РУСТЭК-ЕСУ

Руководство по установке и настройке РУСТЭК-ЕСУ

Версия 3.4.6

2023

СОДЕРЖАНИЕ

1. Поставка РУСТЭК-ЕСУ 4
2. Развёртывание на платформе виртуализации РУСТЭК 5
2.1. Системные требования 5
2.2. Порядок развёртывания 5
3. Установка РУСТЭК-ЕСУ 13
4. Настройка сегментов 19
4.1. Авторизация в панели управления 19
4.2. Настройка сегмента РУСТЭК 19
4.2.1. Настройка сетевых зон для сегмента РУСТЭК 19
4.2.2. Настройка OpenStack-раннера 22
4.2.3. Настройка ресурсного пула для сегмента РУСТЭК 24
4.2.4. Создание шаблонов ВМ для сегмента РУСТЭК 28
4.3. Настройка сегмента VMware vSphere 31
4.3.1. Создание маршрутизируемой сети 32
4.3.2. Создание директории для ВЦОДов клиентов 35
4.3.3. Настройка сетевых зон для сегмента VMware vSphere 35
4.3.4. Настройка vSphere-раннера РУСТЭК-ЕСУ 37
4.3.5. Настройка ресурсного пула для сегмента VMware vSphere 39
4.3.6. Развёртывание Edge-роутера 43
4.3.7. Создание шаблонов ВМ для сегмента VMware vSphere 45
5. Проверка работы сегментов инсталляции 56
5.1. Создание партнёра и домена 56
5.2. Создание клиента, проекта и ВЦОД 58
6. Настройка РУСТЭК-ЕСУ для работы с кластерами Kubernetes 62
6.1. Создание шаблонов Kubernetes для сегмента VMware vSphere 62
6.2. Создание шаблонов Kubernetes для сегмента РУСТЭК 71
6.3. Создание кластеров Kubernetes в РУСТЭК-ЕСУ 78
6.4. Особенности и поддерживаемый функционал 80
7. Расширенная настройка 81
7.1. Настройка NGINX реверс-прокси 81
7.2. Настройка управления DNS-зонами в РУСТЭК-ЕСУ 82
7.3. Настройка сети для роутеров (Edge) сегмента VMware vSphere 84
7.4. Универсальный скрипт развёртывания 91
7.5. Подготовка сервера с Veeam Backup & Replication для работы с РУСТЭК-ЕСУ 94
7.6. Подключение S3-хранилища к РУСТЭК-ЕСУ 99
7.6.1. Подключение сервиса MinIO Storage 100
7.6.2. Подключение сервиса NetApp StorageGRID 101

7.7. Подключение ЮKassa к РУСТЭК-ЕСУ 101
7.8. Подключение Telegram-бота к РУСТЭК-ЕСУ для управления облачной инфраструктурой 103
7.9. Подключение Telegram-бота к РУСТЭК-ЕСУ для двухфакторной авторизации 105
8. Развёртывание на платформе виртуализации VMware vSphere 107
8.1. Системные требования 107
8.2. Порядок развёртывания 107
8.3. Примечания по установке и дальнейшей настройке 116
9. Обновление РУСТЭК-ЕСУ 117
Приложение 1. Пример Auto DevOps-скрипта 119

1. Поставка РУСТЭК-ЕСУ

РУСТЭК-ЕСУ поставляется в виде образа виртуальной машины (ВМ) ESU-box. В зависимости от целевой платформы виртуализации, на которой будет производиться инсталляция, используются форматы:

- .qcow2 — для установки на РУСТЭК (KVM).
- .ova — для установки на VMware vSphere (ESXi).

В качестве гостевой операционной системы (ОС) используется Debian 10 (может меняться производителем). В ESU-box встроен инсталлятор, а также запущены необходимые для работы сервисы и программное обеспечение в виде docker-контейнеров. Это удобно для быстрого запуска РУСТЭК-ЕСУ.

Минимальные требования для ВМ ESU-box:

- vCPU — 4 ядра.
- RAM — 8 ГБ.
- Размер диска — 30 ГБ.

2. Развёртывание на платформе виртуализации РУСТЭК

2.1. Системные требования

Для развёртывания на платформе виртуализации РУСТЭК необходимы:

- РУСТЭК,
- одна маршрутизируемая сеть с префиксом маски /24 с доступом до Сети управления РУСТЭК. В качестве минимального требования допускается сеть с префиксом маски /27.

Пример схемы сетевой связности РУСТЭК-ЕСУ, установленной внутри платформы виртуализации РУСТЭК с подключенной к ней инсталляцией VMware vSphere (Рисунок 1).

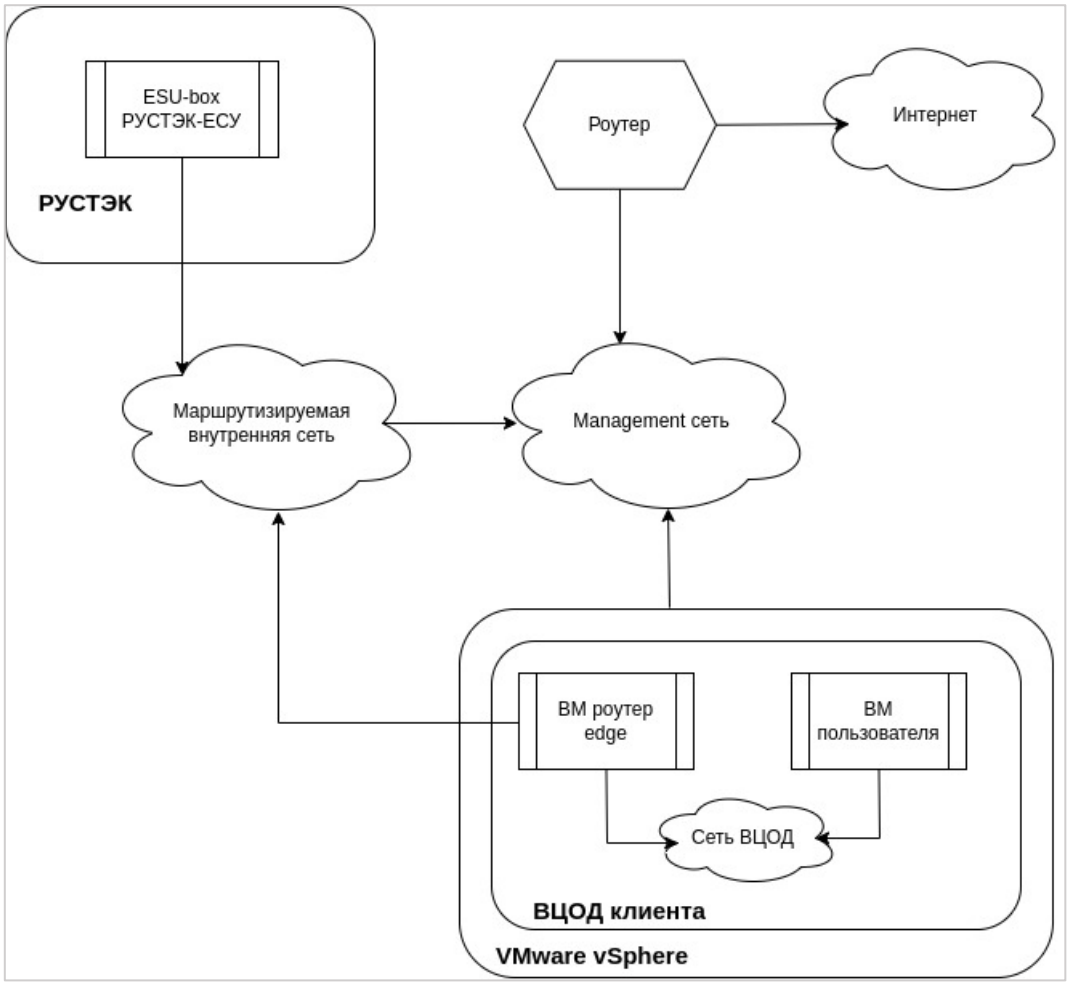

Рисунок 1

2.2. Порядок развёртывания

1. Вход в панель управления РУСТЭК по ссылке https://[Virtual_IP], где Virtual_IP — виртуальный IP-адрес инсталляции.

2. Создание образа РУСТЭК-ЕСУ.

Для создания образа перейдите в раздел меню **Копии и образы** → **Образы** и нажмите кнопку **Создать** (Рисунок 2).

Рисунок 2

В открывшемся окне с параметрами образа заполните поля (Рисунок 3):

- **Имя** — указать произвольное имя.
- **Проект** — выбрать в раскрывающемся списке проект, для которого создается образ.
- **Имя ОС** — указать произвольное имя ОС.
- **Контейнер** — оставить значение «bare».
- **Формат диска** — указать «qcow2».
- **RAM, МБ** — указать минимальное количество ОЗУ для будущей ВМ — 8192 МБ.
- **Размер диска, ГБ** — указать минимальный размер диска для будущей ВМ — 30 ГБ.
- **Сетевой адаптер** — выбрать «virtio».
- **Дисковый контроллер** — выбрать «virtio-scsi».
- **Публичный** — снять флаг.
- **Метод загрузки** — выбрать «Файл».

После заполнения полей нажмите **Создать**.

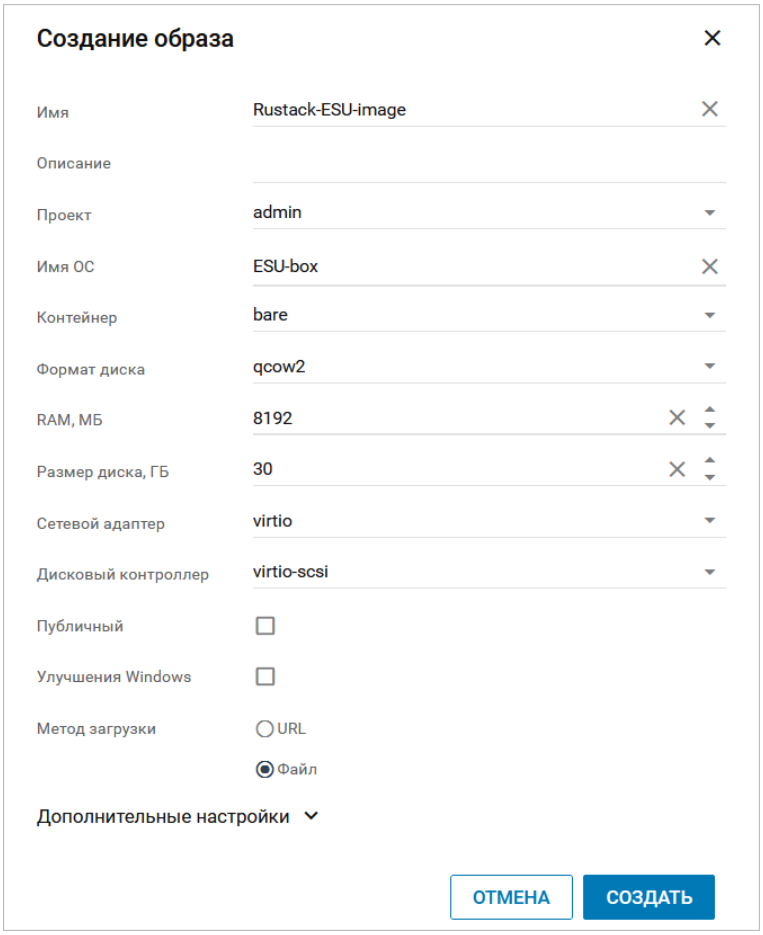

Рисунок 3

3. Загрузка образа.

Найдите в списке новый образ, выберите его и нажмите кнопку **Загрузить образ** (Рисунок 4).

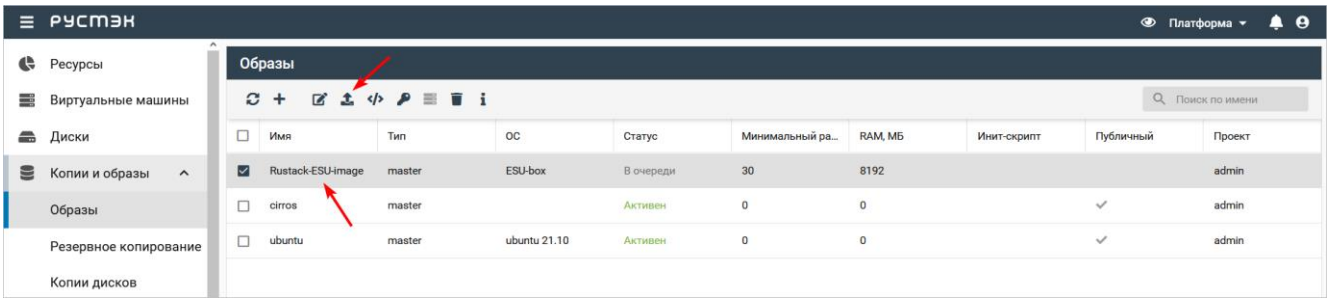

Рисунок 4

В открывшейся форме **Загрузка образа** нажмите кнопку **Добавьте файл** и выберите предоставленный дистрибутив в формате .qcow2.

Далее нажмите кнопку **Загрузить**. Начнётся процесс загрузки образа.

4. Создание конфигурации ВМ.

Перейдите в раздел **Конфигурация** → **Конфигурации ВМ** и нажмите кнопку **Создать** (Рисунок 5).

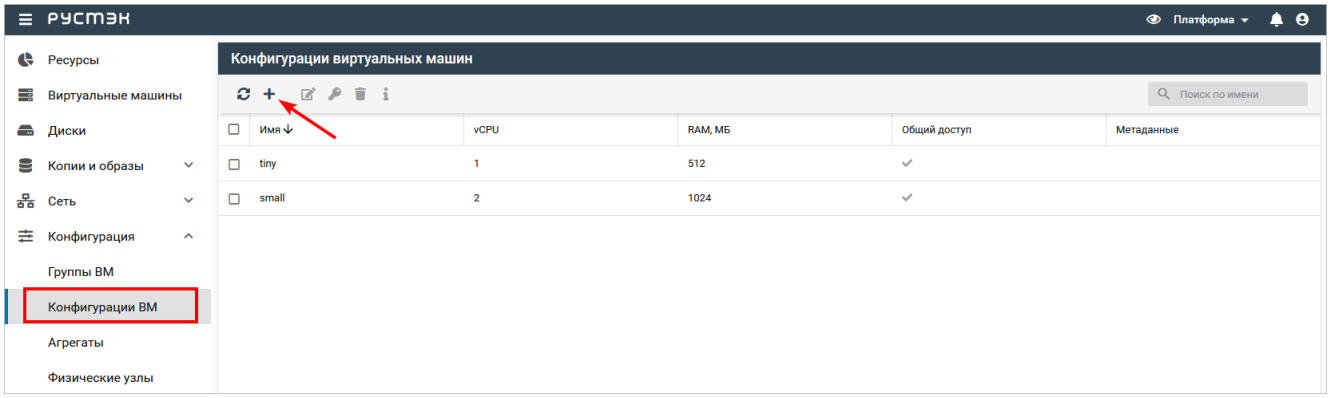

Рисунок 5

В открывшемся окне заполните поля будущей конфигурации (Рисунок 6):

- **Имя** — указать произвольное имя.
- **vCPU** — ввести количество виртуальных ядер.
- **RAM, МБ** — ввести количество ОЗУ в МБ.

После заполнения полей нажмите кнопку **Создать**.

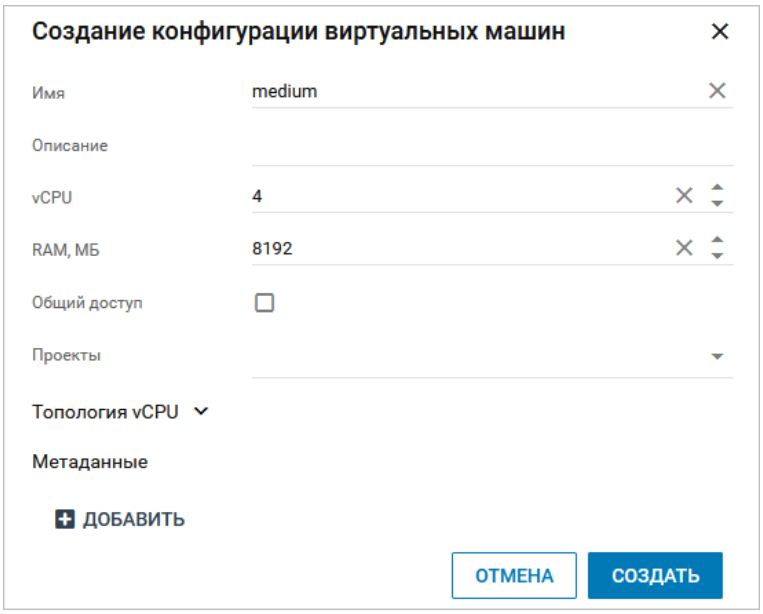

Рисунок 6

5. Создание маршрутизируемой сети.

Создайте сеть для РУСТЭК-ЕСУ. Для этого перейдите в раздел **Сеть** → **Сети** и нажмите кнопку **Создать**  (Рисунок 7).

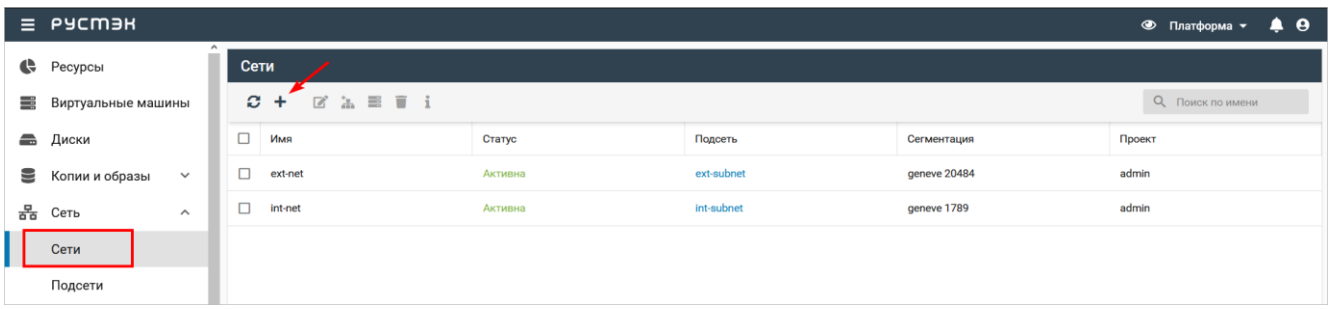

Рисунок 7

В открывшемся окне заполните поля (Рисунок 8):

- **Имя** — указать произвольное имя.
- **Тип сегментации** — VLAN.
- **Номер VLAN** — номер выделенного VLAN для маршрутизируемой сети РУСТЭК-ЕСУ.
- **Безопасность портов** — снять флаг.
- **Внешняя** — установить флаг.

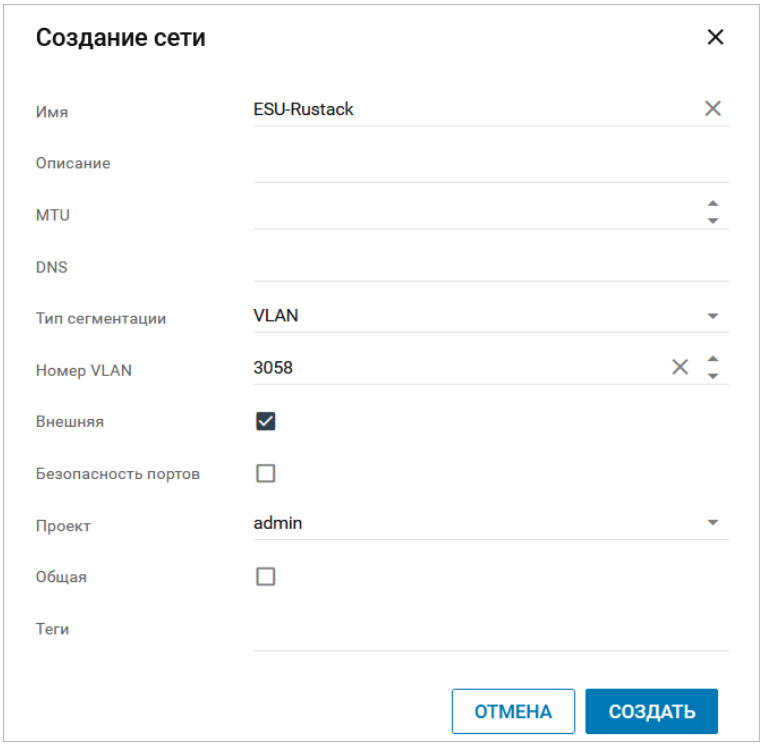

Рисунок 8

После заполнения полей нажмите **Создать**.

6. Создание подсети для маршрутизируемой сети.

После создания сети создайте подсеть. Для этого перейдите в раздел **Сеть** → **Подсети** и нажмите кнопку **Создать** + (Рисунок 9).

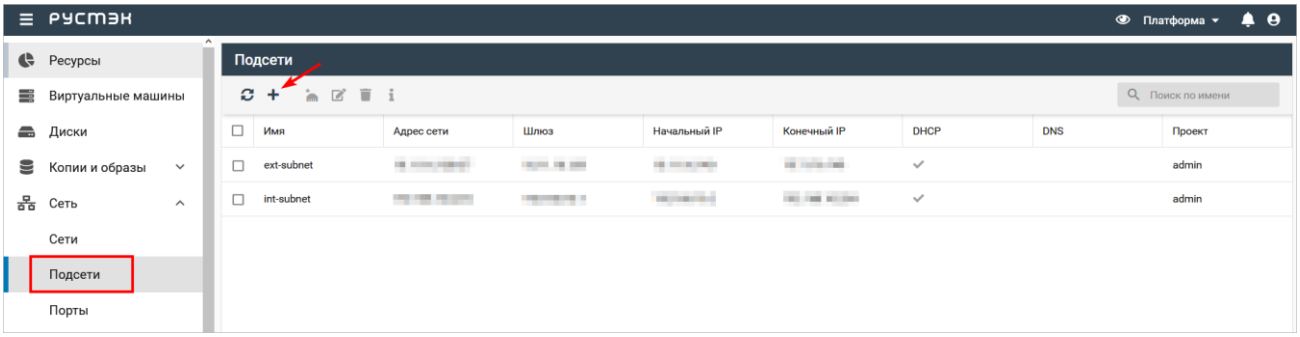

Рисунок 9

В открывшемся окне заполните поля (Рисунок 10):

- **Имя** — указать произвольное имя.

- **Сеть** — выбрать сеть, созданную на предыдущем этапе.
- **Версия IP** — IPv4.
- **Адрес сети** — указать CIDR сети.
- **Шлюз** — указать шлюз.
- **DHCP** — снять флаг, потому что в РУСТЭК-ЕСУ работает собственный DHCP-сервер.

После заполнения полей нажмите кнопку **Создать**.

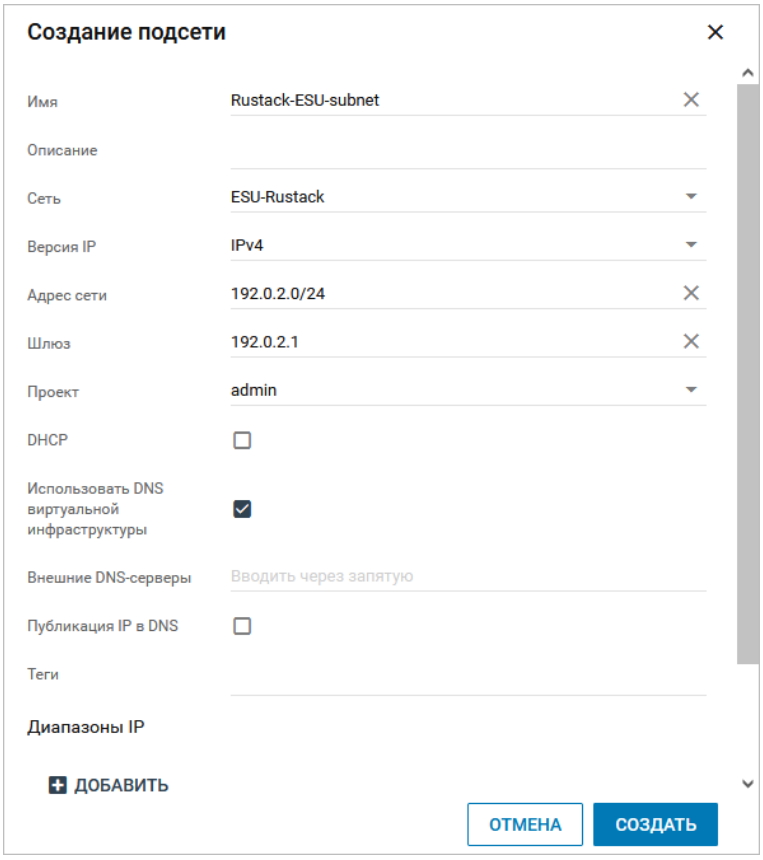

Рисунок 10

Из создаваемой сети для будущей ВМ ESU_box должен быть организован доступ до Сети управления физических узлов РУСТЭК!

7. Создание ВМ.

Перейдите на вкладку **Виртуальные машины** и нажмите кнопку **Создать** (Рисунок 11).

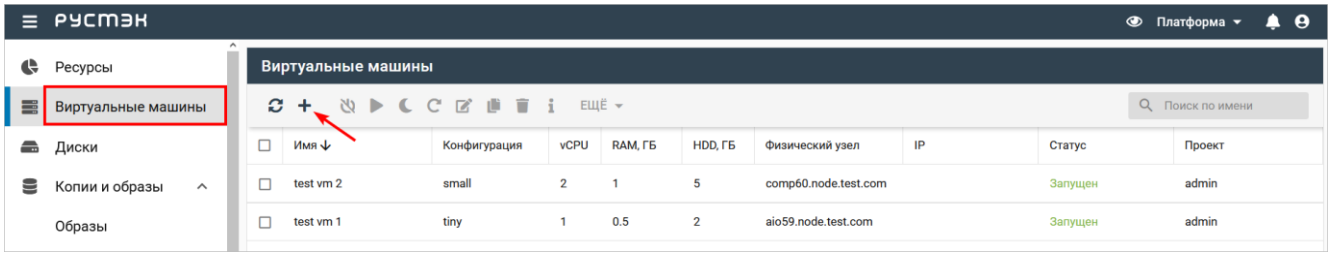

Рисунок 11

В открывшемся окне заполните поля (Рисунок 12):

- **Имя** — указать произвольное имя.
- **ОС** — выбрать ранее загруженный образ.
- **Конфигурация** — указать необходимую конфигурацию: минимальная 4 vCPU, 8 ГБ RAM.
- **Размер диска** — указать размер диска ВМ, минимальный размер 30 ГБ.
- **Удалять диск вместе с сервером** — рекомендуется снять флаг.
- **Сети** — выбрать ранее созданную маршрутизируемую сеть.

После заполнения полей нажмите кнопку **Создать**.

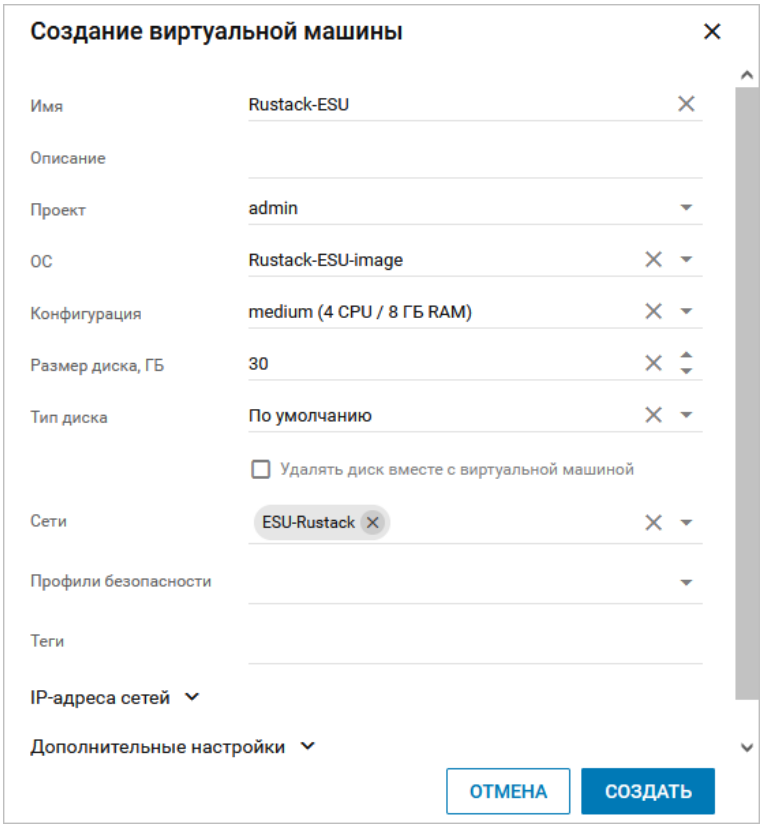

Рисунок 12

Дождитесь окончания создания ВМ — статус изменится на «Запущен» (Рисунок 13).

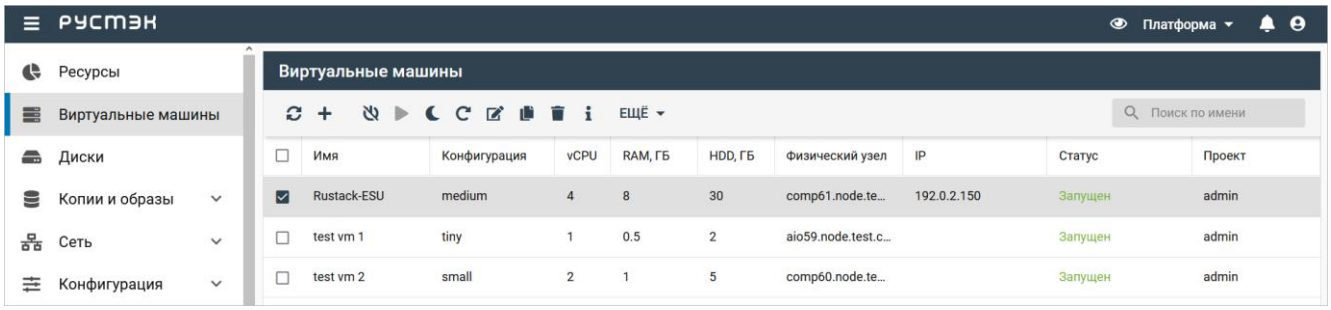

Рисунок 13

8. Открытие VNC-консоли для созданной ВМ.

Для открытия консоли ВМ в разделе меню **Виртуальные машины** выберите созданную ВМ и нажмите **ЕЩЁ** (Рисунок 14):

- откройте консоль сервера, нажав **Открыть консоль**,
- получите ссылку, нажав на **Ссылка на консоль ВМ,** и откройте её в новой вкладке.

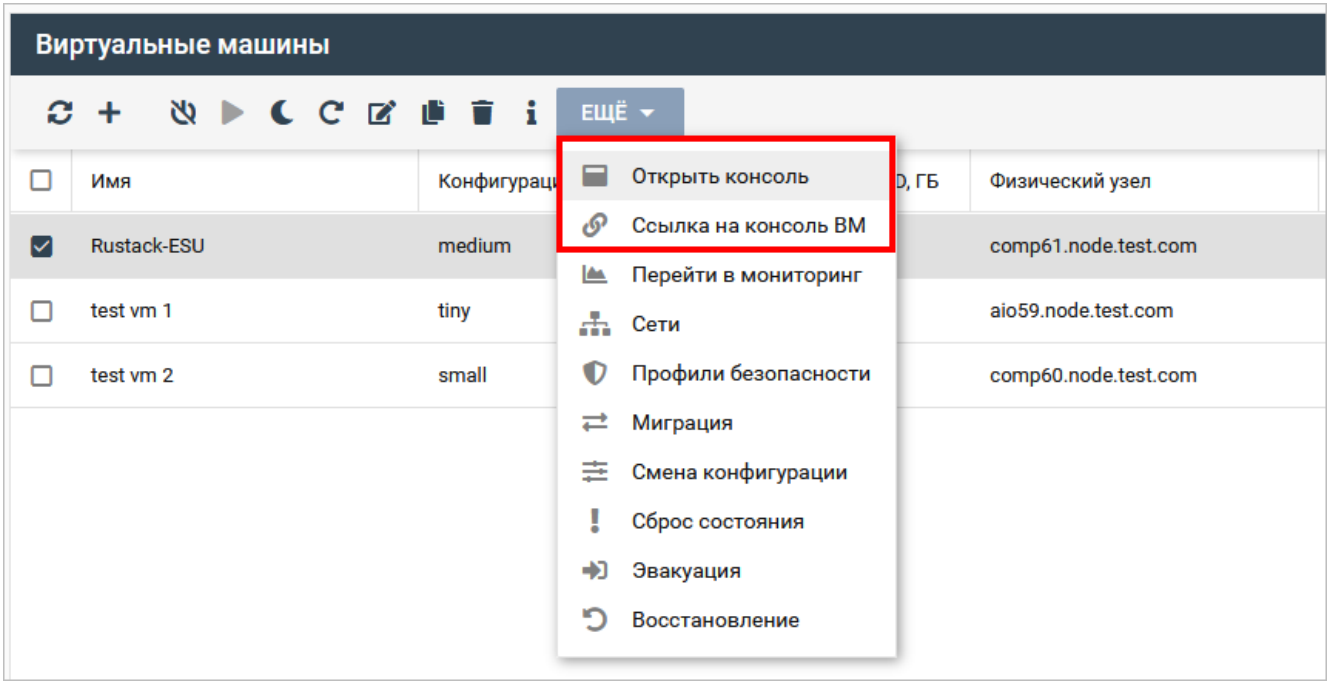

Рисунок 14

Стандартная учётная запись на ВМ с РУСТЭК-ЕСУ (ESU-box):

- логин — **deploy**
- пароль — **1-qpALzm/**

3. Установка РУСТЭК-ЕСУ

Установка запускается автоматически при запуске ВМ с РУСТЭК-ЕСУ.

Сначала произойдет распаковка контейнеров. Дождитесь завершения процесса (Рисунок 15):

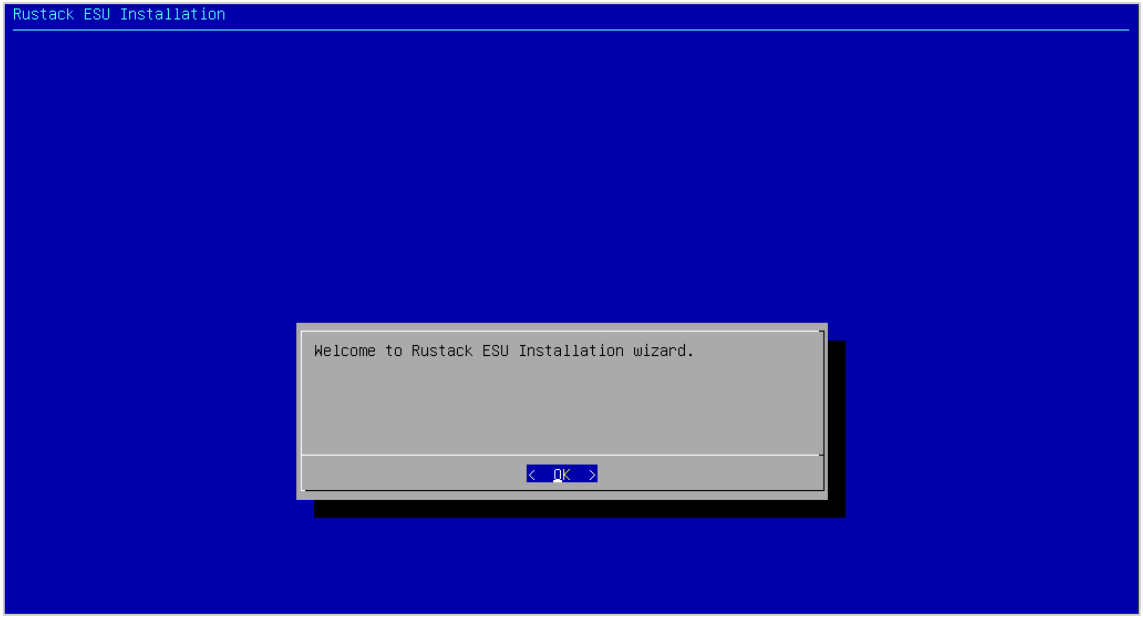

Рисунок 15

Далее будет задано несколько вопросов относительно сетевой конфигурации.

Сначала укажите IP-адрес в формате CIDR (адрес и префикс маски подсети), который был назначен ВМ ESU-box внутри РУСТЭК (Рисунок 16 и Рисунок 17).

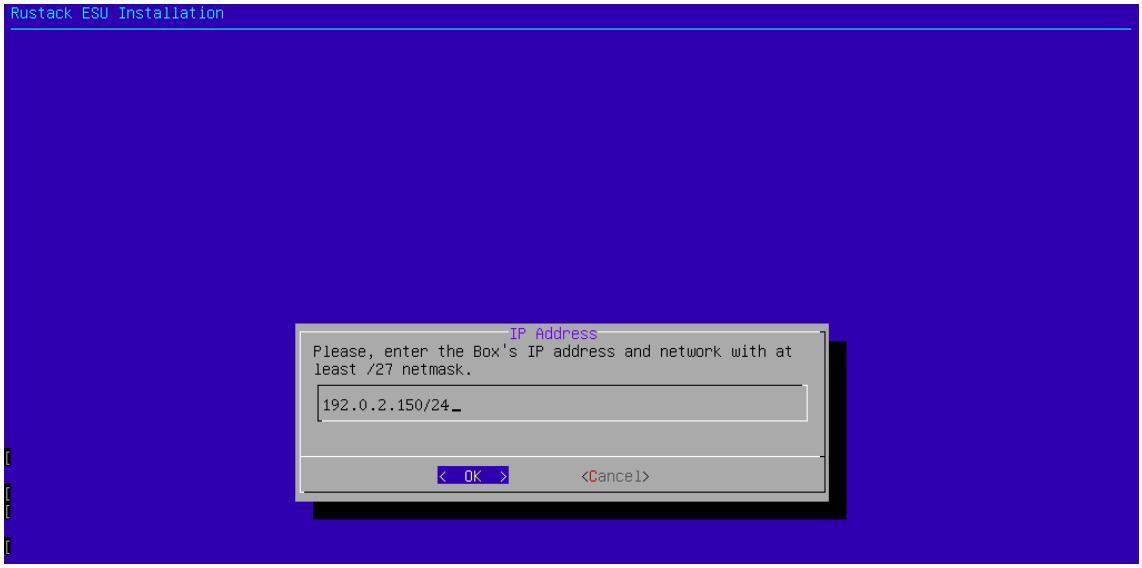

Рисунок 16

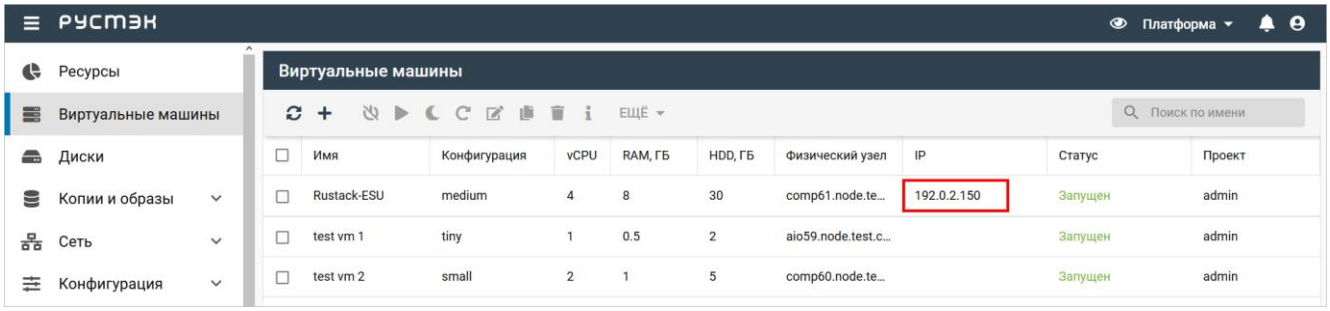

Рисунок 17

Далее введите шлюз подсети (Рисунок 18).

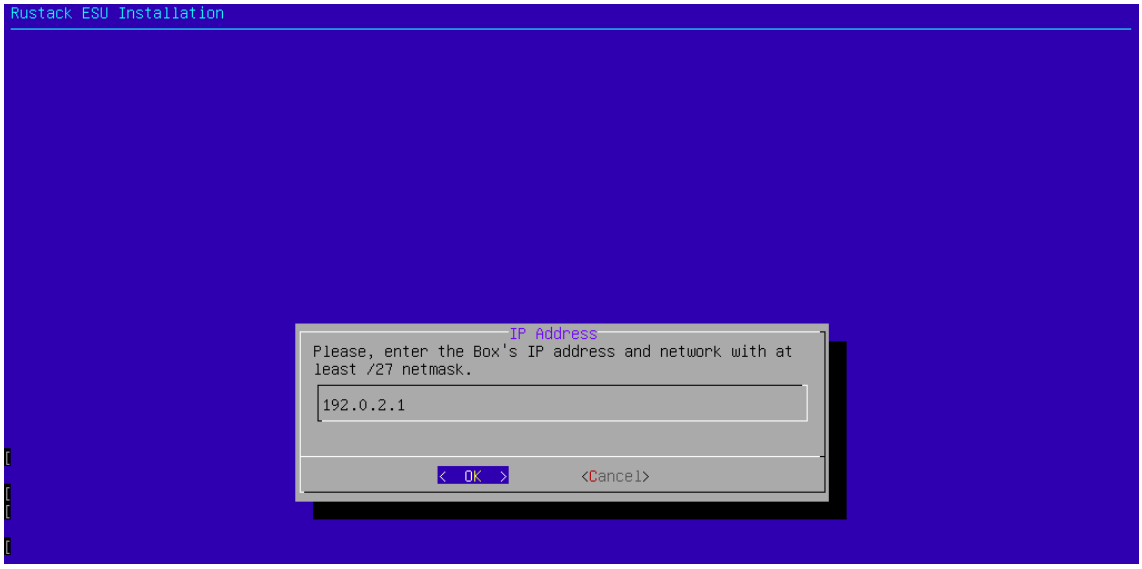

Рисунок 18

В следующем окне инсталлятора введите VLAN ID, если на ESU-box подана сеть с несколькими VLAN. Если используется один VLAN, оставьте данное поле пустым (Рисунок 19).

Рисунок 19

На вопрос «Хотите ли вы включить DHCP-сервер в ESU-box?» надо ответить **Yes**, поскольку в данной сети его нет. Для выбора опции (Yes) используйте клавишу «Пробел» (Рисунок 20).

Запуск DHCP-сервера на ESU-box обязателен!

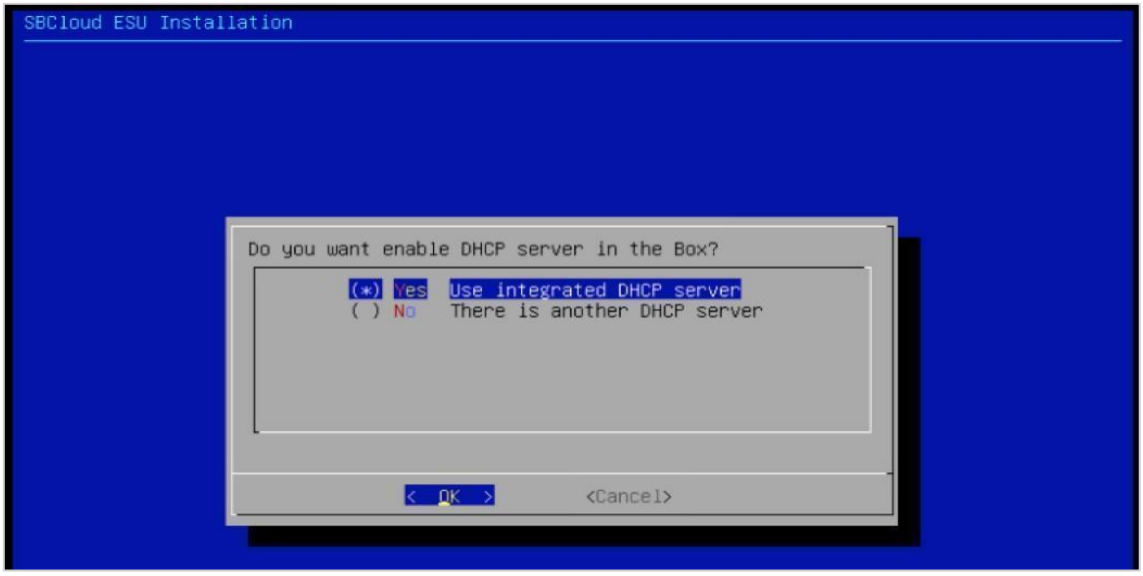

Рисунок 20

Затем введите адрес DNS-сервиса (Рисунок 21).

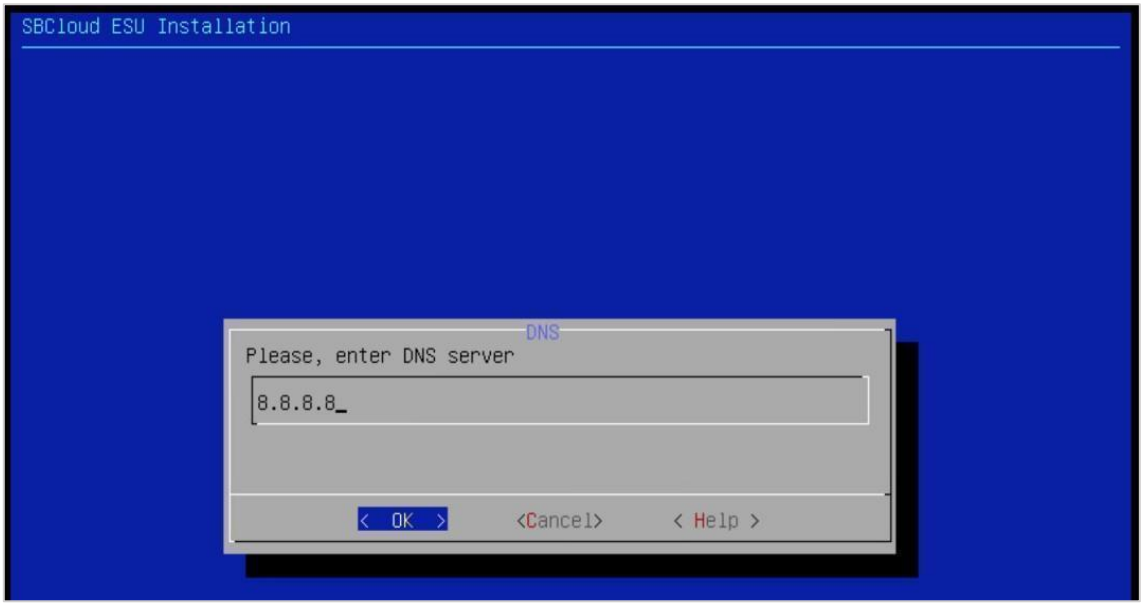

Рисунок 21

При использовании внешнего SMTP-сервера введите его адрес. Он должен поддерживать подключение без авторизации. Оставьте значение по умолчанию для использования встроенного SMTP-сервера (Рисунок 22).

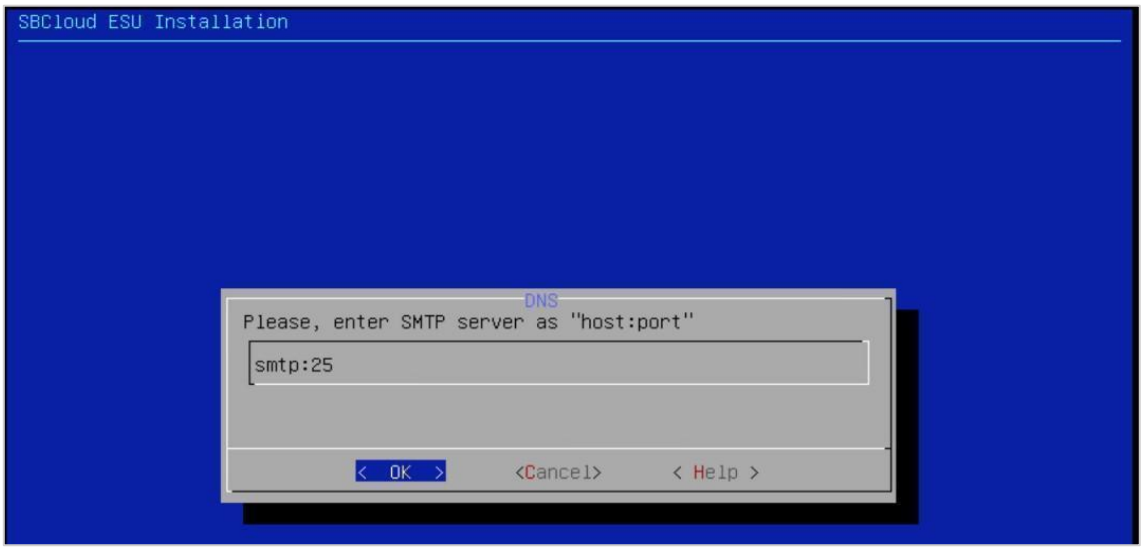

Рисунок 22

Укажите пароль, который будет установлен для пользователя admin с правами администратора платформы (Рисунок 23).

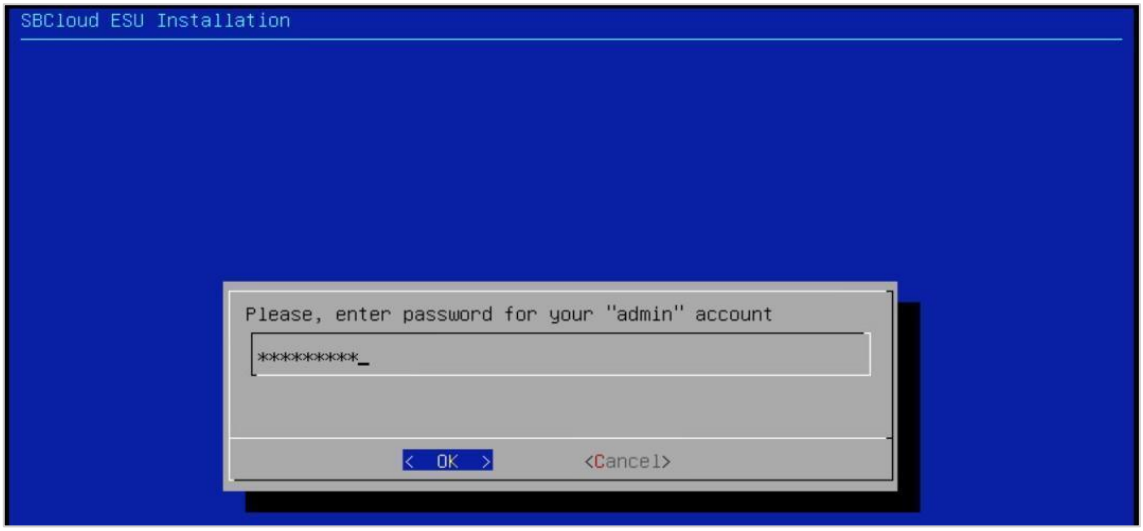

Рисунок 23

После этого дождитесь завершения процесса настройки (Рисунок 24–Рисунок 26).

