- **Кластерное хранилище настроек:** реализует общее хранилище файлов, используемое различными компонентами РУСТЭК;
- **Сервис времени:** отвечает за настройку локального NTP, позволяет настроить синхронизацию с внешними источниками времени;
- **Кэш:** кластерная NoSQL БД. Используется преимущественно ролью **Сервис авторизации** для кэширования аутентификационных данных;
- **Очередь сообщений:** брокер сообщений на основе стандарта AMQP для координации операций и информации о состоянии между сервисами;
- **Web-службы:** веб-сервер для обработки API запросов, с функцией балансировки нагрузки;
- **База данных:** основное хранилище данных платформы;
- **Хранилище логов:** сервис управления логами. Используется для централизованного сбора логов и записи их в СУБД.

1.2 Обязательные роли

- **Сервис авторизации:** обеспечивает авторизацию, аутентификацию пользователей и служб системы, реализует мультитенантную модель доступа;
- **Сервис DNS:** обеспечивает управление доменами и записями в них, интегрирован с ролями **Управление VM** и **Управление сетями** для автоматического создания записей для объектов виртуальной инфраструктуры;
- **Управление образами:** реализует репозиторий образов, предоставляет инструменты для работы с ним;
- **Служебный каталог облачных ресурсов:** реализует системный каталог ресурсов (CPU, RAM и т.д.). Используется ролями **Управление VM, Управление сетями и Управление дисками**;
- **Управление VM:** предоставляет инструменты для создания и взаимодействия VM;

- **Управление сетями:** обеспечивает создание и управление виртуальной сетевой инфраструктурой. Сетевая подсистема предоставляет абстрактные сети, подсети, порты и роутеры;
- **Вычислительный узел:** непосредственно взаимодействует с гипервизором KVM, создаёт/редактирует/удаляет/мигрирует VM;
- **Управление дисками:** обеспечивает управление постоянным блочным хранилищем для виртуальных дисков. Позволяет пользователю создавать и удалять блочные устройства и управлять их подключением к виртуальным машинам. Предоставляет механизм для создания и восстановления резервных копий дисков и снимков;
- **Агент событий очереди:** обеспечивает перехват сообщений между другими сервисами в **Очереди сообщений** для реализации дополнительной логики при работе с объектами виртуальной инфраструктуры;
- **Сервис оптимизации ресурсов:** реализует сбор и хранение метрик физических узлов и VM, предоставляет инструменты для оптимизации нагрузки платформы в соответствии с заданными правилами и значениями метрик;
- **Сервис построения облачных процессов:** предоставляет инструменты для выполнения комплексных задач автоматизации;
- **Web-интерфейс:** веб-интерфейс для работы с платформой РУСТЭК.

1.3 Дополнительные роли

- **Сервис балансировки нагрузки:** позволяет создавать сетевые балансировщики нагрузки;
- **Сервис оркестрации:** позволяет создавать комплексные среды и управлять ими, используя концепцию инфраструктуры как код;
- **Сервис управления инфраструктурой контейнеров:** позволяет создавать и настраивать кластер Kubernetes, а после создания кластера добавлять новые ноды Kubernetes в ручном режиме или в режиме автомасштабирования (autoscaling);
- **Служба хранения ключей шифрования:** обеспечивает безопасное хранение, предоставление и управление секретными данными.

2 Ограничения переконфигурации после развертывания

Для перемещения или удаления некоторых ролей существуют ограничения.

2.1.1 Сервис обнаружения

- Нельзя выключить роль на всех действующих узлах и переназначить ее на новые узлы;
- Нельзя конфигурировать платформу с четным количеством узлов с этой ролью.

В случае выхода из строя $(N/2 - 1)$ узлов с этой ролью — необходимо как можно скорее переназначить ее на какие-либо из оставшихся узлов, иначе выход из строя следующего узла приведет к неработоспособности кластера. Кластер перестанет отвечать на DNS запросы, как следствие остальные сервисы платформы потеряют доступ к **Базе данных, Очереди сообщений, Кэшу**.

Для корректной работы системы допустимы потери 1/3, 2/5, 3/7 узлов с ролью Сервиса обнаружения. Не рекомендуется включать роль Сервиса обнаружения более чем на 7 узлах.

Перезагрузку узлов с этой ролью необходимо осуществлять строго последовательно или одновременно, для корректного старта сервиса.

2.1.2 Кэш

- Для корректной работы сервиса кэширования в режиме высокой доступности необходимы как минимум:
 - один «основной» узел, один «дополнительный» и один «арбитр» — в этом случае возможна потеря «основного» узла;
 - один «основной» и два «дополнительных» узла — в этом случае в этом случае возможна потеря сначала «основного», затем «дополнительного» узлов (который не стал «основным»);
- Нельзя конфигурировать платформу с четным количеством узлов с ролью **Кэш**.

2.2 Очередь сообщений

- Нельзя конфигурировать платформу с четным количеством узлов с ролью **Очередь сообщений**.

2.3 База данных

- Для корректной работы отказоустойчивости БД необходим хотя бы один узел с ролью БД «арбитр»;
- Нельзя сменить роль БД «*включено*» → «*арбитр*» или «*арбитр*» → «*включено*» за одну переконфигурацию, нужно:
 - выключить роль, применить конфигурацию;
 - включить нужный режим и применить конфигурацию еще раз;
- Общее число узлов с ролью БД ограничено десятью узлами: 9 с ролью БД «*включено*» + 1 «*арбитр*».

По умолчанию отключен функционал синхронных реплик. Это может привести к потере данных между последней записью в БД и последним сеансом репликации в случае аварийного отключения текущего мастера. Включить функционал можно в РУСТЭК.Конфигураторе в разделе «Общие настройки», изменив количество синхронных реплик на отличное от нуля. Количество синхронных реплик должно быть меньше или равно (количество узлов с ролью БД «включено»)

1. При недоступности всех синхронных реплик кластер БД перестает обслуживать запросы, так как не может закрыть транзакцию. Не рекомендуется включать этот функционал в инсталляциях с общим количеством узлов БД < 4.

Вычислительный узел:

- Следует убедиться, что на выключаемых вычислительных узлах отсутствуют виртуальные машины в следующих состояниях: **Active, Paused, Suspended**. Такие виртуальные машины следует перевести в состояние **Shutoff**, если:
 - роль выключается на всех действующих узлах, и эта же роль включается на новом узле или;
 - одновременно изменяется имя домена и выключается роль хотя бы на одном узле;
 - в кластере одновременно изменяется имя всех вычислительных узлов и выключается роль хотя бы на одном узле;
- При выключении вычислительного узла с виртуальными машинами, следует убедиться, что на других вычислительных узлах достаточно свободных ресурсов для миграции на них этих виртуальных машин, при этом надо учитывать оверкоммит;
- Нельзя менять имена узлов между собой во время одного запуска конфигурации.

2.4 Кластерное хранилище данных

- Нельзя за одну переконфигурацию добавить и удалить (или наоборот) роль **Кластерное хранилище данных**. Необходимо:
 - сделать первое действие и применить конфигурацию;
 - затем сделать второе действие и еще раз применить конфигурацию;
- Если используется 1 сервер кластерного хранилища настроек, то невозможно переименовать узел.

2.5 Удаление узлов

- OCFS2: для полного исключения нод из OCFS2 кластера необходима остановка всего кластера. На момент версии ocfs-tools 1.8.7 не реализовано online удаление узлов из кластера.