Рисунок 24

```
Config file: /opt/box/toochka.conf
Configure BOX...
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit
localhost does not match 'all'

PLAY [localhost] ***************************************************************************

TASK [Gathering Facts] *********************************************************************
ok: [localhost]

TASK [box_configure : Fix resolv.conf] *****************************************************
changed: [localhost -> localhost]

TASK [box_configure : Fix docker conf] *****************************************************
changed: [localhost -> localhost]

TASK [box_configure : Set timezone to Europe/Moscow] ***************************************
         Starting Time & Date Service...
[  OK  ] Started Time & Date Service.
         Starting Rotate log files...
         Starting Daily apt download activities...
changed: [localhost -> localhost]

TASK [box_configure : Restart services] ****************************************************
[  OK  ] Started Rotate log files.
         Stopping Network Time Service...
[  OK  ] Stopped Network Time Service.
         Starting Network Time Service...
[  OK  ] Started Network Time Service.
changed: [localhost -> localhost] => (item=ntp)

TASK [box_configure : Create docker-compose.yml from template] *****************************
changed: [localhost -> localhost]

TASK [box_configure : Restart docker-compose] **********************************************
```

Рисунок 25

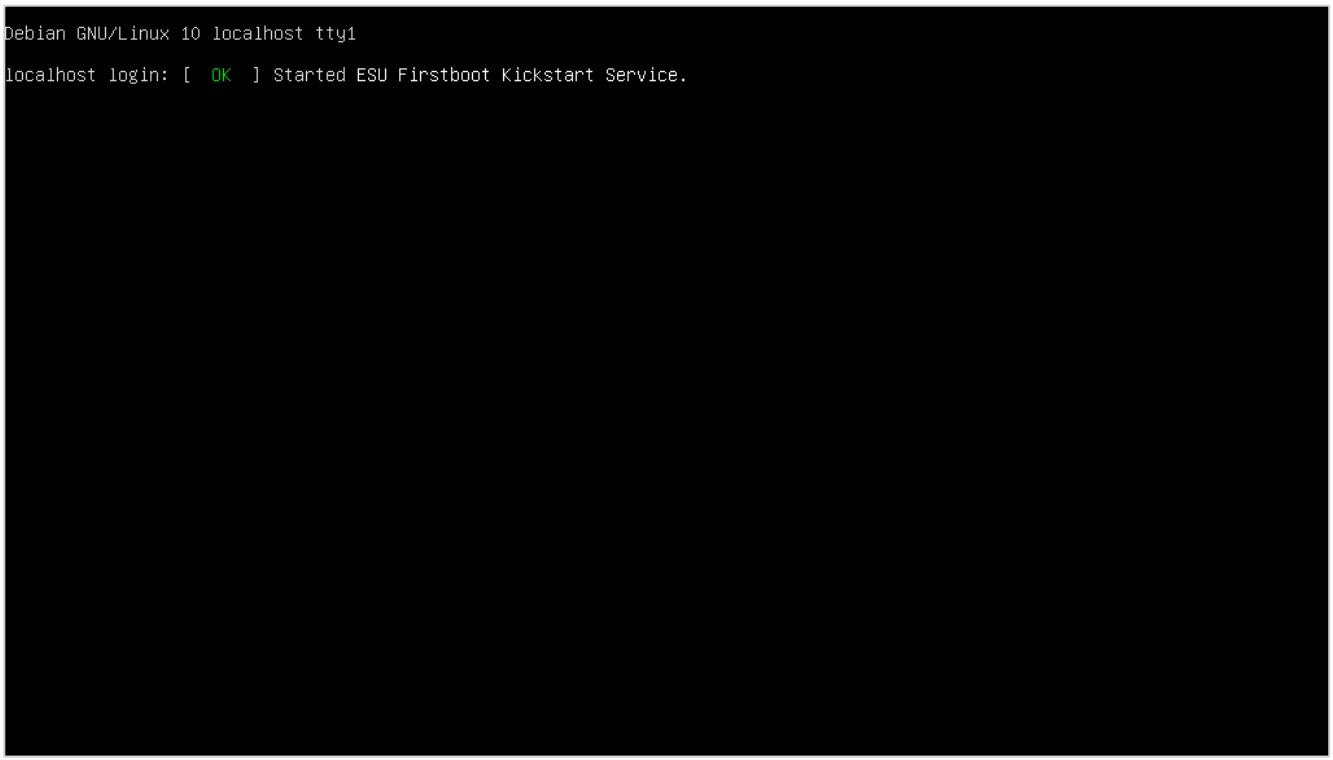

Рисунок 26

На этом установка РУСТЭК-ЕСУ завершена.

4. Настройка сегментов

В разделе подробно описаны настройки, необходимые для добавления в РУСТЭК-ЕСУ инсталляций (сегментов) РУСТЭК и сегментов VMware vSphere.

4.1. Авторизация в панели управления

Для работы в веб-панели управления РУСТЭК-ЕСУ подходят все популярные современные браузеры: Google Chrome, Firefox, Opera и т.д.

После завершения установки по IP-адресу порта созданного сервера ESU-box, который указывался при инсталляции, будет доступна панель управления РУСТЭК-ЕСУ. В данном примере это **https://192.0.2.150**.

Для входа в панель управления задайте в адресной строке браузера адрес https://192.0.2.150.

При вводе адреса панели управления используйте https://.

Авторизуйтесь с логином **admin** и паролем, заданным при инсталляции (см. предыдущий раздел 3).

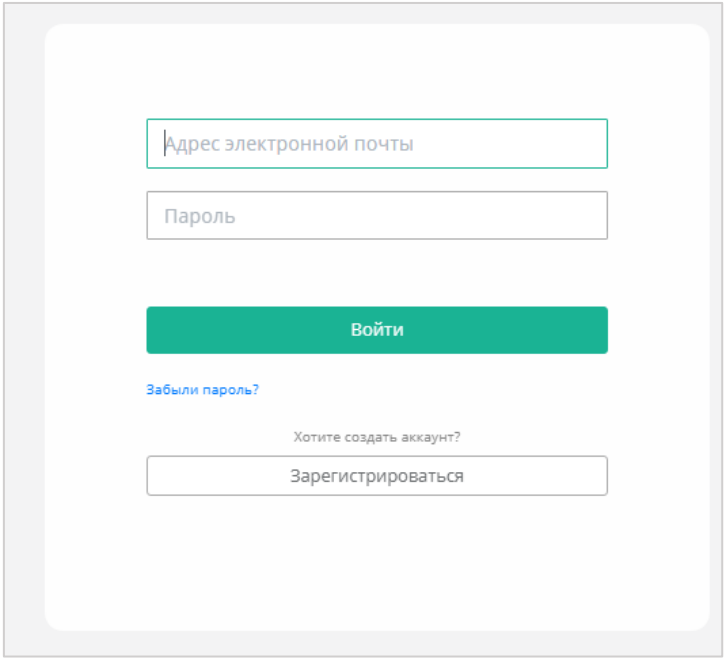

Рисунок 27

4.2. Настройка сегмента РУСТЭК

Если необходимо добавить несколько инсталляций РУСТЭК (сегментов), то для каждой из них выполните все нижеперечисленные настройки.

4.2.1. Настройка сетевых зон для сегмента РУСТЭК

Создайте сетевую зону для пользовательских внутренних сетей.

Для этого перейдите в раздел меню **Инсталляция** → **Ресурсы** → **Сетевые зоны** и нажмите кнопку **Создать сетевую зону** (Рисунок 28).

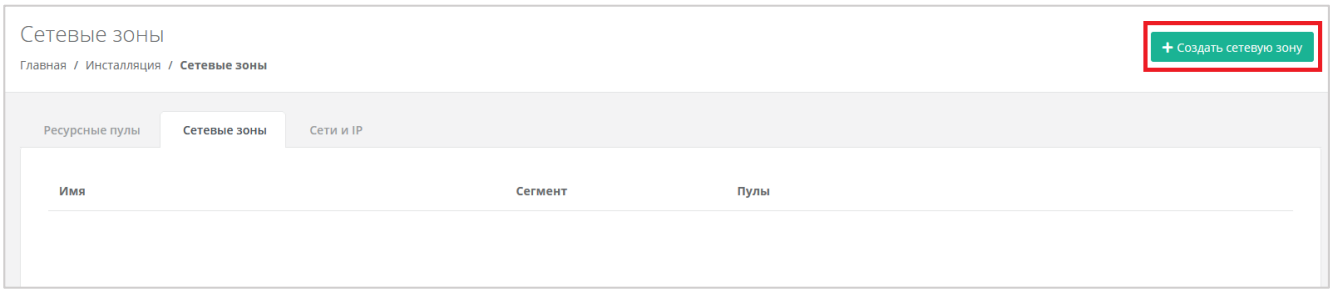

Рисунок 28

Введите название сетевой зоны, выберите сегмент, например, VLAN и нажмите кнопку **Далее** (Рисунок 29). Появится возможность добавления пулов.

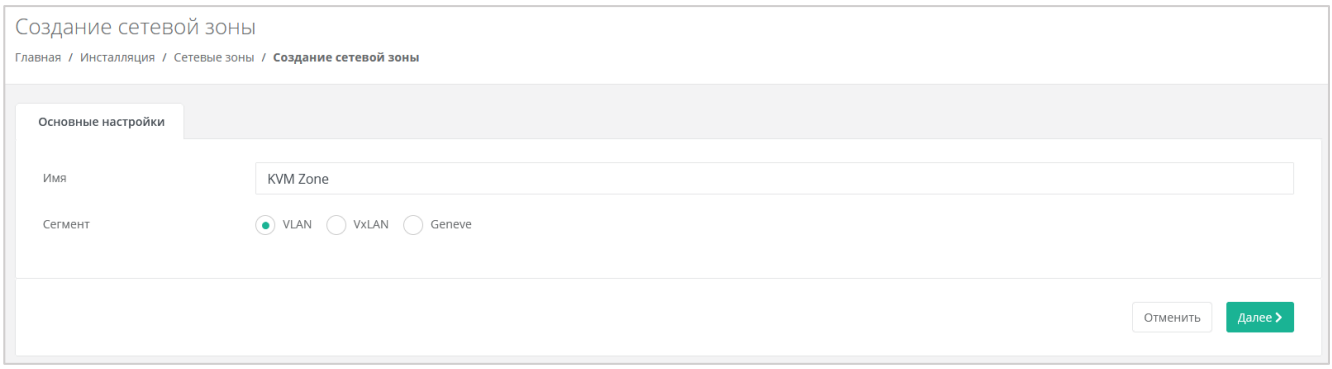

Рисунок 29

Укажите диапазон VLAN для пользовательских сетей: в данном случае — 701–1000. Для этого нажмите кнопку **Добавить пул** и в открывшемся окне введите значения начала и конца диапазона. В результате в поле **Пулы** появится новый диапазон (Рисунок 30).

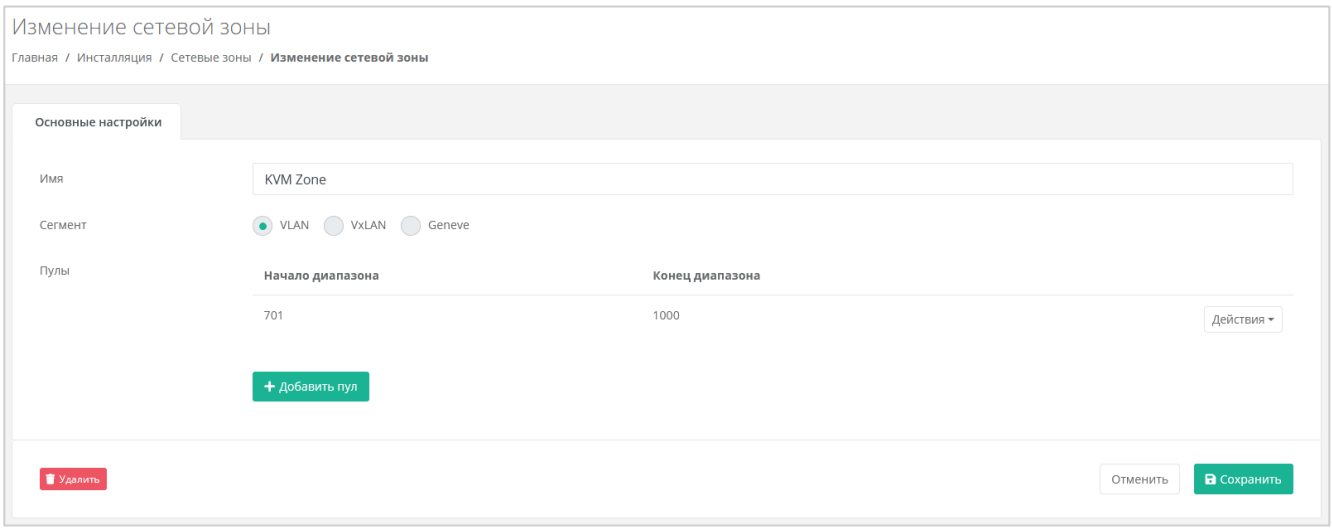

Рисунок 30

Аналогично создайте вторую сетевую зону для **внешней** сети, например, в сегменте VLAN (Рисунок 31).

VLAN 41 будет использоваться для публичных IP-адресов пользовательских ВЦОД — установите его в начало и конец диапазона.

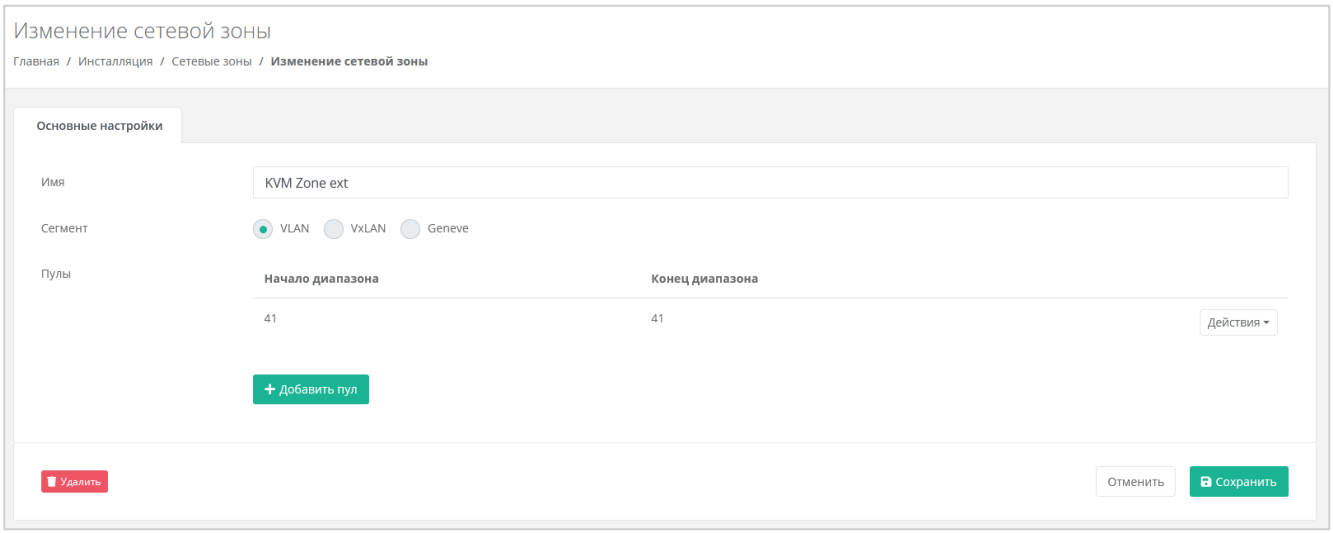

Рисунок 31

В меню **Инсталляция** → **Ресурсы** → **Сети и IP** создайте внешнюю сеть нажатием кнопки **Создать сеть**.

В открывшейся форме заполните следующие поля настроек (Рисунок 32):

- **Имя** — любое название сети.
- **Сетевая зона** — созданная ранее для *внешней* сети сегмента РУСТЭК.
- **VID/VNID** — VLAN внешней сети: в данном случае — 41.
- **Тип сети** — внешняя.
- **Имя на платформе виртуализации** — введите имя сети на платформе виртуализации, которая соответствует указанному VLAN.

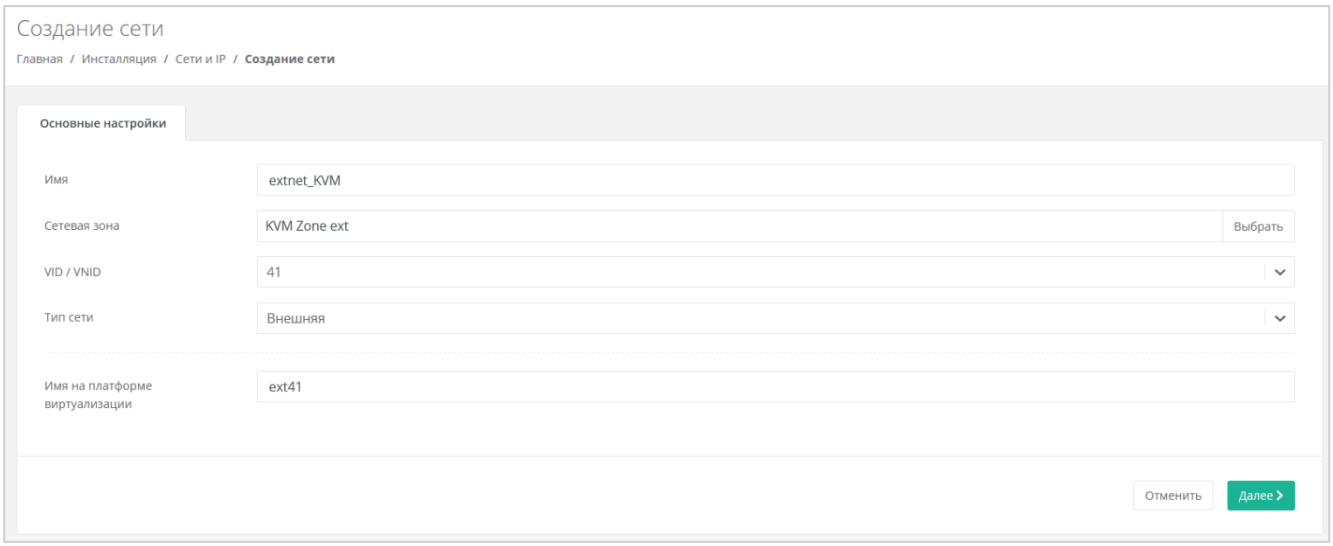

Рисунок 32

После заполнения основных настроек нажмите кнопку **Далее** — появится возможность добавления подсетей.

Добавьте подсеть с конфигурацией сети с помощью кнопки **Добавить подсеть** — откроется окно **Добавление подсети**.

DHCP должен быть **выключен**, CIDR надо указывать полный. Если нужно уменьшить диапазон выдаваемых IP-адресов, можно указать произвольный диапазон (Рисунок 33).

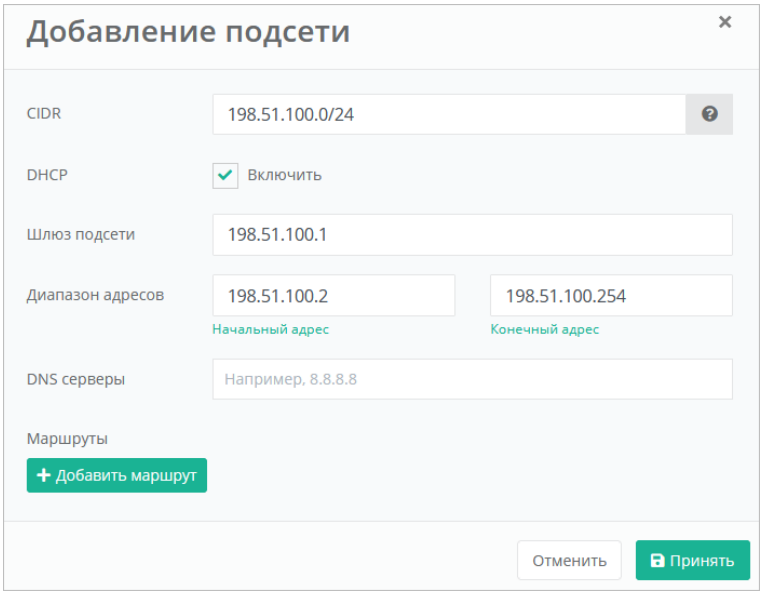

Рисунок 33

Нажмите кнопку **Принять** для добавления подсети.

Данная внешняя сеть автоматически будет создана при первом создании виртуального центра обработки данных (ВЦОД) в РУСТЭК.

4.2.2. Настройка OpenStack-раннера

Перейдите в раздел меню **Инсталляция** → **Система** → **Раннеры** и нажмите на имя раннера **default-openstack-runner** или на кнопку **Изменить**.

В открывшейся форме вставьте содержимое файла `clouds.yml`, описывающее параметры подключения к OpenStack Identity, в соответствующее текстовое поле (Рисунок 34). Файл `clouds.yml` находится по пути `/etc/openstack/clouds.yml` на управляющем узле РУСТЭК.

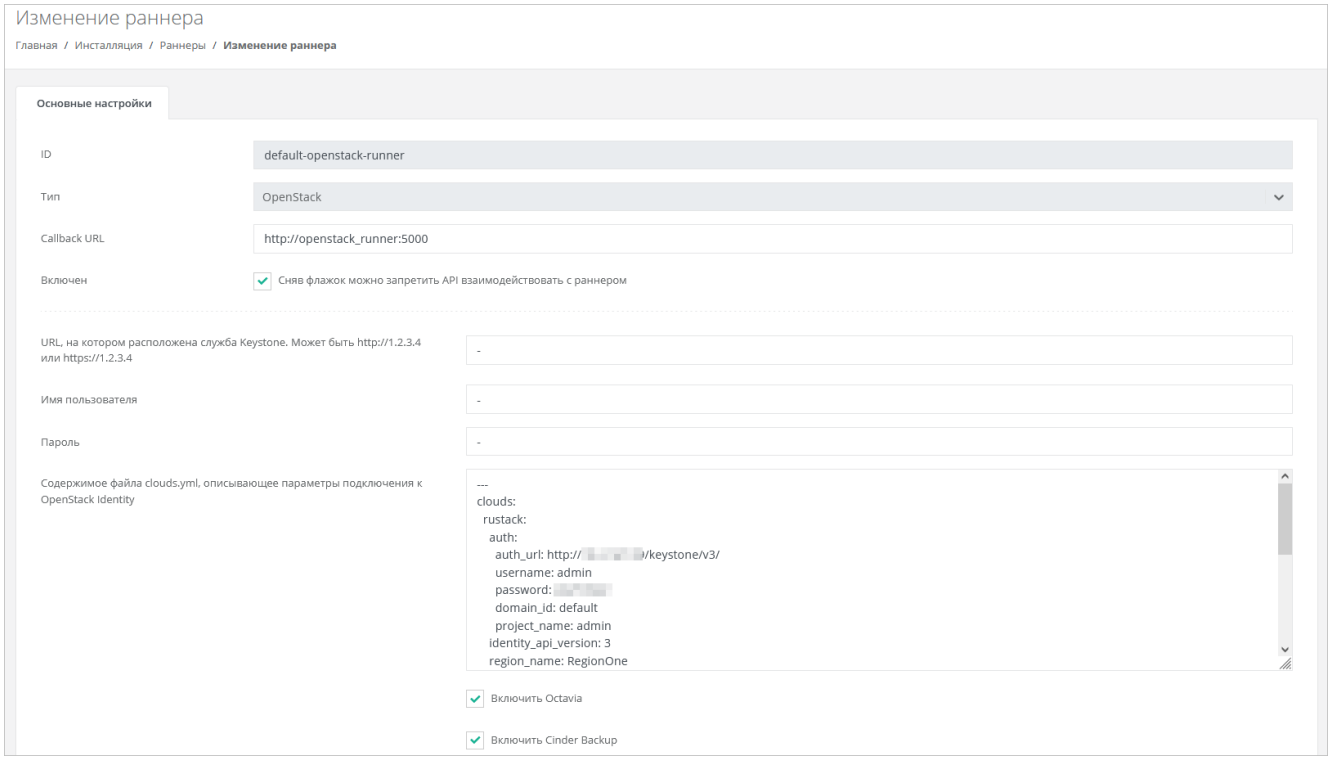

Рисунок 34

Также здесь можно настроить функциональность резервного копирования и управления балансировщиками. Если необходимо включить балансировку нагрузки, установите флаг **Включить Octavia**, если необходимо включить резервное копирование, установите флаг **Включить Cinder Backup**.

Для корректной работы балансировщиков убедитесь, что в файле `clouds.yml` в разделе `rustack` и в разделе `rustack_system` для поля `interface` установлено `public` (Рисунок 35, Рисунок 36).

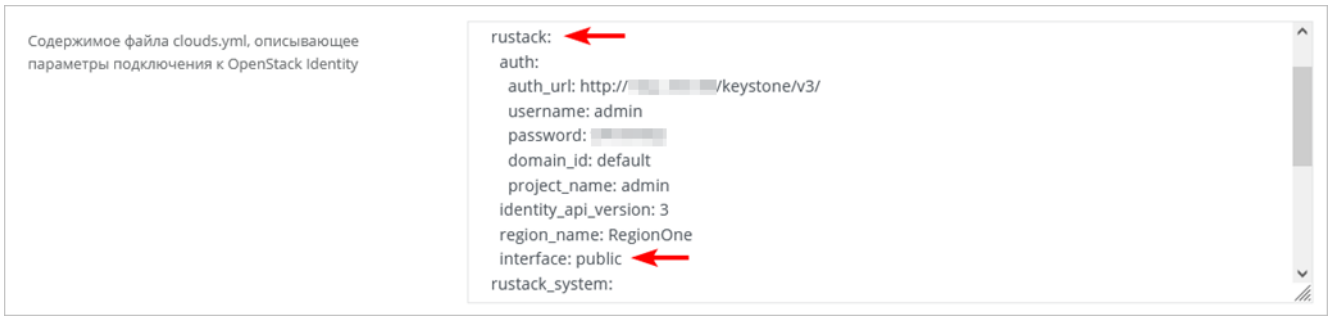

Рисунок 35

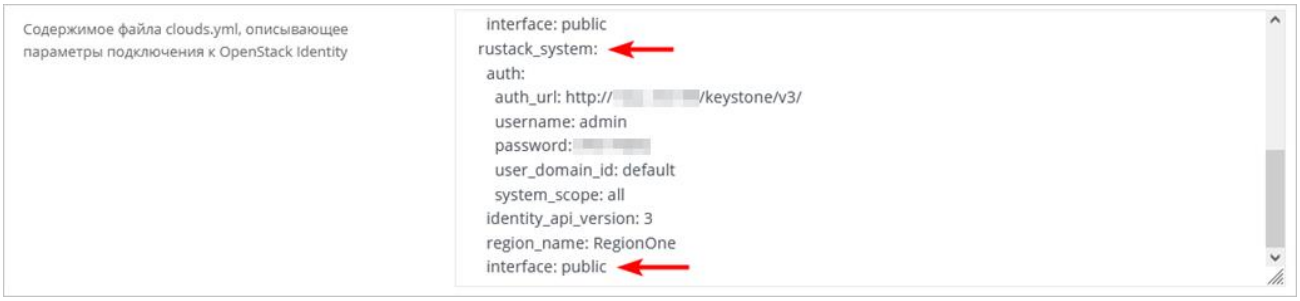

Рисунок 36

Нажмите **Сохранить**.

Если настройки произведены правильно, то индикатор OpenStack-раннера должен быть зелёным (Рисунок 37).

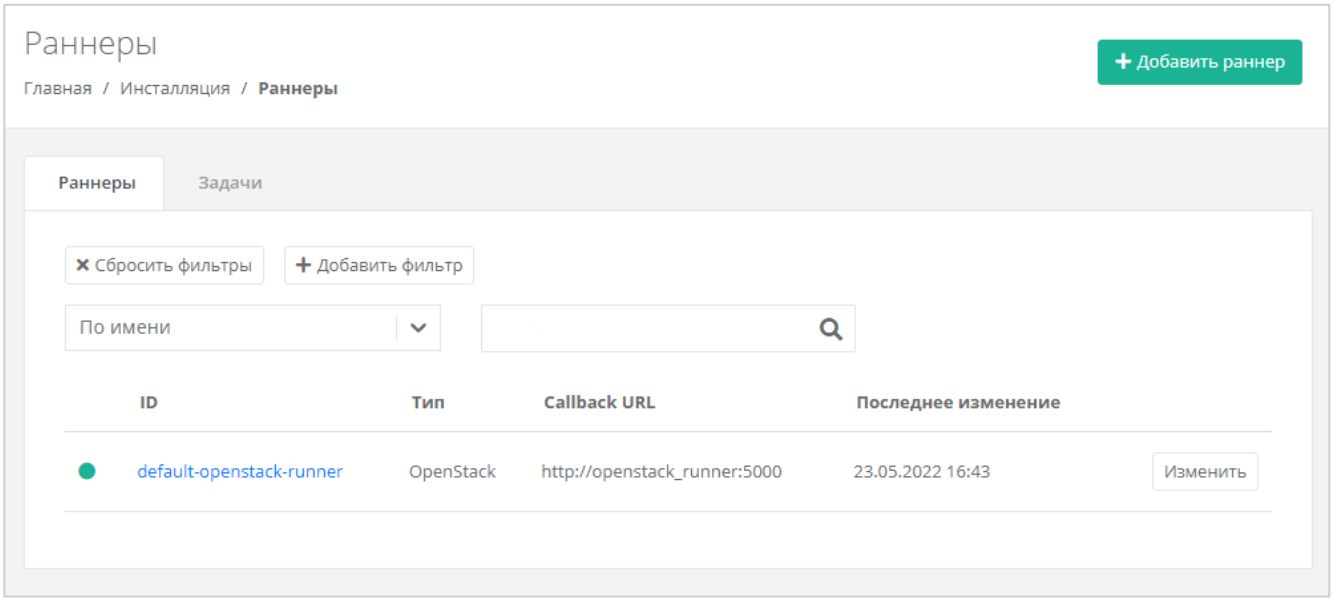

Рисунок 37

4.2.3. Настройка ресурсного пула для сегмента РУСТЭК

Перейдите в раздел меню **Инсталляция** → **Ресурсы** → **Ресурсные пулы** и нажмите на имя ресурсного пула **РУСТЭК** или на кнопку **Изменить**.

На вкладке **Основные настройки** заполните поля настроек (Рисунок 38):

- **Тип** — KVM.
- **Сетевая зона** — сетевая зона для пользовательских внутренних сетей, в данном примере — KVM Zone.
- **Внешняя сеть** — созданная ранее внешняя сеть, в данном примере — extnet_KVM.
- **Раннер** — default-openstack-runner.
- **Включен** — установите флаг.
- **Переподписка vCPU** — для РУСТЭК можно установить любое значение для переподписки vCPU, например, 1.
- **Переподписка RAM** — для РУСТЭК можно установить любое значение для переподписки RAM, например, 1.
- **Ограничения на один сервер**:
  - **vCPU** — максимальное количество виртуальных ядер.
  - **RAM** — максимальный объём оперативной памяти.
  - **Диски** — максимальное количество дисков.
  - **Подключения** — максимальное количество портов, подключённых к серверу и роутеру.

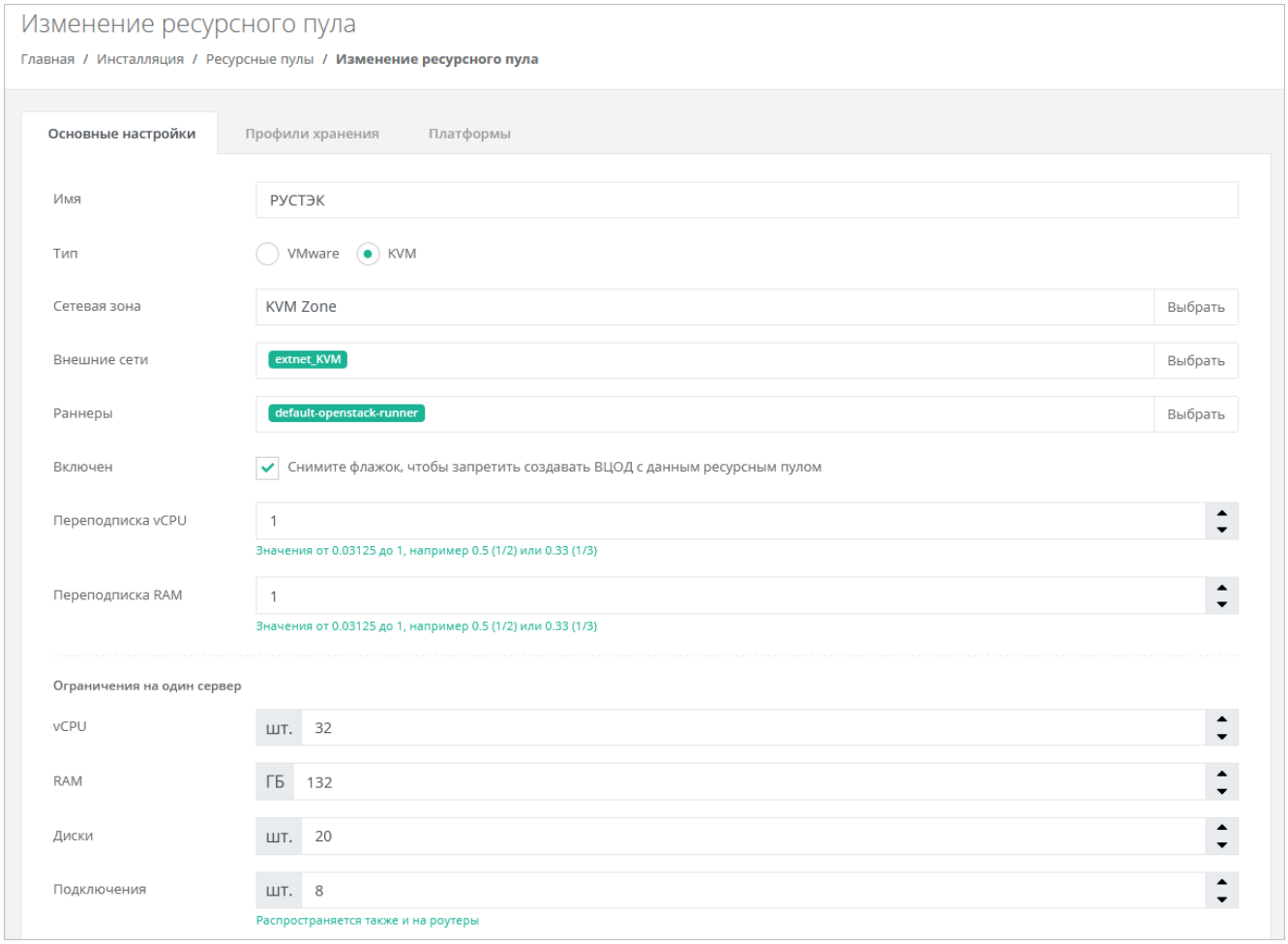

Рисунок 38

Для сегмента РУСТЭК заполнять поля ниже не нужно.

При необходимости можно задать логотип для ресурсного пула — кнопка **Выберите файл…** напротив поля **Иконка** в нижней части вкладки.

Нажмите **Изменить**.

После сохранения новых настроек ресурсного пула РУСТЭК-ЕСУ заберёт адреса сервисных портов РУСТЭК в свою базу данных. В этом можно убедиться, запустив в консоли ВМ ESU-box команду:

```
sudo docker-compose exec api make shell
```

В открывшейся консоли ввести:

```
Port.objects.table('id', 'type', 'network_id', 'ip_address')
```

Появится табличная форма аналогично представленной ниже (Рисунок 39).

Рисунок 39

Количество записей в таблице может отличаться в зависимости от инсталляции, но таблица не должна быть пустой. Если таблица пуста, проверьте, не была ли допущена ошибка в названии внешней сети — поле **Имя на платформе виртуализации** в настройках внешней сети, см. п. 4.2.1. Список внешних сетей в РУСТЭК можно получить, выполнив на одном из управляющих узлов РУСТЭК команду:

```
openstack network list --external
```

Для добавления профиля хранения перейдите на вкладку **Профили хранения** и нажмите кнопку **Добавить профиль хранения**.

В открывшемся окне заполните поля настроек (Рисунок 40):

- **Имя** — в соответствии с подсказкой (SSD, SATA, SAS).
- **Имя типа диска** — в соответствии с доступными типами диска в РУСТЭК.
- **Биллинг-класс** — выберите соответствующий биллинг-класс.
- **Макс. размер диска** — максимальный размер диска в ГБ, который сможет создать пользователь.
- **Позиция** — позиция определяет порядок расположения профилей хранения, который напрямую влияет на то, с каким первым типом диска будет изначально предложено создать новый сервер пользователям клиента.

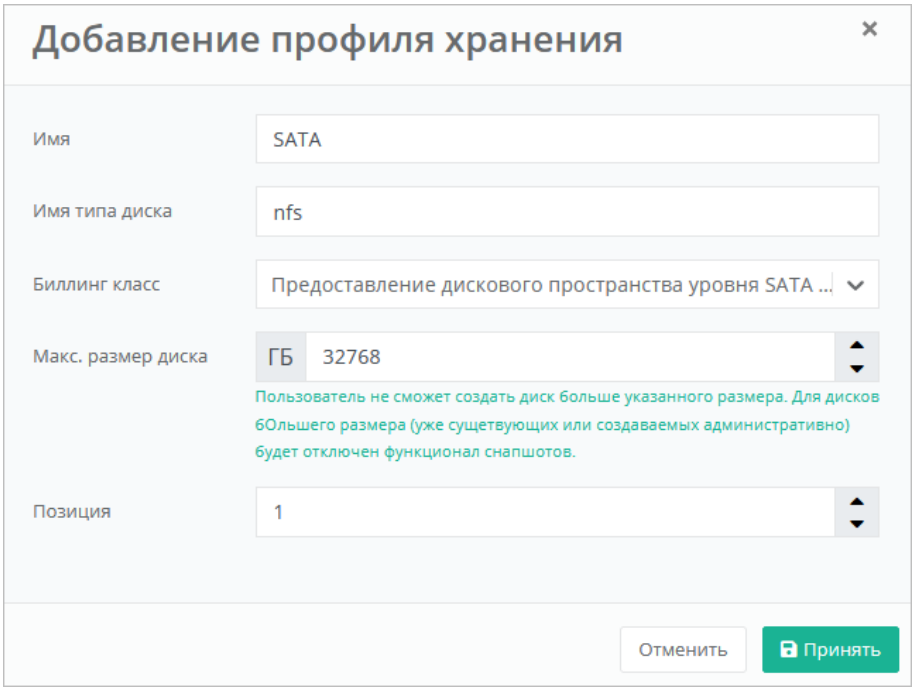

Рисунок 40

Нажмите кнопку **Принять** для добавления профиля хранения.

Имя типа диска в РУСТЭК можно получить, выполнив на одном из управляющих узлов РУСТЭК команду:

```
openstack volume type list --public
```

Будет выведен приблизительно следующий список (Рисунок 41):

```
aio ~ # openstack volume type list --public
+--------------------------------------+-------------+-----------+
| ID                                   | Name        | Is Public |
+--------------------------------------+-------------+-----------+
| c5c47b8e-352c-42ba-94af-9116bf5fb886 | nfs         | True      |
| 77110d5f-0b96-45bf-9df5-65d87df4ed76 | __DEFAULT__ | True      |
+--------------------------------------+-------------+-----------+
```

Рисунок 41

В качестве типа диска в панели управления РУСТЭК-ЕСУ укажите значение поля **Name**. В данном случае это **nfs**.

Далее проверьте правильность заполнения вкладки **Платформа**. Если настройки отсутствуют — нажмите кнопку **Добавить платформу**.

В открывшемся окне заполните поля настроек платформы (Рисунок 42):

- **Имя** — имя платформы, которое будет отображаться у пользователя при конфигурировании платформы.
- **Бил. класс (vCPU)** — выберите биллинг-класс, предназначенный для расчёта стоимости использования виртуальных ядер.
- **Бил. класс (RAM)** — выберите биллинг-класс, предназначенный для расчёта стоимости использования виртуальной оперативной памяти.

- **Позиция** — позиция определяет порядок расположения платформ, который напрямую влияет на то, с каким первым типом vCPU будет изначально предложено создать новый сервер пользователям клиента.
- **Имя агрегата** — имя агрегата из РУСТЭК.

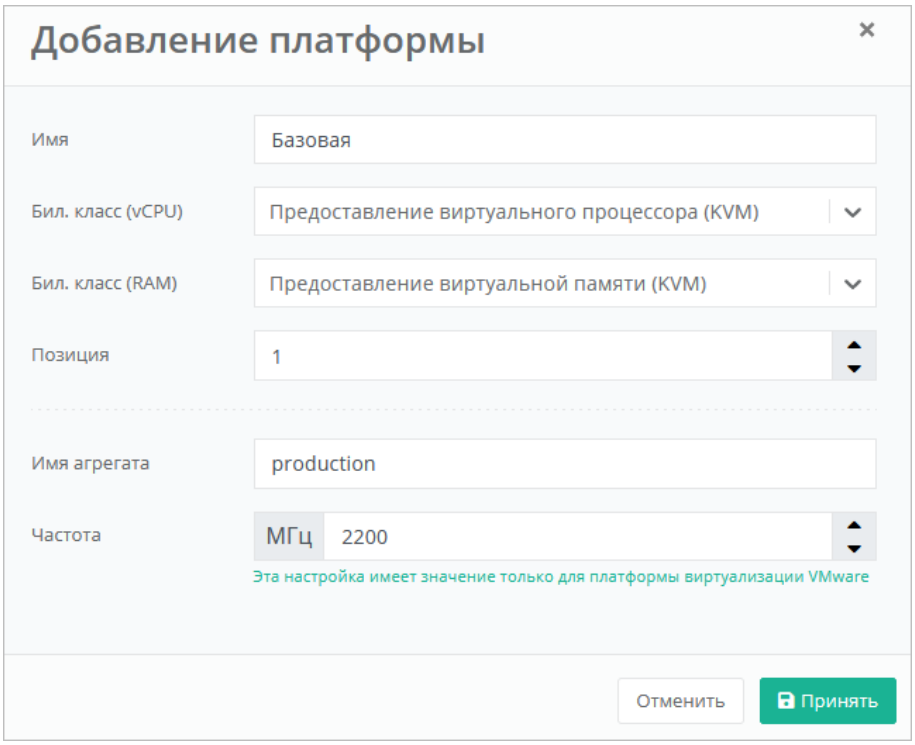

Рисунок 42

Список агрегатов можно получить, выполнив на одном из управляющих узлов РУСТЭК команду:

```
OS_CLOUD=rustack_system openstack aggregate list
```

Будет выведен приблизительно следующий список (Рисунок 43):

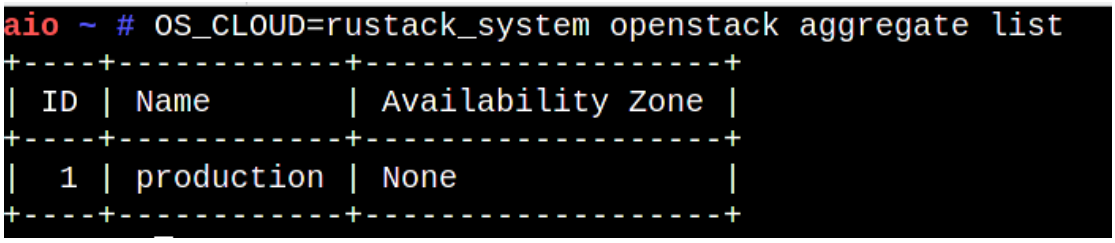

Рисунок 43

Нажмите **Принять** для добавления платформы.

После того, как введены все настройки, в форме изменения ресурсного пула нажмите кнопку **Изменить**.

4.2.4. Создание шаблонов ВМ для сегмента РУСТЭК

Для создания шаблона ВМ необходим образ ОС с cloud-init. На сайте OpenStack есть ссылки для скачивания таких образов: https://docs.openstack.org/image-guide/obtain-images.html

Далее будет рассмотрен пример создания шаблона ВМ с операционной системой Ubuntu 18.04 LTS.

Подключитесь по SSH к одному из управляющих узлов РУСТЭК (логин — **root**, пароль — **rustack**) и скачайте целевой образ, после чего создайте образ в РУСТЭК:

```
curl https://cloud-images.ubuntu.com/bionic/current/bionic-server-cloudimg-
amd64.img --output bionic-server-cloudimg-amd64.img

openstack image create --public --disk-format qcow2 --container-format bare --
property distro=Ubuntu --property hw_disk_bus=scsi --property
hw_scsi_model=virtio-scsi --property hw_vif_model=virtio --property
image_type=master --file bionic-server-cloudimg-amd64.img --min-disk 10 --min-ram
2048 Ubuntu-Bionic-ESU3
```

Последний параметр команды (`Ubuntu-Bionic-ESU3`) — имя образа в РУСТЭК, его необходимо записать или запомнить.

Далее создайте шаблон в РУСТЭК-ЕСУ через панель управления.

Для этого перейдите в меню **Инсталляция** → **Шаблоны** → **Серверы** и нажмите кнопку **Создать шаблон**.

В открывшейся форме заполните поля (Рисунок 44):

- **Ресурсные пулы** — нажмите кнопку **Выбрать** и в открывшемся окне выберите ресурсный пул РУСТЭК.
- **Имя** — введите произвольное имя для шаблона, например, имя ОС.
- **Группа шаблонов** — выберите группу шаблонов или оставьте по умолчанию.
- **Имя шаблона** — нажмите кнопку **Выбрать** — откроется список образов РУСТЭК, в котором необходимо выбрать ранее созданный образ. Нажмите **Применить**.

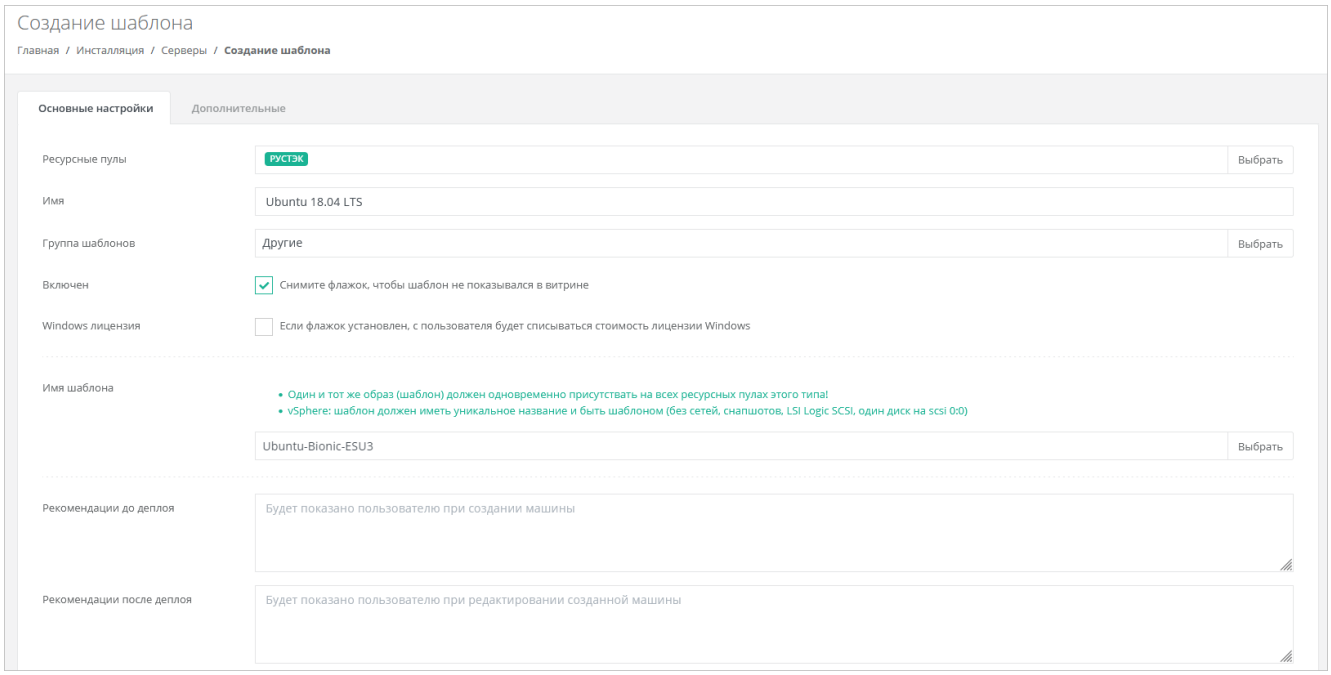

Рисунок 44

Перейдите на вкладку **Дополнительные**.

Укажите минимальное число ядер vCPU (минимум 1 ядро) и объём RAM (минимум 2 Гб — Рисунок 45).

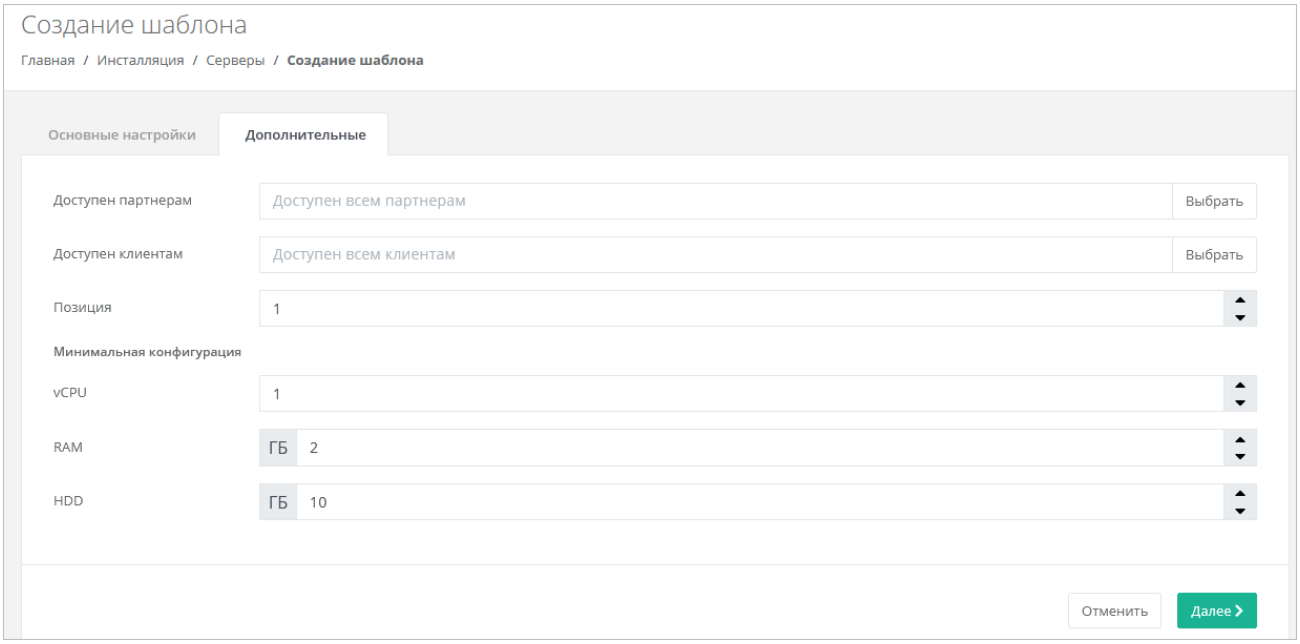

Рисунок 45

Нажмите кнопку **Далее**. Будет создан новый шаблон сервера и появятся дополнительные вкладки в форме изменения шаблона сервера: **Поля для скрипта**, **Скрипт развёртывания** и **Auto DevOps**.

Перейдите на вкладку **Поля для скрипта**. На вкладке добавляются поля метаданных для скрипта развёртывания виртуального сервера. Эти поля появляются на вкладке **Создание сервера** после выбора шаблона при создании пользователем нового сервера. Пользователь заполняет поля различной информацией в зависимости от настроек полей.

Рекомендуется заполнить поля, указанные на скриншоте (Рисунок 46).

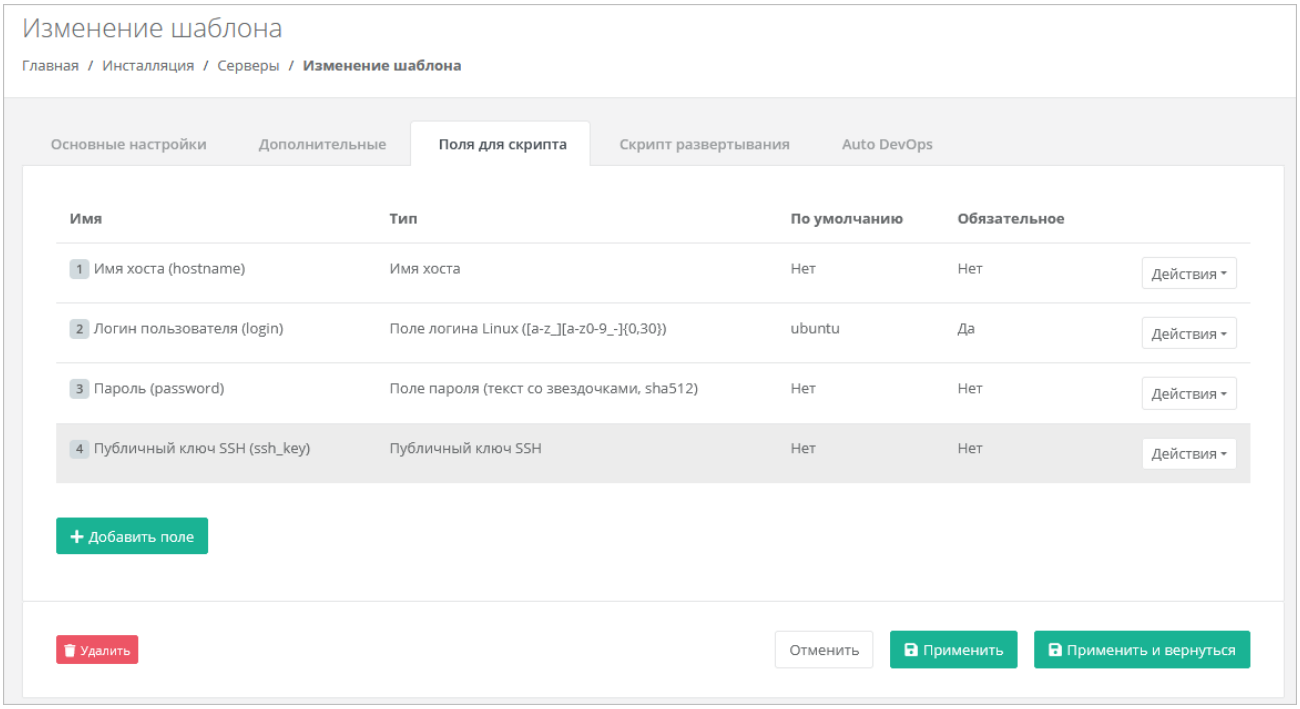

Рисунок 46

Далее на вкладке **Скрипт развёртывания** добавьте скрипт развёртывания.

Скрипт развёртывания применяется во время развёртывания виртуальной машины внутри операционной системы сервера.

Примечание: универсальный скрипт развёртывания для Linux OS приложен ниже в документации в разделе 7.4.

На вкладке **Auto DevOps** можно настроить Auto DevOps-скрипт. Скрипт обращается к API РУСТЭК-ЕСУ для выполнения указанных в скрипте операций.

Auto DevOps-скрипт пишется на языке Python и используется для выполнения дополнительных операций с сервером во время его создания и/или запуска.

Примечание: внесение изменений в Auto DevOps-скрипт рекомендуется только для вендоров. Просьба не редактировать настройки скрипта самостоятельно.

Пример скрипта приведён в Приложении 1.

После внесения изменений в скрипт обязательно нажмите кнопку Применить!

В результате редактирования настроек Auto DevOps-скрипта вносятся изменения в панели управления. Например, применяются необходимые шаблоны брандмауэра после разворачивания виртуальной машины.

После внесения изменений нажмите кнопку **Применить и вернуться**. Созданный шаблон ВМ появится в списке шаблонов, и из него можно будет создавать ВМ.

4.3. Настройка сегмента VMware vSphere

Если для РУСТЭК-ЕСУ необходимо добавить несколько инсталляций VMware vSphere (сегментов), то для каждой из них выполните все нижеперечисленные настройки.

Необходимые работы на стороне VMware для подключения к РУСТЭК-ЕСУ:

1. Создать пользователя esu-admin с правами администратора.
2. Создать Datacenter.
3. Создать кластер хоста(ов) в Datacenter, внутри которого будут создаваться ВМ и Edge-роутеры.
4. Создать Datastore Cluster из датастора(ов), на котором будут размещаться пользовательские Edge-роутеры и служебные сервисы.
5. Создать Datastore Cluster из датастора(ов), на котором будут размещаться диски пользователей (можно использовать из пункта 4).
6. Создать vSphere Distributed Switch (vDS), под которым будут создаваться пользовательские сети (порт-группы).

4.3.1. Создание маршрутизируемой сети

Создайте маршрутизируемую сеть, в которой развёрнута и работает ВМ с РУСТЭК-ЕСУ (ESU-box), настройки сети должны совпадать с настройками маршрутизируемой сети внутри РУСТЭК. Маршрутизируемая сеть — портгруппа на vDS в vSphere (требуется один VLAN ID). Необходимо учитывать, что в эту сеть будут подключены пользовательские роутеры для сегмента VMware. В разделе 7.3 описана процедура, позволяющая изменить такое поведение, для этого следует создать отдельную сеть для роутеров.

Таким образом, размер подсети напрямую влияет на максимальное число ВЦОД. ESU-box станет DHCP-сервером в этой подсети (также возможна установка в сеть, где уже присутствует DHCP-сервер). В данном примере сеть называется vlan3058 (*Создание:* Рисунок 47, Рисунок 48*, Редактирование:* Рисунок 49 и Рисунок 50).

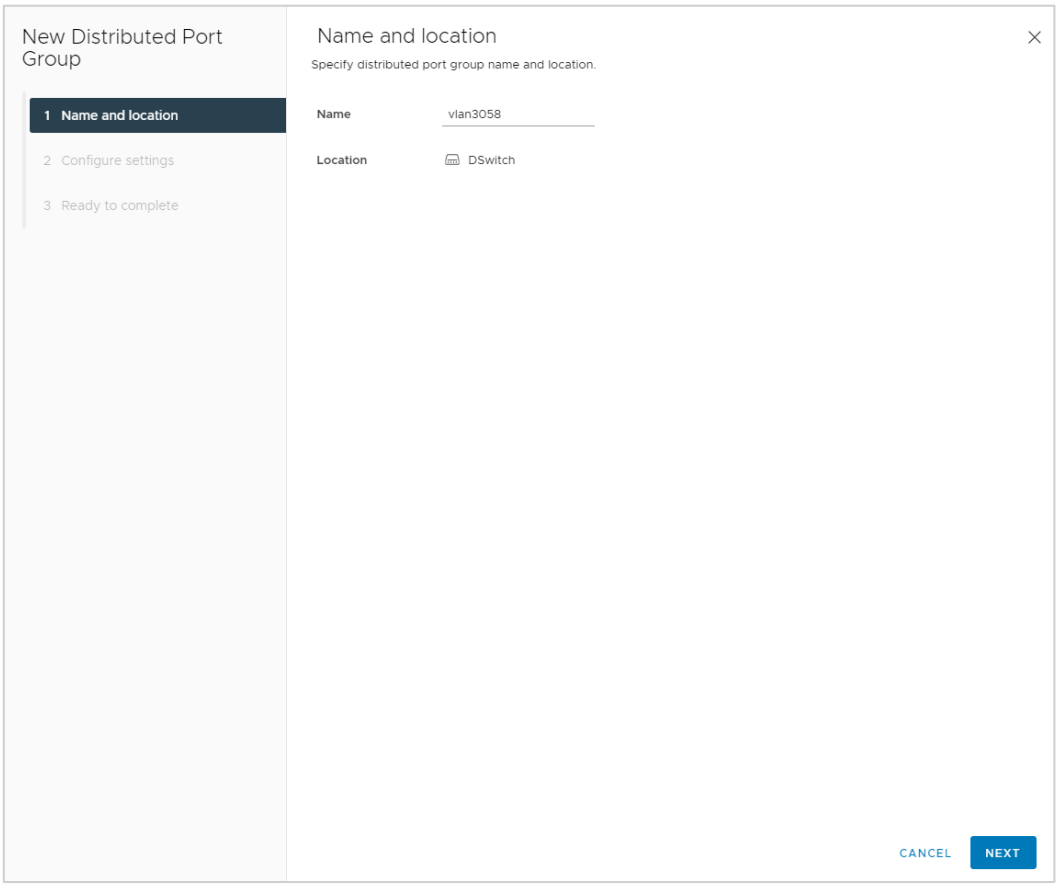

Рисунок 47

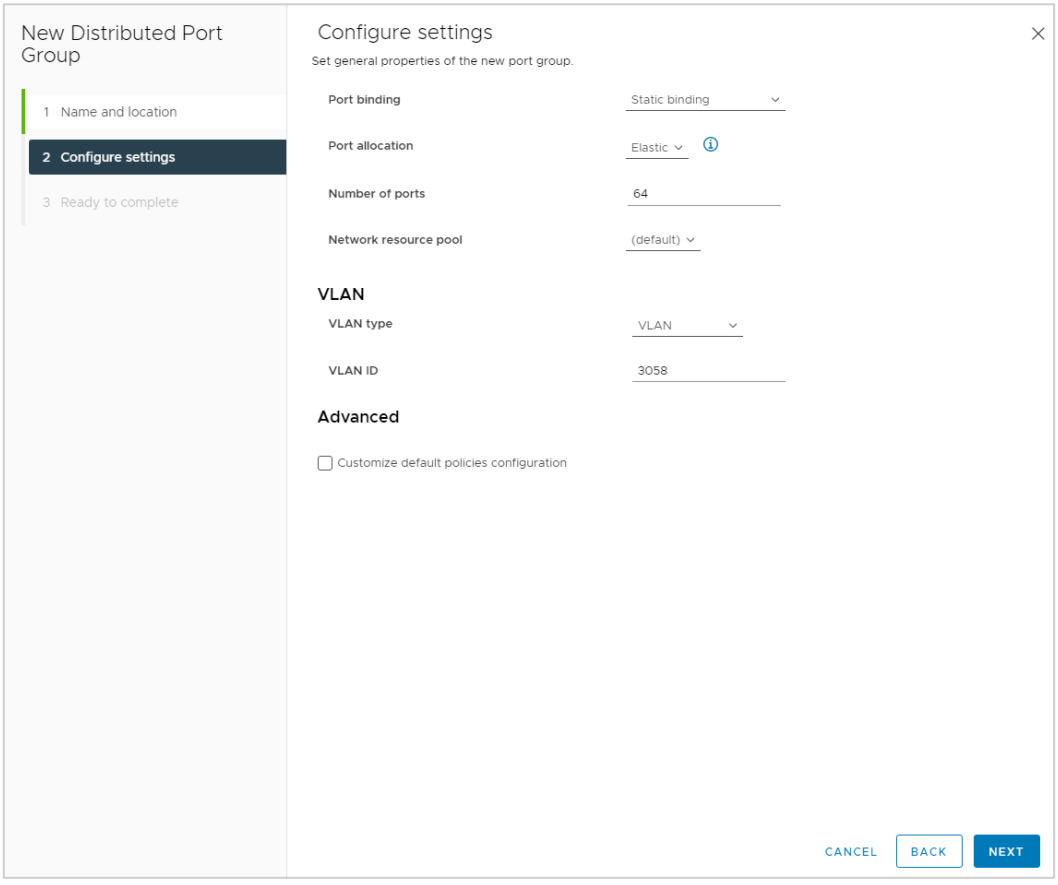

Рисунок 48

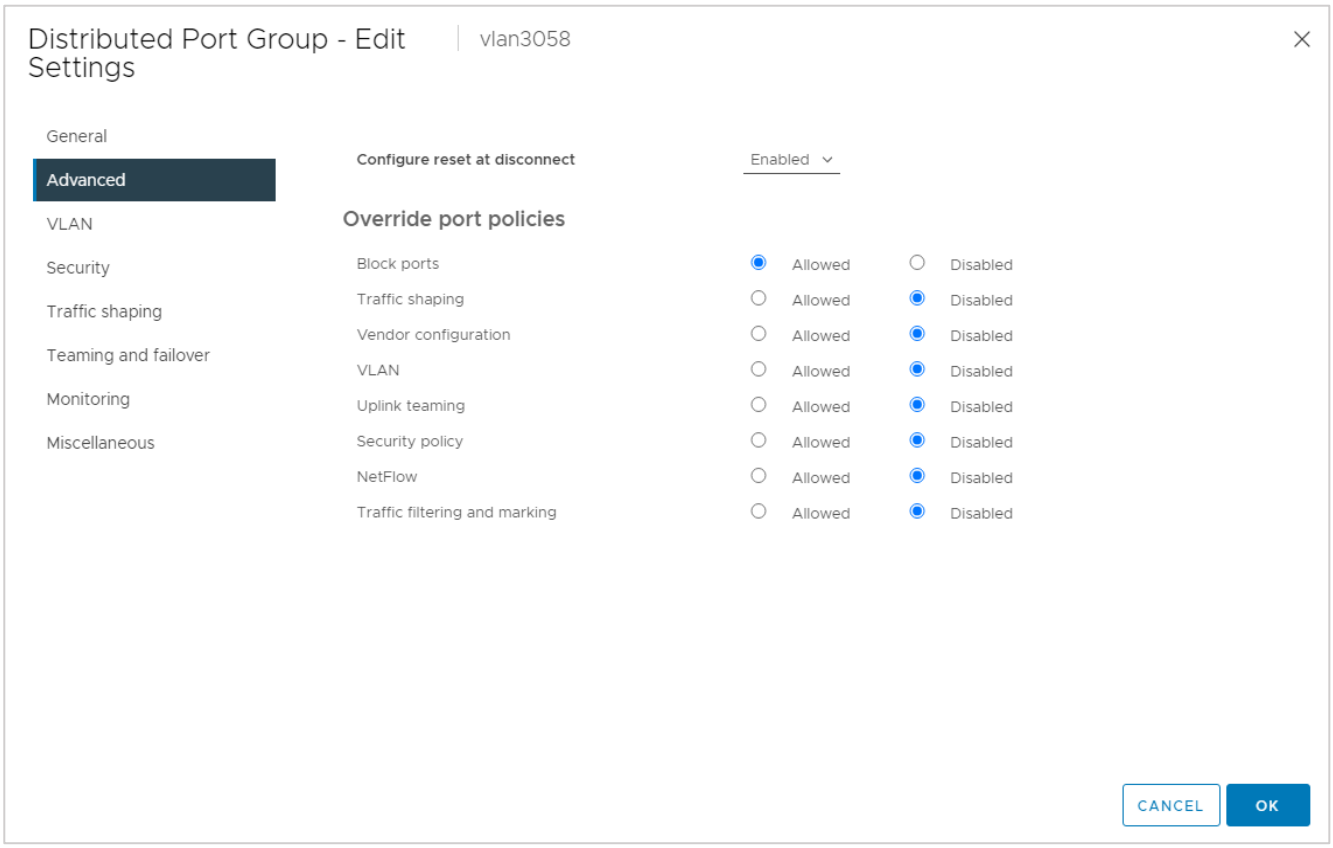

Рисунок 49

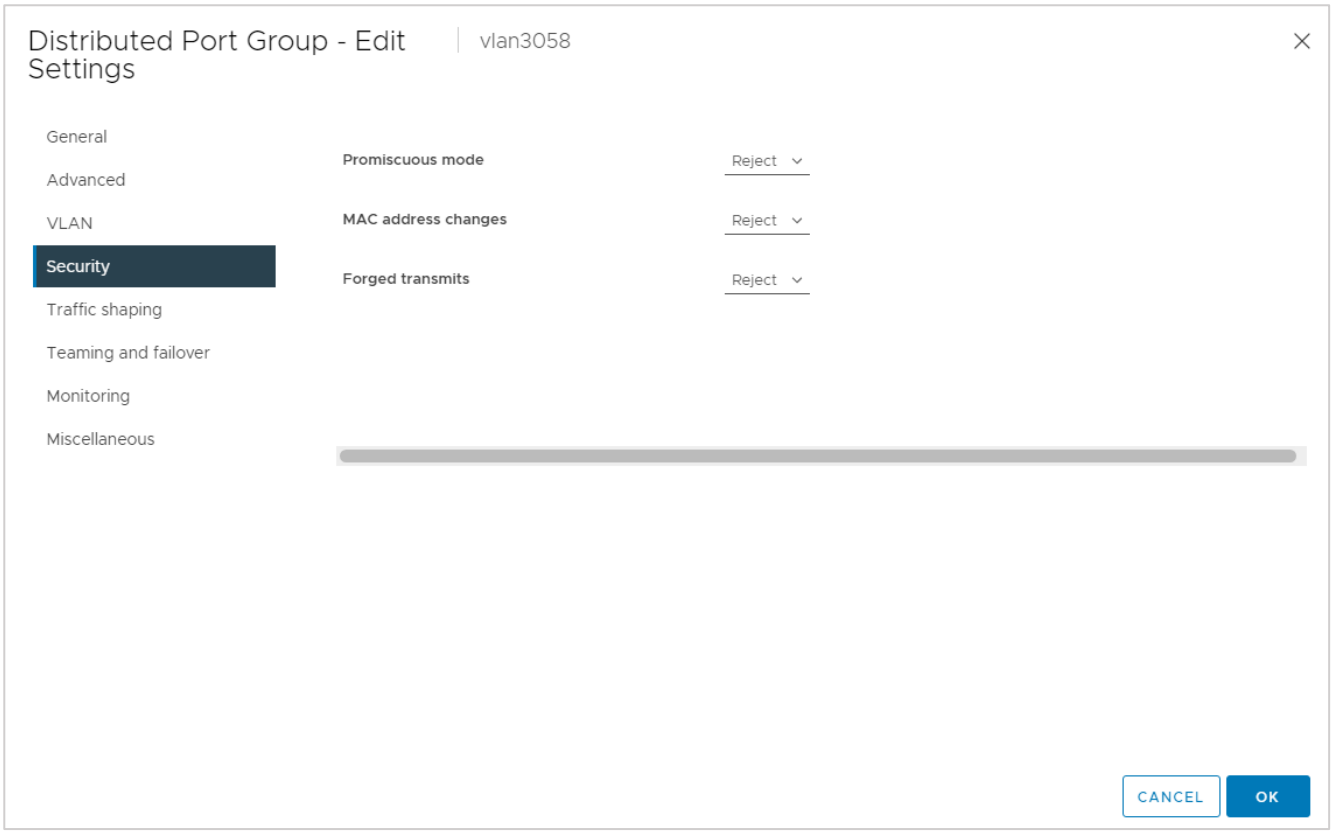

Рисунок 50

4.3.2. Создание директории для ВЦОДов клиентов

Создайте в датацентре корневую директорию, в которой будут располагаться ВЦОДы клиентов, например, ESU3-Test. В этой директории создайте директорию Management (Рисунок 51), которая понадобится при развёртывании Edge-роутера.

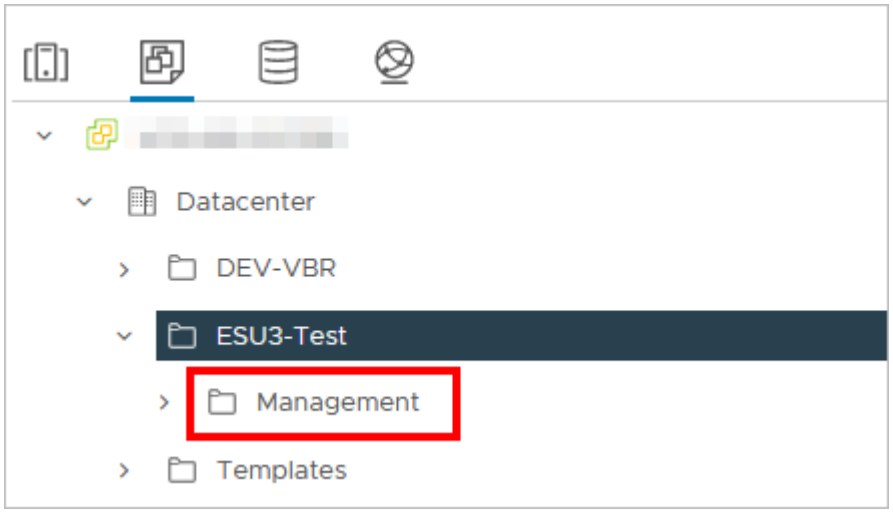

Рисунок 51

4.3.3. Настройка сетевых зон для сегмента VMware vSphere

Создайте сетевую зону для пользовательских внутренних сетей.

Для этого перейдите в раздел меню **Инсталляция** → **Ресурсы** → **Сетевые зоны** и нажмите кнопку **Создать сетевую зону**.

Введите название сетевой зоны, выберите сегмент, например, VLAN и нажмите кнопку **Далее** (Рисунок 52). Появится возможность добавления пулов.

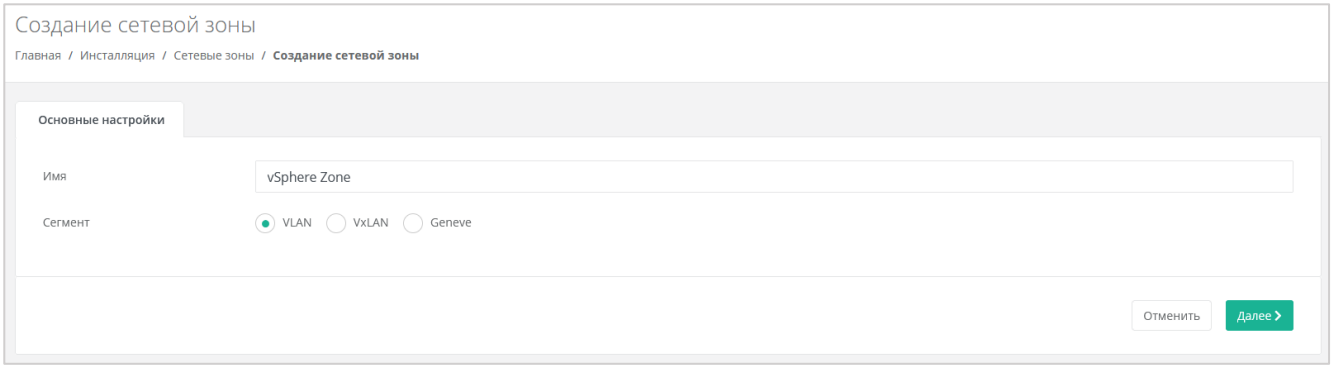

Рисунок 52

Укажите диапазон VLAN для пользовательских сетей: в данном случае 3060–3090. Для этого нажмите кнопку **Добавить пул** и в открывшемся окне введите значения начала и конца диапазона. В результате в поле **Пулы** появится новый диапазон (Рисунок 53).

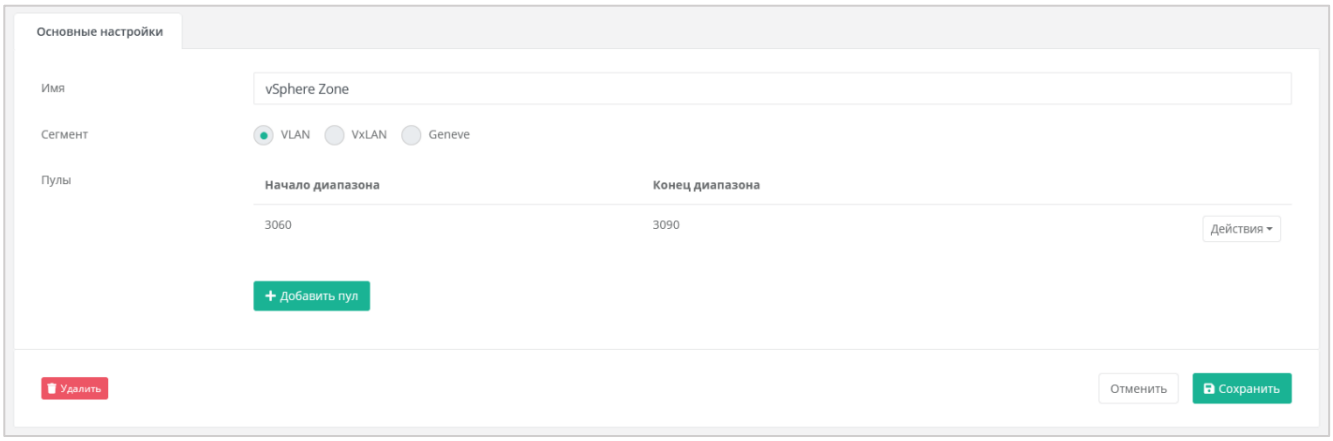

Рисунок 53

Аналогично создайте вторую сетевую зону для **внешней** сети, например, в сегменте VLAN (Рисунок 54).

VLAN 3227 будет использоваться для публичных IP-адресов пользовательских ВЦОД — установите его в начало и конец диапазона.

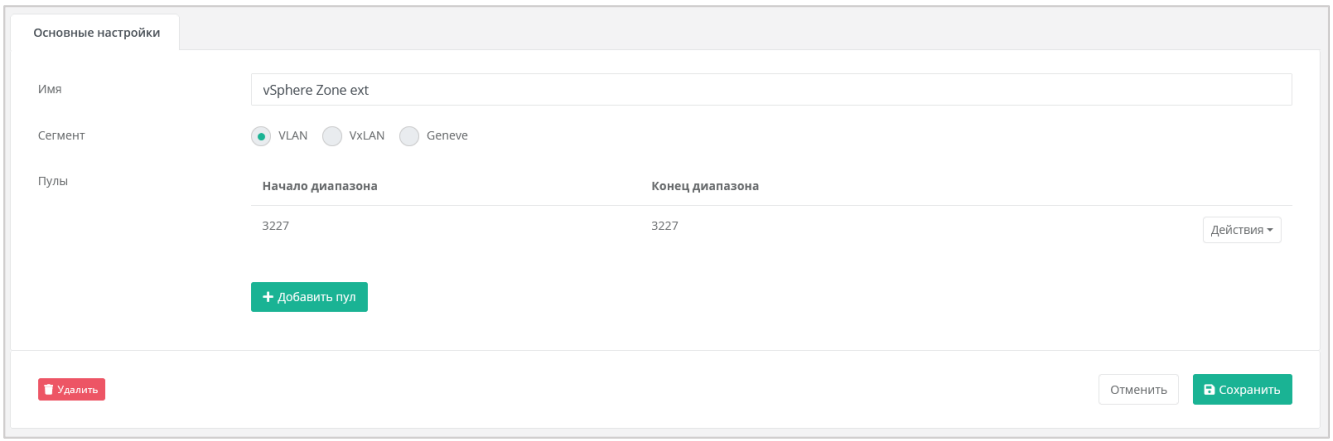

Рисунок 54

Создайте внешнюю сеть для сегмента VMware vSphere.

Перейдите в меню **Инсталляция** → **Ресурсы** → **Сети и IP** и нажмите кнопку **Создать сеть**.

В открывшейся форме заполните следующие поля настроек (Рисунок 55):

- **Имя** — любое название сети.
- **Сетевая зона** — созданная ранее для внешней сети VMware-сегмента.
- **VID/VNID** — VLAN внешней сети: в нашем случае — 3227.
- **Тип сети** — внешняя.
- **Имя на платформе виртуализации** — введите имя сети на платформе виртуализации, которая соответствует указанному VLAN.

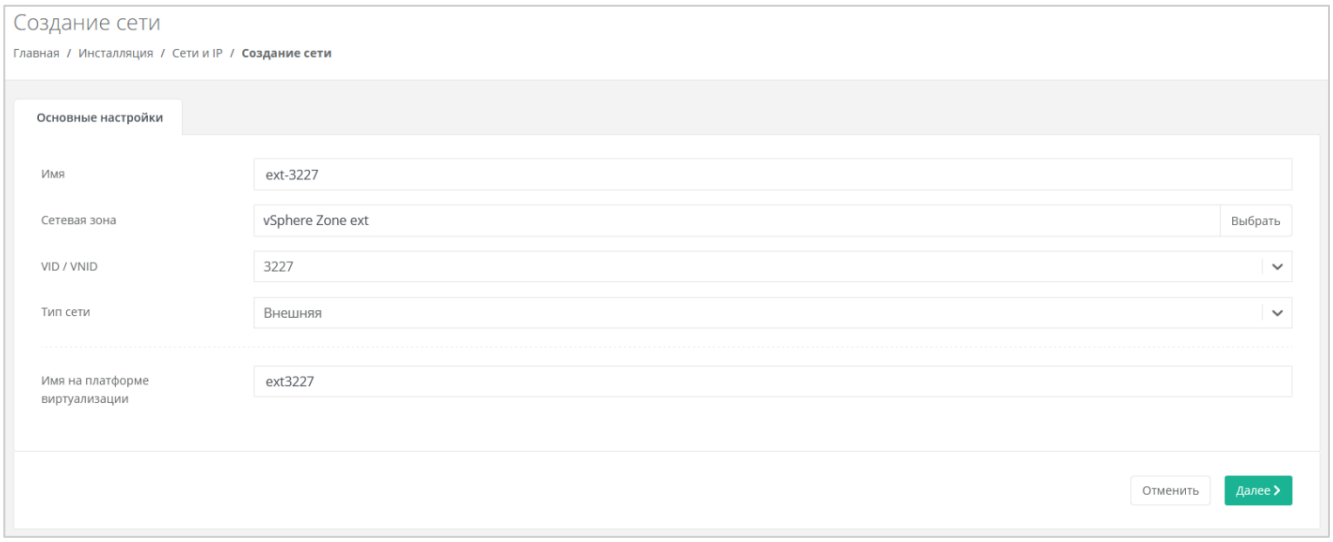

Рисунок 55

После заполнения основных настроек нажмите кнопку **Далее**. Появится возможность добавления подсетей.

Нажмите кнопку **Добавить подсеть**. Откроется окно **Добавление подсети**.

DHCP должен быть **выключен**, CIDR необходимо указывать полный. Если нужно уменьшить диапазон выдаваемых IP-адресов, можно указать произвольный диапазон (Рисунок 56).

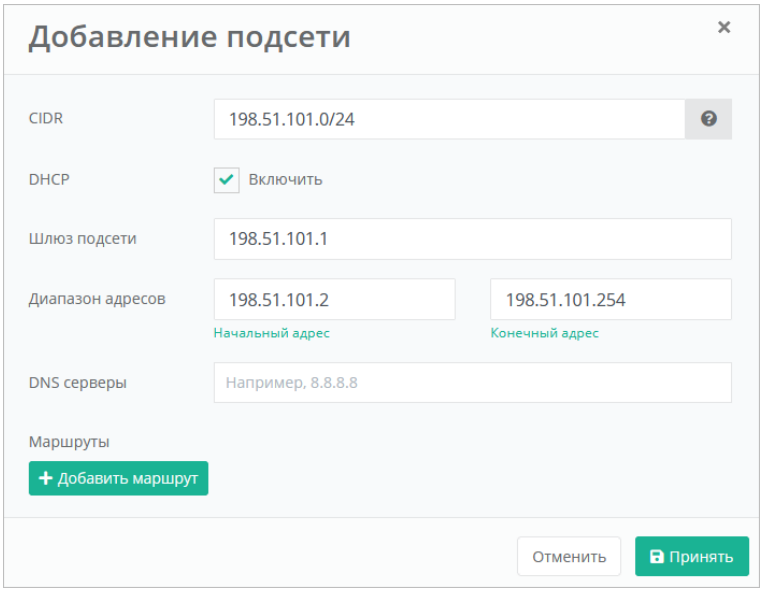

Рисунок 56

Нажмите кнопку **Принять** для добавления подсети.

4.3.4. Настройка vSphere-раннера РУСТЭК-ЕСУ

Перейдите в раздел меню **Инсталляция** → **Система** → **Раннеры** и выберите раннер **default-vsphere-runner**. В открывшейся форме заполните поля (Рисунок 57):

- **Название датацентра** — название должно соответствовать фактическому названию в vSphere (например, Datacenter, см. Рисунок 58).
- **IP-адрес хоста vCenter** — IP-адрес хоста, на котором установлен vCenter.

- **Имя пользователя для взаимодействия с vCenter** — имя администратора в vSphere.
- **Пароль** — пароль администратора в vSphere.
- **Имя dvswitch, под которым будут создаваться сети** — имя vDS, под которым будут создаваться сети (порт-группы). Например: DSwitch0.

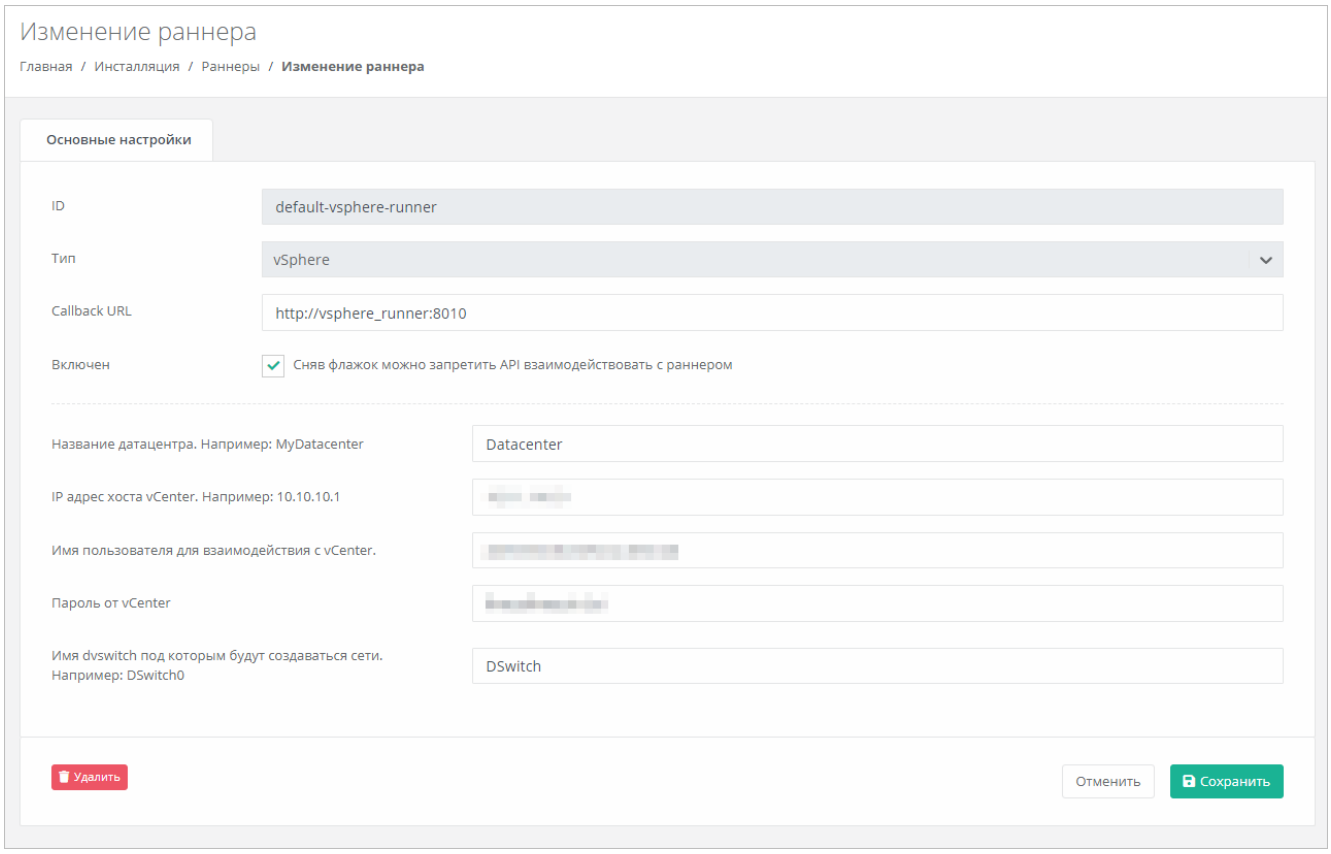

Рисунок 57

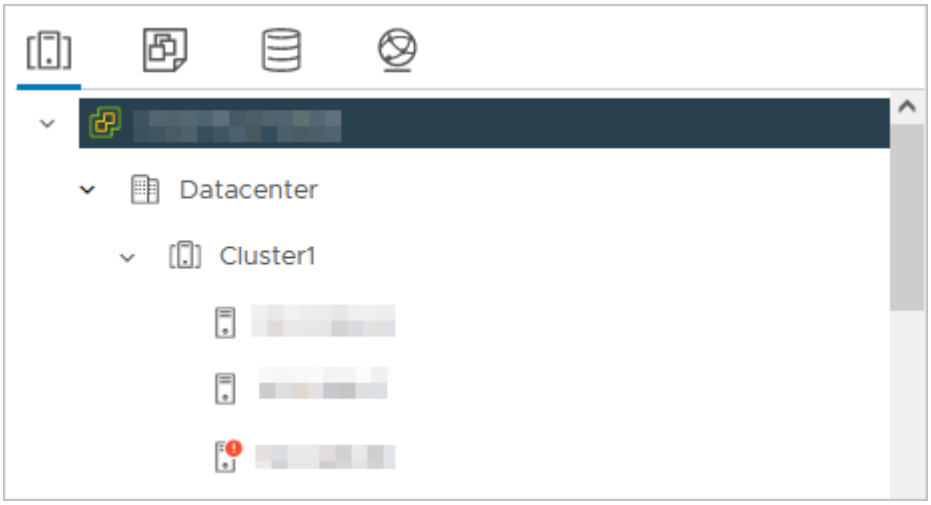

Рисунок 58

Нажмите **Сохранить**.

Если настройки введены правильно, индикатор vSphere-раннера должен быть зелёным ● (Рисунок 59).

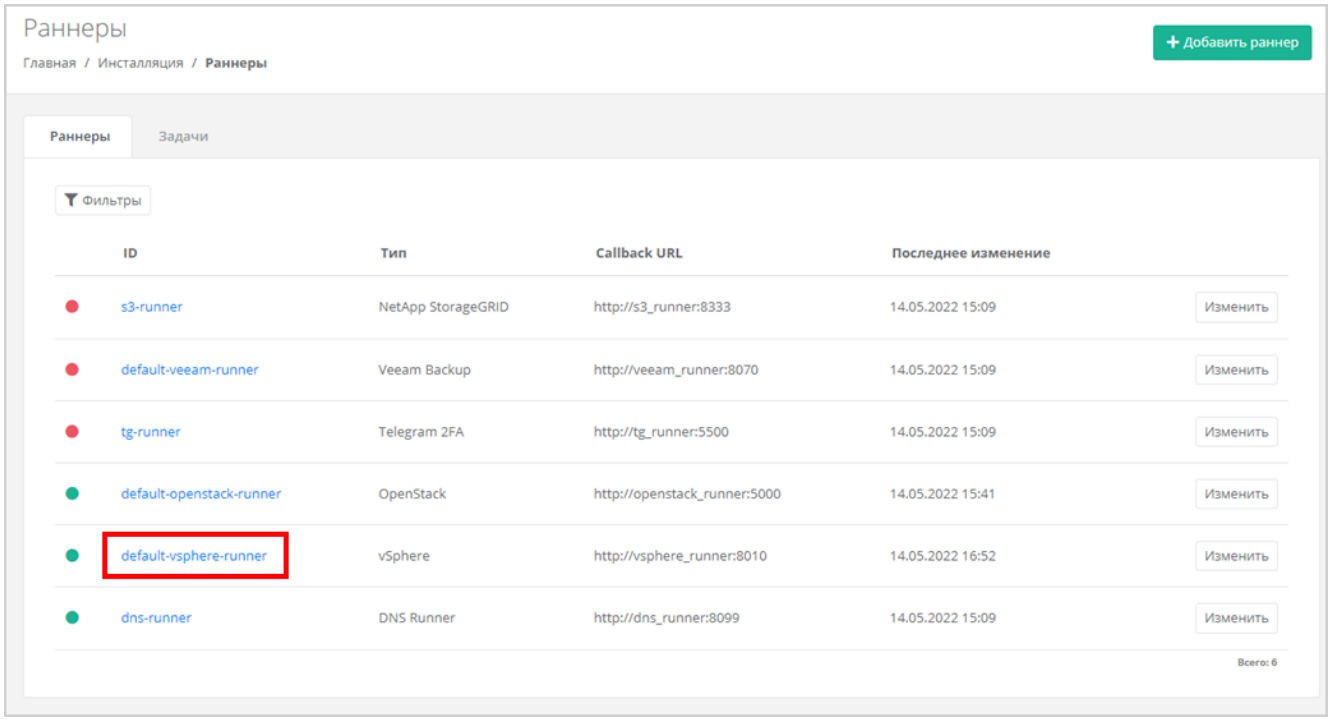

Рисунок 59

Создайте новый токен для пользователя runner — он понадобится для дальнейших настроек. Для создания токена перейдите в раздел меню **Администрирование** → **Пользователи** и для пользователя runner нажмите **Действия** → **Создать токен**. После подтверждения действия скопируйте токен.

4.3.5. Настройка ресурсного пула для сегмента VMware vSphere

Перейдите в раздел меню **Инсталляция** → **Ресурсы** → **Ресурсные пулы** и нажмите на имя ресурсного пула **VMware** или на кнопку **Изменить**.

На вкладке **Основные настройки** заполните поля настроек (Рисунок 60):

- **Тип** — VMware.
- **Сетевая зона** — сетевая зона для пользовательских внутренних сетей, в данном примере — vSphere Zone.
- **Внешняя сеть** — созданная ранее внешняя сеть, в данном примере — ext-3227.
- **Раннер** — default-vsphere-runner.
- **Включен** — установите флаг.
- **Переподписка vCPU** — отношение количества физических ядер к количеству выделенных для ВМ виртуальных ядер. Значение переподписки должно находиться в диапазоне от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3).
- **Переподписка RAM** — отношение объёма физической оперативной памяти к суммарному объёму выделенной для ВМ виртуальной оперативной памяти. Значение переподписки должно находиться в диапазоне от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3).
- **Ограничения на один сервер**:
  - **vCPU** — максимальное количество виртуальных ядер.
  - **RAM** — максимальный объём оперативной памяти.

- **Диски** — максимальное количество дисков.
- **Подключения** — максимальное количество портов, подключённых к серверу и роутеру.

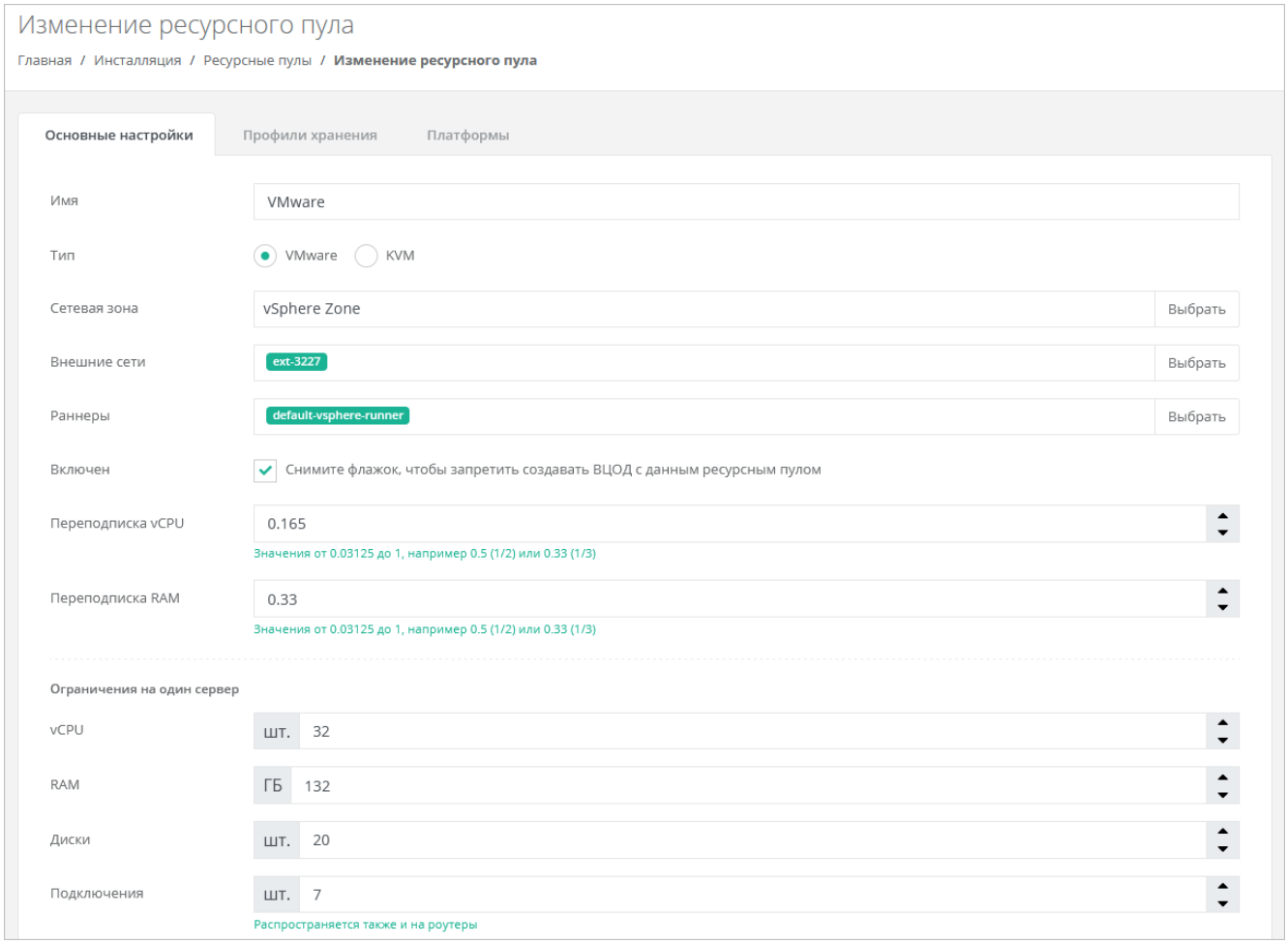

Рисунок 60

Ниже на той же странице укажите следующие настройки (Рисунок 61):

- **Название шаблона роутера** — укажите «edge».
- **Название management-сети (порт-группы), в которой работает РУСТЭК-ЕСУ** — введите название маршрутизируемой сети, создание которой рассматривалось в подразделе 4.3.1.
- **Название служебного датастора**, на котором будут размещаться пользовательские роутеры и служебные сервисы.
- **Адрес РУСТЭК-ЕСУ в management-сети, по которому будет доступно API** — адрес ВМ с РУСТЭК-ЕСУ в маршрутизируемой сети.
- **Токен, который будет использоваться Edge-роутерами для работы с РУСТЭК-ЕСУ** (был создан шагом выше).
- **Название директории, в которой будут расположены ВЦОДы клиентов** — укажите директорию ESU3-Test, создание которой рассматривалось в подразделе 4.3.2.
- При необходимости можно задать логотип для ресурсного пула — кнопка **Выберите файл…** напротив поля **Иконка**.

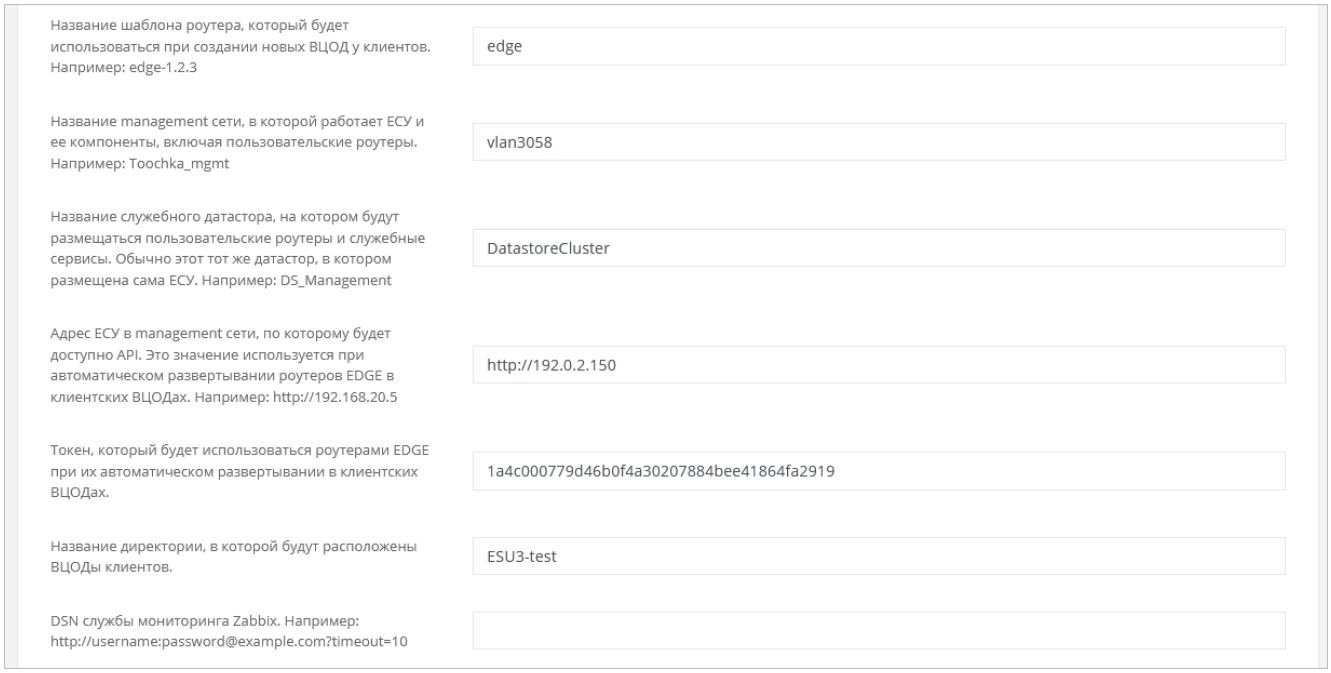

Рисунок 61

На вкладке **Профили хранения** добавьте профили хранения.
Для этого нажмите кнопку **Добавить профиль хранения**.
В открывшемся окне заполните поля настроек (Рисунок 62):

- **Имя** — в соответствии с подсказкой: SSD, SATA, SAS.
- **Имя SDRS-кластера** — название Storage DRS-кластера vSphere (Рисунок 63), который будет использоваться для хранения дисков ВМ.
- **Биллинг-класс** — выберите соответствующий биллинг-класс.
- **Макс. размер диска** — максимальный размер диска в ГБ, который сможет создать пользователь.
- **Позиция** — определяет порядок расположения профилей хранения, который напрямую влияет на то, с каким первым типом диска будет изначально предложено создать новый сервер пользователям клиента.

Нажмите **Принять** для добавления профиля хранения.

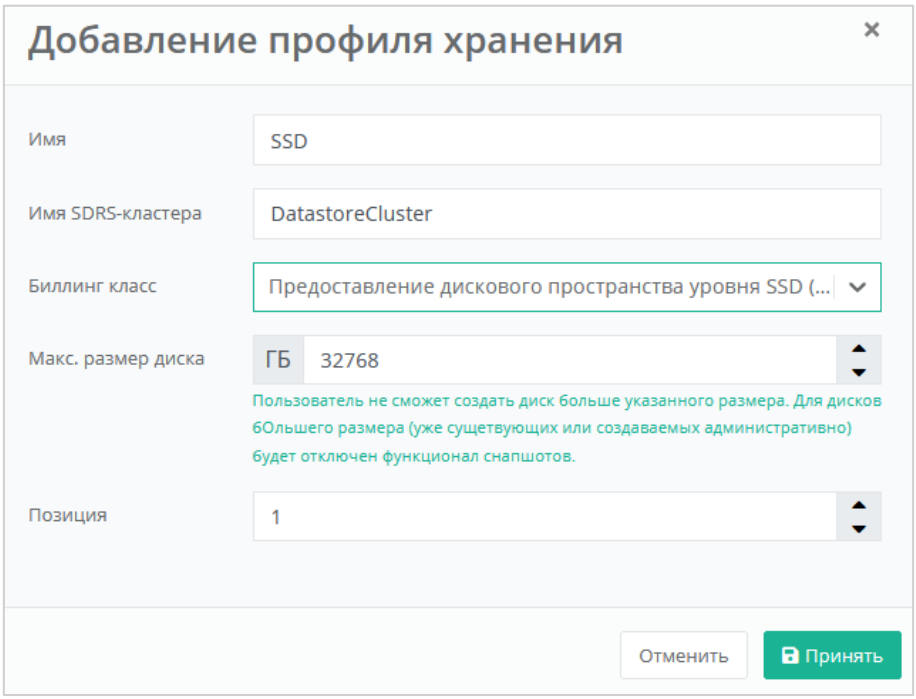

Рисунок 62

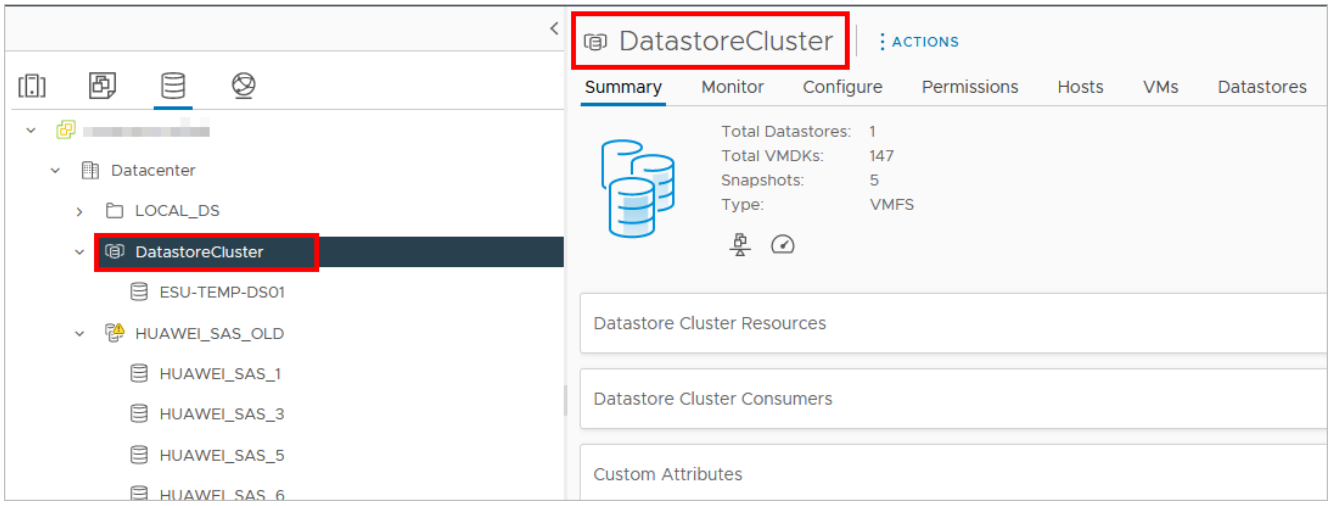

Рисунок 63

Далее перейдите на вкладку **Платформы** (Рисунок 60) и нажмите кнопку **Добавить платформу**, если в списке нет ни одной платформы.

В открывшемся окне заполните поля настроек платформы (Рисунок 64):

- **Имя** — имя платформы, которое будет отображаться у пользователя при конфигурировании платформы.
- **Бил. класс (vCPU)** — выбирается биллинг-класс, предназначенный для расчёта стоимости использования виртуальных ядер.
- **Бил. класс (RAM)** — выбирается биллинг-класс, предназначенный для расчёта стоимости использования виртуальной оперативной памяти.
- **Позиция** — определяет порядок расположения платформ, который напрямую влияет на то, с каким первым типом vCPU будет изначально предложено создать новый сервер пользователям клиента.

- **Имя кластера** — имя созданного кластера — в данном примере **Cluster1**.

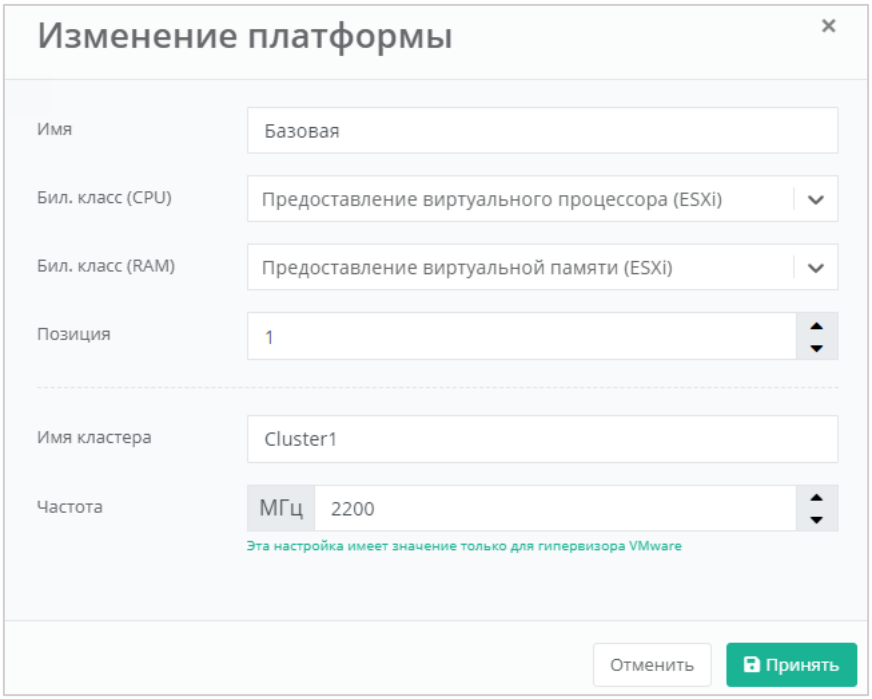

Рисунок 64

Нажмите кнопку **Принять** для добавления платформы.

После того, как введены все настройки, в форме изменения ресурсного пула нажмите кнопку **Изменить**.

4.3.6. Развёртывание Edge-роутера

После настройки раннера vSphere и ресурсного пула выполните развёртывание Edge-роутера из готового шаблона в формате .ova.

Edge-роутер — виртуальная машина, которая выполняет функции маршрутизации трафика, а также реализует функции балансировки нагрузки, брандмауэра, DHCP, NAT и др.

Развёртывание будет произведено на все ресурсные пулы VMware, настроенные в системе.

Для развёртывания роутера подключитесь по SSH к ESU-box со стандартной учётной записью: логин **deploy**, пароль **1-qpALzm/**, и посмотрите, какая последняя версия роутера доступна в данной версии РУСТЭК-ЕСУ с помощью команды:

```
ls -lah | grep edge*.ova
```

Затем выполните команду:

```
toochkactl edge-deploy --filename edge-x.x.x.ova
```

где `x.x.x` — последняя доступная версия роутера.

В целях безопасности измените логин и пароль учётной записи после настройки!

Инструмент toochkactl произведёт развёртывание шаблона роутера (в формате .ova) на ресурсных пулах (Рисунок 65).

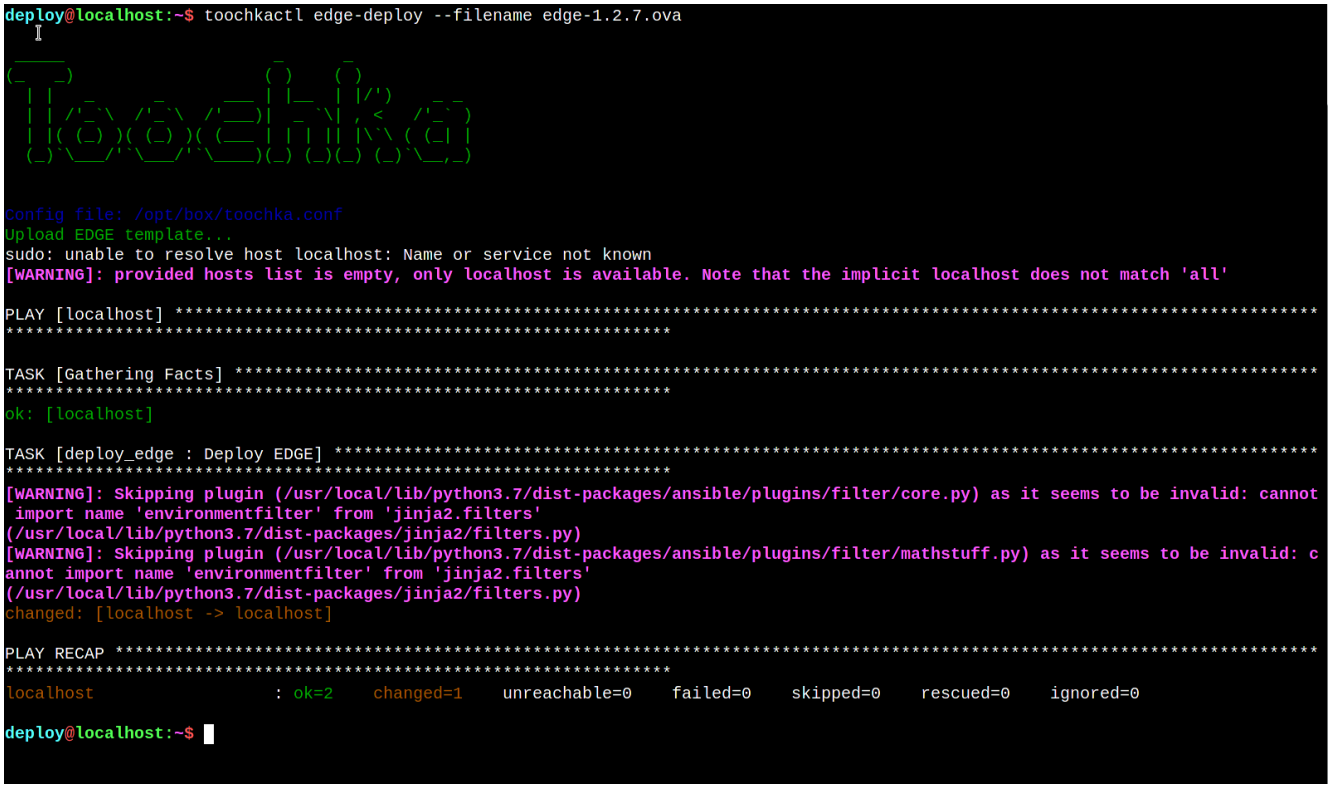

Рисунок 65

В силу особенностей развёртывания шаблона у вас должна быть стандартная портгруппа с названием «VM Network».

После завершения развёртывания на vSphere появится выключенная ВМ с названием «edge-x.x.x» (Рисунок 66), а в настройках ресурсного пула вместо «edge» будет прописана актуальная версия роутера.

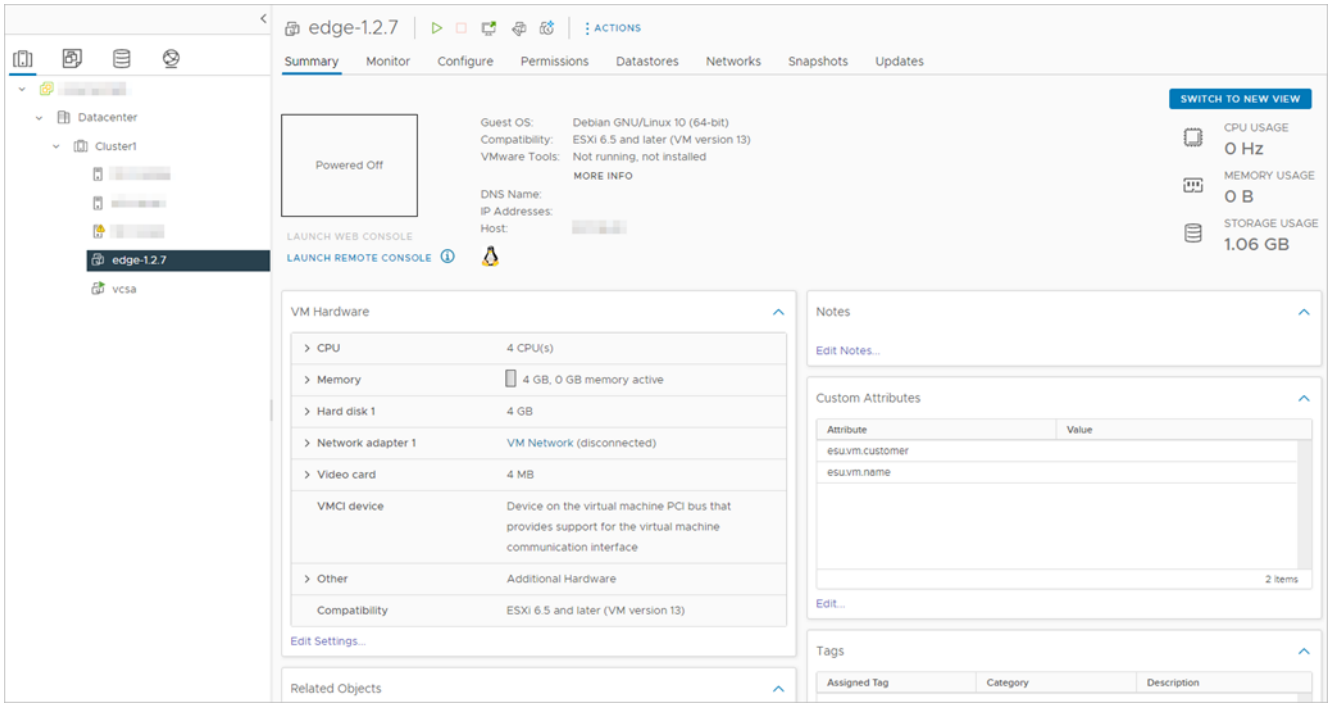

Рисунок 66

После этого РУСТЭК-ЕСУ будет готова к созданию ВЦОД в сегменте VMware.

4.3.7. Создание шаблонов ВМ для сегмента VMware vSphere

Для создания шаблона ВМ необходим образ ОС с cloud-init в формате .ova.

Далее будет рассмотрен пример создания шаблона ВМ с операционной системой Ubuntu 18.04 LTS.

Ссылка на используемый в примере образ:

https://cloud-images.ubuntu.com/bionic/current/bionic-server-cloudimg-amd64.ova

Выполните вход в vSphere Client. Создайте папку, где будут храниться шаблоны, затем нажмите правой кнопкой мыши на папку и выберите **Deploy OVF Template**.

Далее в мастере развёртывания (Рисунок 67–Рисунок 74) укажите ссылку на используемый образ, имя создаваемой ВМ, папку, кластер, на котором она будет развёрнута, хранилище, на котором будет находиться ВМ (при указании типа диска укажите **Thin provision**).

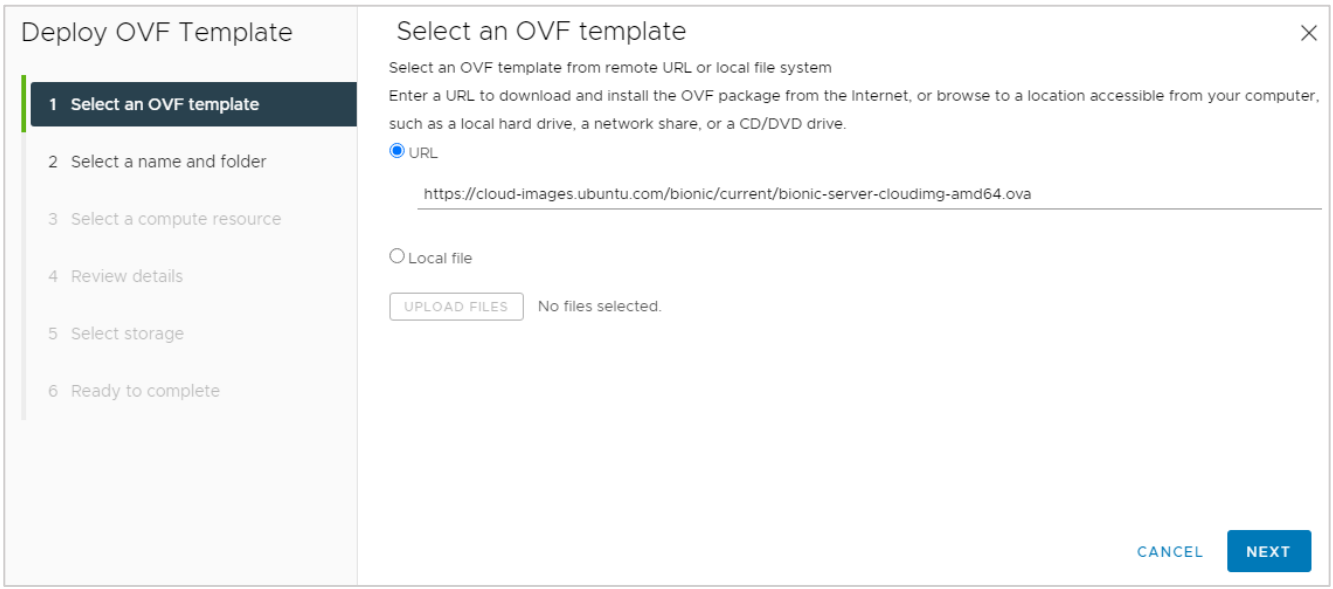

Рисунок 67

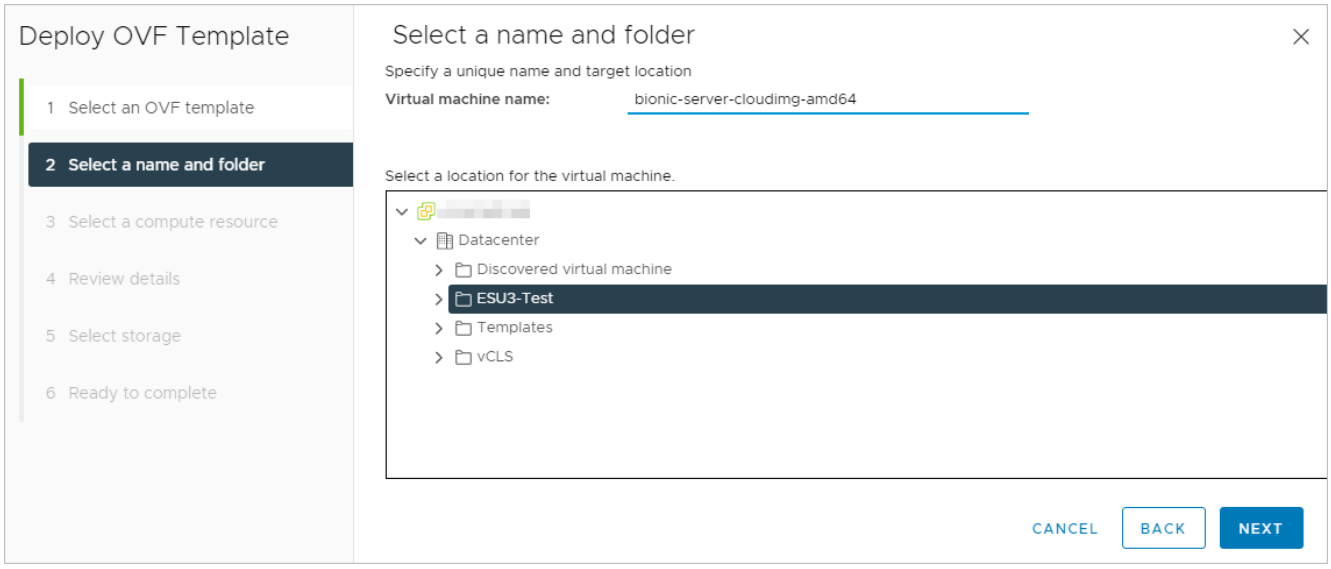

Рисунок 68

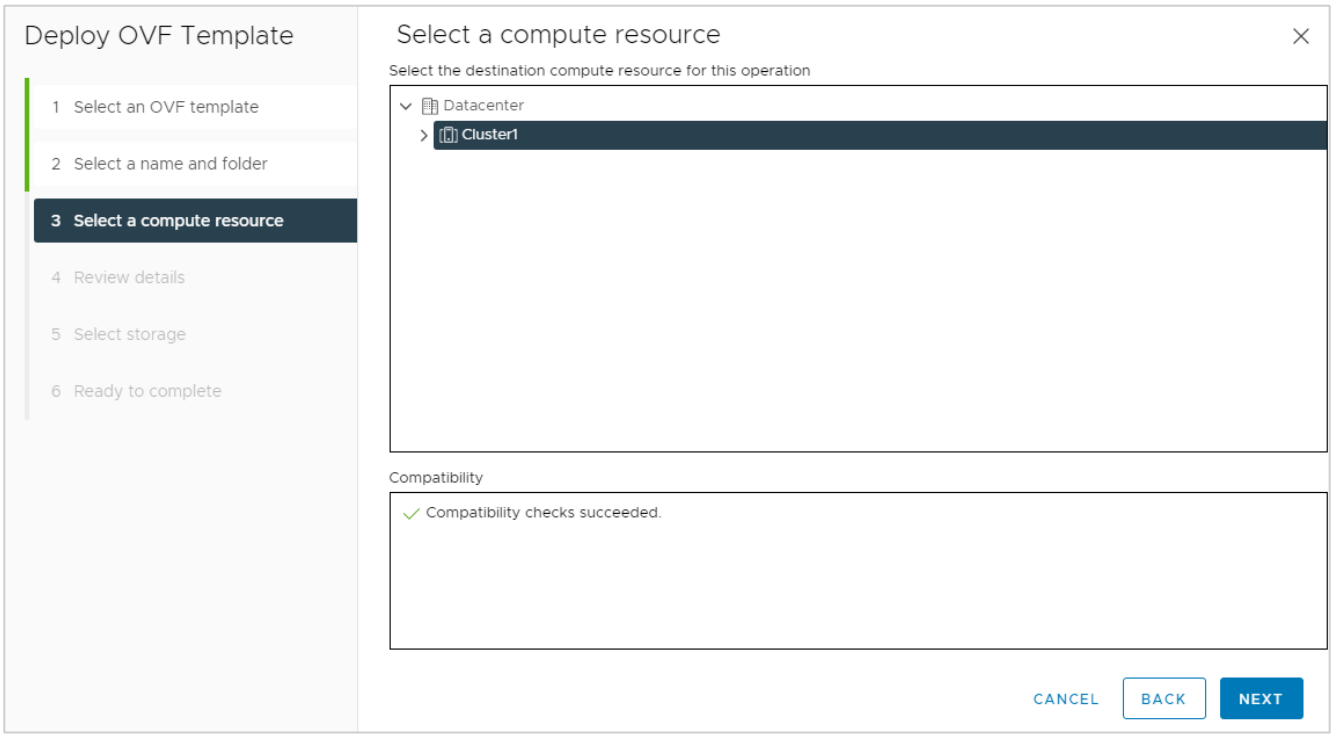

Рисунок 69

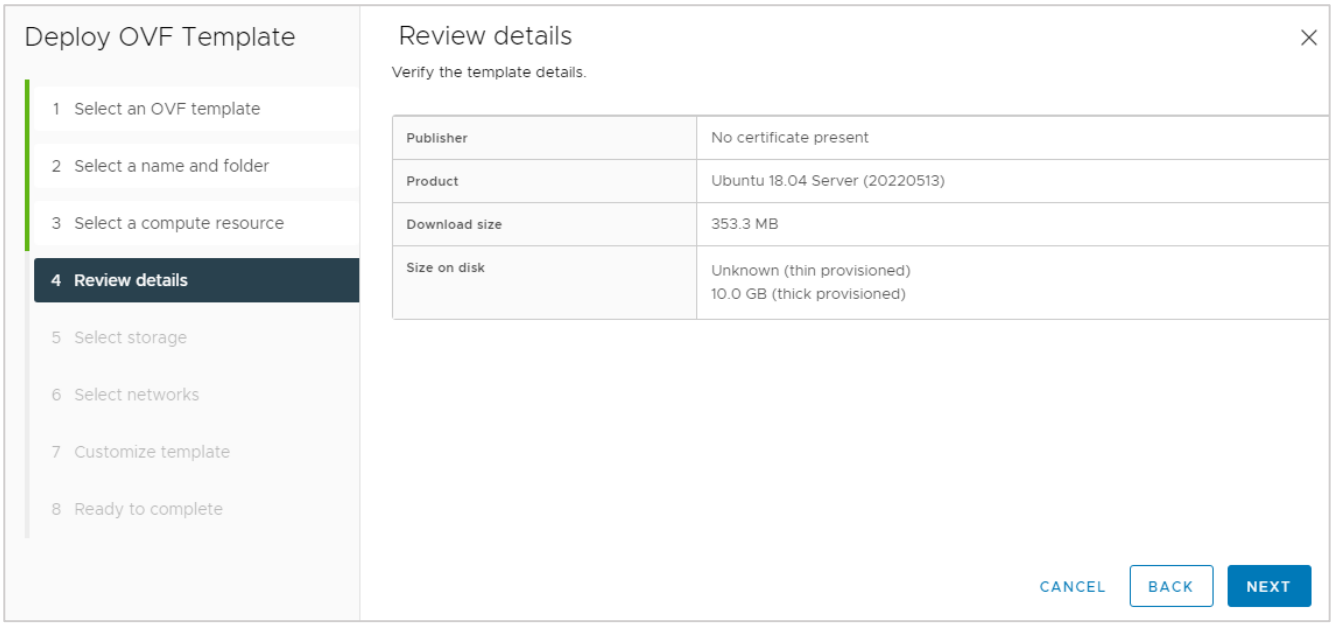

Рисунок 70

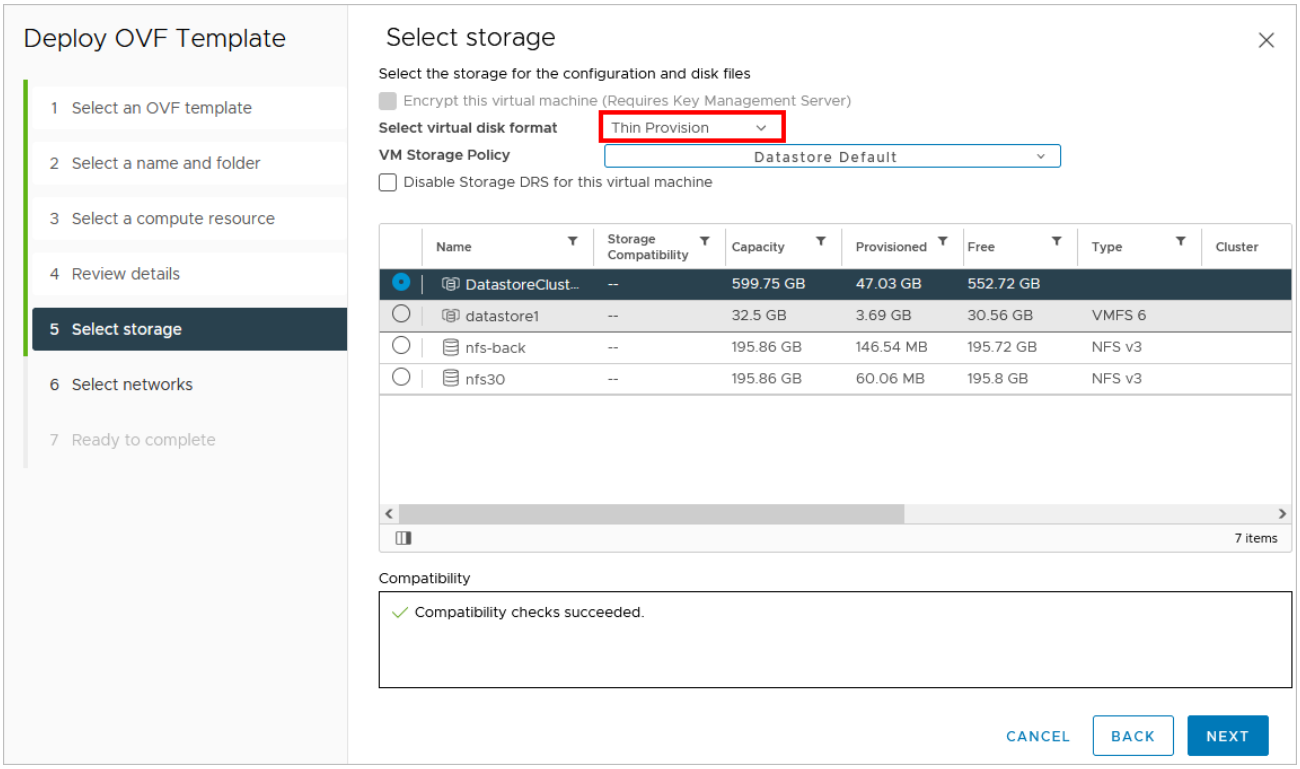

Рисунок 71

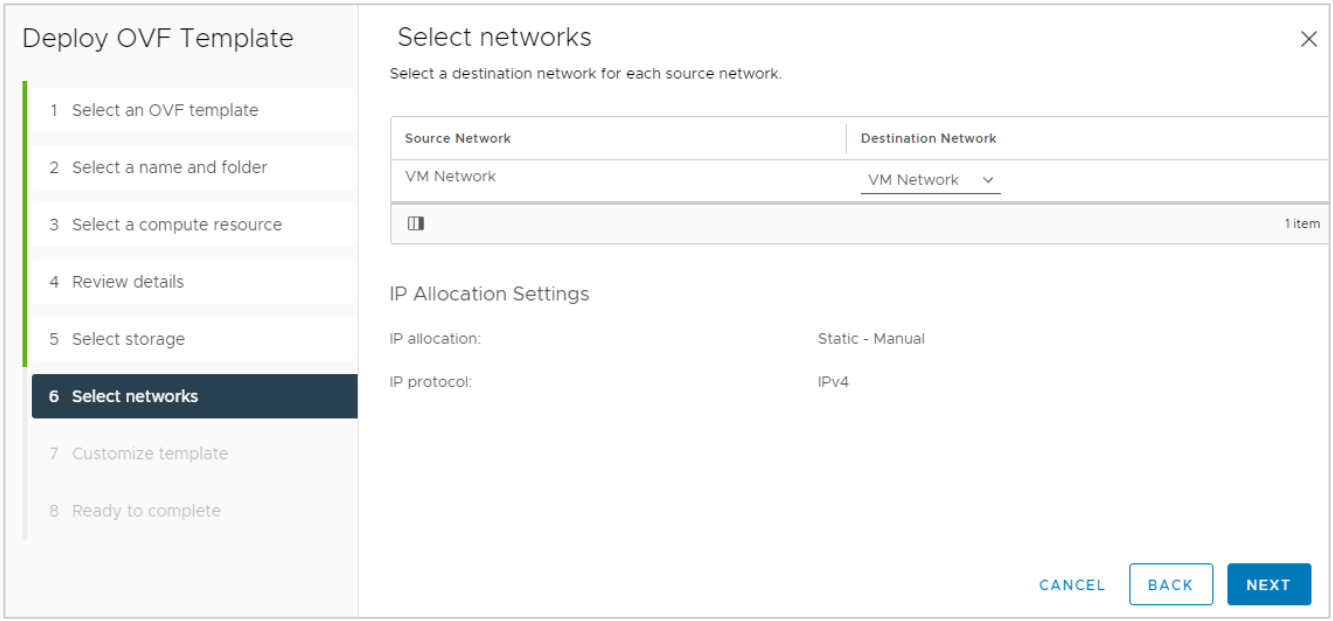

Рисунок 72

Установите пароль на ВМ (Рисунок 73).

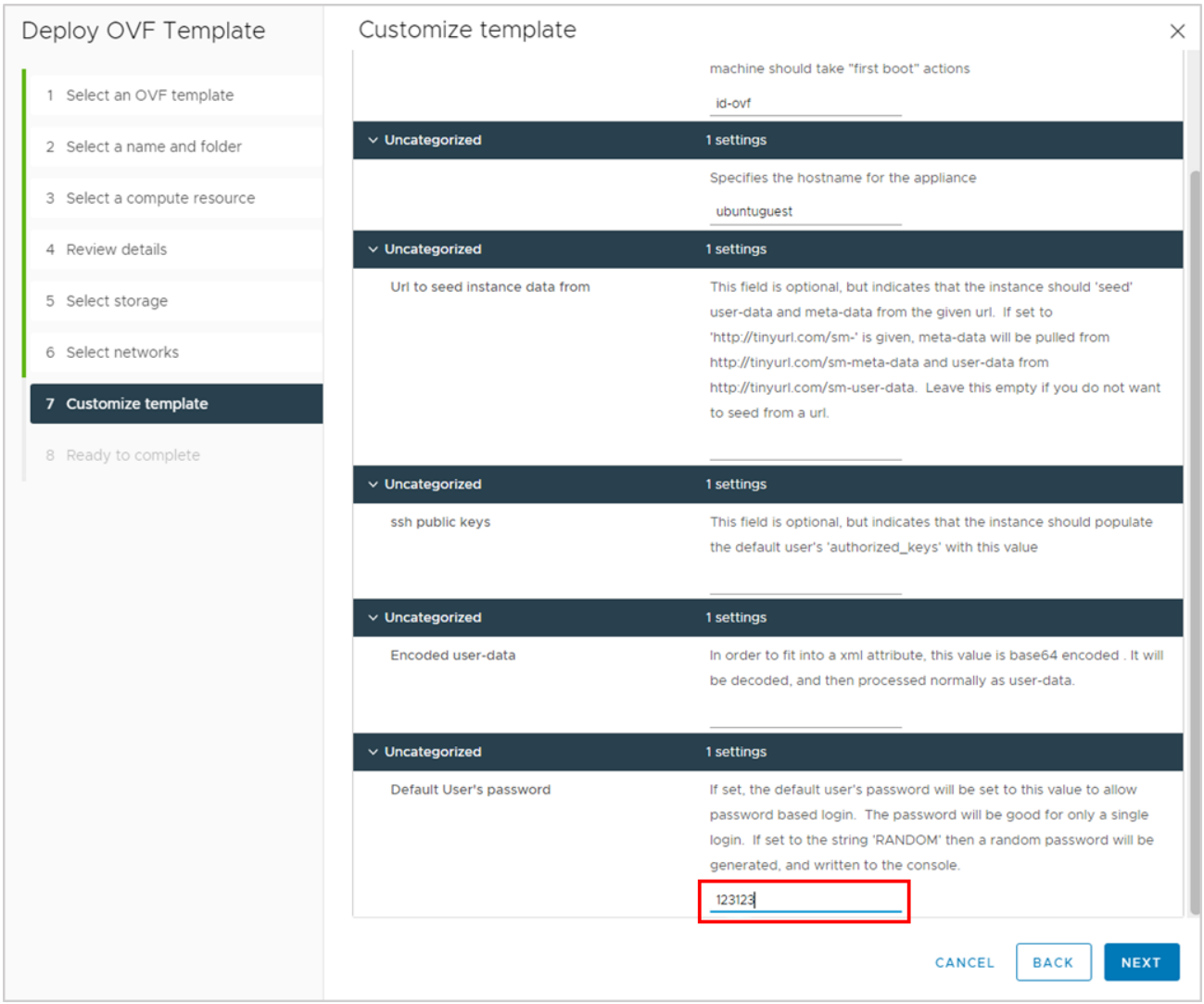
Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete
Customize template
machine should take "first boot" actions
id-ovf
Uncategorized
1 settings
Specifies the hostname for the appliance
ubuntuguest
Uncategorized
1 settings
Url to seed instance data from
This field is optional, but indicates that the instance should 'seed' user-data and meta-data from the given url. If set to 'http://tinyurl.com/sm-' is given, meta-data will be pulled from http://tinyurl.com/sm-meta-data and user-data from http://tinyurl.com/sm-user-data. Leave this empty if you do not want to seed from a url.
Uncategorized
1 settings
ssh public keys
This field is optional, but indicates that the instance should populate the default user's 'authorized_keys' with this value
Uncategorized
1 settings
Encoded user-data
In order to fit into a xml attribute, this value is base64 encoded . It will be decoded, and then processed normally as user-data.
Uncategorized
1 settings
Default User's password
If set, the default user's password will be set to this value to allow password based login. The password will be good for only a single login. If set to the string 'RANDOM' then a random password will be generated, and written to the console.
123123
CANCEL
BACK
NEXT

Рисунок 73

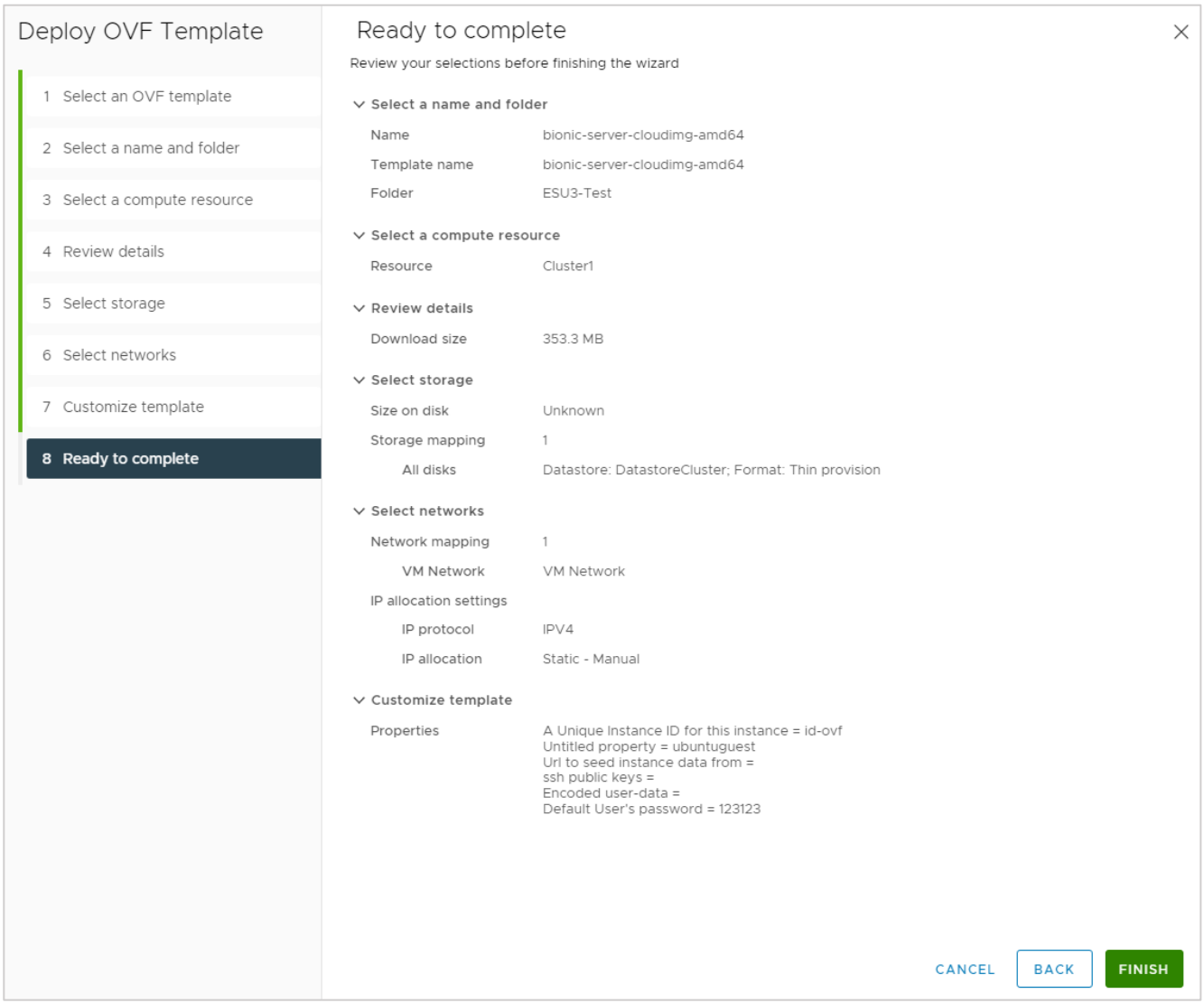

Рисунок 74

После нажатия кнопки **FINISH** дождитесь завершения развёртывания .ova-шаблона.

Далее отредактируйте настройки ВМ.

Для этого нажмите правой кнопкой мыши на ВМ и выберите **Edit Settings** (Рисунок 75):

- на вкладке **Hard disk 1** проверьте, что в поле **Type** установлен тип **Thin Provision**;
- на вкладке **SCSI controller 0** в поле **Change Type** выберите **VMware Paravirtual**,
- наведите на вкладку **Network adapter 1** и нажмите на значок  для удаления сетевого адаптера,
- на вкладке **CD/DVD drive 1** в поле **Virtual Device Node** укажите параметры **IDE 0** и **IDE(0:0) CD/DVD drive 1**.

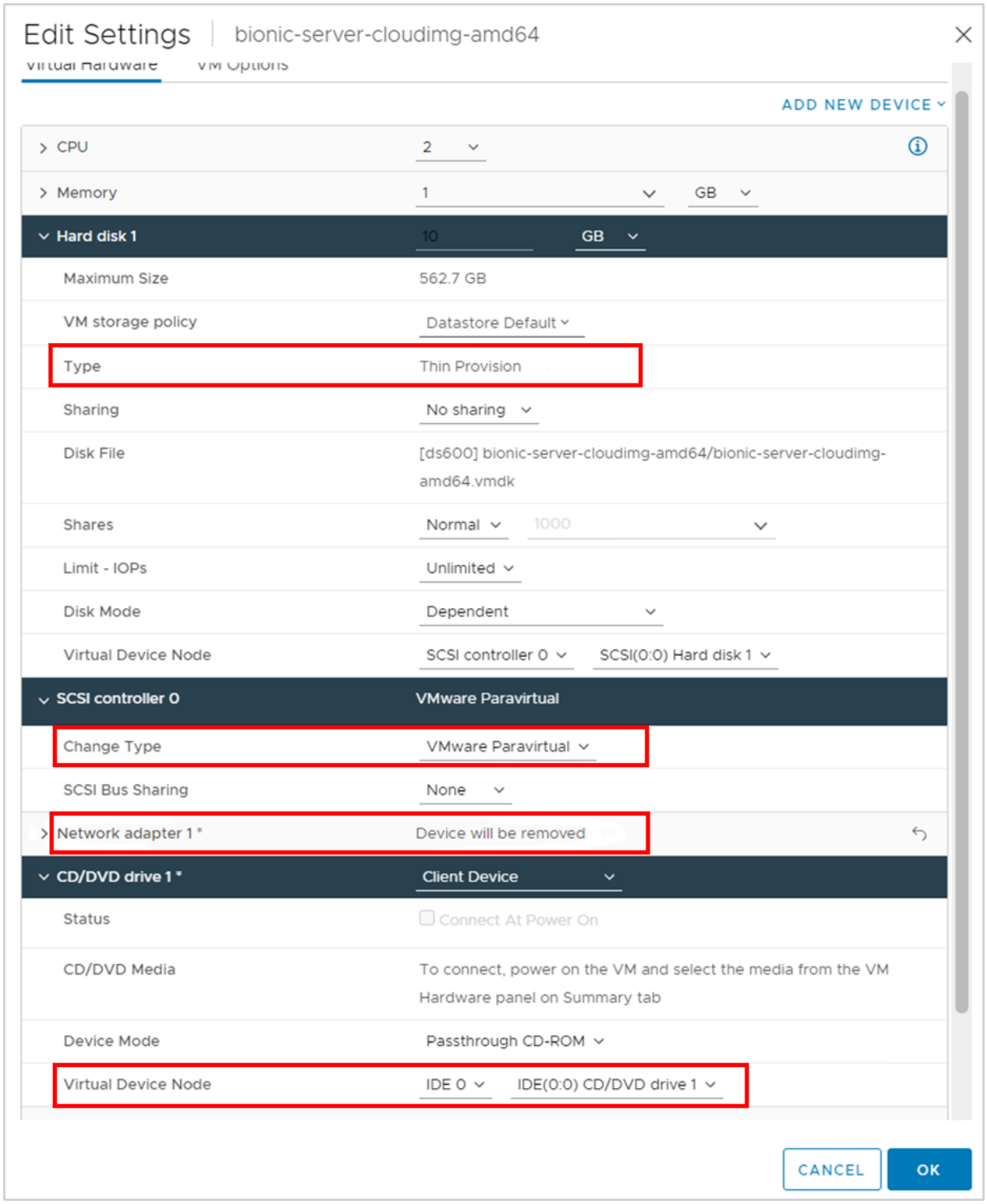

Рисунок 75

Запустите ВМ. Введите ранее установленный пароль для пользователя ubuntu, войдите в систему. Потребуется сменить пароль. Измените на любой.

Отредактируйте файл `cloud.cfg`.

Cloud-init config может находиться в двух местах:

```
/etc/cloud/cloud.cfg
/etc/cloud/cloud.cfg.d/*.cfg
```

- Перейдите в директорию, где расположен файл и выполните команду:

```
sudo nano cloud.cfg
```

- Закомментируйте секцию `users` (Рисунок 76):

```
 GNU nano 2.9.3                        cloud.cfg                          Modified

_
# The top level settings are used as module
# and base configuration.
# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
#users:
#   - default


# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the default $user
disable_root: true


# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false
```

Рисунок 76

- Внизу допишите секцию `datasource` (Рисунок 77):

```
 GNU nano 2.9.3                        cloud.cfg                          Modified

# If you use multi line array, ds-identify script won't read array items.
# Example datasource config
datasource:
  Ec2:
    strict_id: false
    timeout: 10
    max_wait: 20
    metadata_urls:
      - http://169.254.169.254:80
```

Рисунок 77

- Сохраните файл `cloud.cfg`.
- Запустите команду `sudo dpkg-reconfigure cloud-init`. Запуск команды открывает интерфейс, в котором можно включить/отключить секции `datasource`;
- Отключите всё кроме пункта EC2 (Рисунок 78) и нажмите **Ok**. Установка флагов выполняется с помощью клавиши «Пробел».

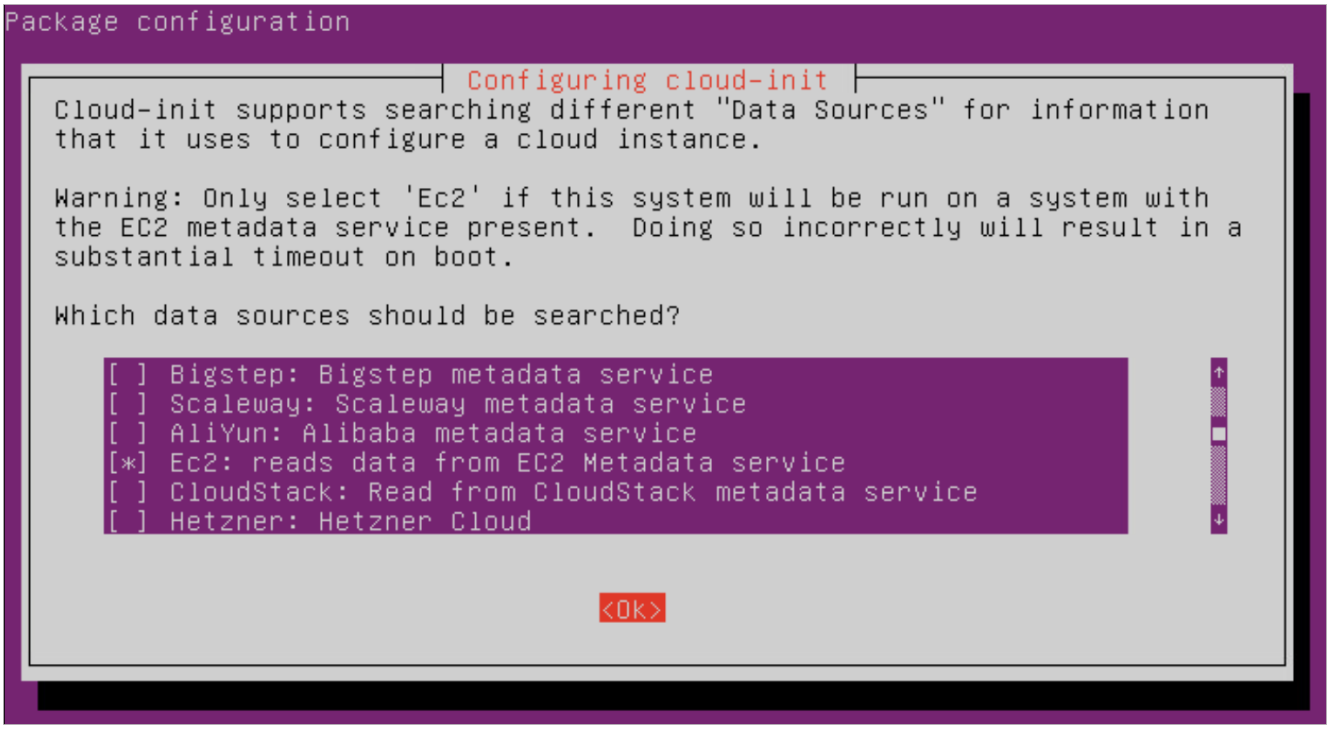

Рисунок 78

- выполните команду `sudo cloud-init clean`;
- выполните команду `sudo userdel -f ubuntu`;
- отключите ВМ.

Сконвертируйте ВМ в шаблон (Рисунок 79). Для этого нажмите на ВМ правой кнопкой мыши и выберите **Template → Convert to Template**.

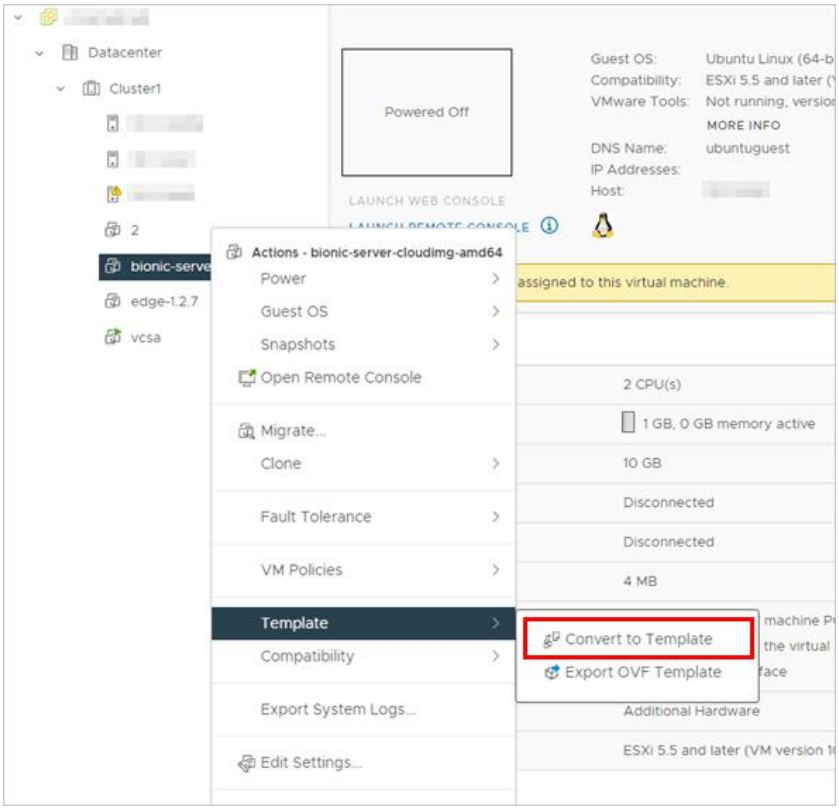

Рисунок 79

После этого создайте шаблон в РУСТЭК-ЕСУ (Рисунок 80 – Рисунок 82). Процедура аналогична созданию шаблона для сегмента РУСТЭК (см. раздел 4.2.4), необходимо только выбрать другой ресурсный пул — VMware и другое имя шаблона — выбрать созданный на предыдущих шагах шаблон из списка.

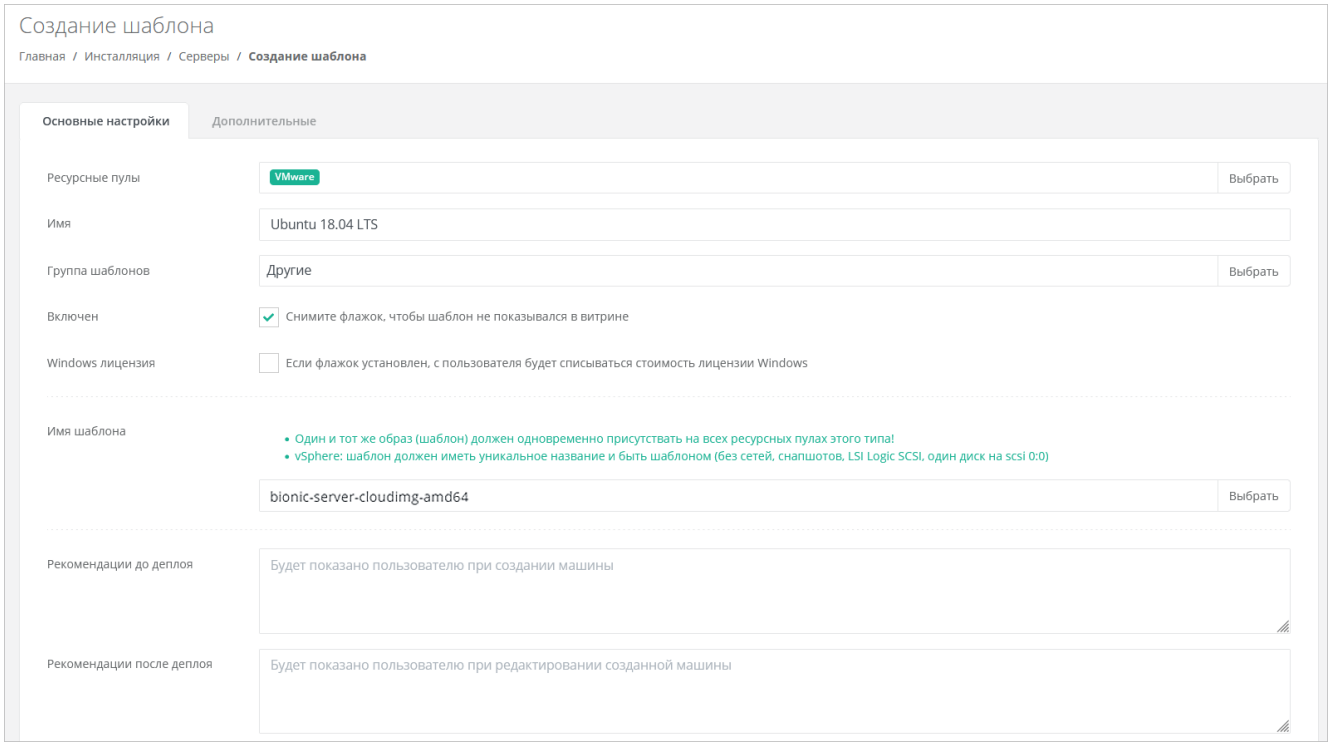

Рисунок 80

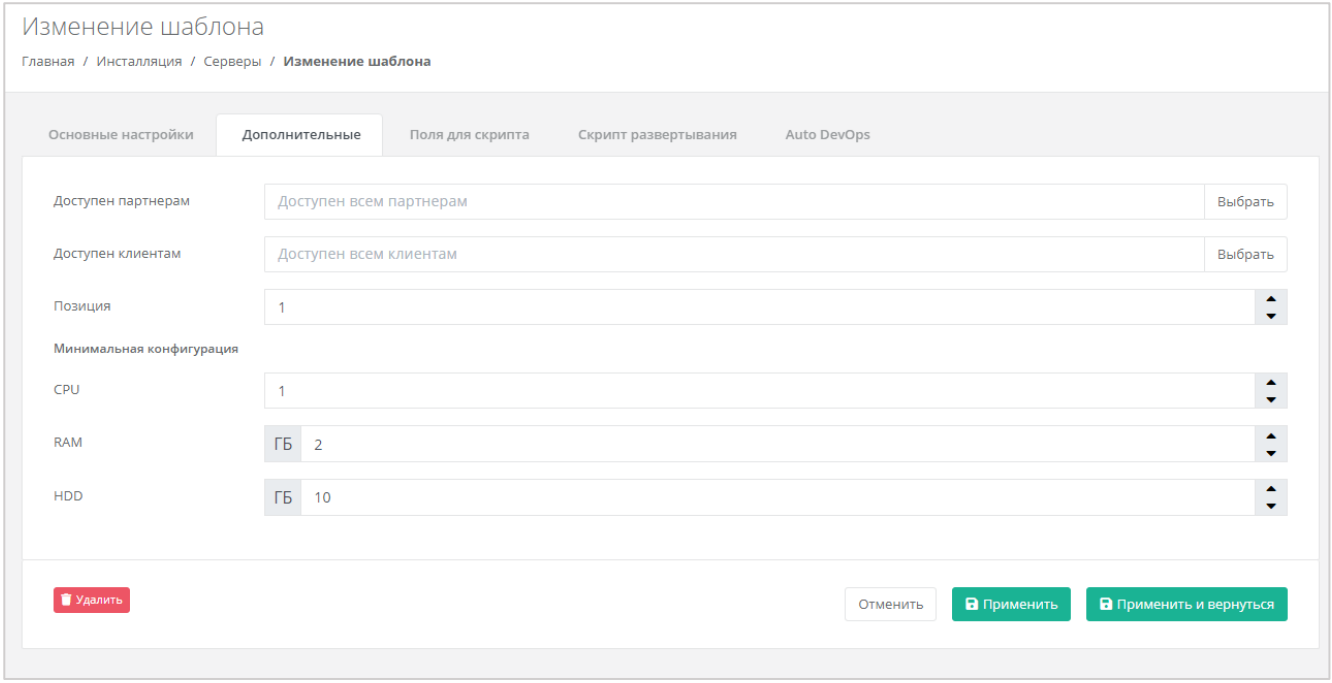

Рисунок 81

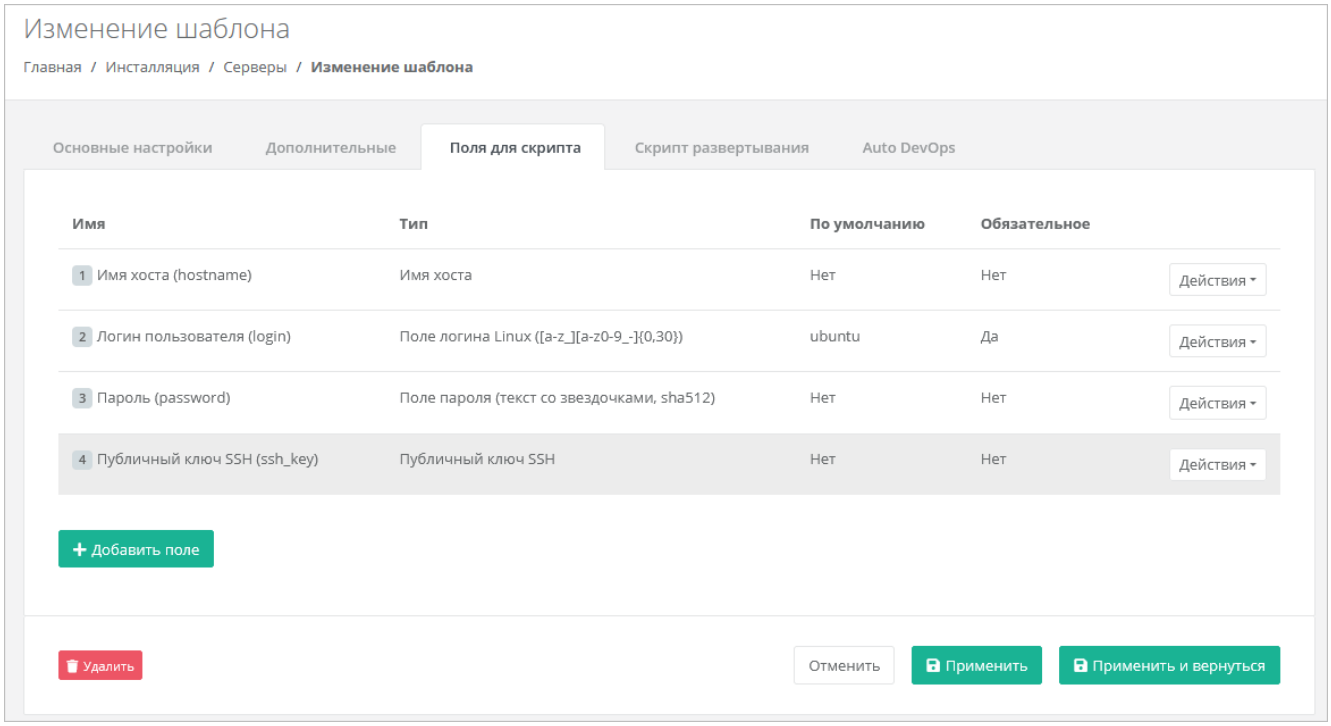

Рисунок 82

Далее на вкладке **Скрипт развёртывания** добавьте скрипт развёртывания.

Скрипт развёртывания применяется во время развёртывания виртуальной машины внутри операционной системы сервера.

Примечание: универсальный скрипт развёртывания для Linux OS приложен ниже в документации в разделе 7.4.

На вкладке **Auto DevOps** можно настроить Auto DevOps-скрипт. Скрипт обращается к API РУСТЭК-ЕСУ для выполнения указанных в скрипте операций.

Auto DevOps-скрипт пишется на языке Python и используется для выполнения дополнительных операций с сервером во время его создания и/или запуска.

Примечание: внесение изменений в Auto DevOps-скрипт рекомендуется только для вендоров. Просьба не редактировать настройки скрипта самостоятельно.

Пример скрипта приведён в Приложении 1.

После внесения изменений в скрипт нужно обязательно нажать кнопку Применить!

В результате редактирования настроек Auto DevOps-скрипта вносятся изменения в панели управления. Например, применяются необходимые шаблоны брандмауэра после разворачивания виртуальной машины.

После внесения изменений нажимаем кнопку **Применить и вернуться**. Созданный шаблон ВМ появится в списке шаблонов, и из него можно будет создавать ВМ.

5. Проверка работы сегментов инсталляции

Для проверки работоспособности системы рекомендуется создать по одному ВЦОД в каждом сегменте.

ВЦОД (виртуальный центр обработки данных) — пул ресурсов облачной инфраструктуры: виртуальные машины, сети, роутеры, диски, балансировщики нагрузки и т.д.

Для создания ВЦОД сначала следует создать сущность партнёра, клиента и один проект для клиента. Рассмотрим кратко основные сущности РУСТЭК-ЕСУ.

Партнёр — набор данных о канале предоставления услуг. В частном облаке это сущность для распределения ресурсов провайдера, связанная с менеджером или администратором провайдера. В частном облаке провайдер и партнёр могут относиться к одному отделу в организации. В публичном облаке это брокер услуг, осуществляющий вспомогательную деятельность по продаже услуг провайдера потребителям, при этом партнёр может использовать ресурсы облака как для предоставления услуг своим клиентам под собственным брендом, так и для перепродаж услуг облака — реселлинга.

Для предоставления услуг в РУСТЭК-ЕСУ должен быть сконфигурирован хотя бы один партнёр и связанный с ним домен. Для управления партнёром назначается один или несколько администраторов.

Клиент — набор данных о потреблении услуг организованной группой людей, часто на возмездной основе. В частном облаке это некоторый коллектив или подразделение, центр затрат для учёта потребления, центр (финансовой) ответственности. В публичном облаке это хозяйствующий субъект (юридическое или физическое лицо), потребляющий услуги облака по договору с провайдером или партнёром.

Каждому клиенту должен быть назначен ответственный пользователь (управляющий менеджер), взаимодействующий при необходимости с провайдером — администратор клиента.

Проект — именованное объединение виртуальных ресурсов и услуг, потребляемых клиентом. Минимальный объект назначения прав доступа в службе облачных вычислений. Клиент может создать несколько проектов на своё усмотрение. В состав проекта входят один и более ВЦОД, а также виртуальные сущности платформенных услуг (PaaS): хранилища S3, кластеры Kubernetes. Для проекта может быть добавлена DNS-зона, которой клиент управляет с помощью панели управления.

5.1. Создание партнёра и домена

Для создания нового партнёра перейдите в раздел меню **Администрирование** → **Партнёры**.

Нажмите кнопку **Добавить партнёра**.

В открывшейся форме **Добавление партнёра** заполните основные настройки (Рисунок 83):

- **Имя** — введите любое имя партнёра.
- **Тарифный план** — выберите из списка тарифный план «Для партнёра».

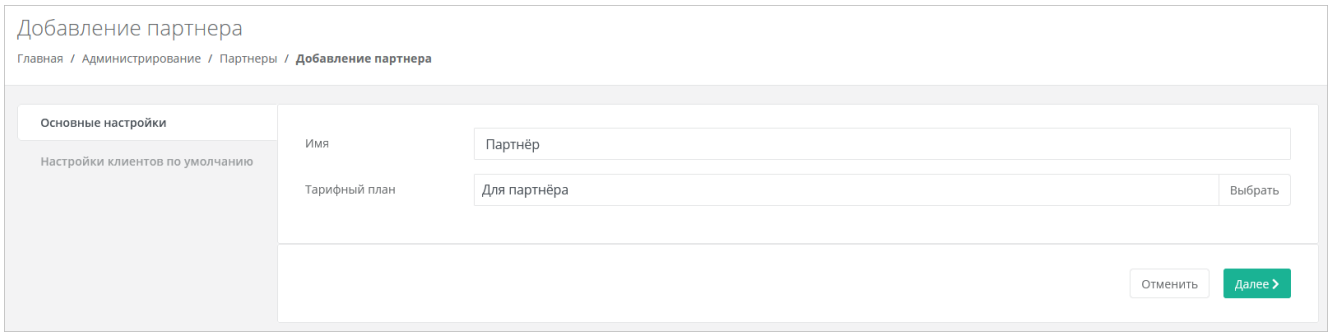

Рисунок 83

Далее перейдите на вкладку **Настройки клиентов по умолчанию**. Эти настройки устанавливаются для каждого нового клиента партнёра.

На первом этапе достаточно установить тарифный план для клиентов. В поле **Тарифный план** выберите из списка тарифный план «Для клиента».

Остальные настройки можно отредактировать после добавления партнёра. После выбора тарифного плана клиента нажмите кнопку **Далее** для создания нового партнёра.

После создания партнёра на вкладке **Изменение партнера** появятся дополнительные вкладки и настройки.

Добавьте ресурсные пулы для партнёра. Для этого в поле **Ресурсные пулы** выберите ресурсные пулы **РУСТЭК** и **VMware** (Рисунок 84).

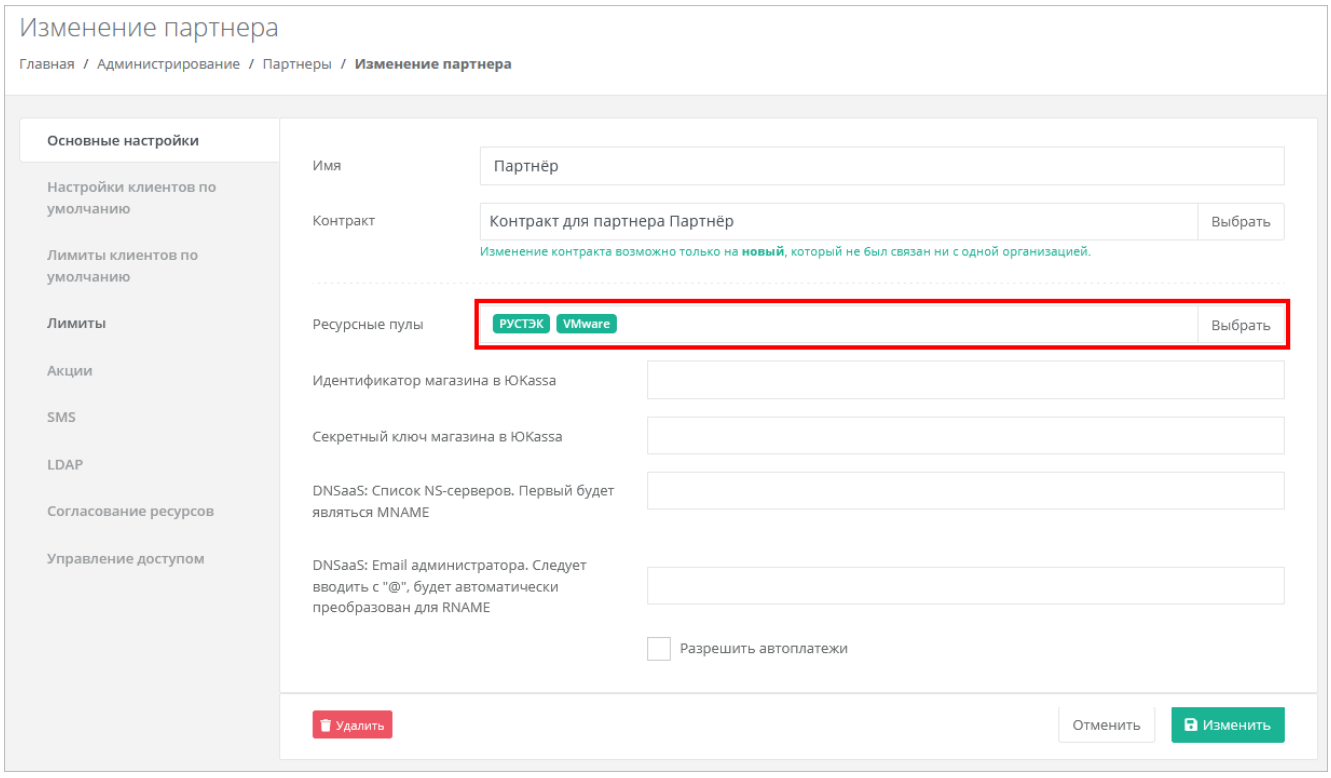

Рисунок 84

Для сохранения настроек нажмите кнопку **Изменить**.

В меню **Администрирование** → **Домены** можно создавать и изменять домены, к которым привязываются партнёры.

Для создания домена в разделе меню **Администрирование** → **Домены** нажмите кнопку **Добавить домен**.

В открывшейся форме заполните поля (Рисунок 85):

- **Имя** — имя домена для обозначения в системе.
- **Домены** — ввод уникальных доменных имён. Если доменных имён несколько, нужно их ввести через запятую.
- **DNS-зона** — выбор DNS-зоны.
- **Связанный партнёр** — выберите созданного партнёра.

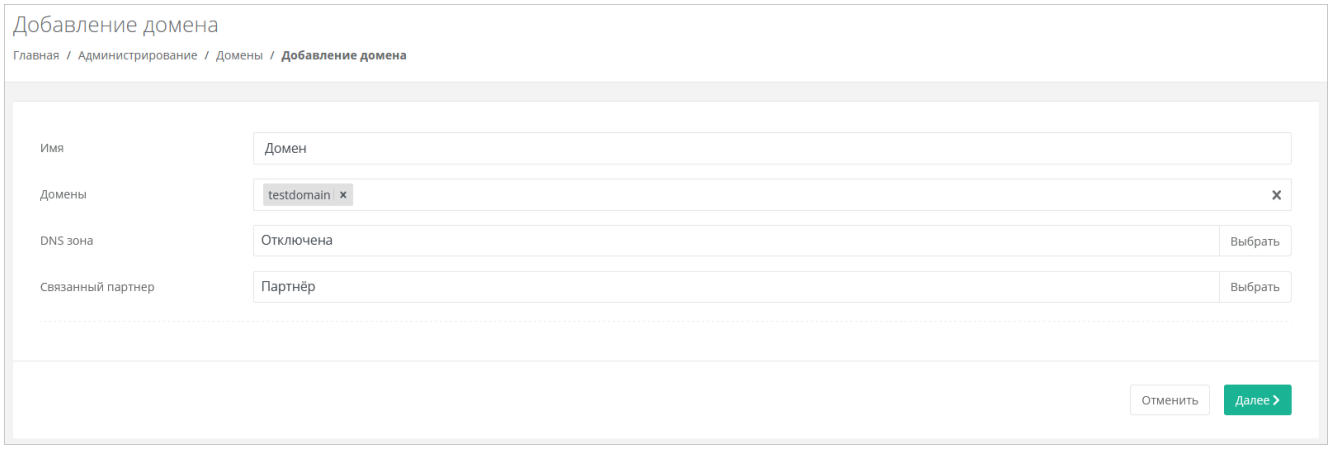

Рисунок 85

⚠ **У каждого партнёра должен быть свой связанный домен**, иначе администратор партнёра не сможет создавать пользователей и предоставлять им доступ к клиентам.

После ввода данных нажмите кнопку **Далее**. Будет создан новый домен и откроется форма **Изменение домена**, в которой можно редактировать различные настройки домена: логотип, тексты на формах авторизации, регистрации, шаблоны писем и т.д.

Более подробное описание настроек тарифных планов, партнёров и доменов приведено в **Руководстве администратора платформы**.

5.2. Создание клиента, проекта и ВЦОД

Для создания тестового клиента перейдите в раздел меню **Администрирование** → **Клиенты** и нажмите кнопку **Добавить клиента**.

В открывшейся форме заполните поля:

- **Имя** — введите любое имя клиента.
- **Партнёр** — выберите созданного партнёра.
- **Тарифный план** — по умолчанию установлен план «Для клиента».
- **Интернет** — рекомендуется установить флаг.

    - **Скорость доступа в Интернет** — при включённом доступе в Интернет можно настраивать скорость доступа.
- **Скорость локальной сети** — можно настраивать скорость локальной сети.
- **Методы оплаты** — рекомендуется выбрать безналичную оплату.
- **Модель оплаты** — рекомендуется выбрать постоплату.
- **Согласование ресурсов** — флаг должен быть снят. При установленном флаге согласование у вышестоящего лица становится обязательным шагом при запросе ресурсов для клиента и его проектов. Подробнее см. в **Руководстве администратора партнёра**.
- **Биллинг** — при снятом флаге для клиента отключаются все финансовые расчёты и автоматически снимается флаг **Отображать информацию о биллинге**.
- **Отображать информацию о биллинге** — при снятом флаге для клиента скрываются элементы панели управления, связанные с балансом клиента и расчётом стоимости ресурсов: раздел меню **Баланс**, блок расходов на главной странице панели управления, калькуляторы стоимости ресурсов и т.д. Снятие флага **не** отключает финансовые расчёты для клиента.

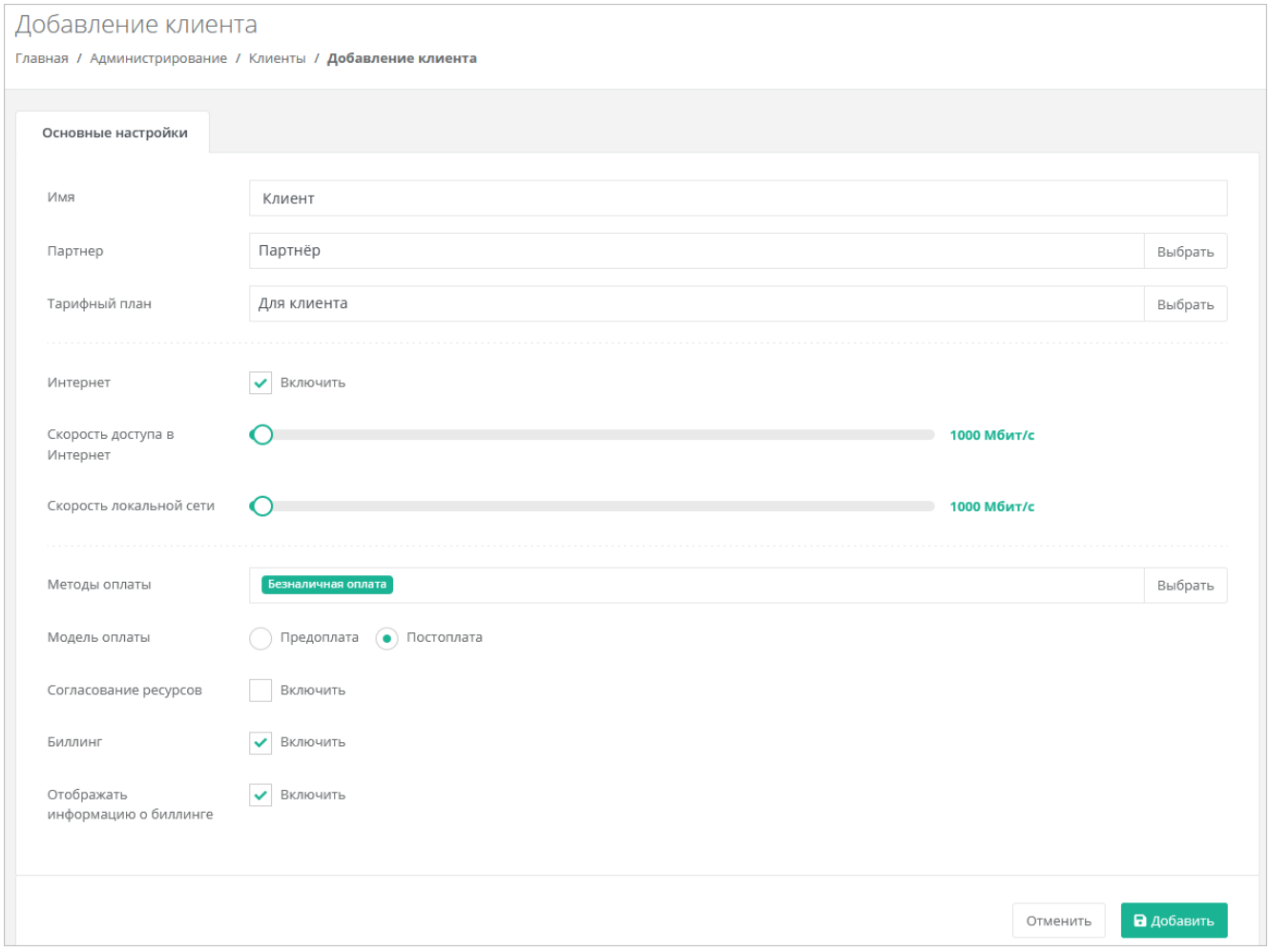

Рисунок 86

Нажмите кнопку **Добавить** для создания клиента.

В разделе **Администрирование** → **Клиенты** отобразится созданный клиент.

Для клиента будет автоматически создан проект с названием «Мой проект».

В списке клиентов в столбце **Проекты** нажмите на ссылку **Мой проект** (Рисунок 87). Будет выполнен переход в раздел меню **Облачные вычисления** (Рисунок 88).

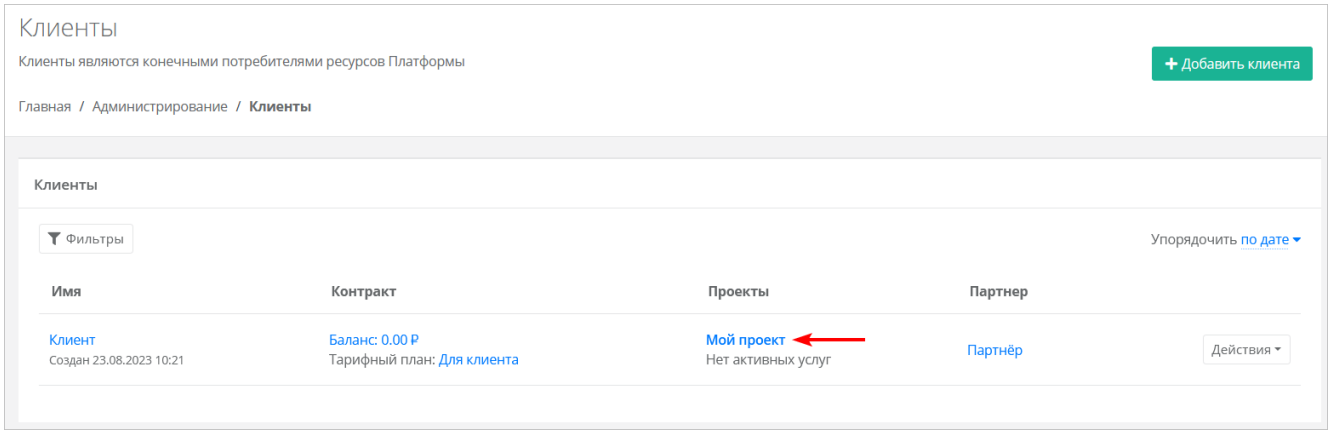

Рисунок 87

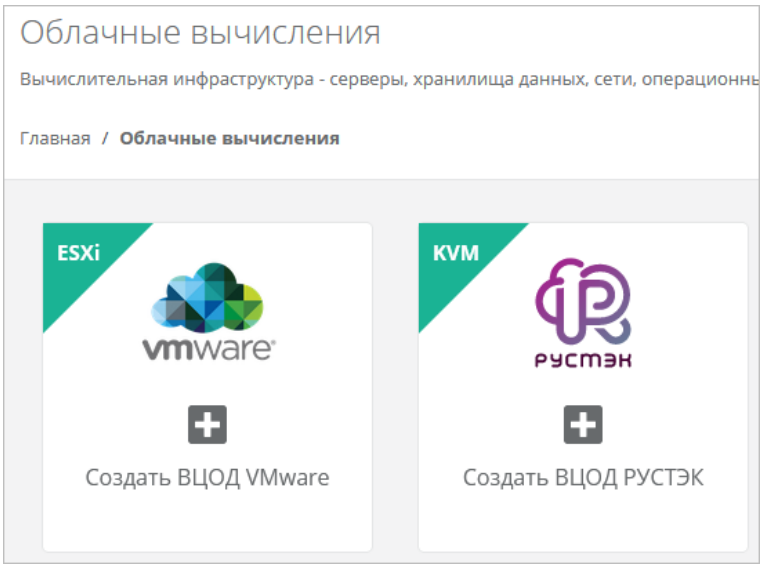

Рисунок 88

Активируйте один из ВЦОД, например VMware, нажатием на кнопку.

После некоторого времени ВЦОД создастся и будет иметь статус «работает». В нём можно создать виртуальную машину (Рисунок 89).

В данном примере создано по одному ВЦОД в каждом сегменте: VMware и РУСТЭК.

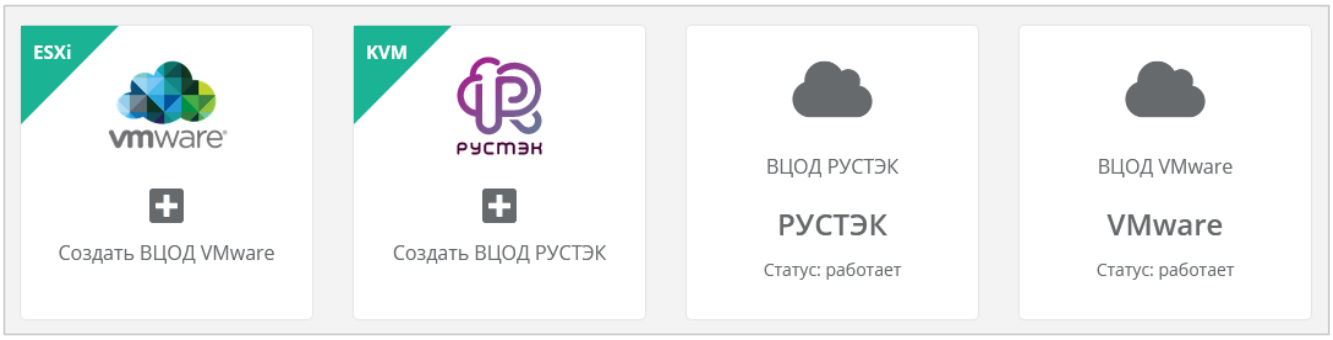
ESXi
vmware
Создать ВЦОД VMware
KVM
РУСТЭК
Создать ВЦОД РУСТЭК
ВЦОД РУСТЭК
РУСТЭК
Статус: работает
ВЦОД VMware
VMware
Статус: работает

Рисунок 89

6. Настройка РУСТЭК-ЕСУ для работы с кластерами Kubernetes

6.1. Создание шаблонов Kubernetes для сегмента VMware vSphere

Для разворачивания кластеров Kubernetes в РУСТЭК-ЕСУ необходимо подготовить шаблоны master-ноды, с которой будет происходить управление кластером, и обычной ноды (worker-ноды).

Рассматривается подготовка шаблонов на примере Kubernetes версии 1.22.1.

Скачайте подготовленные нашей командой шаблоны в архивах. Распакуйте архивы.

Master-нода: https://file.rustack.ru/s/9ixCrwtC5S5GL8p

Нода: https://file.rustack.ru/s/6eQ8rTPGBqsfyMo

Зайдите в панель управления VMware vSphere и загрузите распакованные образы. Для этого выберите директорию, в которую будут загружены образы, в данном случае это ESU3-Test, нажмите на ней правой кнопкой мыши и выберите **Deploy OVF Template** (Рисунок 90).

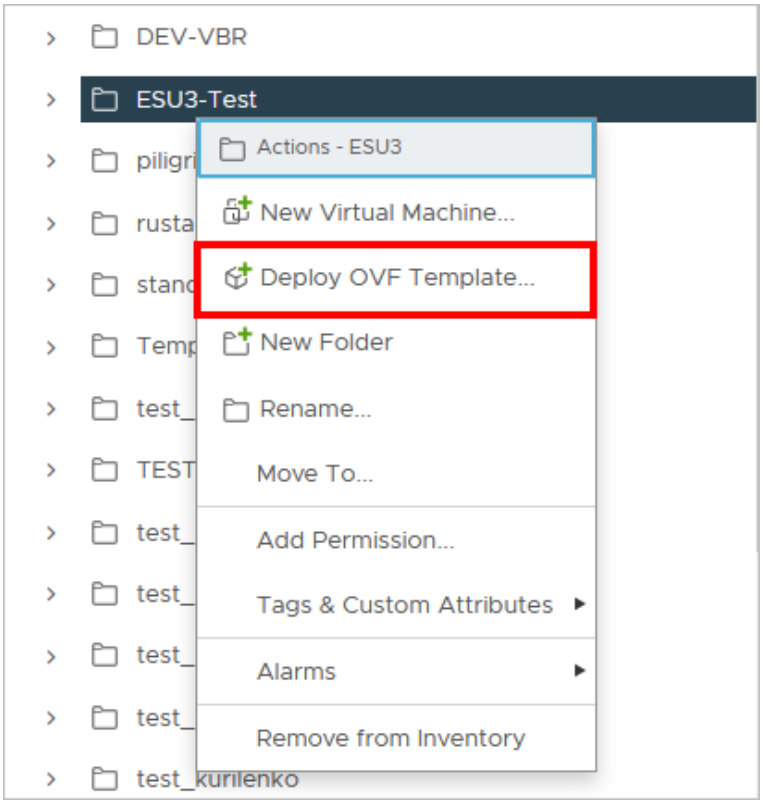

Рисунок 90

В открывшемся окне выберите **Local file** для загрузки файлов с компьютера. Нажмите **UPLOAD FILES** и выберите файлы образа. После выбора файлов нажмите кнопку **NEXT** (Рисунок 91).

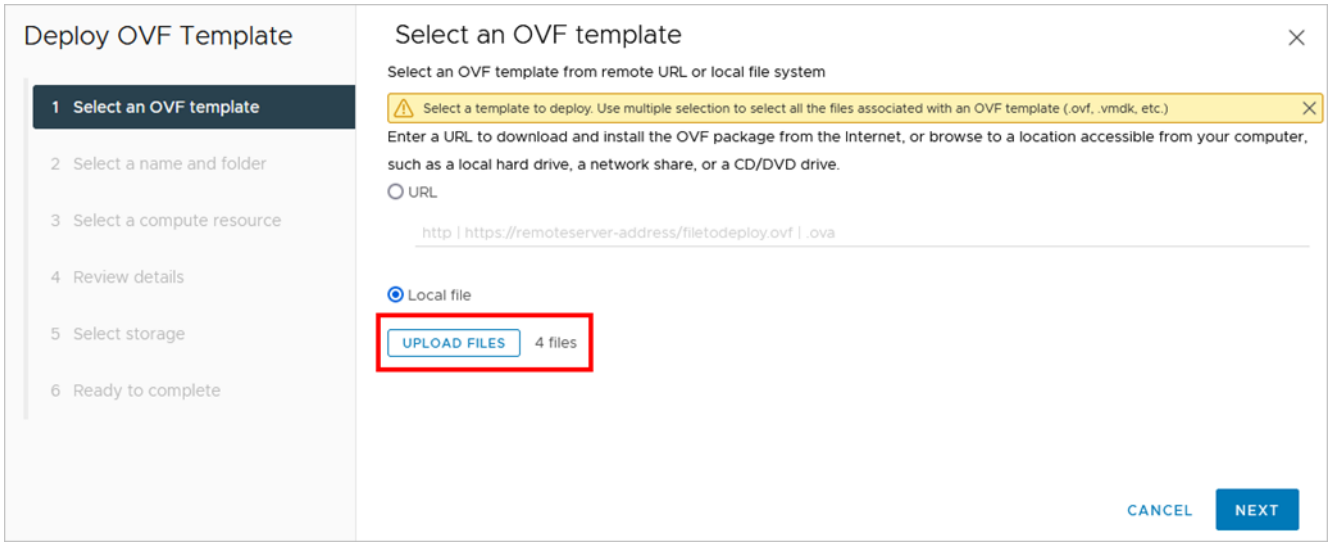

Рисунок 91

Выберите название шаблона и папку для хранения (Рисунок 92). Нажмите **NEXT**.

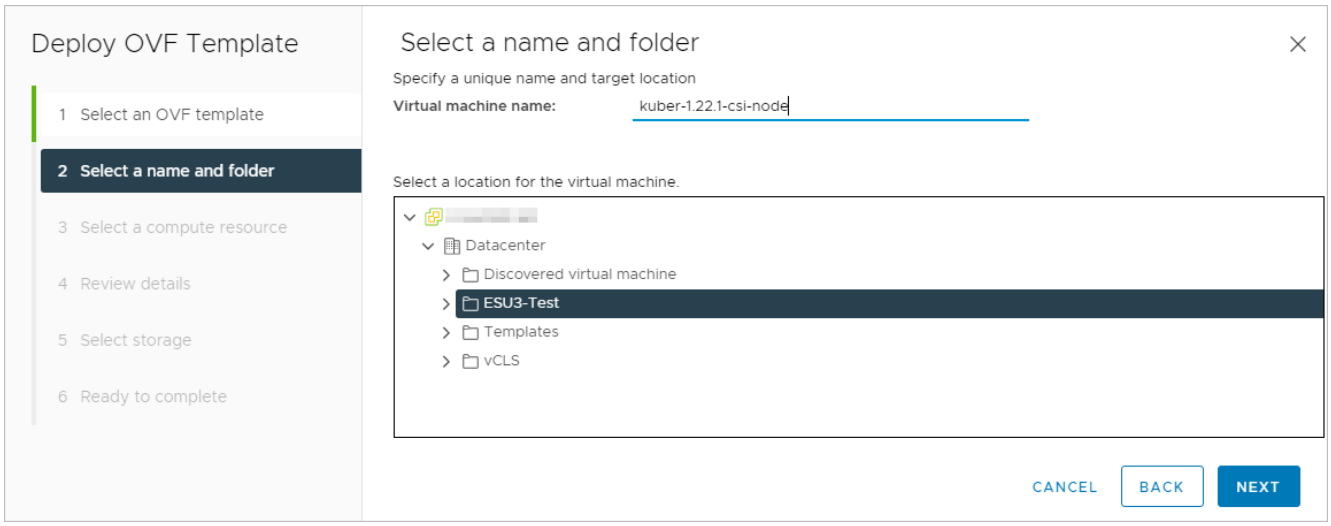

Рисунок 92

Выберите кластер, где будет храниться шаблон и нажмите **NEXT** (Рисунок 93).

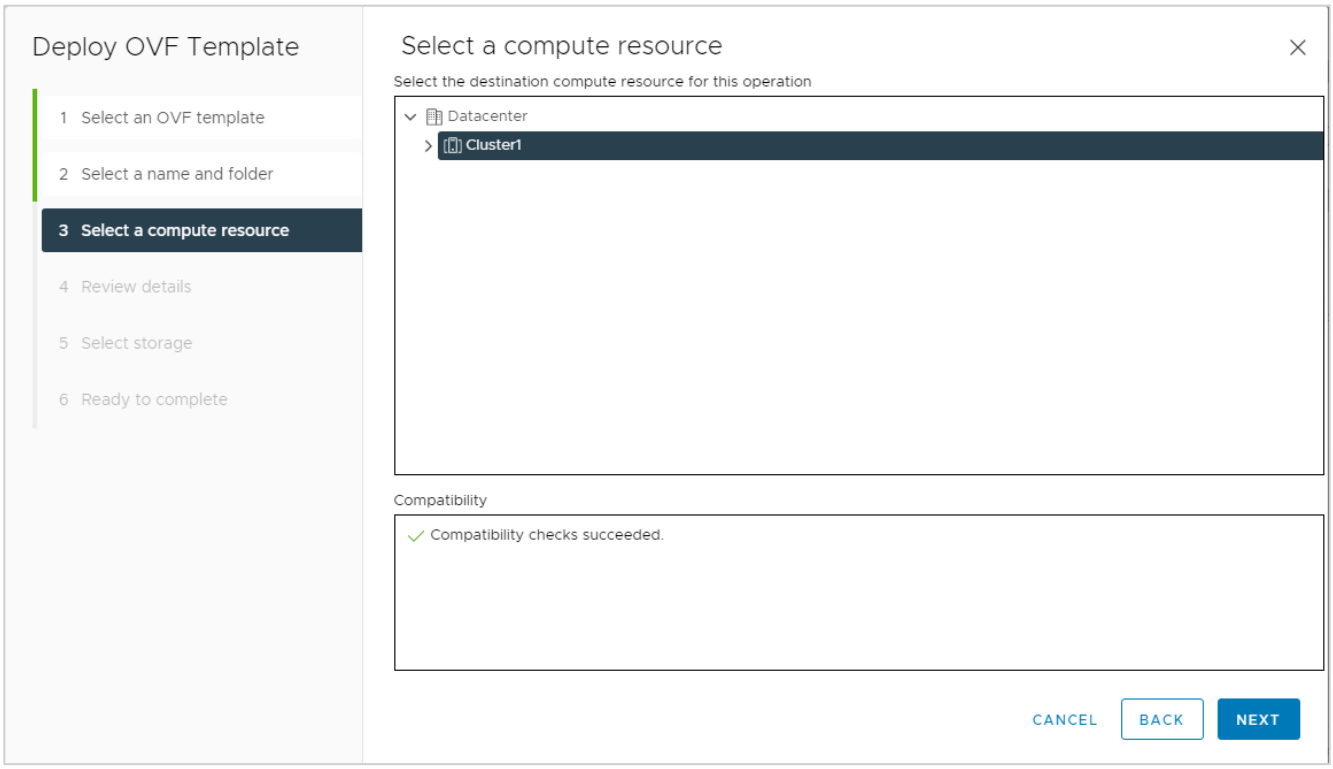

Рисунок 93

После просмотра информации о шаблоне нажмите **NEXT** (Рисунок 94).

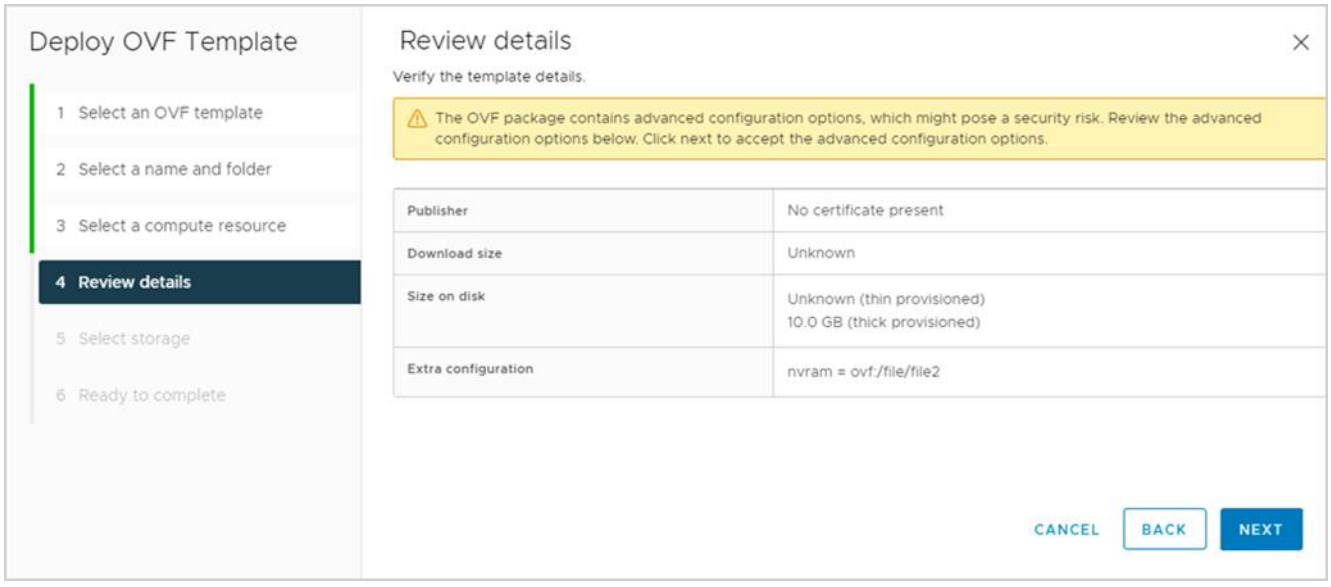

Рисунок 94

Выберите датастор для хранения шаблона и нажмите **NEXT** (Рисунок 95).

Обязательно выберите формат диска Thin Provision!

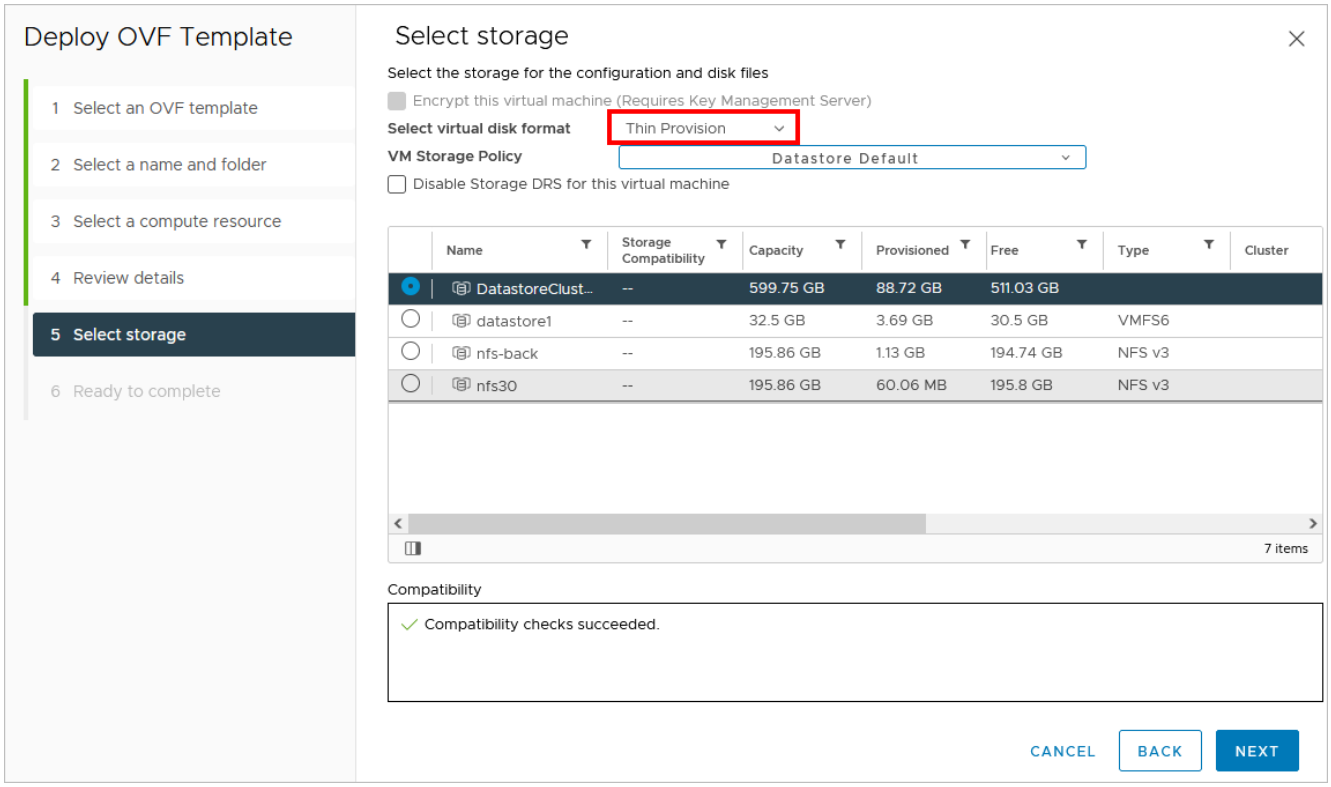

Рисунок 95

Завершите процесс нажатием кнопки **FINISH** (Рисунок 96).

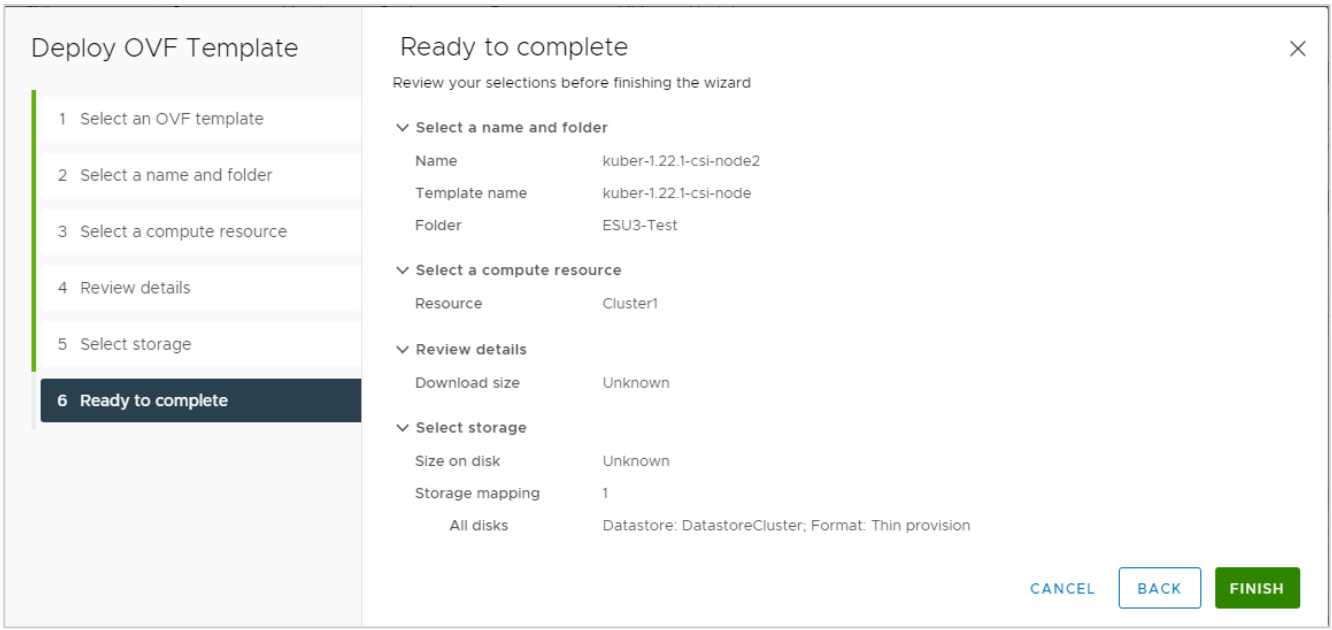

Рисунок 96

После успешной загрузки сконвертируйте созданную ВМ в шаблон. Для этого нажмите по ней правой кнопкой мыши и выберите **Template → Convert to Template** (Рисунок 97).

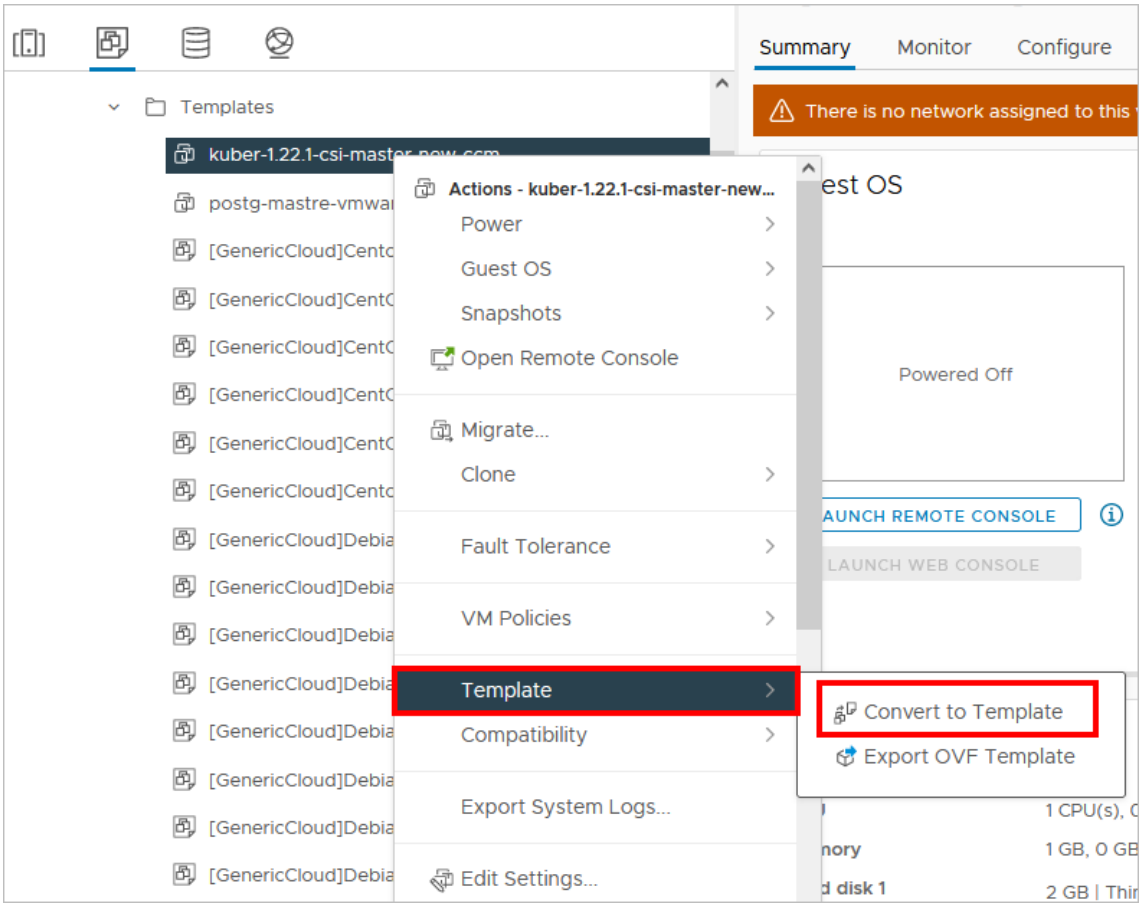

Рисунок 97

Данную операцию по загрузке и конвертации необходимо проделать для шаблона master-ноды и для обычной ноды!

После успешной загрузки шаблонов в VMware vSphere настройте РУСТЭК-ЕСУ для работы с ними. Для этого в панели управления РУСТЭК-ЕСУ перейдите в раздел меню **Инсталляция** → **Шаблоны** → **Kubernetes** и нажмите кнопку **Создать**.

В открывшемся окне заполните поля настроек (Рисунок 98):

- **Ресурсные пулы** — выберите ресурсный пул VMware.
- **Имя** — произвольное имя.
- **Включен** — установите флаг.
- **Позиция** — позиция определяет расположение имени шаблона в раскрывающемся списке в поле **Версия** при создании кластера Kubernetes пользователем. Можно оставить по умолчанию.
- **Темплейт мастера** — выберите шаблон master-ноды, загруженный в vSphere, из списка в отдельном окне.
- **Темплейт ноды** — выберите шаблон ноды, загруженный в vSphere, из списка в отдельном окне.
- **Видимый шаблон ОС** — выберите любой шаблон из списка, влияет только на название, которое будет отображаться в списке серверов.
- **Минимальная конфигурация** — рекомендуемая конфигурация для наших шаблонов: vCPU — 2, RAM — 2 ГБ, HDD — 10 ГБ.

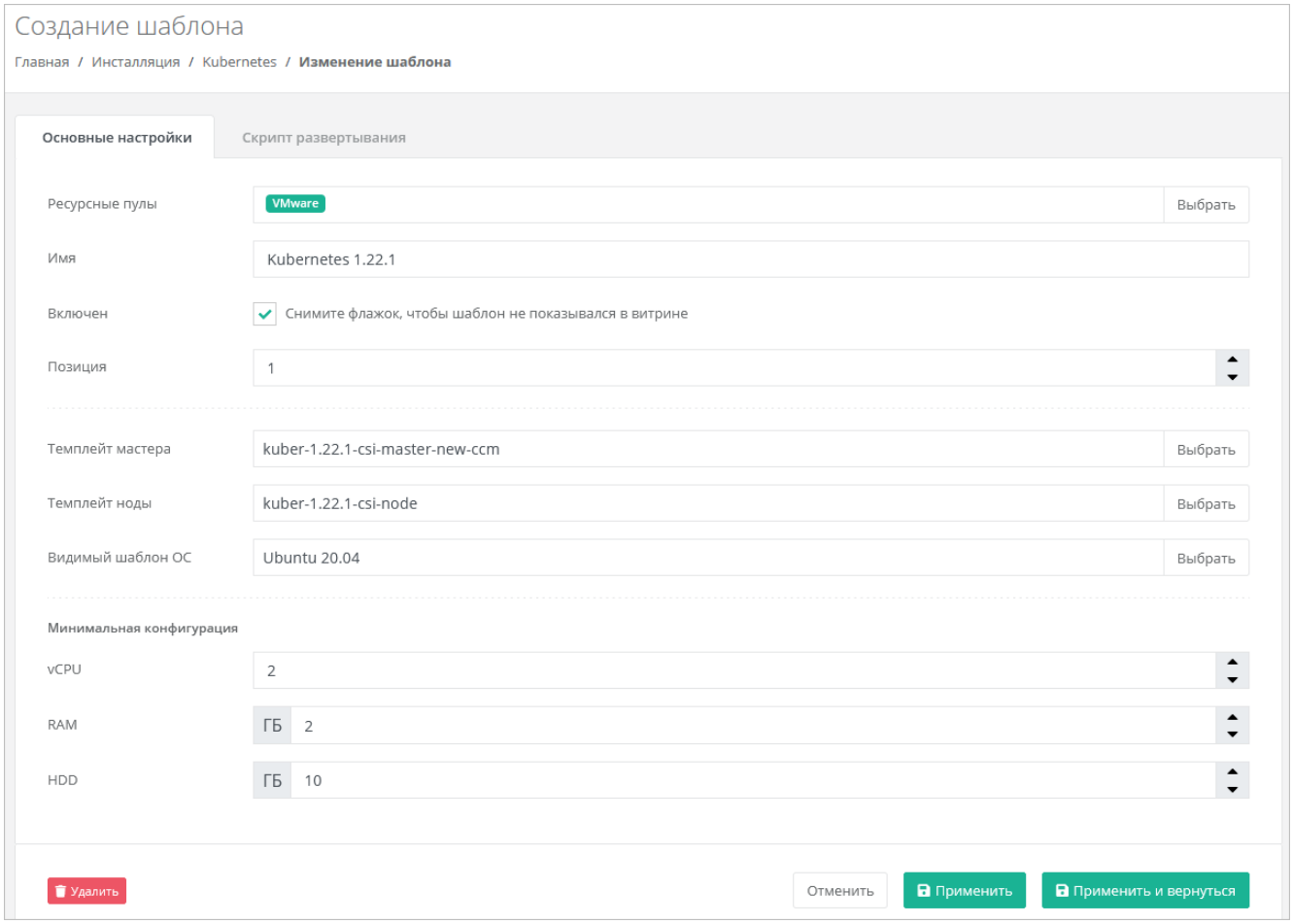

Рисунок 98

Далее во вкладке **Скрипт развёртывания** добавьте скрипт:

```
from authentication.models import PubKey, Token

def get_metadata(master=None, node=None):
    if master:
        return _prepare_master(master)
    else:
        return _prepare_node(node)

def _prepare_master(master):
    hypervisor = master.vdc.hypervisor
    api_url = hypervisor.get_setting('platform_internal_url')
    api_token = hypervisor.get_setting('edge_api_token')

    sa_token = Token(user=master.service_user)
    sa_token.save()
    sa_token = sa_token.original_key

    return {
        'user_data': f"""\
#cloud-config
debug:
  verbose: true
```

```
cloud_init_modules:
  - migrator
  - seed_random
  - bootcmd
  - write-files
  - growpart
  - resizefs
  - set_hostname
  - update_hostname
  - update_etc_hosts
  - users-groups
  - ssh
  - runcmd
runcmd:
  - runner install --api_url="{api_url}" --token="{api_token}" --
sa_token="{sa_token}" --runner_id="{master.short_id}" --ifname=eth0 --
kubernetes_uuid="{master.id}" --version="1.22.1"
fqdn: "{master.master_hostname}"
manage_etc_hosts: true
disable_root: false
ssh_pwauth: yes
users:
  - default
ssh_authorized_keys:
  - ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKZnwlDIoHsfZukwf/QnHP8KR/diFMQgLFxG0Doe9qdZ/nE7xf3
bUF9WNXwMEemQv6Vo6Jdp0kTswT+ZuELlxcvd4OgnIBChdY8qym/4/BFMqFJz6IJ1Bhenp/+bvy/cWR2b
BKNiYb0Cw5dWU+0xbS75l6jy0oH3zCwVTNGQ7ieB5cwJaq3w9LYuXGITUN6pko3mJKMhQ1JB7mre8ZGkz
KIwux5Eut4me1JCFfi/bGFlUUB/uFkzJIHtv4nlAmz3pW+Wv/6eqXXoaBrGp9Dmp3qPmnXtAywsnKGZ6o
hp2jIcmJZ69ceJvB1jx5IoIR9W+ntBwlVhvmOdkSVy4yHiGL deploy@localhost
chpasswd:
  expire: false
  list:
    - root:
timezone: "Europe/Moscow"
package_update: false
datasource:
  Ec2:
    strict_id: false
    timeout: 5
    max_wait: 5
    metadata_urls:
      - http://169.254.169.254:80
""",
        'hostname': master.master_hostname[:15],
        'instance-id': master.short_id,
    }

def _prepare_node(node):
    pub_keys = [node.kubernetes.service_public_key,
node.kubernetes.user_public_key]
    pub_keys = '\n'.join([f'  - "{k}"' for k in pub_keys])
```

```
    internal_ip = node.ports[0].ip_address

    return {
        'user_data': f"""\
#cloud-config
debug:
  verbose: true
cloud_init_modules:
  - seed_random
  - bootcmd
  - write-files
  - growpart
  - resizefs
  - set_hostname
  - users-groups
  - ssh
bootcmd:
  - echo {internal_ip} {node.hostname or node.short_id[:15]} > /etc/hosts
  - echo "127.0.0.1 localhost" >> /etc/hosts
disable_root: false
fqdn: "{node.hostname or node.short_id[:15]}"
ssh_pwauth: yes
users:
  - default
ssh_authorized_keys:
{pub_keys}
chpasswd:
  expire: false
  list:
    - root:
timezone: "Europe/Moscow"
package_update: false
datasource:
  Ec2:
    strict_id: false
    timeout: 5
    max_wait: 5
    metadata_urls:
      - http://169.254.169.254:80
""",
        'hostname': node.short_id[:15],
        'instance-id': node.short_id,
    }
```

После установки скрипта развёртывания нажмите **Создать** (Рисунок 99).

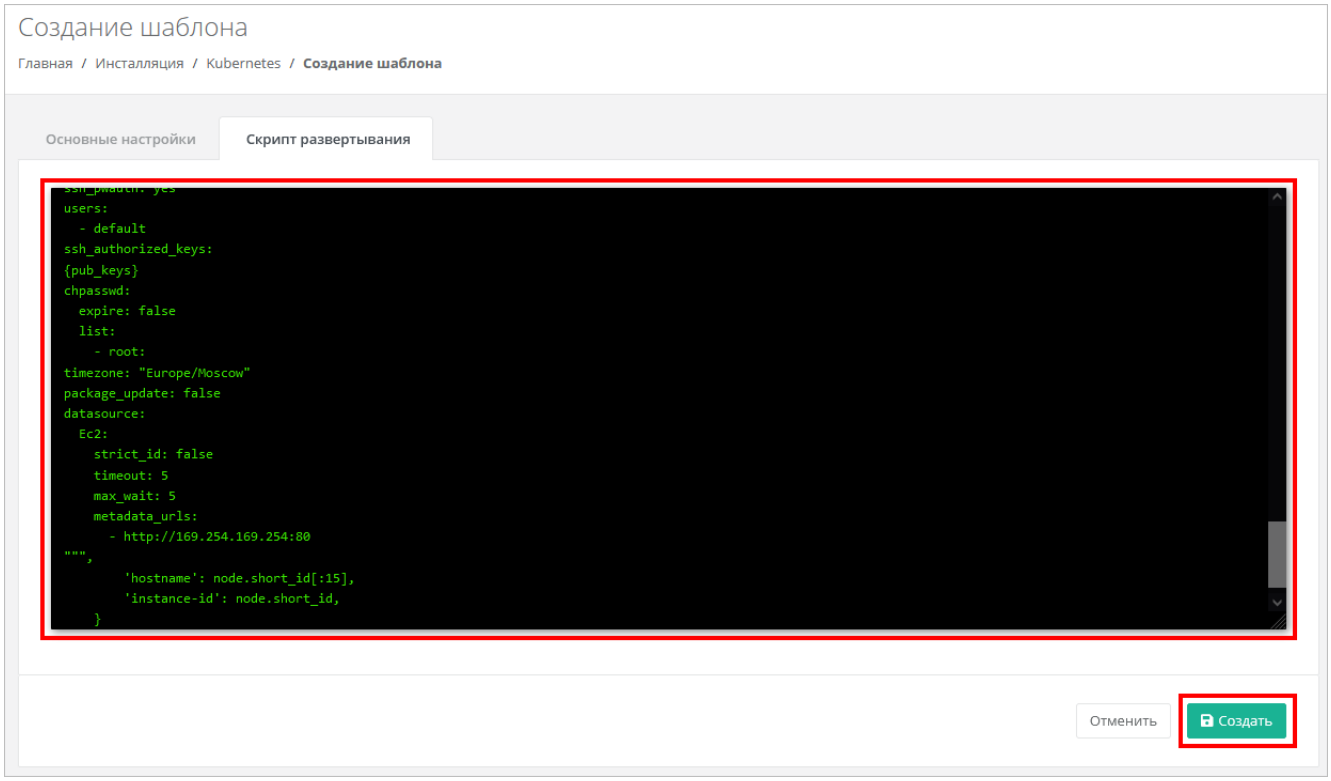

Рисунок 99

На этом настройка шаблона завершена, и он отобразится в списке шаблонов Kubernetes (Рисунок 100), а также будет доступен для создания в меню **Кластеры Kubernetes** для пользователя (Рисунок 101).

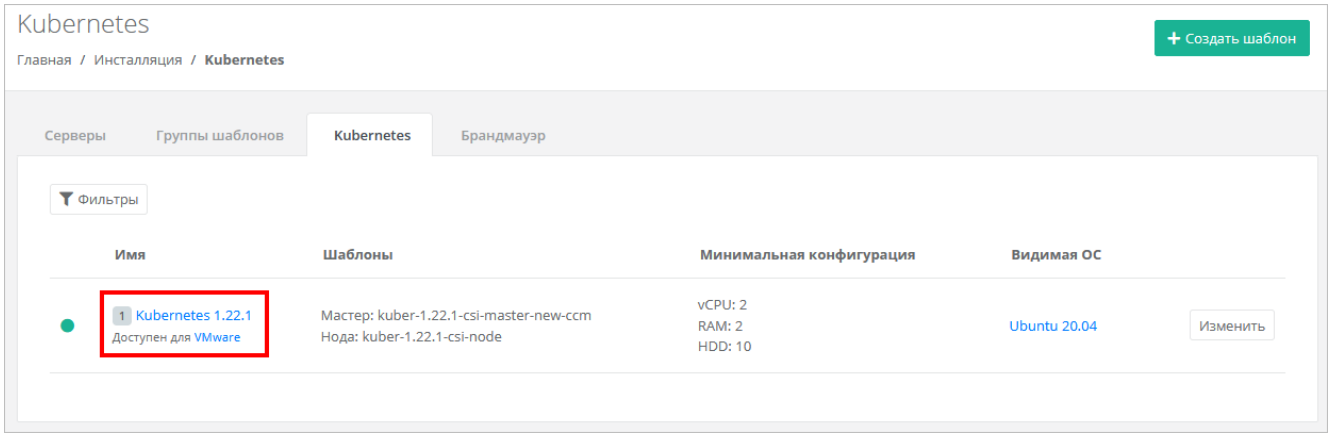

Рисунок 100

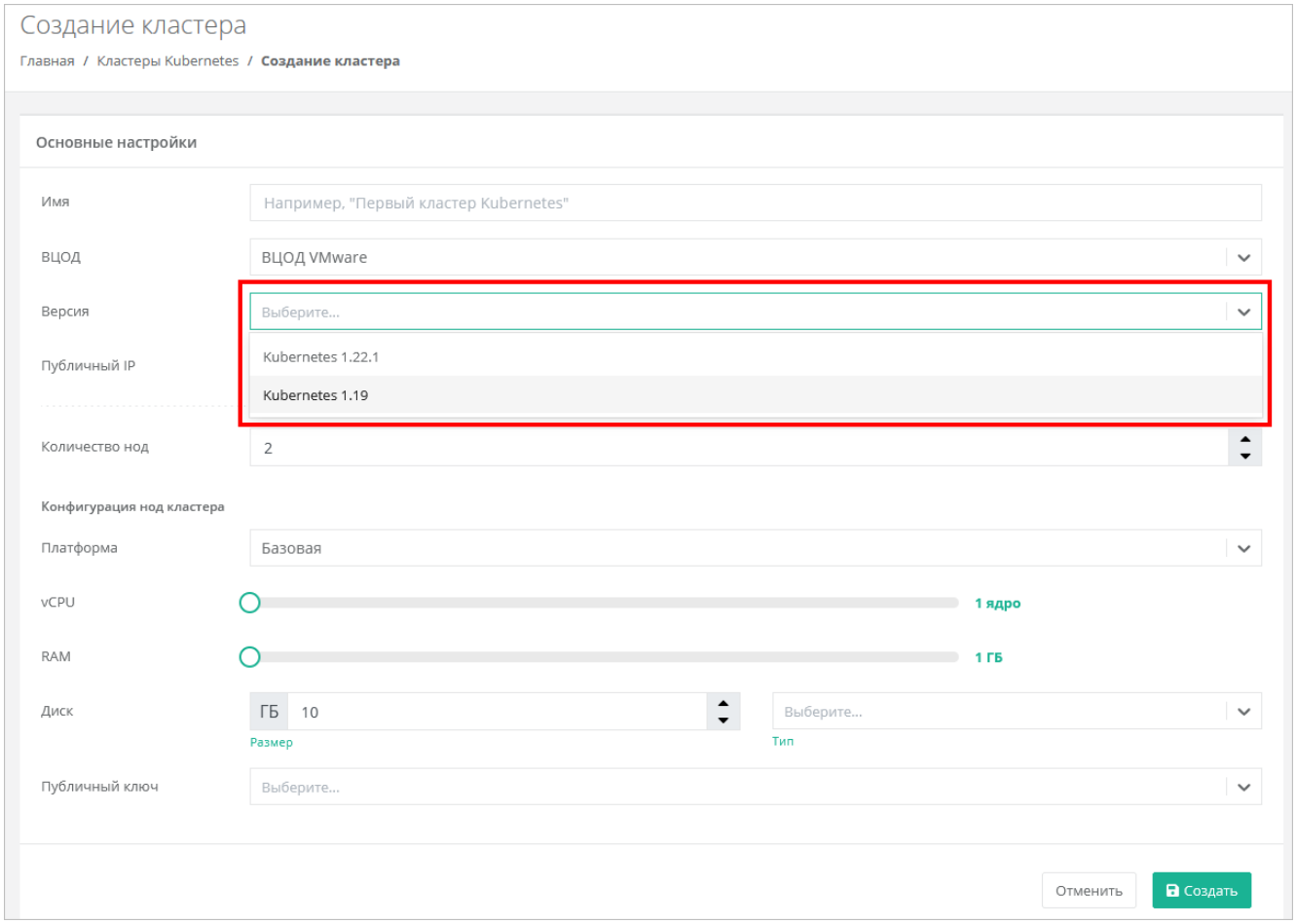

Рисунок 101

6.2. Создание шаблонов Kubernetes для сегмента РУСТЭК

Рассматривается подготовка шаблонов на примере Kubernetes версии 1.22.1.

1. Подключитесь по SSH (логин — **root**, пароль — **rustack**) к одному из управляющих узлов РУСТЭК.
2. Скачайте vmdk образы master-ноды и worker-ноды в директорию **/tmp**, используя указанные в команде ссылки:

```
cd /tmp

curl -O -L https://file.rustack.ru/s/STwca5F8FxqoMjy/download/kuber-1.22.1-csi-master-new-ccm-1.vmdk

curl -O -L https://file.rustack.ru/s/9bX4NK86YFzDBjr/download/kuber-1.22.1-csi-node-1.vmdk
```

3. Сконвертируйте образы в формат .qcow2:

```
qemu-img convert -p -O qcow2 kuber-1.22.1-csi-master-new-ccm-1.vmdk kuber-1.22.1-csi-master-new-ccm-1.qcow2

qemu-img convert -p -O qcow2 kuber-1.22.1-csi-node-1.vmdk kuber-1.22.1-csi-node-
```

```
1.qcow2
```

4. Удалите исходники образов (.vmdk):

```
rm kuber-1.22.1-csi-node-1.vmdk
rm kuber-1.22.1-csi-master-new-ccm-1.vmdk
```

5. Создайте images (Рисунок 102):

```
openstack image create --disk-format qcow2 --container-format bare --public --
property hw_disk_bus=scsi --property hw_scsi_model=virtio-scsi --property
hw_vif_model=virtio --property image_type=master --file kuber-1.22.1-csi-master-
new-ccm-1.qcow2 kuber-1.22.1-csi-master-new-ccm

openstack image create --disk-format qcow2 --container-format bare --public --
property hw_disk_bus=scsi --property hw_scsi_model=virtio-scsi --property
hw_vif_model=virtio --property image_type=master --file kuber-1.22.1-csi-node-
1.qcow2 kuber-1.22.1-csi-node
```

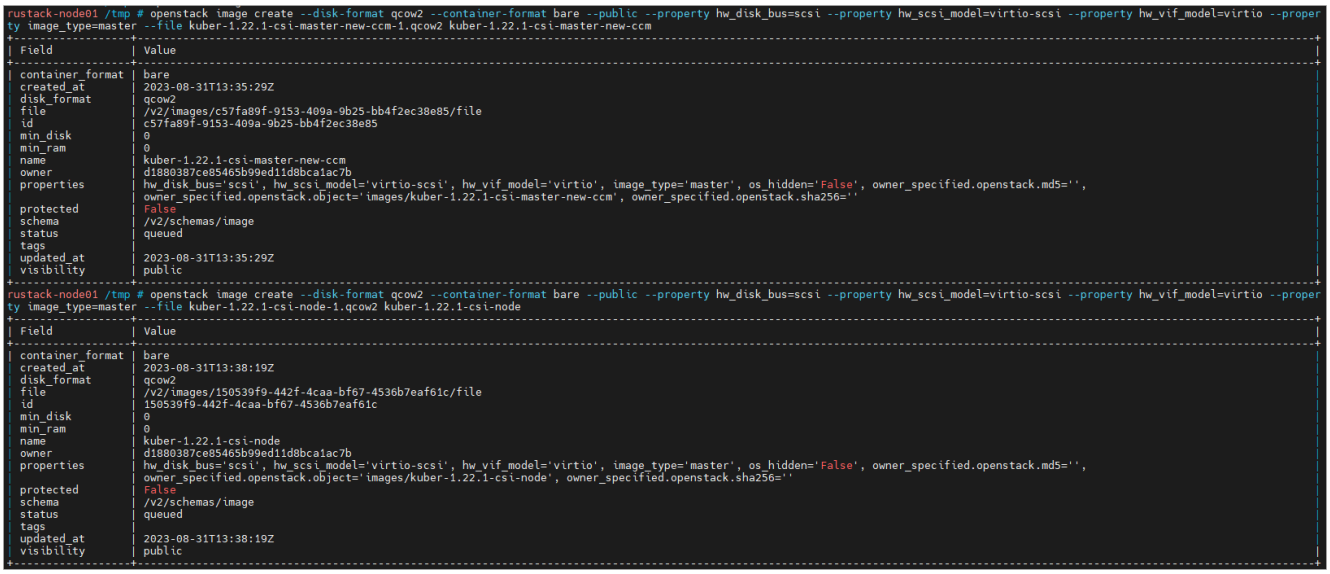

Рисунок 102

6. Удалите образы (.qcow2):

```
rm kuber-1.22.1-csi-node-1.qcow2
rm kuber-1.22.1-csi-master-new-ccm-1.qcow2
```

После успешной загрузки шаблонов в РУСТЭК необходимо настроить РУСТЭК-ЕСУ для работы с ними. Для этого в панели управления РУСТЭК-ЕСУ перейдите в раздел меню **Инсталляция** → **Шаблоны** → **Kubernetes** и нажмите кнопку **Создать шаблон**.

В открывшемся окне заполните поля настроек (Рисунок 103):

- **Ресурсные пулы** — выберите ресурсный пул РУСТЭК.
- **Имя** — произвольное имя.

- **Включен** — установите флаг.
- **Позиция** — позиция определяет расположение имени шаблона в раскрывающемся списке в поле **Версия** при создании кластера Kubernetes пользователем. Можно оставить по умолчанию.
- **Темплейт мастера** — выберите шаблон master-ноды, загруженный в РУСТЭК, из списка в отдельном окне.
- **Темплейт ноды** — выберите шаблон ноды, загруженный в РУСТЭК, из списка в отдельном окне.
- **Видимый шаблон ОС** — выберите любой шаблон из списка, влияет только на название, которое будет отображаться в списке серверов.
- **Минимальная конфигурация** — рекомендуемая конфигурация для наших шаблонов: vCPU — 2, RAM — 2 ГБ, HDD — 10 ГБ.

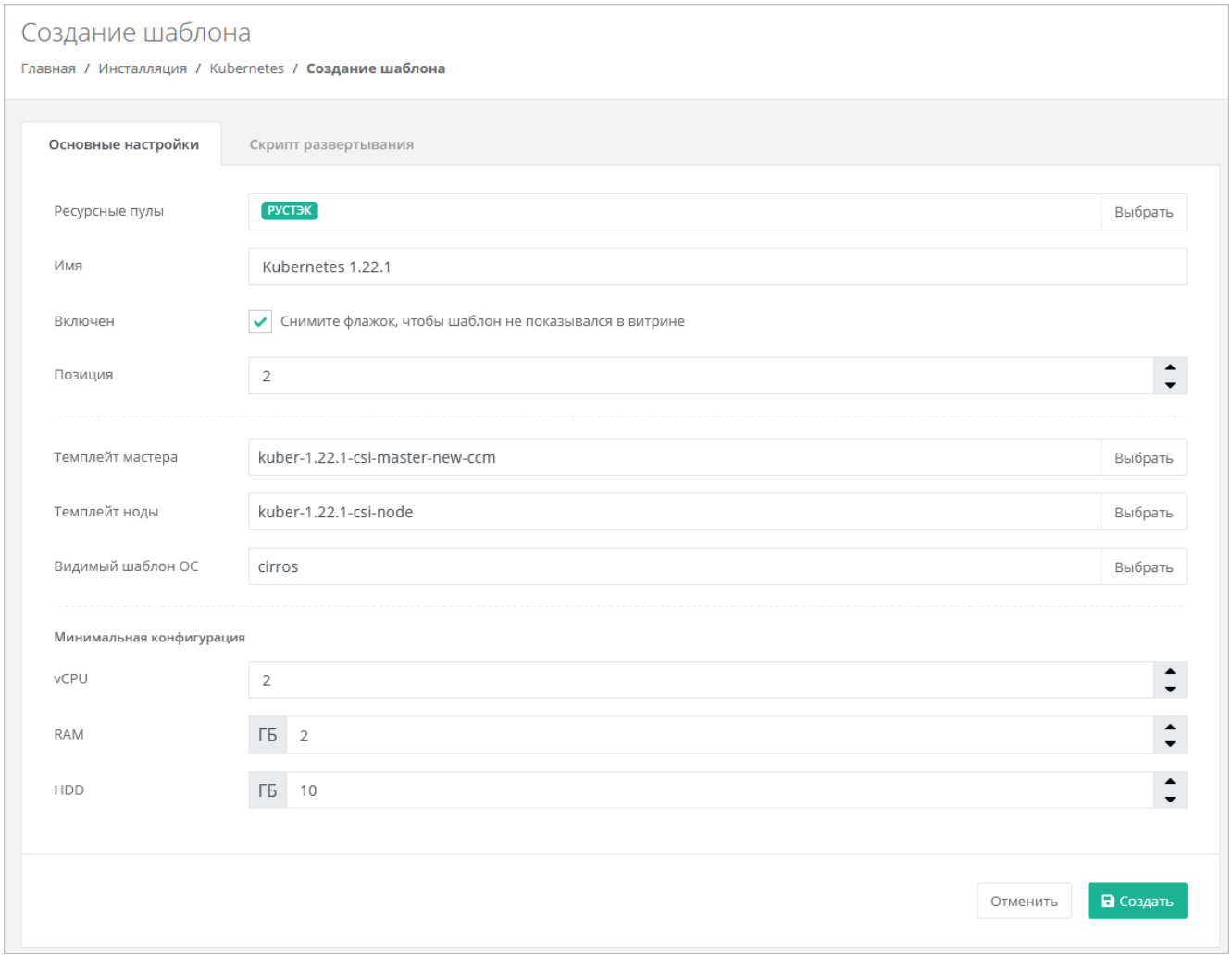

Рисунок 103

Далее на вкладке **Скрипт развёртывания** добавьте скрипт:

```
from authentication.models import PubKey, Token

def get_metadata(master=None, node=None):
    if master:
        return _prepare_master(master)
    else:
        return _prepare_node(node)

def _prepare_master(master):
    hypervisor = master.vdc.hypervisor
    api_url = hypervisor.get_setting('platform_internal_url')
    api_token = hypervisor.get_setting('edge_api_token')

    sa_token = Token(user=master.service_user)
    sa_token.save()
    sa_token = sa_token.original_key

    return {
        'user_data': f"""\
#cloud-config
debug:
  verbose: true
cloud_init_modules:
  - migrator
  - seed_random
  - bootcmd
  - write-files
  - growpart
  - resizefs
  - set_hostname
  - update_hostname
  - update_etc_hosts
  - users-groups
  - ssh
  - runcmd
runcmd:
  - runner install --api_url="{api_url}" --token="{api_token}" --
sa_token="{sa_token}" --runner_id="{master.short_id}" --ifname=eth0 --
kubernetes_uuid="{master.id}" --version="1.22.1"
fqdn: "{master.master_hostname}"
manage_etc_hosts: true
disable_root: false
ssh_pwauth: yes
users:
  - default
ssh_authorized_keys:
  - ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKZnwlDIoHsfZukwf/QnHP8KR/diFMQgLFxG0Doe9qdZ/nE7xf3
bUF9WNXwMEemQv6Vo6Jdp0kTswT+ZuELlxcvd4OgnIBChdY8qym/4/BFMqFJz6IJ1Bhenp/+bvy/cWR2b
BKNiYb0Cw5dWU+0xbS75l6jy0oH3zCwVTNGQ7ieB5cwJaq3w9LYuXGITUN6pko3mJKMhQ1JB7mre8ZGkz
KIwux5Eut4me1JCFfi/bGFlUUB/uFkzJIHtv4nlAmz3pW+Wv/6eqXXoaBrGp9Dmp3qPmnXtAywsnKGZ6o
```

```
hp2jIcmJZ69ceJvB1jx5IoIR9W+ntBwlVhvmOdkSVy4yHiGL deploy@localhost
chpasswd:
  expire: false
  list:
    - root:
timezone: "Europe/Moscow"
package_update: false
datasource:
  Ec2:
    strict_id: false
    timeout: 5
    max_wait: 5
    metadata_urls:
      - http://169.254.169.254:80
""",
        'hostname': master.master_hostname[:15],
        'instance-id': master.short_id,
    }

def _prepare_node(node):
    pub_keys = [node.kubernetes.service_public_key,
node.kubernetes.user_public_key]
    pub_keys = '\n'.join([f'  - "{k}"' for k in pub_keys])

    internal_ip = node.ports[0].ip_address

    return {
        'user_data': f"""\
#cloud-config
debug:
  verbose: true
cloud_init_modules:
  - seed_random
  - bootcmd
  - write-files
  - growpart
  - resizefs
  - set_hostname
  - users-groups
  - ssh
bootcmd:
  - echo {internal_ip} {node.hostname or node.short_id[:15]} > /etc/hosts
  - echo "127.0.0.1 localhost" >> /etc/hosts
disable_root: false
fqdn: "{node.hostname or node.short_id[:15]}"
ssh_pwauth: yes
users:
  - default
ssh_authorized_keys:
{pub_keys}
chpasswd:
  expire: false
```

```
  list:
    - root:
timezone: "Europe/Moscow"
package_update: false
datasource:
  Ec2:
    strict_id: false
    timeout: 5
    max_wait: 5
    metadata_urls:
      - http://169.254.169.254:80
""",
        'hostname': node.short_id[:15],
        'instance-id': node.short_id,
    }
```

После установки скрипта развёртывания нажмите **Создать** (Рисунок 104).

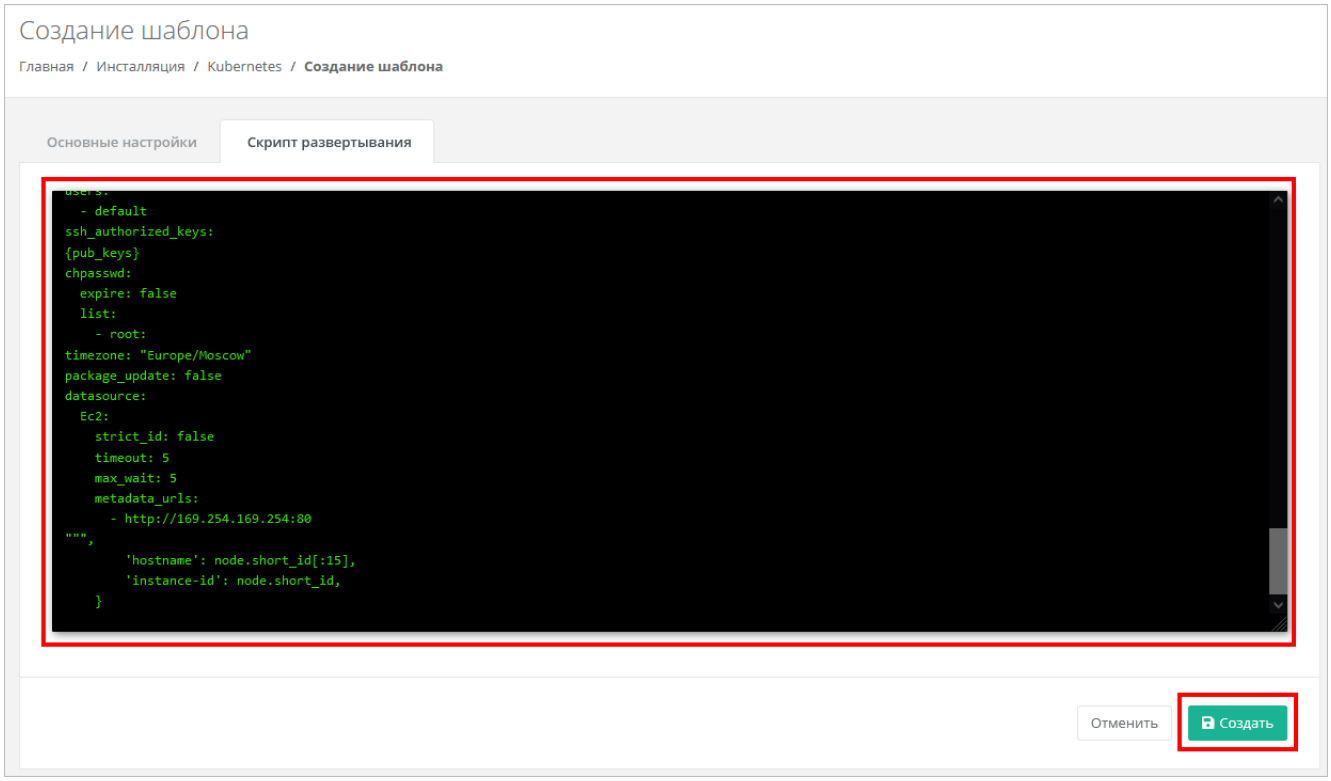

Рисунок 104

На этом настройка шаблона завершена, и он отобразится в списке шаблонов Kubernetes (Рисунок 105), а также будет доступен для создания в меню **Кластеры Kubernetes** для пользователя (Рисунок 106).

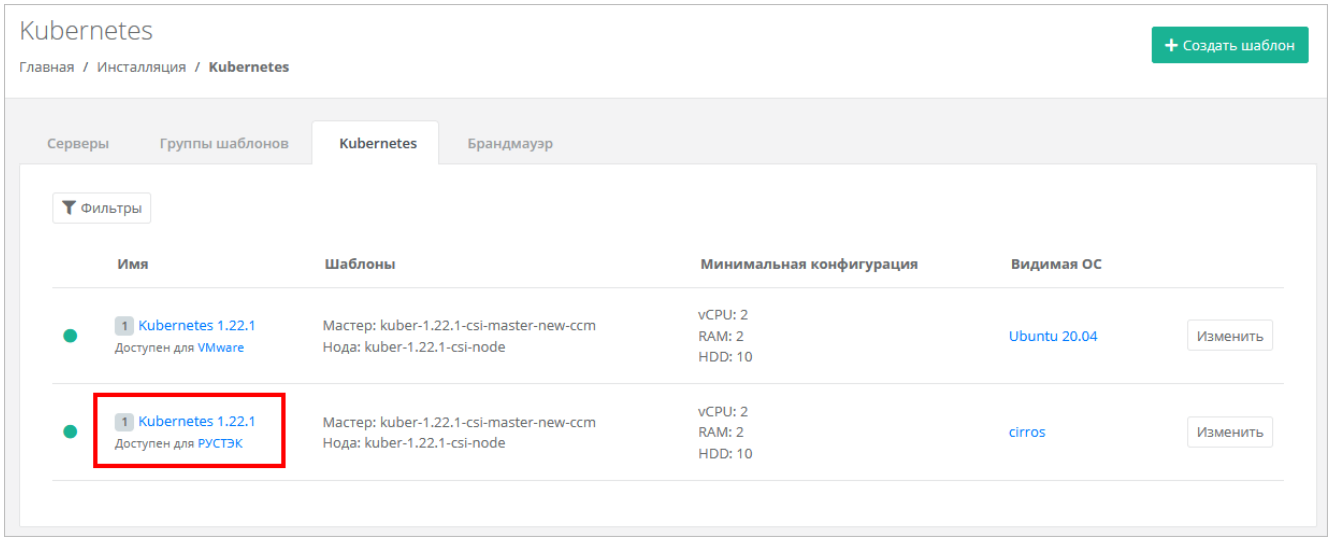

Рисунок 105

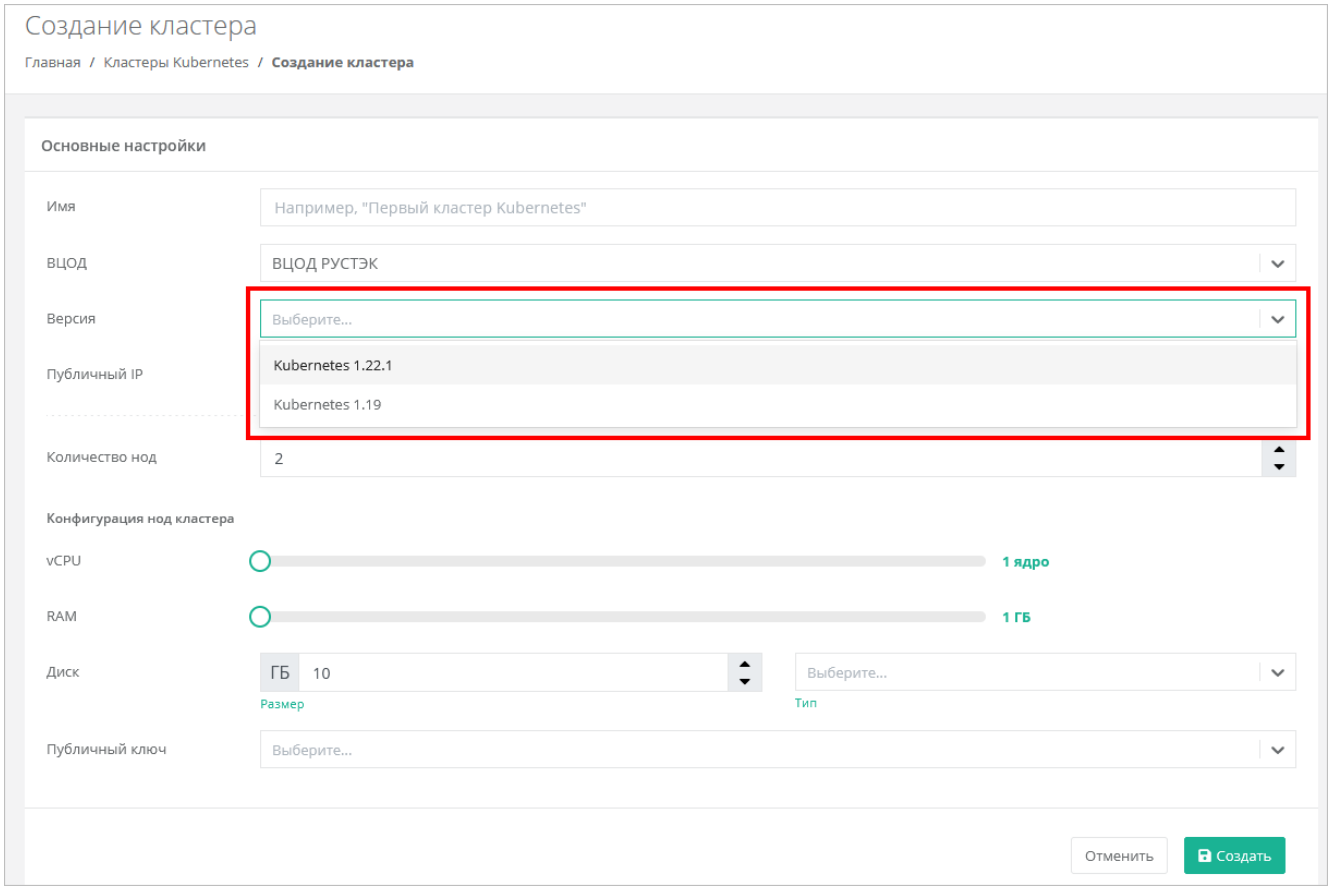

Рисунок 106

Для последующего развёртывания кластеров в сегменте РУСТЭК выполните дополнительную настройку ресурсного пула.

Для этого в главном меню панели управления перейдите в **Инсталляция** → **Ресурсы** → **Ресурсные пулы**. Выберите ресурсный пул РУСТЭК (Рисунок 107).

В открывшемся окне заполните поля настроек:

- **Название management-сети, в которой работает ECУ** — название маршрутизируемой сети, см. подраздел 2.2.

- **Адрес ЕСУ в management-сети, по которому будет доступно API** — адрес BM ESU-box в маршрутизируемой сети, см. подраздел 2.2.
- **Токен, который будет использоваться Edge-роутерами для работы с РУСТЭК-ЕСУ** — токен пользователя (можно скопировать из настроек ресурсного пула vSphere).

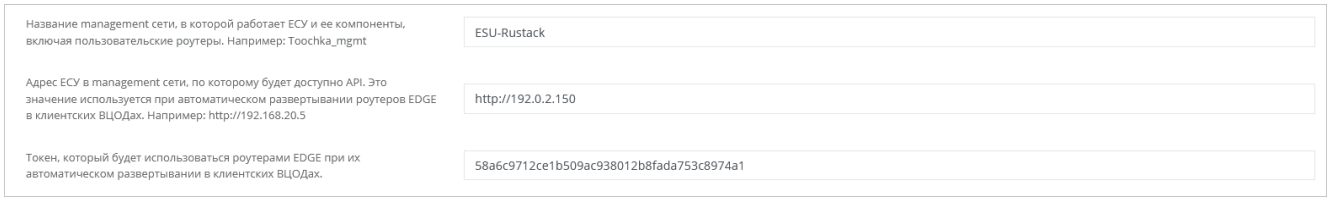

Рисунок 107

6.3. Создание кластеров Kubernetes в РУСТЭК-ЕСУ

Для проверки корректности выполненных настроек создайте кластер Kubernetes.

Для этого в главном меню панели управления перейдите в **Кластеры Kubernetes** и нажмите кнопку **Создать**.

В открывшемся окне **Создание кластера** заполните поля настроек (Рисунок 108):

- **Имя** — произвольное наименование кластера.
- **ВЦОД** — выбор необходимого ВЦОД, либо создание нового.
- **Версия** — выбор версии Kubernetes.
- **Публичный IP** — выбор способа назначения публичного IP-адреса:
  - **Отключен** — кластер Kubernetes не будет иметь публичного IP-адреса.
  - **Новый** — получение нового IP-адреса из пула публичных адресов.
  - **Случайный** — использование выделенного для ВЦОД свободного IP-адреса, в случае отсутствия такого — получение нового из пула публичных адресов.
- **Количество нод** — выбор количества нод для кластера.
- **Конфигурация нод кластера** — выбор параметров конфигурации нод:
  - **vCPU** — количество ядер vCPU ноды.
  - **RAM** — объём оперативной памяти ноды.
  - **Диск**:
    - **Размер диска ноды**.
    - **Тип диска**: SSD, SAS, SATA.
- **Публичный ключ** — в поле выбора ключа нажмите на раскрывающийся список ⌄ и выберите **Создать публичный ключ**. В открывшемся окне введите имя ключа и нажмите кнопку **Сгенерировать** 🔑. Сохраните приватный ключ и нажмите **Принять**.

Все поля должны быть заполнены. Также добавьте публичный ключ (его можно сгенерировать в панели управления), он нужен для доступа мастер-ноды к остальным нодам кластера.

После заполнения всех полей нажмите **Создать**.

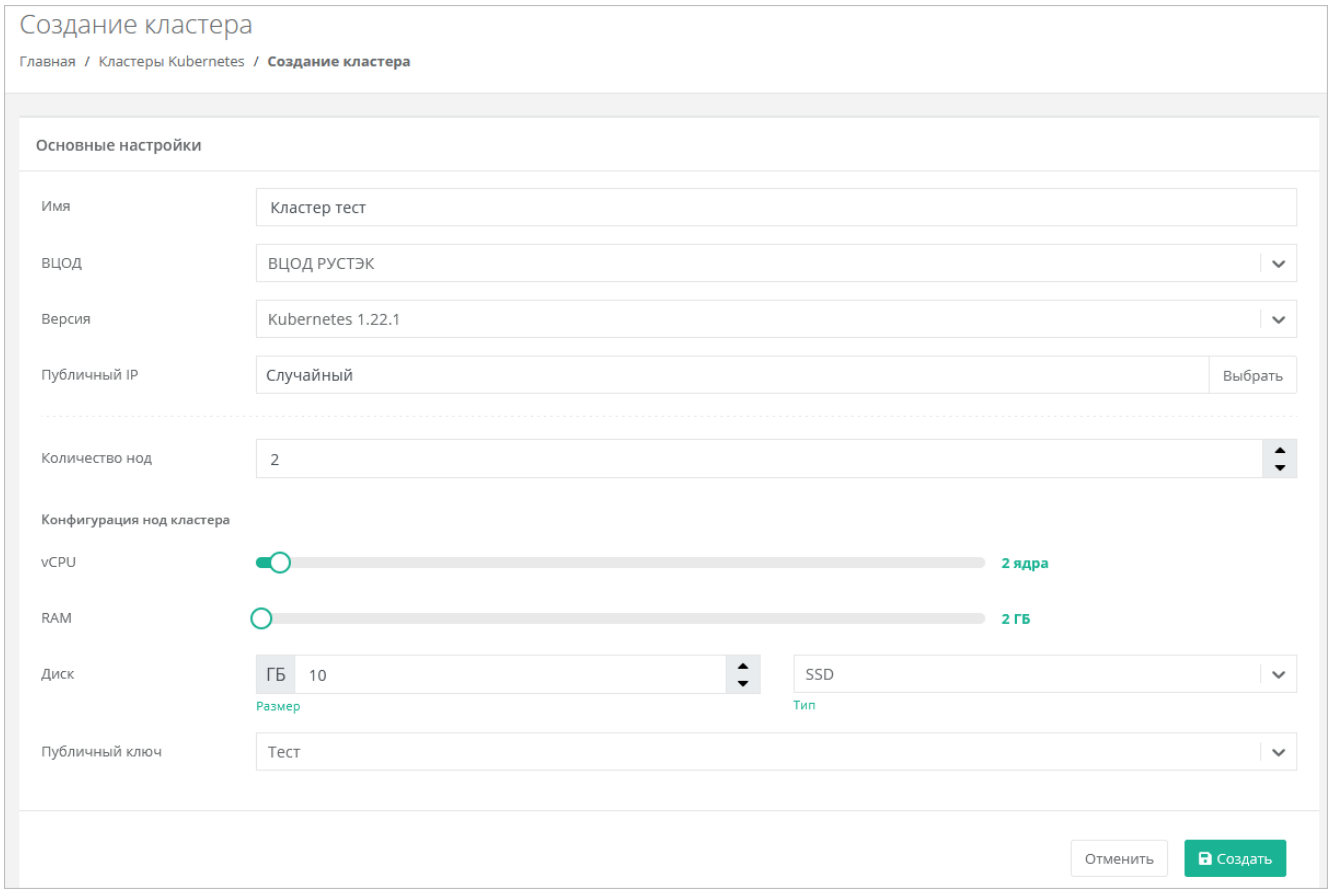

Рисунок 108

После создания кластер отобразится в панели управления (Рисунок 109).

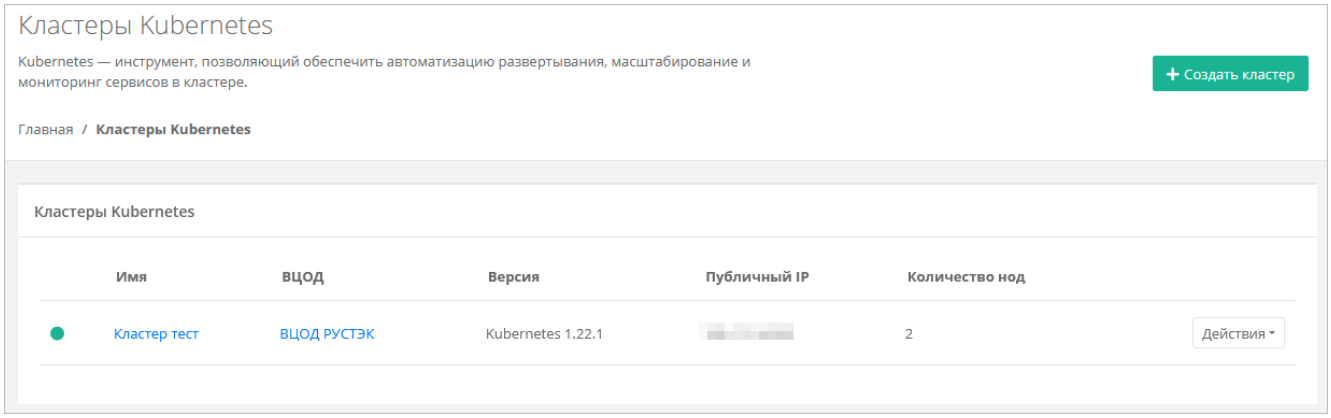

Рисунок 109

Ноды кластера также отображаются в меню **Облачные вычисления → ВЦОД → Серверы**. Нодами кластера Kubernetes можно управлять как обычными серверами — изменять конфигурацию и управлять состоянием сервера (Рисунок 110).

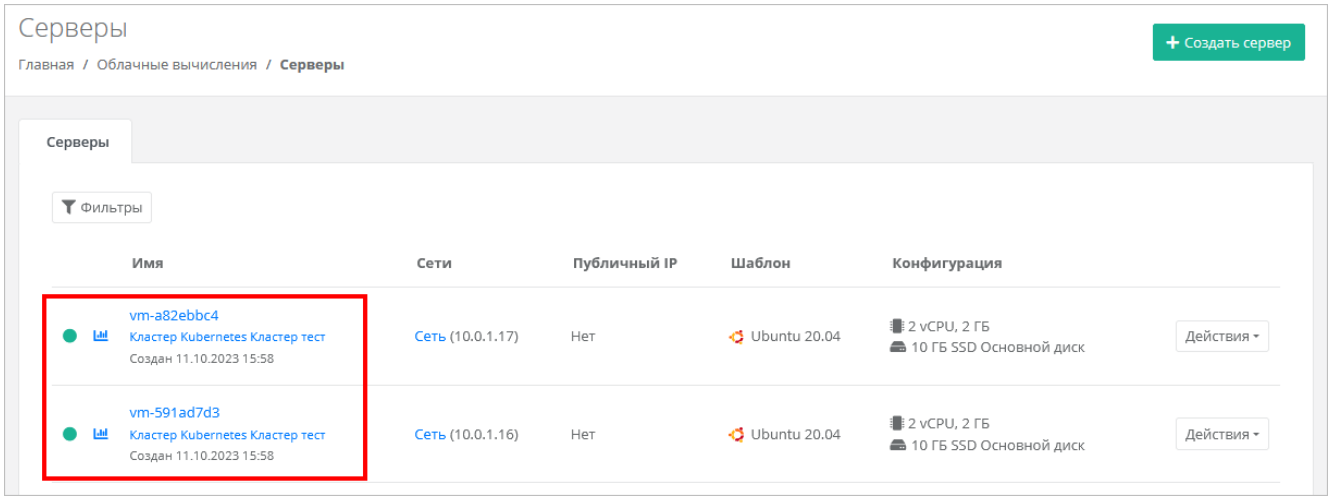

Рисунок 110

6.4. Особенности и поддерживаемый функционал

Особенности:

- Кластер развёртывается только в сервисной сети ВЦОДа (созданной автоматически при создании ВЦОД).
- Требуется наличие пользовательского публичного ключа в профиле, так как ноды будут создаваться без пароля, но с ключом. Это упрощает процедуру развёртывания и настройку опций развёртывания для пользователя.
- Сервисы k8s, отвечающие за работоспособность кластера, физически запущены на одной ВМ. В случае ее «падения» кластер будет неуправляем до момента ее включения.
- Мастер-нода недоступна для управления пользователем и располагается в маршрутизируемой внутренней сети.

Поддерживаемый функционал:

- Балансировщики нагрузки в кластере Kubernetes.
- Создание Persistence Volume Claims (доступны в обоих сегментах, но только создание — изменение недоступно).

7. Расширенная настройка

7.1. Настройка NGINX реверс-прокси

РУСТЭК-ЕСУ должна работать с конечными пользователями только по https.

Рекомендуется настроить проксирование РУСТЭК-ЕСУ для конечных пользователей на специально организованном реверс-прокси, например, nginx. Для упрощения построения проксирования в РУСТЭК-ЕСУ открыт порт 80.

Ниже приведён пример минимальной конфигурации файла `/etc/nginx/conf.d/<любое имя>.conf`, который необходимо создать, где:

- **<your_domain>** — доменное имя сервера nginx.
- **<ip_esu-box>** — IP-адрес, по которому доступна панель управления.
- **<path_to_crt>** — путь к SSL-сертификату.
- **<path_to_key>** — путь к ключу.

```
server {
        server_name <your_domain>;

        location / {
                proxy_read_timeout      1800;
                proxy_connect_timeout   1800;
                proxy_redirect          off;

                proxy_set_header        Host                    $http_host;
                proxy_set_header        X-Real-IP               $remote_addr;
                proxy_set_header        X-Forwarded-For
$proxy_add_x_forwarded_for;
                proxy_set_header        X-Forwarded-Proto       $scheme;
                proxy_set_header        X-Frame-Options         SAMEORIGIN;

                proxy_set_header        Upgrade                 $http_upgrade;
                proxy_set_header        Connection              "upgrade";

                proxy_pass      http://<ip_esu-box>:80;
                proxy_buffering off;

        }

    listen 443 ssl;
    client_max_body_size 150G;
    proxy_ssl_session_reuse off;
    ssl_certificate <path_to_crt>/fullchain.pem;
    ssl_certificate_key <path_to_key>/<your domain>/privkey.pem;
}
```

После создания файла конфигурации запустите службу `nginx`, для этого выполните команду:

```
systemctl start nginx
```

Затем добавьте службу `nginx` в автозапуск, для этого выполните команду:

```
systemctl enable nginx
```

Документация по настройке nginx: https://nginx.org/ru/docs/

Примечания:

- не следует работать с РУСТЭК-ЕСУ напрямую по порту 80, так как в этом случае не будет работать часть функционала, связанного с асинхронными обновлениями данных в браузере пользователя;
- по соображениям безопасности 80-й порт может быть отключён в будущих релизах;
- обратите внимание, что кеширование на стороне реверс-прокси отключено. Замечено, что при использовании модуля modsecurity кеширование на стороне nginx может непреднамеренно включиться.

7.2. Настройка управления DNS-зонами в РУСТЭК-ЕСУ

РУСТЭК-ЕСУ имеет службу, позволяющую пользователям управлять ресурсными записями делегированных в неё доменов. Зоны должны раздаваться как минимум с двух серверов, например, с пакетом BIND, работающих и настроенных отдельно от РУСТЭК-ЕСУ, но находящихся в той же сети. Раннер в РУСТЭК-ЕСУ выполняет роль так называемого каталога зон.

Нужна сетевая связность не только от BIND к РУСТЭК-ЕСУ, но и в обратную сторону.

Пример: в инсталляции РУСТЭК были развёрнуты два сервера на базе Ubuntu 20.04 LTS в той же сети, что и ESU-box.

Ниже показан пример конфигурации BIND 9.11 для работы с каталогом зон из РУСТЭК-ЕСУ.

Пример конфигурации приведен на базе BIND из Ubuntu 20.04 LTS.

Установка BIND 9:

```
apt-get install -y bind9 bind9utils bind9-doc
```

Установка hostname на серверы командой:

```
hostnamectl set-hostname <name>
```

Представим, что ESU-box расположена по адресу 192.0.2.150. Тогда конфигурационный файл **`/etc/bind/named.conf.options`** должен выглядеть так:

```
options {
    directory "/var/cache/bind/";
```

```
    allow-transfer { none;};
    dnssec-validation no;
    minimal-responses yes;

    auth-nxdomain no;
    listen-on port 53 { any; };

    recursion no;
    catalog-zones {
        zone "catalog.local" default-masters {
            192.0.2.150 port 9999;
        };
    };

    allow-notify {
        192.0.2.150;
    };
};

zone "catalog.local" {
    type slave;
    file "catalog.db";
    masters { 192.0.2.150 port 9999; };
};
```

Запуск службы командой:

```
systemctl start bind9
```

Добавление в автозапуск службы BIND:

```
systemctl enable bind9
```

Для созданных серверов добавьте DNS записи (имена).

Для данного примера это было сделано с помощью редактирования файла **`/etc/hosts`** на ВМ ESU-box.

После произведённой настройки укажите имена DNS-серверов и e-mail администратора в панели управления РУСТЭК-ЕСУ.

Для этого перейдите в раздел меню **Администрирование** → **Партнёры**, нажмите на имя партнёра, для домена которого настраиваются DNS-зоны, или на кнопку **Действия** → **Изменить**. На вкладке **Основные настройки** задайте список NS-серверов и адрес электронной почты администратора (Рисунок 111).

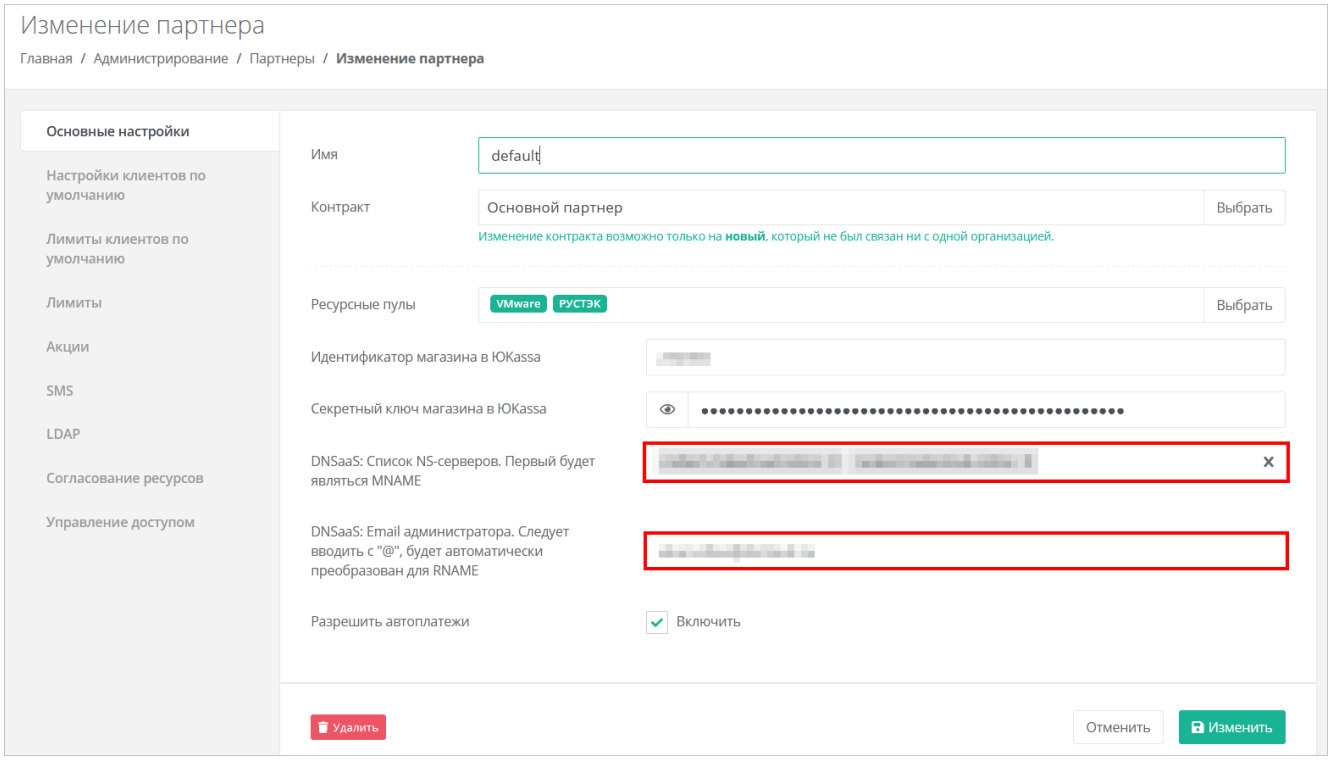

Рисунок 111

После успешной настройки в главном меню панели управления РУСТЭК-ЕСУ появится пункт **Доменные зоны**, из которого можно управлять доменными зонами и записями в них (Рисунок 112).

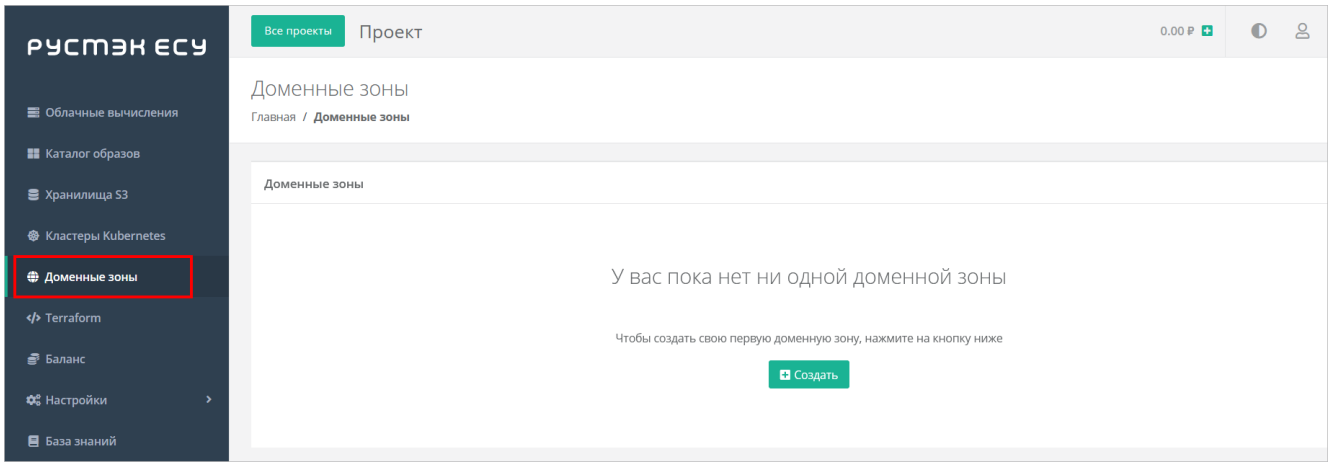

Рисунок 112

7.3. Настройка сети для роутеров (Edge) сегмента VMware vSphere

Базовая установка РУСТЭК-ЕСУ размещает пользовательские роутеры сегмента VMware в своей сервисной сети. Это удобно для быстрого запуска, но может вызывать проблемы при большом числе клиентов (размер сервисной сети ограничит количество клиентов сегмента VMware).

В таком случае необходимо создать отдельную сеть для роутеров внутри РУСТЭК, например, Edge_network (Рисунок 113).

Для этого в панели РУСТЭК перейдите в раздел **Сеть** → **Сети** и нажмите **Создать**.

В открывшемся окне заполните поля:

- **Имя** — указать произвольное.
- **Тип сегментации** — VLAN.
- **Номер VLAN** — номер выделенного VLAN для внешней сети РУСТЭК-ЕСУ.
- **Внешняя** — снять флаг.
- **Безопасность портов** — указывается опционально. Данный функционал добавляет возможность использовать Firewall на уровне порта виртуальной машины.

После заполнения полей нажмите кнопку **Создать**.

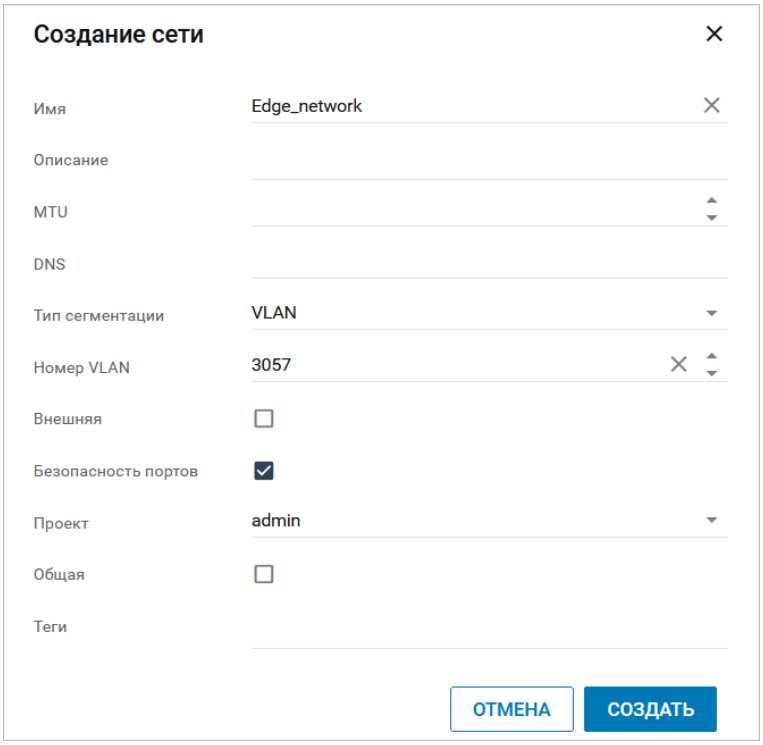

Рисунок 113

Далее создайте подсеть для созданной сети (Рисунок 114).

Для этого перейдите в раздел **Сеть** → **Подсети** и нажмите **Создать**, далее заполните поля:

- **Имя** — указать произвольное.
- **Сеть** — выбрать сеть, созданную на предыдущем этапе.
- **Версия протокола** — IPv4.
- **Адрес сети** — указать CIDR сети.
- **Шлюз** — указать шлюз.
- **DHCP** — снять флаг.
- **DNS-серверы** — прописать по желанию.

После заполнения полей нажмите кнопку **Создать**.

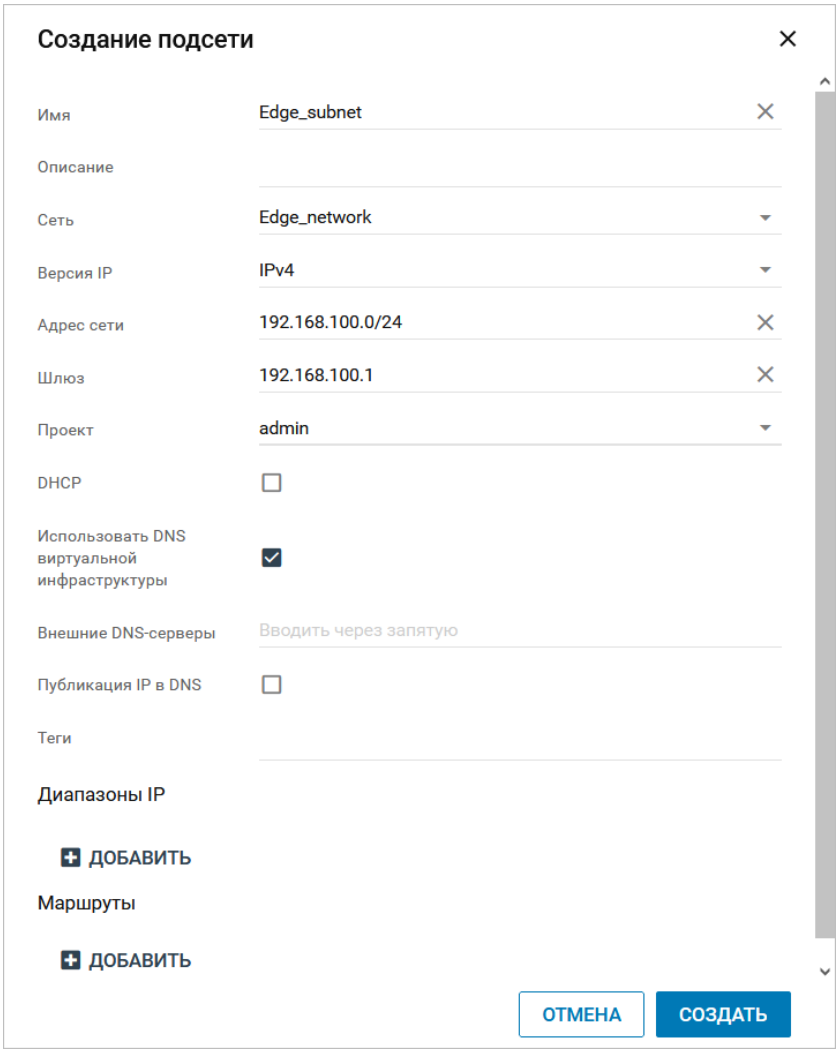

Рисунок 114

Затем подключите ESU-box (ВМ с РУСТЭК-ЕСУ) к этой сети.

Для этого перейдите в раздел **Виртуальные машины**, выберите ВМ с установленной РУСТЭК-ЕСУ (ESU-box), правой кнопкой мыши раскройте меню действий и выберите **Сети**  , затем добавьте новую созданную сеть (Рисунок 115).

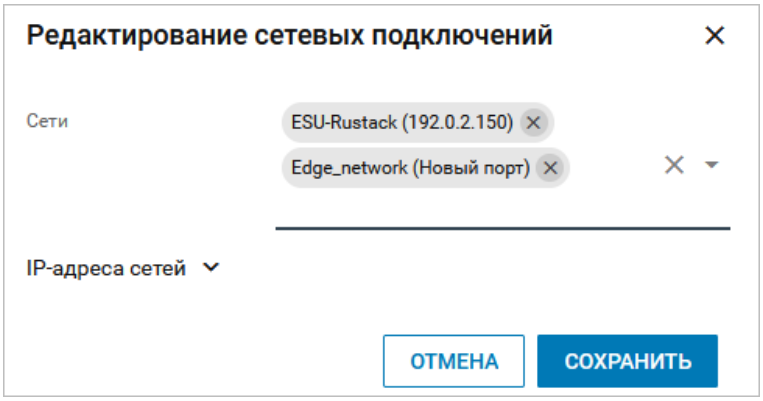

Рисунок 115

Нажмите **Сохранить**.

Чтобы узнать IP-адрес, назначенный для ESU-box в сети **Edge_network**, обновите страницу в меню **Виртуальные машины** (Рисунок 116):

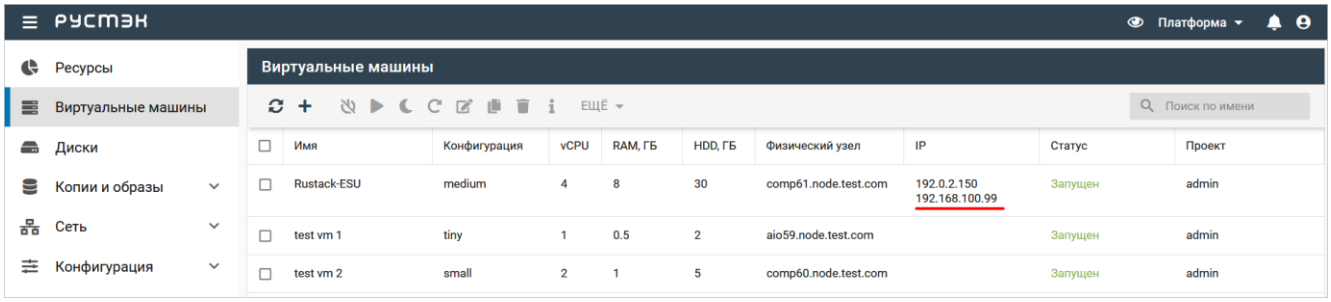

Рисунок 116

Затем подключитесь по SSH к ESU-box, где необходимо настроить новый сетевой интерфейс.

Сначала узнайте имя нового сетевого интерфейса, для этого выполните команду:

```
ip a | grep en
```

В данном случае имя нового сетевого интерфейса enp7s0.

Затем настройте этот интерфейс, для этого выполните следующие команды:

```
sudo nano /etc/network/interfaces
```

Вставьте в файл следующее содержимое и сохраните изменения:

```
auto enp7s0
iface enp7s0 inet static
 address 192.168.100.99
 netmask 255.255.255.0
 gateway 192.168.100.1
```

Затем настройте DHCP-сервер на ESU-box для нового сетевого интерфейса. Для этого выполните команды ниже.

Добавьте имя нового интерфейса в файл **`/etc/default/isc-dhcp-server`** (Рисунок 117):

```
sudo nano /etc/default/isc-dhcp-server
```

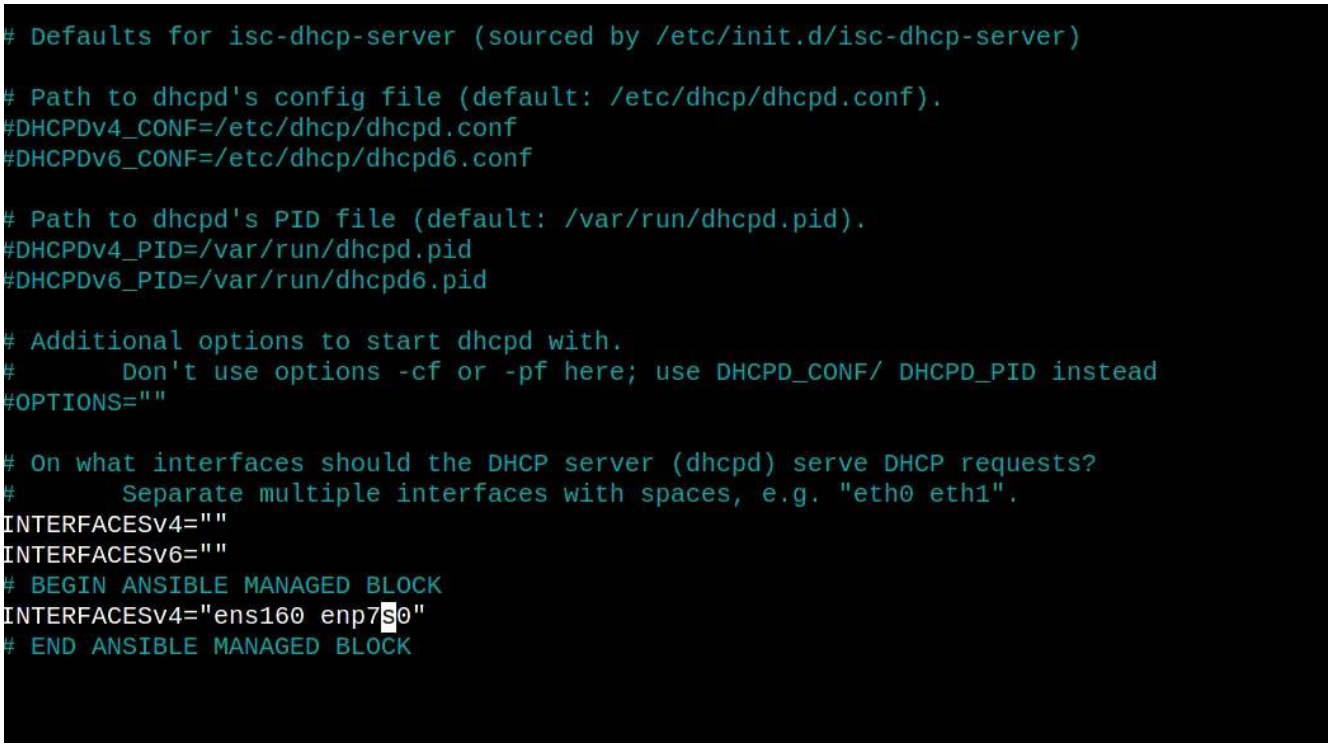

Рисунок 117

Теперь произведите настройку DHCP-сервера (Рисунок 118):

```
sudo nano /etc/dhcp/dhcpd.conf
```

В содержимое файла вставить:

```
subnet 192.168.100.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option routers 192.168.100.1;
  option domain-name-servers 8.8.8.8;
  range 192.168.100.11 192.168.100.255;
  default-lease-time 600;
  max-lease-time 10800;
}
```

```
# BEGIN ANSIBLE MANAGED BLOCK
subnet 192.0.2.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option routers 192.0.2.1;
  option domain-name-servers 8.8.8.8;
  range 192.0.2.2 192.0.2.254;
  default-lease-time 600;
  max-lease-time 7200;
}
subnet 192.168.100.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option routers 192.168.100.1;
  option domain-name-servers 8.8.8.8;
  range 192.168.100.11 192.168.100.255;
  default-lease-time 600;
  max-lease-time 10800;
}
# END ANSIBLE MANAGED BLOCK
```

Рисунок 118

Перезагрузите службы DHCP-сервера и сети:

```
sudo service isc-dhcp-server restart
sudo service networking restart
```

После этого создайте и настройте сеть (портгруппа на vDS) в VMware vSphere (Рисунок 119, Рисунок 120).

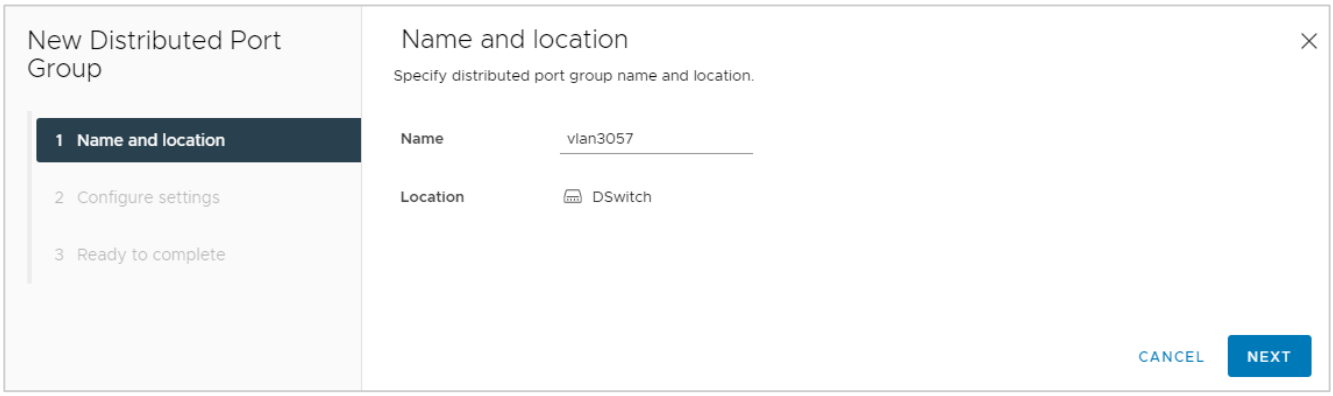

Рисунок 119

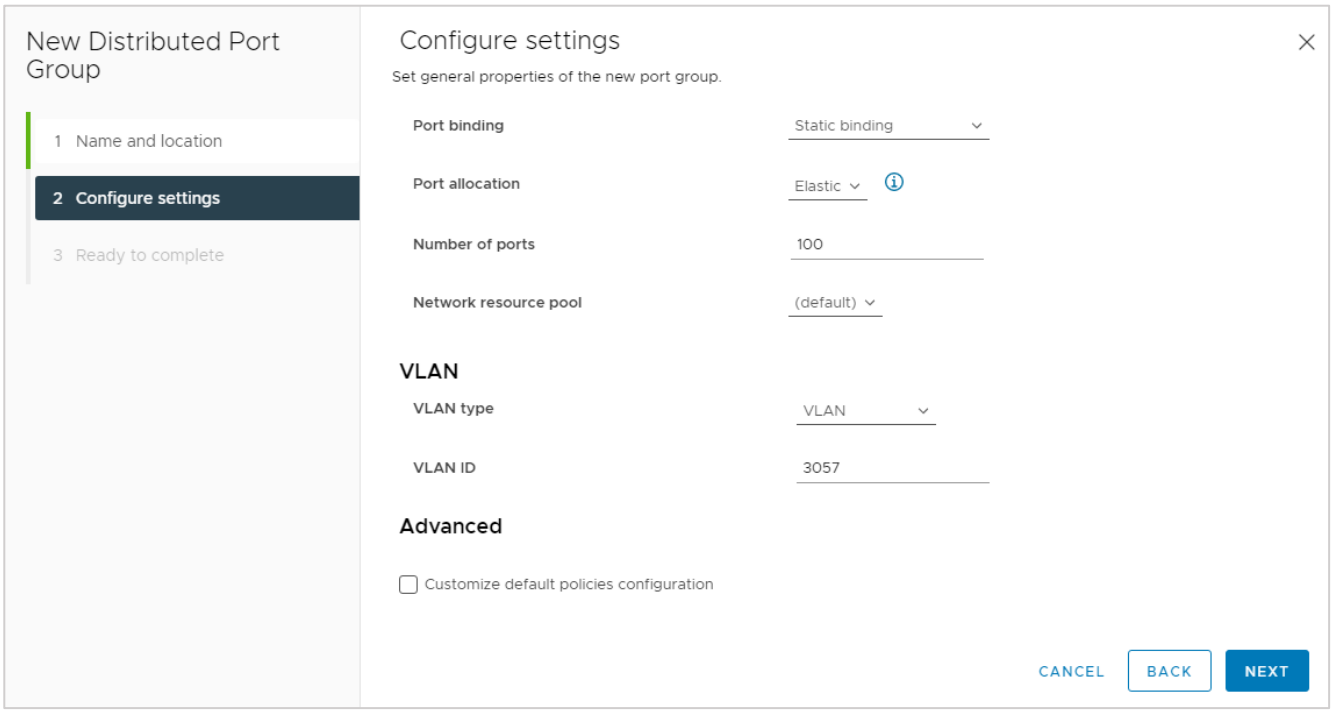

Рисунок 120

Далее укажите в настройках ресурсного пула VMware данную сеть как management-сеть для роутеров.

Для этого в панели управления РУСТЭК-ЕСУ перейдите в меню **Инсталляция** → **Ресурсы** → **Ресурсные пулы**.

Выберите ресурсный пул VMware vSphere и измените настройки (Рисунок 121):

- **Название management-сети для пользовательских роутеров** — укажите название созданной сети в VMware vSphere.
- **Адрес ЕСУ в management-сети, в которой будут создаваться роутеры** — укажите адрес сервера ESU-box в новой сети (Рисунок 116).

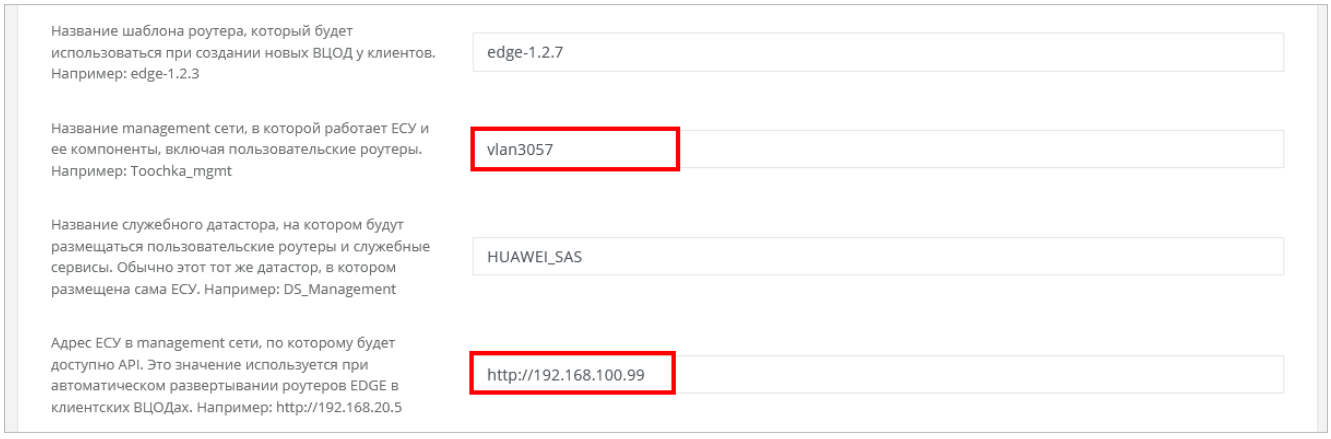

Рисунок 121

Нажмите **Изменить** для сохранения настроек.

На этом настройка завершена.

Следует отметить, что уже созданные Роутеры (Edge) останутся в той сети, в которой были созданы. Новые роутеры будут создаваться в новой настроенной сети.

Чтобы проверить это, создайте новый ВЦОД в сегменте VMware vSphere (Рисунок 122).

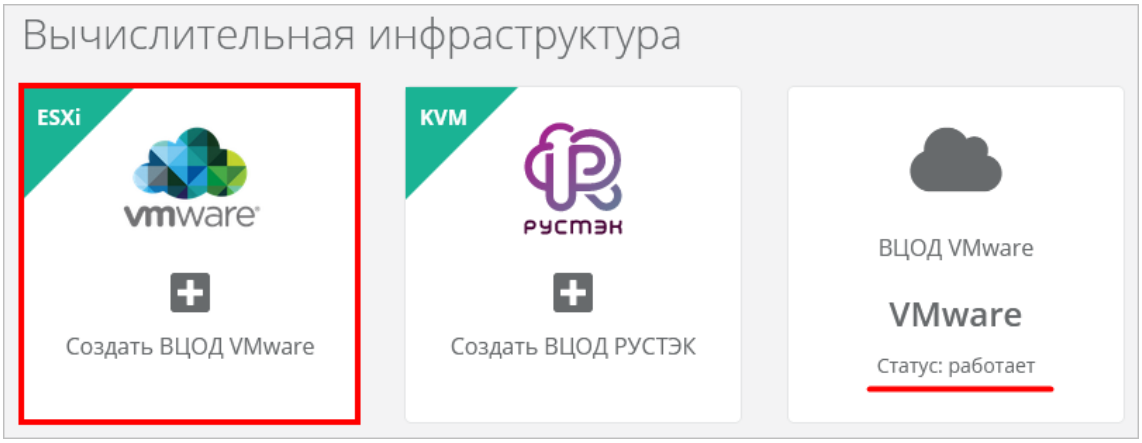

Рисунок 122

После создания ВЦОД перейдите в панель VMware vSphere и убедитесь, что роутер (Edge), созданный внутри нового ВЦОД, подключен к новой настроенной сети (Рисунок 123).

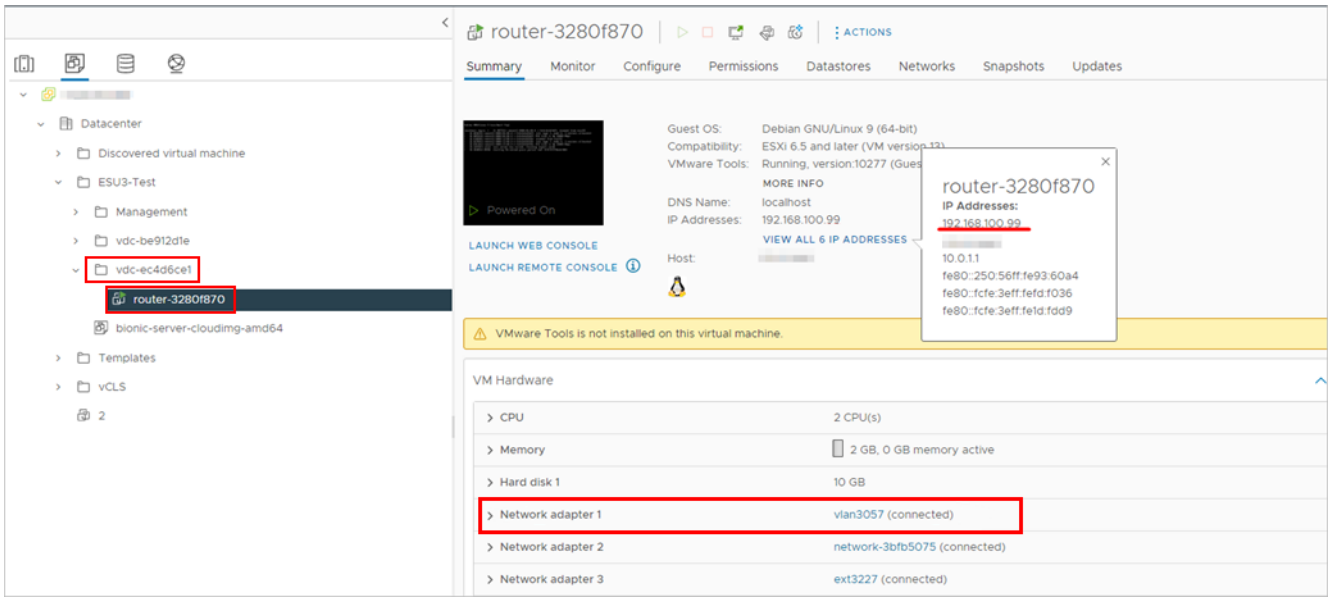

Рисунок 123

7.4. Универсальный скрипт развёртывания

Скрипт развёртывания используется в процедуре создания шаблонов для последующего развёртывания серверов в панели управления РУСТЭК-ЕСУ. Создать шаблоны можно в меню **Инсталляция** → **Шаблоны** → **Серверы**.

Для начала необходимо подготовить шаблон и загрузить на платформы виртуализации согласно инструкциям раздела 4.2.4 (для сегмента РУСТЭК) и раздела 4.3.7 (для сегмента VMware vSphere).

Скрипт пишется на языке Python и должен содержать функцию `get_metadata(vmInfo, userData)`, возвращающую набор полей для передачи через EC2.

При создании шаблона ВМ в меню **Инсталляция** → **Шаблоны** → **Серверы** на вкладке **Поля для скрипта** добавьте следующие поля (Рисунок 124):

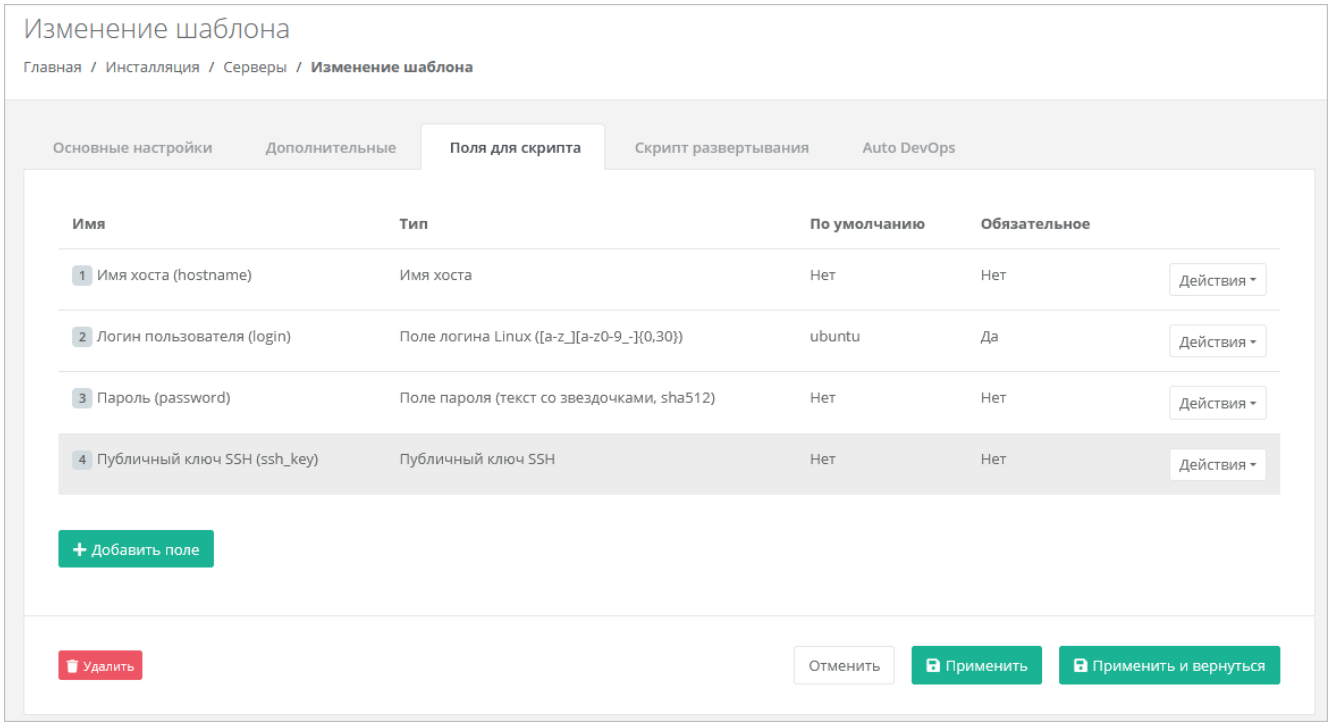

Рисунок 124

Универсальный скрипт, подходящий для Ubuntu 16, Ubuntu 18, Ubuntu 20, Debian 9, Debian 10, Centos 7, Centos 8:

```
from loguru import logger
from rest_framework import serializers

"""
ESU metadata script
Version 3.1 (2021-07-02)

CUSTOM!
"""


def get_metadata(vm, user_data):
    # В логи контейнера API попадет следующая информация:
    logger.info('Create metadata for {}. vm: {}, user_data: {}', vm.template, vm,
user_data)

    # В отличии от user_data['hostname'], в vm.hostname всегда что-то есть. Если
```

```
не от пользователя,
    # то от системы:
    hostname = vm.hostname

    # Фрагменты для подмешивания в YAML cloud-config'a
    ssh_fragment = password_fragment = ''

    # Если пользователь указал ключ, добавим его
    if user_data['ssh_key']:
        ssh_fragment = fr"""
    ssh_authorized_keys:
      - "{user_data['ssh_key']}"
"""

    # Если пользователь указал пароль, добавим его
    if user_data['password']:
        password_fragment = fr"""
    passwd: "{user_data['password']}"
    lock_passwd: false
"""

    # Если пользователь не указал ни ключ, ни пароль, покажем ошибку
    if not ssh_fragment and not password_fragment:
        raise serializers.ValidationError('Чтобы иметь доступ на сервер,
необходимо или ввести пароль или выбрать публичный ключ. Допустимо также задать
пароль вместе с публичным ключом.')

    cloud_config = fr"""
#cloud-config
debug:
  verbose: false
cloud_init_modules:
  - migrator
  - seed_random
  - bootcmd
  - write-files
  - growpart
  - resizefs
  - set_hostname
  - update_hostname
  - update_etc_hosts
  - users-groups
  - ssh
bootcmd:
  - [ cloud-init-per, once, rmdefaultuser1, userdel, -r, centos ]
  - [ cloud-init-per, once, rmdefaultuser2, userdel, -r, debian ]
  - [ cloud-init-per, once, rmdefaultuser3, userdel, -r, ubuntu ]
  - [ sh, -c, echo "your_OS ver.1.10" ]
users:
  - name: {user_data['login']}
    groups: [adm, audio, cdrom, dialout, dip, floppy, lxd, netdev, plugdev, sudo,
video]
```

```
    sudo: ["ALL=(ALL) NOPASSWD:ALL"]
    shell: /bin/bash
{password_fragment}
{ssh_fragment}
disable_root: true
timezone: "Europe/Moscow"
package_update: false
manage_etc_hosts: localhost
fqdn: "{hostname}"
datasource:
  Ec2:
    strict_id: false
    timeout: 5
    max_wait: 5
    metadata_urls:
      - http://169.254.169.254:80
"""

    # Возвращаем данные для сервера метадаты
    return {
        'user_data': cloud_config,
        'hostname': hostname,
        'instance-id': vm.short_id
    }
```

7.5. Подготовка сервера с Veeam Backup & Replication для работы с РУСТЭК-ЕСУ

Перед настройкой Veeam Backup & Replication необходимо подготовить хранилище для резервных копий.

1. Разверните базовую ОС Windows согласно техническим требованиям продукта Veeam.
2. Установите Veeam Backup & Replication 11 *(с другими версиями РУСТЭК-ЕСУ не работает).*
3. Настройте взаимодействие Veeam Backup & Replication и VMware vSphere.
4. Настройте ScaleOut Repository.
5. Установите и настройте OpenSSH внутри OS Windows.
6. Настройте Veeam Backup & Replication-раннер в панели управления РУСТЭК-ЕСУ.

Пункты 1–3 выполнить согласно официальной документации:

https://helpcenter.veeam.com/docs/backup/vsphere/distributed.html?ver=110

Пункт 4 выполнить согласно документации:

https://helpcenter.veeam.com/docs/backup/vsphere/backup_repository_sobr.html?ver=110

РУСТЭК-ЕСУ взаимодействует с Veeam Backup & Replication отправкой команд через PowerShell. Для этого на сервере, где доступна оснастка Veeam Backup & Replication, должен быть установлен SSH-сервер.

Порядок настройки SSH-сервера:

- Скачайте OpenSSH-Win64.zip по ссылке https://github.com/PowerShell/Win32-OpenSSH/releases
- Разархивируйте в C:\Program Files\OpenSSH-Win64.
- Перейдите в панель управления **System** → **Advanced System Settings** → **Advanced** → **Environmental Variables** (Рисунок 125):

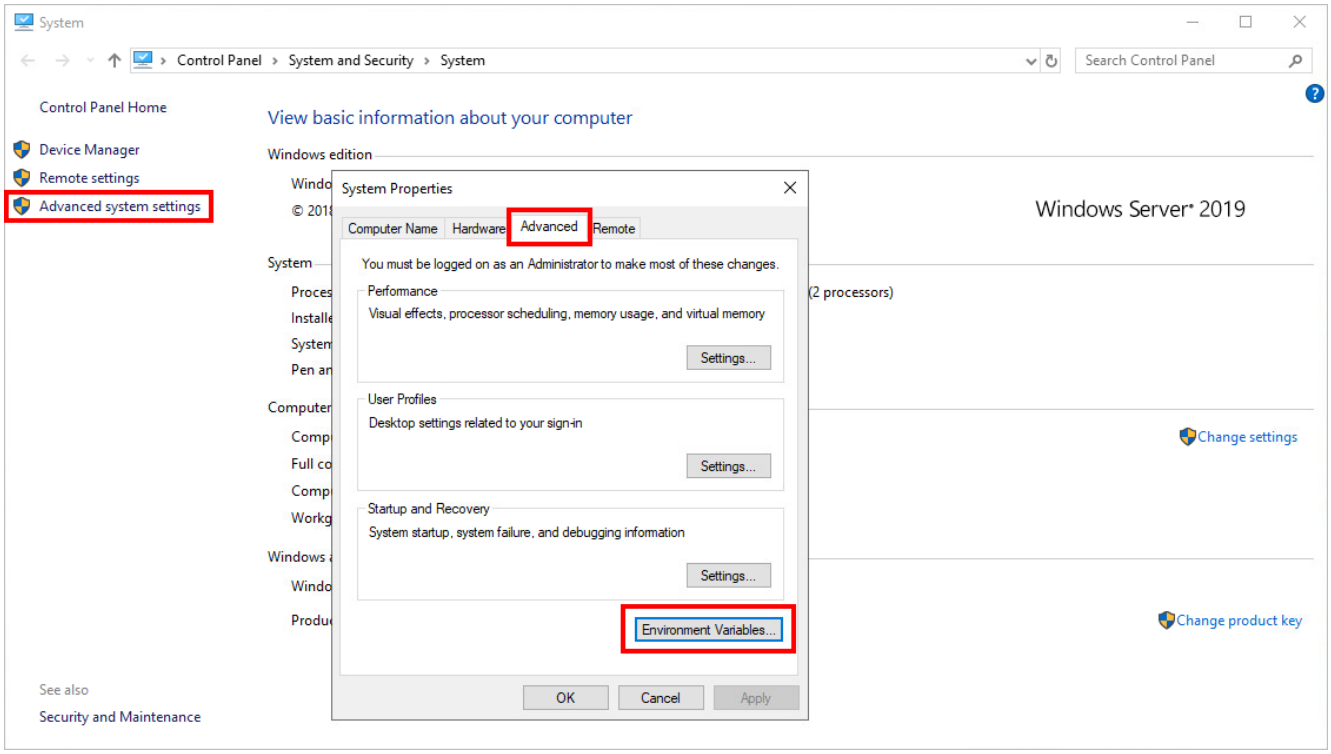

Рисунок 125

- В **System variables** (второй блок) выберите **Path**, нажмите **Edit** (Рисунок 126):

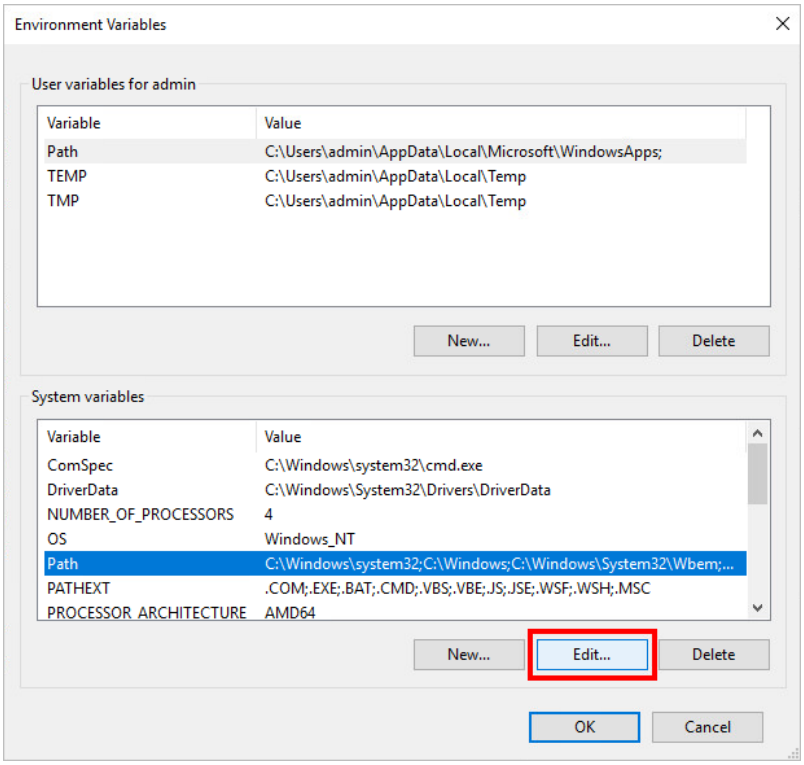

Рисунок 126

- Добавьте путь C:\Program Files\OpenSSH-Win64 (Рисунок 127):

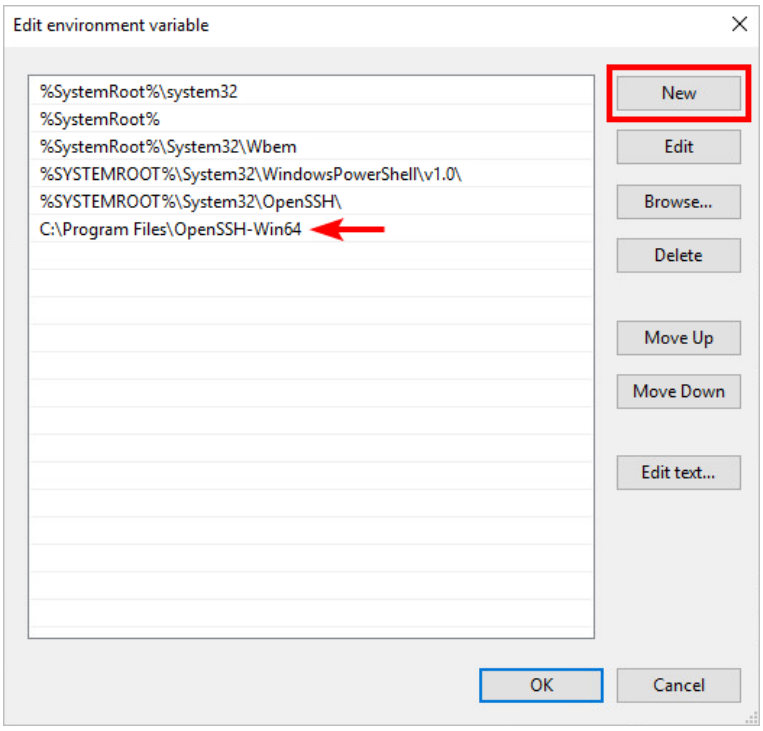

Рисунок 127

- Запустите PowerShell как администратор (Рисунок 128):

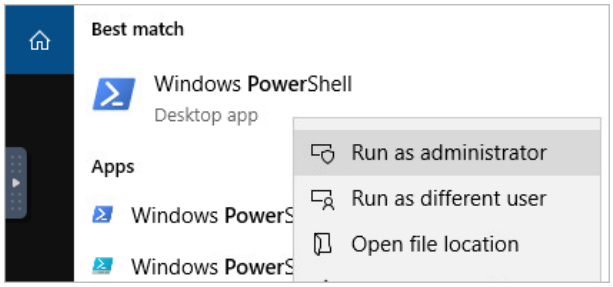

Рисунок 128

- Перейдите в директорию C:\Program Files\OpenSSH-Win64.
- Запустите команду:

```
powershell.exe -ExecutionPolicy Bypass -File install-sshd.ps1
```

Если надпись «`sshd and ssh-agent services successfully installed`» появилась — всё верно (Рисунок 129):

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd 'C:\Program Files\OpenSSH-Win64'
PS C:\Program Files\OpenSSH-Win64> powershell.exe -ExecutionPolicy Bypass -File install-sshd.ps1
  [*] C:\Program Files\OpenSSH-Win64\moduli
      looks good

  [*] C:\ProgramData\ssh
      looks good

[SC] SetServiceObjectSecurity SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
[SC] ChangeServiceConfig2 SUCCESS
sshd and ssh-agent services successfully installed
```

Рисунок 129

- Создайте правило брандмауэра, пропускающее входящие подключения на 22-й порт (Рисунок 130):

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True
-Direction Inbound -Protocol TCP -Action Allow -LocalPort 22
```

```
PS C:\Program Files\OpenSSH-Win64> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Di
rection Inbound -Protocol TCP -Action Allow -LocalPort 22


Name                  : sshd
DisplayName           : OpenSSH Server (sshd)
Description           :
DisplayGroup          :
Group                 :
Enabled               : True
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the store. (65536)
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local
```

Рисунок 130

- Запустите `sshd` (SSH Server) с помощью команды (Рисунок 131):

```
net start sshd
```

Рисунок 131

Автоматически будут сгенерированы ключи для хоста в директории C:\ProgramData\ssh, если их ещё нет.

- Настройте автозапуск для сервисов sshd и ssh-agent (Authentication Agent) и включите ssh-agent (Рисунок 132):

```
Set-Service sshd -StartupType Automatic
Set-Service ssh-agent -StartupType Automatic
Start-Service ssh-agent
```

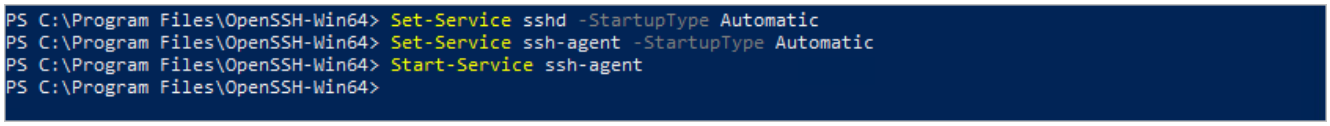

Рисунок 132

Если сервис не включается, выполните `.\FixHostFilePermissions.ps1` в директории с проектом.

- С ВМ ESU-box подключитесь по SSH к серверу с Veeam Backup & Replication и проверьте доступность PowerShell-плагина Veeam следующими командами (Рисунок 133):

```
powershell
Add-PSSnapin VeeamPSSnapin
Get-PSSnapin VeeamPSSnapin
```

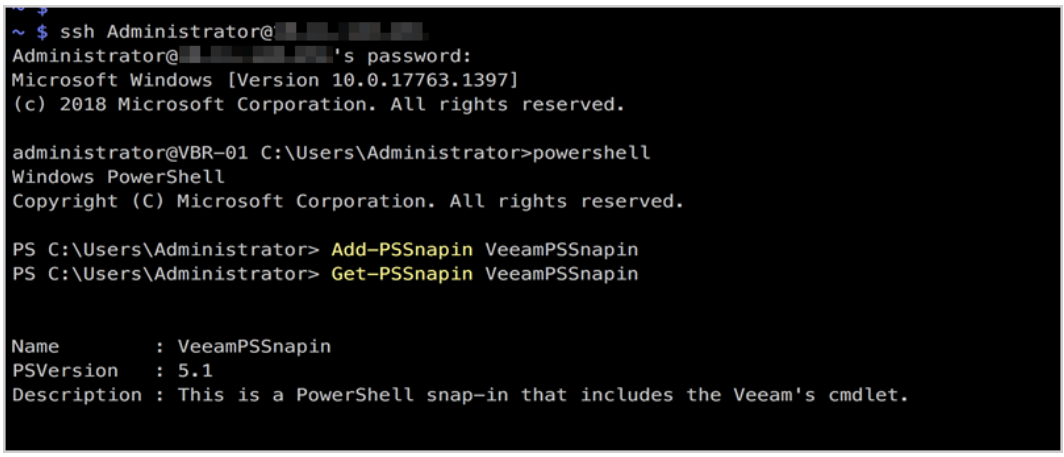

Рисунок 133

- Посмотрите, как называются обычные и ScaleOut репозитории, для этого выполните команду:

```
GET-VBRBackupRepository -ScaleOut
```

В выводе команды должен отобразиться настроенный репозиторий (Рисунок 134).

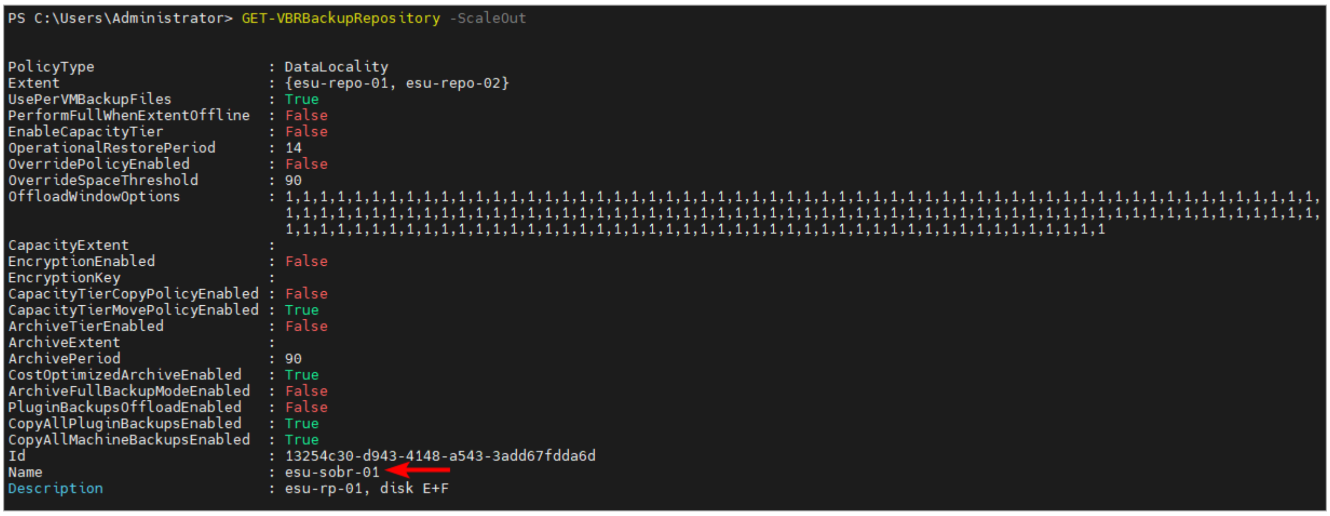

Рисунок 134

Теперь можно сконфигурировать раннер на стороне РУСТЭК-ЕСУ. Необходимо указать IP-адрес хоста, логин и пароль администратора сервера, имя ScaleOut backup репозитория и тайм-зону (Рисунок 135):

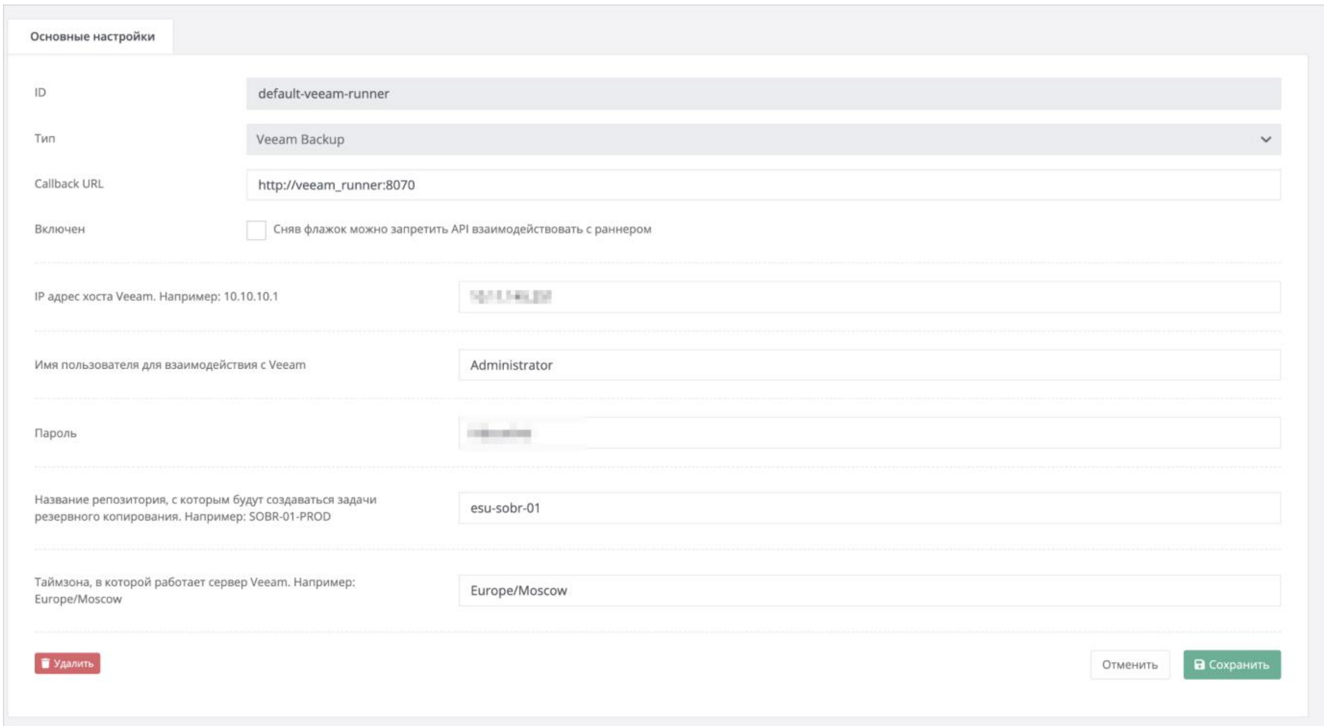

Рисунок 135

7.6. Подключение S3-хранилища к РУСТЭК-ЕСУ

РУСТЭК-ЕСУ поддерживает интеграцию с хранилищами S3 на базе сервисов MinIO Storage и NetApp StorageGRID.

7.6.1. Подключение сервиса MinIO Storage

Для подключения сервиса MinIO Storage к РУСТЭК-ЕСУ выполните настройку соответствующего S3 раннера.

Для этого перейдите в раздел меню **Инсталляция** → **Система** → **Раннеры**, найдите **s3-minio-runner** и нажмите на его ID или на кнопку **Изменить**.

В открывшейся форме введите информацию в соответствующие поля (Рисунок 136):

- **Адрес API MinIO** — указать адрес, по которому доступно API MinIO Storage. По этому адресу раннер обращается к API MinIO.
- **Имя пользователя-администратора** — указать логин администратора MinIO Storage.
- **Пароль пользователя-администратора** — указать пароль администратора MinIO Storage.
- **URL к хранилищу S3** — указать URL, по которому S3 хранилище будет доступно пользователям.

API URL хранилища S3 должен быть доступен с ВМ ESU-box.

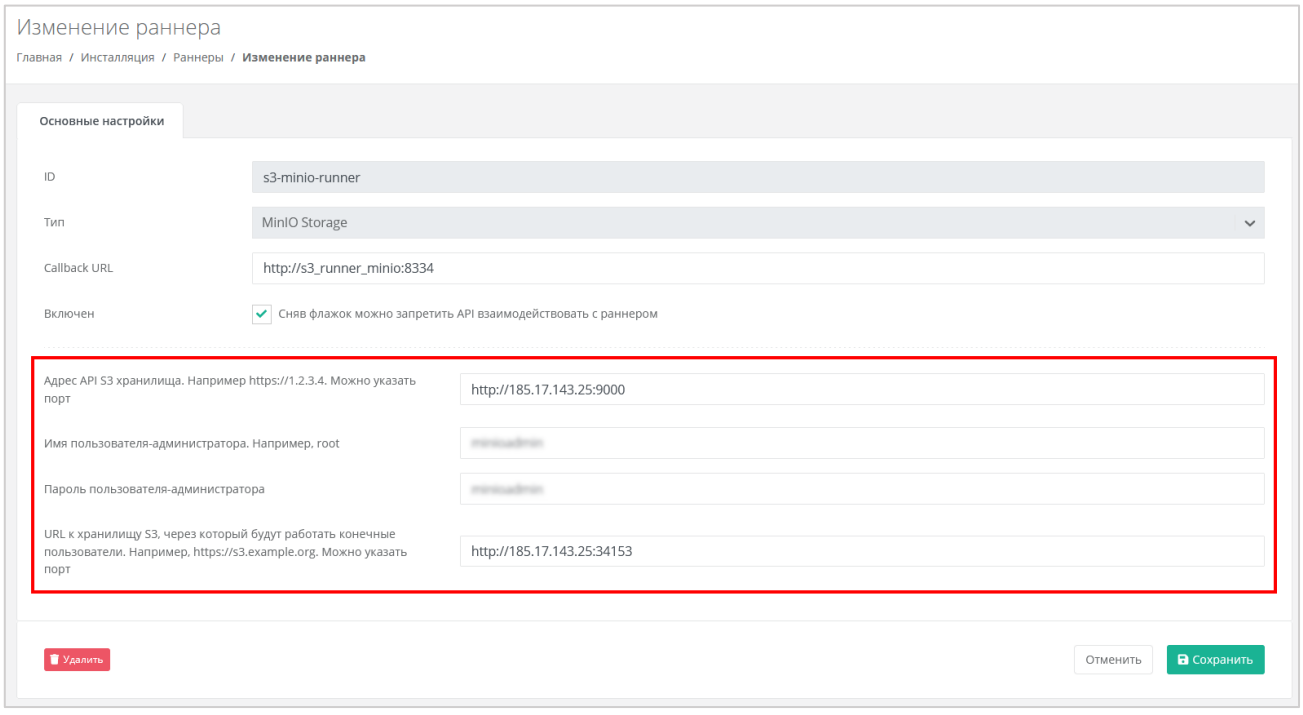

Рисунок 136

После сохранения изменений индикатор S3-раннера должен стать зелёным. После перезагрузки страницы в вертикальном меню слева появится пункт **Хранилища S3**.

⚠ Создать хранилище MinIO (аккаунт хранилища) и бакет необходимо из панели управления или API РУСТЭК-ЕСУ, дальнейшие операции с папками и файлами возможны через сторонние приложения или через API РУСТЭК-ЕСУ.

7.6.2. Подключение сервиса NetApp StorageGRID

Для подключения сервиса NetApp StorageGRID к РУСТЭК-ЕСУ выполните настройку соответствующего S3 раннера.

Для этого перейдите в раздел меню **Инсталляция** → **Система** → **Раннеры**, найдите **s3-runner** и нажмите на его ID или на кнопку **Изменить**.

В открывшейся форме введите информацию в соответствующие поля (Рисунок 137):

- **Адрес API NetApp** — указать адрес, по которому доступно API NetApp StorageGRID. По этому адресу раннер обращается к API NetApp.
- **Имя пользователя-администратора** — указать логин администратора NetApp StorageGRID.
- **Пароль пользователя-администратора** — указать пароль администратора NetApp StorageGRID.
- **URL к хранилищу S3** — указать URL, по которому S3 хранилище будет доступно пользователям.

API URL хранилища S3 должен быть доступен с ESU-box.

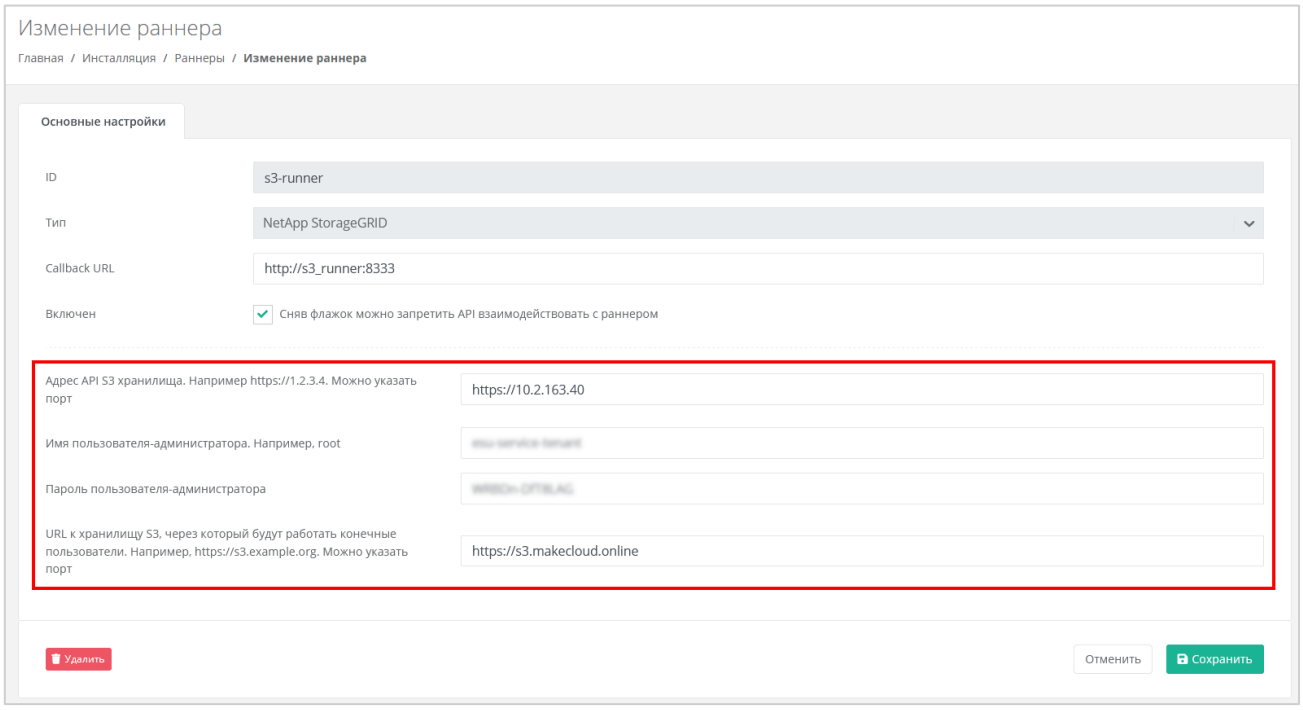

Рисунок 137

После сохранения изменений индикатор S3-раннера должен стать зелёным. После перезагрузки страницы в вертикальном меню слева появится пункт **Хранилища S3**.

7.7. Подключение ЮKassa к РУСТЭК-ЕСУ

В РУСТЭК-ЕСУ для клиентов предусмотрена возможность пополнения баланса с помощью платёжного провайдера ЮKassa. Это особенно актуально для провайдеров, которые ведут расчёты с клиентами-физическими лицами по предоплатной системе.

Для подключения к сервису ЮKassa:

1. Зарегистрируйтесь на сайте https://yookassa.ru и получите идентификатор (ID) магазина и секретный ключ, подробнее см. в официальной документации сервиса.
2. Перейдите в раздел меню **Администрирование** → **Партнёры**.
3. Нажмите на имя выбранного партнёра или на кнопку **Действия** → **Изменить**.
4. На вкладке **Основные настройки** введите полученный идентификатор магазина и секретный ключ в соответствующие поля.

При необходимости установите флаг **Разрешить автоплатежи** — в этом случае для администратора клиента с атрибутом «Владелец» будет доступно автопополнение баланса клиента.

5. Нажмите **Изменить** для сохранения настроек партнёра.
6. Далее выполните настройку HTTP-уведомлений в личном кабинете ЮKassa для отправки уведомлений о пополнении в РУСТЭК-ЕСУ (Рисунок 138).

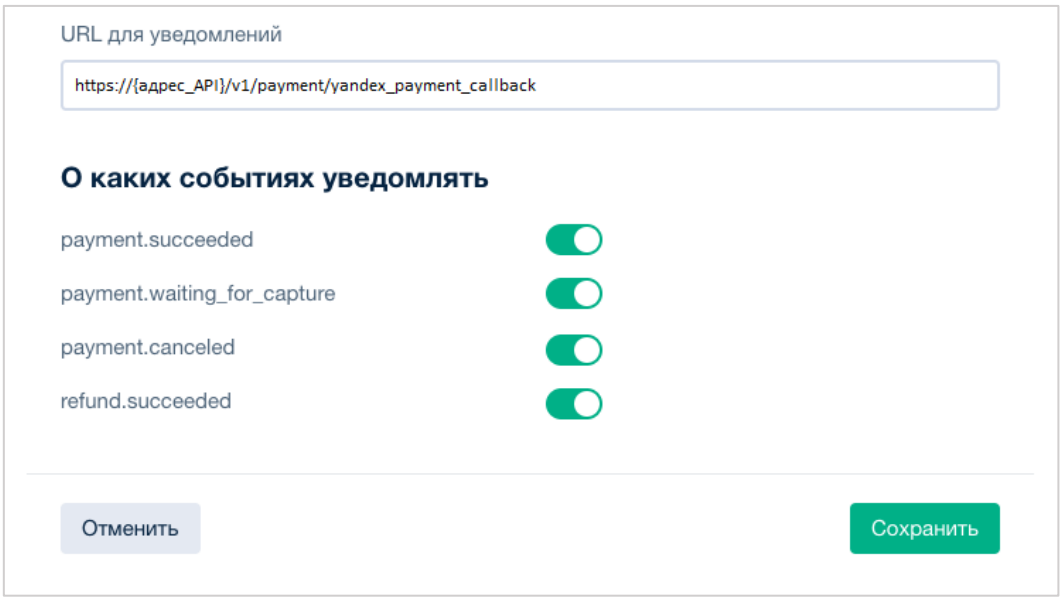

Рисунок 138

URL для уведомлений: https://{адрес_API}/v1/payment/yandex_payment_callback.

Требования к URL для уведомлений — протокол HTTPS и TCP-порт 443 или 8443. TLS/SSL-сертификат подойдет любой: самоподписанный или выданный центром сертификации. Версия TLS/SSL — 1.2 или выше. Подробнее в официальной документации.

Для проверки работы интеграции рекомендуется использовать тестовый магазин, подробнее в официальной документации.

В РУСТЭК-ЕСУ метод оплаты ЮKassa для клиента задаётся администратором партнёра при создании или изменении клиента в меню **Администрирование** → **Клиенты**. Администратор платформы также может задать метод оплаты в настройках клиентов по умолчанию при создании и редактировании партнёров.

7.8. Подключение Telegram-бота к РУСТЭК-ЕСУ для управления облачной инфраструктурой

Для администраторов клиентов (клиентских организаций) есть возможность ограниченного управления облачной инфраструктурой с помощью мессенджера Telegram. Бот Telegram поставляется в виде контейнера, запущенного на ESU-box.

Этапы настройки:

1. С помощью Telegram обратитесь к специальному боту @botfather по ссылке https://t.me/BotFather.
2. В Telegram отправьте команду **/newbot** боту @botfather.
3. Бот @botfather запросит желаемое название бота — введите название (name).
4. Бот @botfather запросит желаемое имя (username) бота — введите имя бота, оно должно быть уникальным.
5. Если имя (username) бота свободно, @botfather пришлёт сообщение, в котором содержится токен — скопируйте его.
6. Зайдите по SSH на ESU-box и выполните команду:

```
nano toochka.conf
```

В результате в консоль должны быть выведены настройки конфигурации ESU-box.

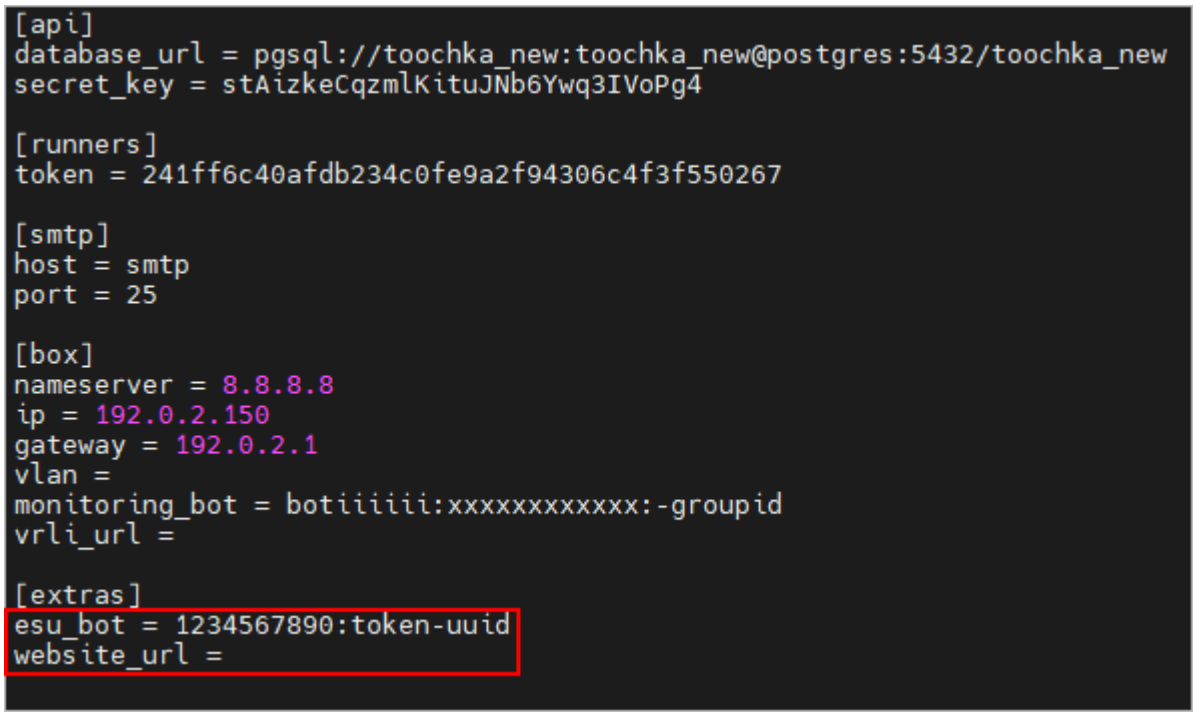

Рисунок 139

7. Измените выделенные строки (Рисунок 139) на:

```
esu_bot = токен, который прислал @botfather
website_url = адрес, по которому доступна панель управления
```

8. Сохраните изменения в конфигурационном файле `toochka.conf`. Выполните команду:

```
sudo toochkactl configure
```

В результате в консоль будет выведен процесс конфигурации.

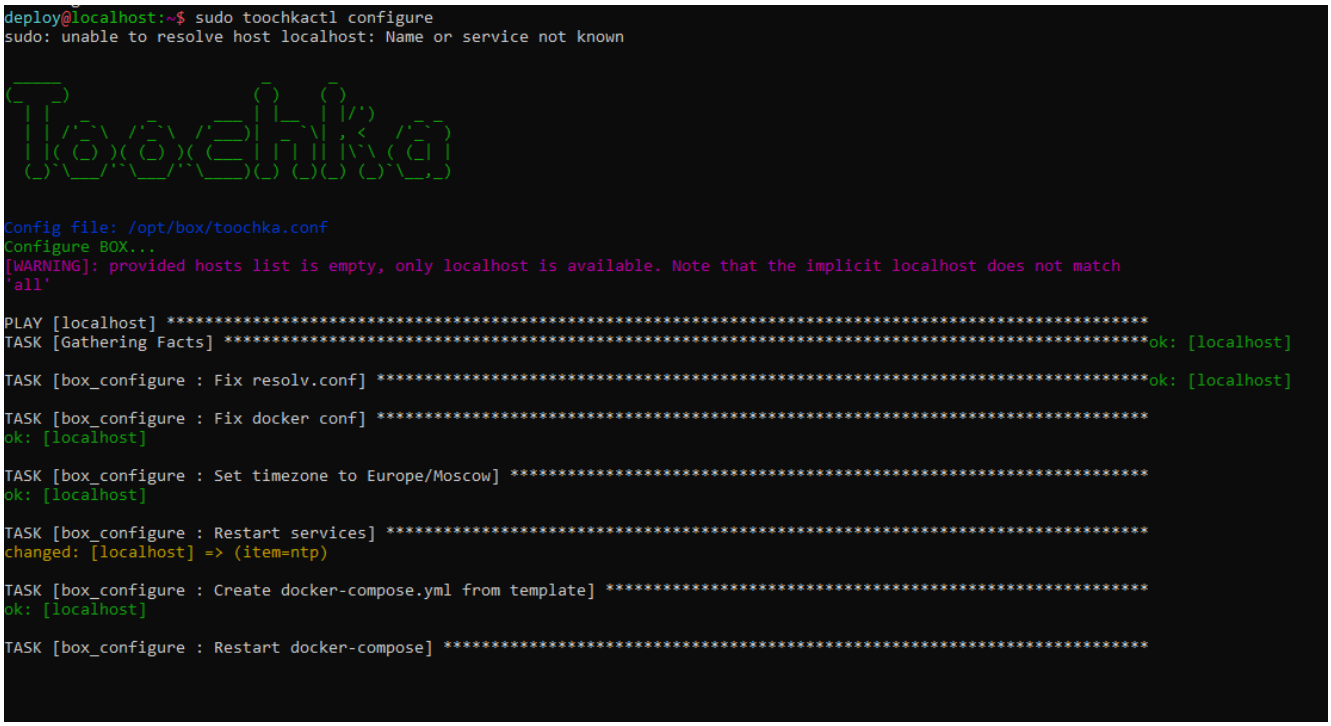

Рисунок 140

9. Отключитесь от ESU-box.
10. В панели управления РУСТЭК-ЕСУ перейдите в меню **Администрирование** → **Домены** и выберите домен, к которому будет прикреплён бот. Во вкладке **Изменение домена** найдите поле **Имя бота Telegram для управления виртуальной инфраструктурой** и введите имя (username) бота, которое вы задали на шаге 4.

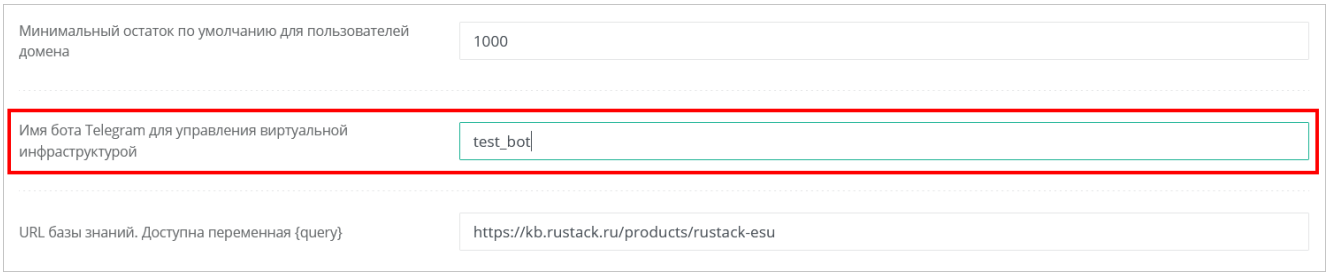

Рисунок 141

11. Нажмите кнопку **Изменить** для сохранения изменений в настройках домена.

Теперь каждый администратор и пользователь клиента сможет подключиться к боту для управления инфраструктурой, нажав соответствующую кнопку в своём профиле пользователя (Рисунок 142).

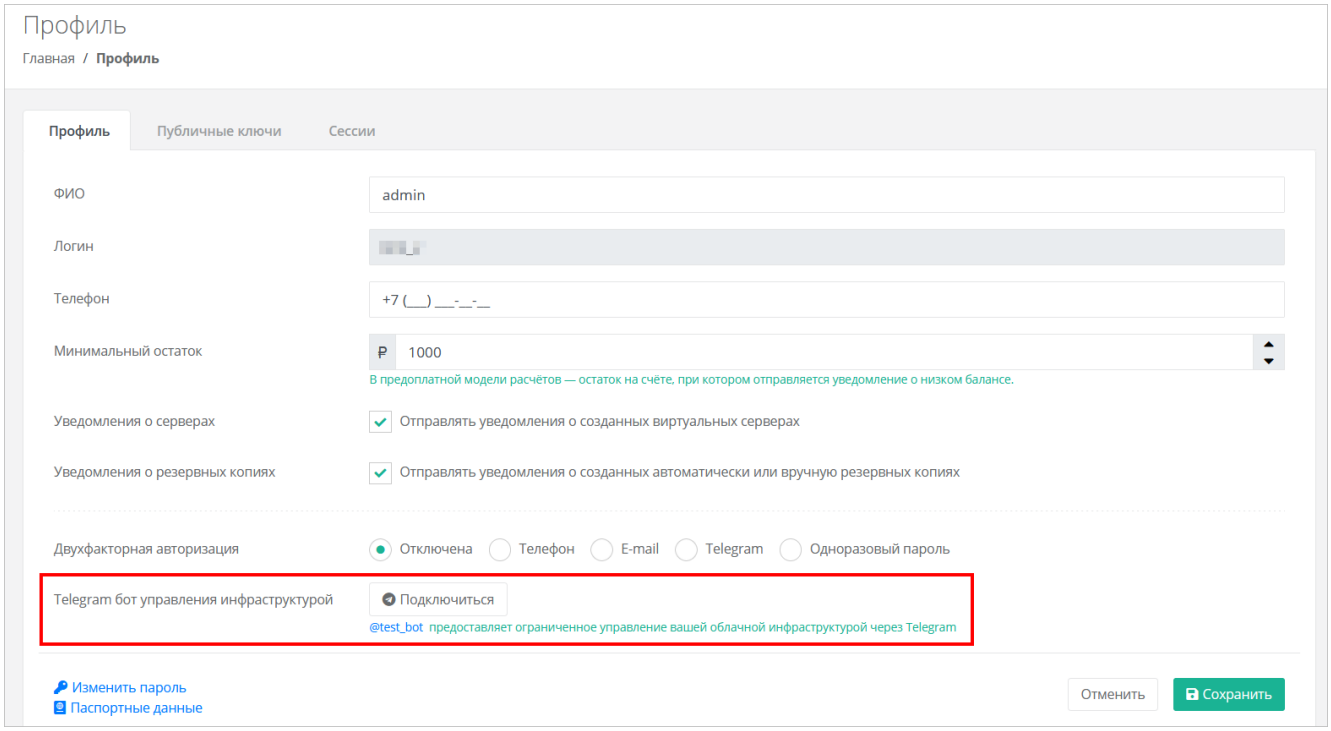

Рисунок 142

7.9. Подключение Telegram-бота к РУСТЭК-ЕСУ для двухфакторной авторизации

Для всех пользователей РУСТЭК-ЕСУ есть возможность подключения двухфакторной авторизации на портале для повышения безопасности аккаунта. РУСТЭК-ЕСУ поддерживает двухфакторную авторизацию с помощью мессенджера Telegram. Бот Telegram для авторизации поставляется в виде контейнера, запущенного на ESU-box. В РУСТЭК-ЕСУ он настраивается в панели управления, поскольку работает как раннер.

Этапы настройки:

1. С помощью Telegram обратитесь к специальному боту @botfather по ссылке https://t.me/BotFather.
2. В Telegram отправьте команду **/newbot** боту @botfather.
3. Бот @botfather запросит желаемое название бота — введите название (name).
4. Бот @botfather запросит желаемое имя (username) бота — введите имя бота, оно должно быть уникальным.
5. Если имя (username) бота свободно, @botfather пришлёт сообщение, в котором содержится токен — скопируйте его.
6. В панели управления РУСТЭК-ЕСУ перейдите в меню **Инсталляция** → **Система** → **Раннеры**. В списке раннеров найдите tg-runner и откройте его настройки.
7. В поле **Токен вида aaaa:bbbb** (Рисунок 143, 1) введите (вставьте) токен, полученный от @botfather на шаге 5.

8. В поле **Ссылка на бот вида…** (Рисунок 143, 2) введите **https://t.me/xxxx**, где **xxxx** — username бота, который вы вводили на шаге 4.

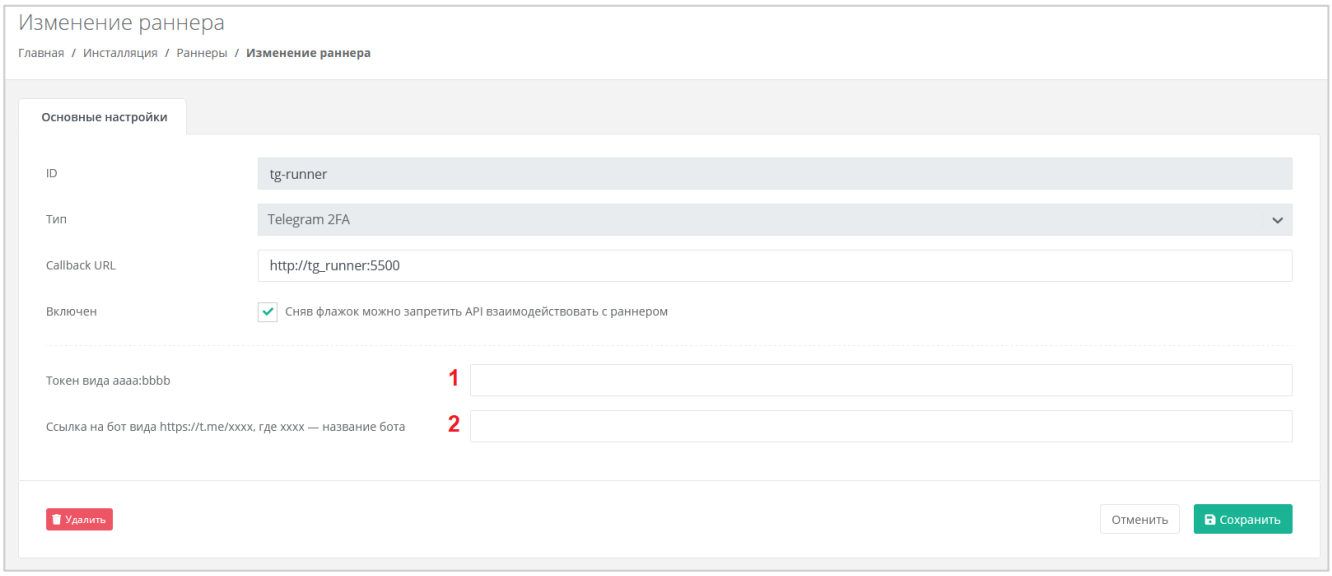

Рисунок 143

9. После заполнения указанных полей нажмите кнопку **Сохранить**. Обновите страницу, если всё настроено верно — раннер загорится зелёным.

8. Развёртывание на платформе виртуализации VMware vSphere

В инструкции описан процесс установки и настройки РУСТЭК-ЕСУ на платформе виртуализации РУСТЭК, данный способ является предпочтительным и рекомендуемым, но продуктом также поддерживается установка на платформу виртуализации VMware vSphere.

8.1. Системные требования

Для развёртывания на платформе виртуализации VMware vSphere необходимы:

- VMware vSphere (6.7, 7.0),
- vSphere Distributed Switch (vDS) и сервисная портгруппа, одна маршрутизируемая подсеть с префиксом маски /24 с доступом до сетей хостов VMware ESXi и VMware vCenter. В качестве минимального требования допускается подсеть с префиксом маски /27.

Необходимые работы на стороне VMware для подключения к РУСТЭК-ЕСУ:

1. Создать пользователя esu-admin с правами администратора.
2. Создать Datacenter.
3. Создать кластер хоста(ов) в Datacenter, внутри которого будут создаваться ВМ и Edge-роутеры.
4. Создать Datastore Cluster из датастора(ов), на котором будут размещаться пользовательские Edge-роутеры и служебные сервисы.
5. Создать Datastore Cluster из датастора(ов), на котором будут размещаться диски пользователей (можно использовать из пункта **4**).
6. Создать vDS, под которым будут создаваться пользовательские сети (порт-группы).

8.2. Порядок развёртывания

1. Создайте маршрутизируемую сеть РУСТЭК-ЕСУ — портгруппу на vDS в vSphere (требуется один VLAN ID). Необходимо учитывать, что в эту сеть будут подключены пользовательские роутеры для сегмента VMware. Таким образом, размер подсети напрямую влияет на максимальное число ВЦОД. ВМ с установленной РУСТЭК-ЕСУ (ESU-box) станет DHCP-сервером в этой подсети.

Этапы создания портгруппы показаны на рисунках ниже. В данном примере она называется ESU_management_vlan3235, VLAN ID 3235.

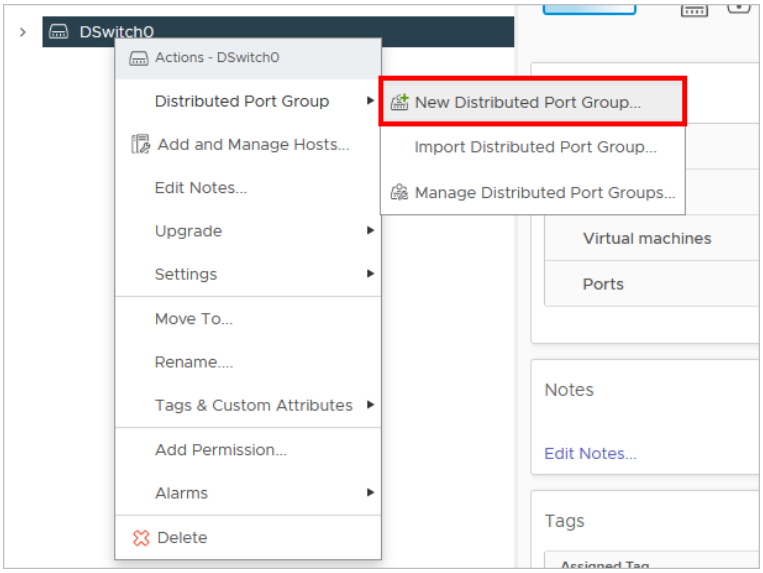

Рисунок 144

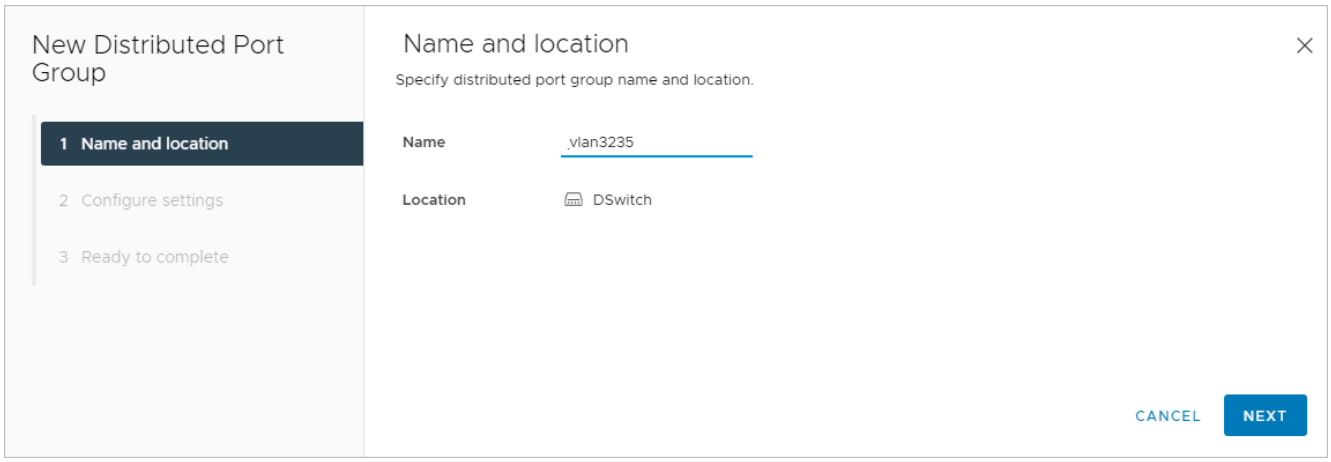

Рисунок 145

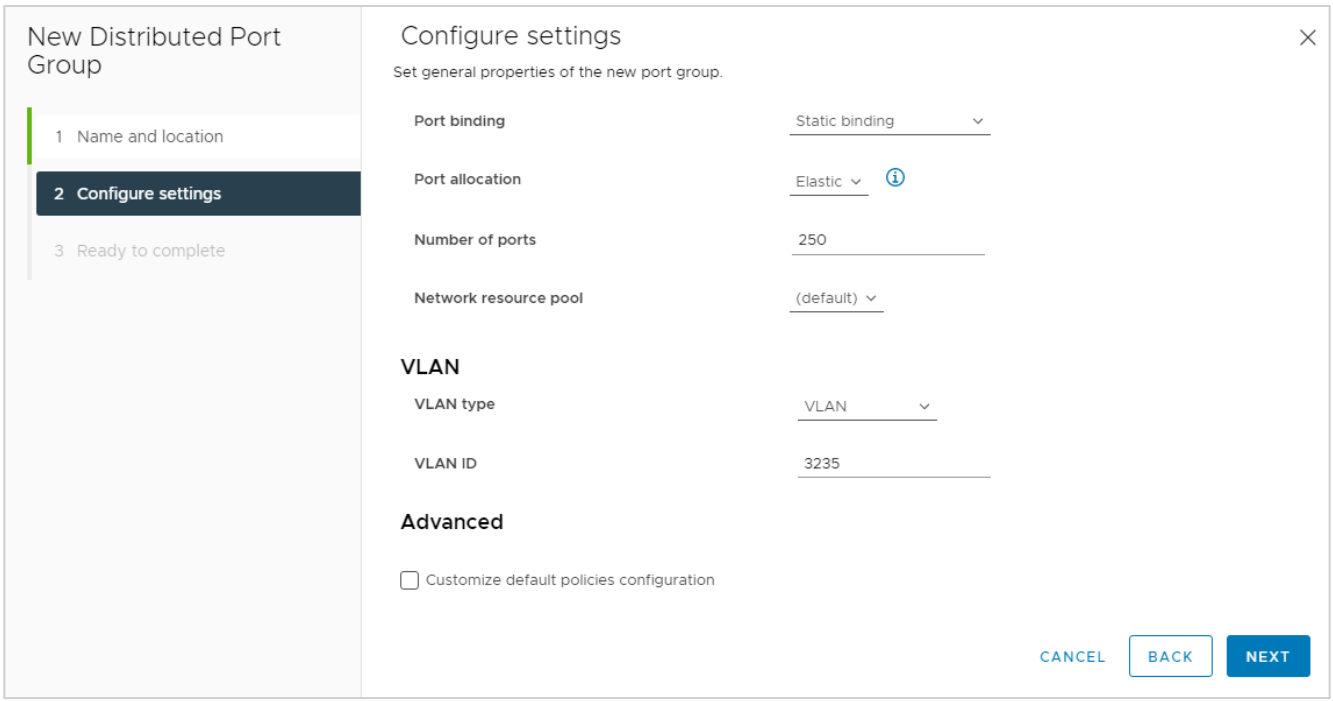

Рисунок 146

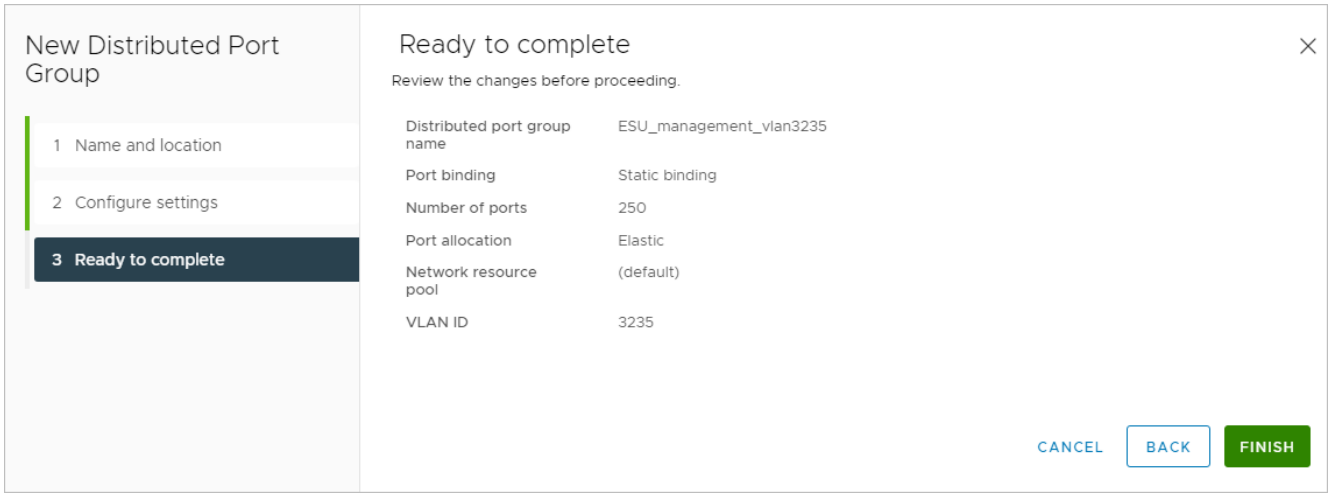

Рисунок 147

2. Перейдите в редактирование созданной портгруппы и удостоверьтесь, что параметры установлены в соответствии с указанными ниже (Рисунок 148 – Рисунок 149).

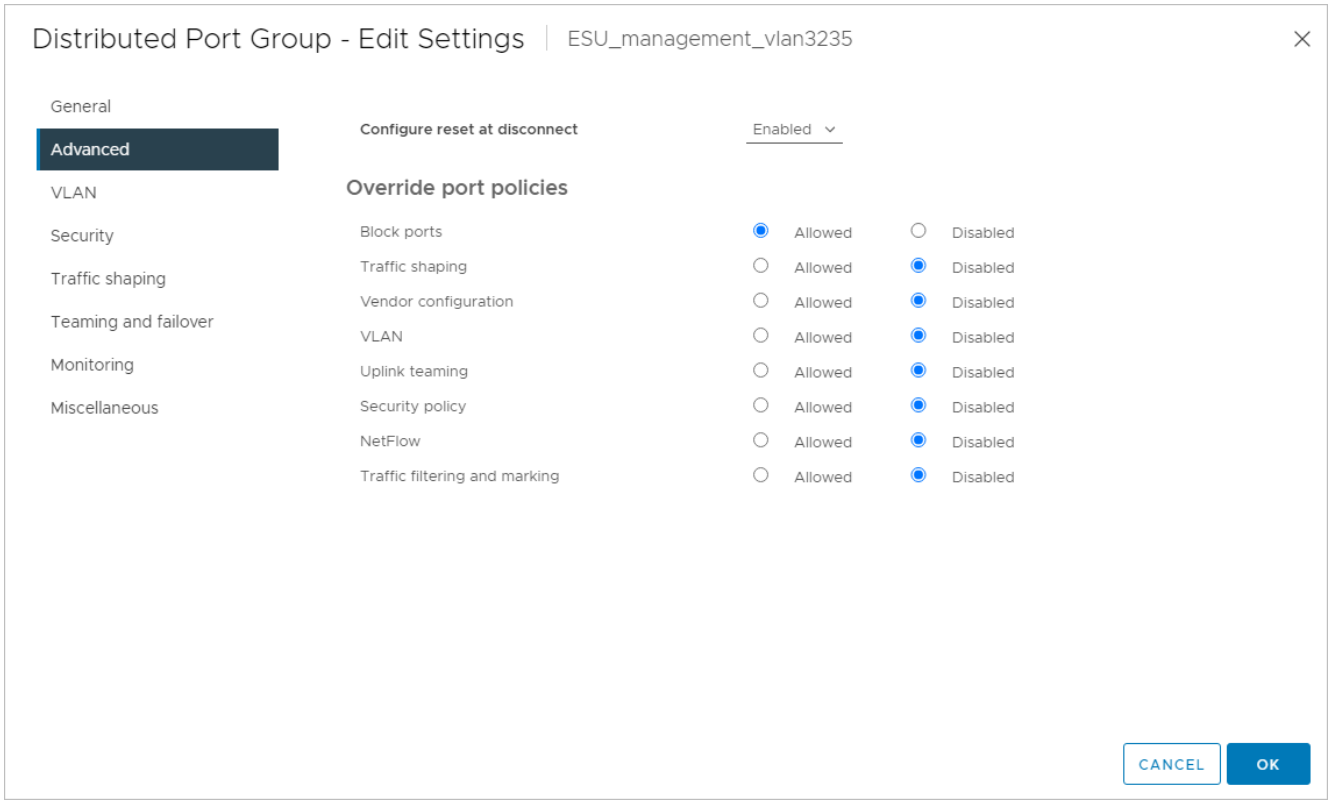

Рисунок 148

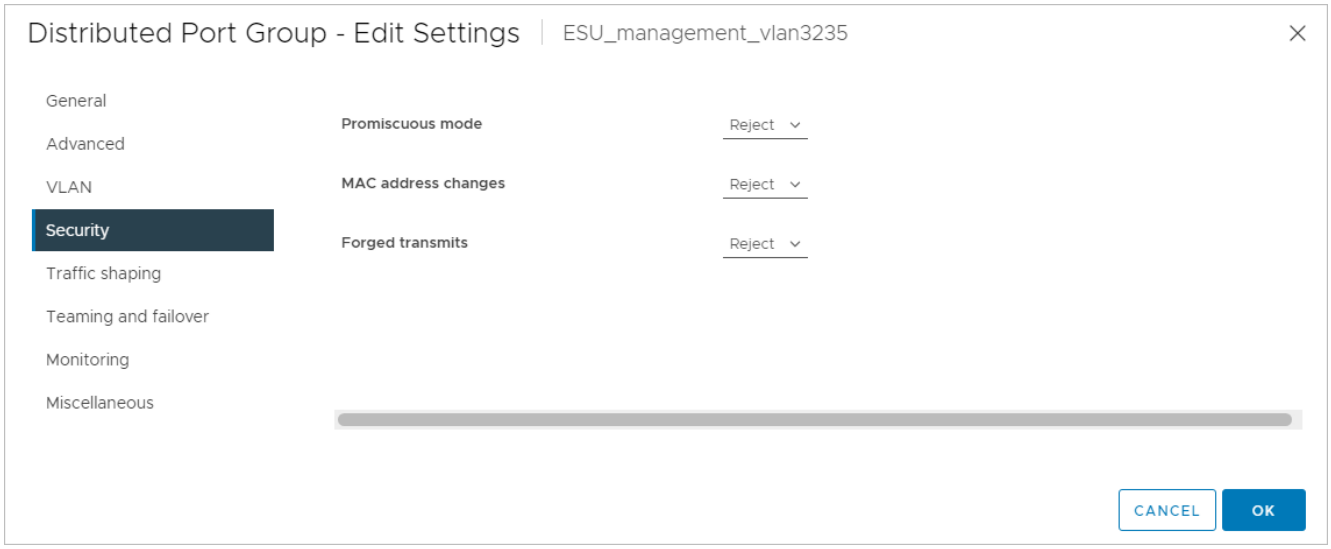

Рисунок 149

3. Создайте директорию, в которой будут расположены ВЦОДы клиентов и сама ВМ с РУСТЭК-ЕСУ (ESU-box), например, ESU3. Создайте в ней папку Management (Рисунок 150 – Рисунок 153):

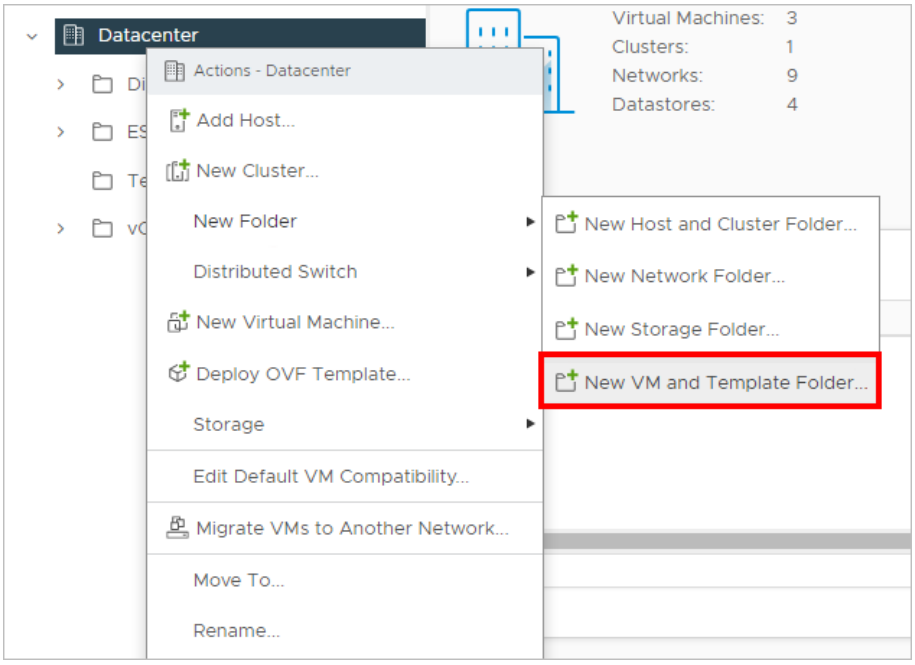

Рисунок 150

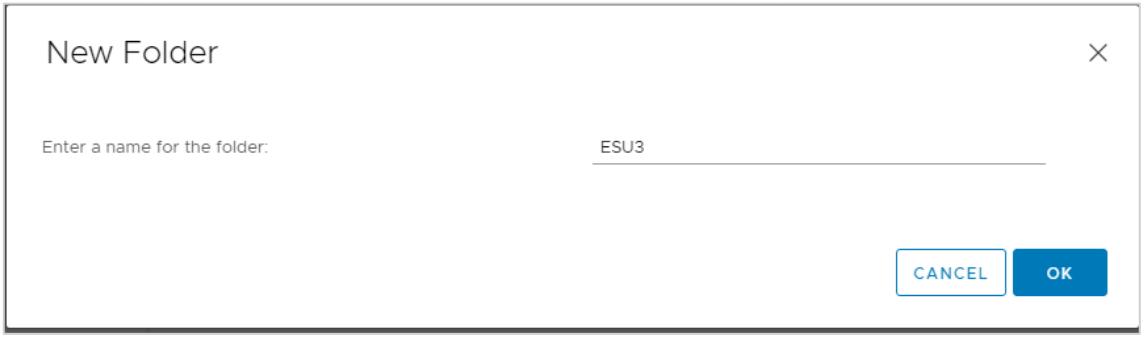

Рисунок 151

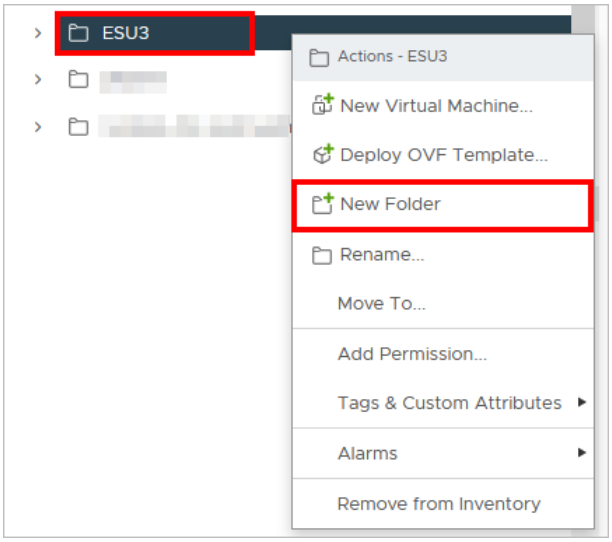

Рисунок 152

Рисунок 153

4. Загрузите предоставленный образ ВМ с РУСТЭК-ЕСУ в vSphere. Для этого выберите папку Management, нажмите на ней правой кнопкой мыши и выберите **Deploy OVF Template** (Рисунок 154).

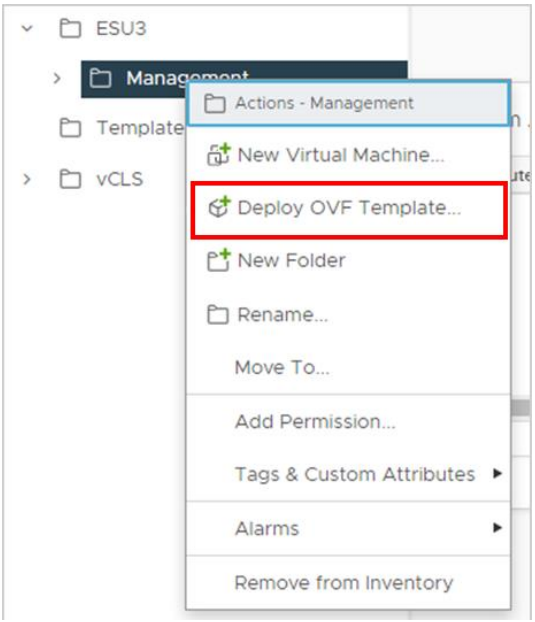

Рисунок 154

Выберите предоставленный .ova-образ (Рисунок 155).

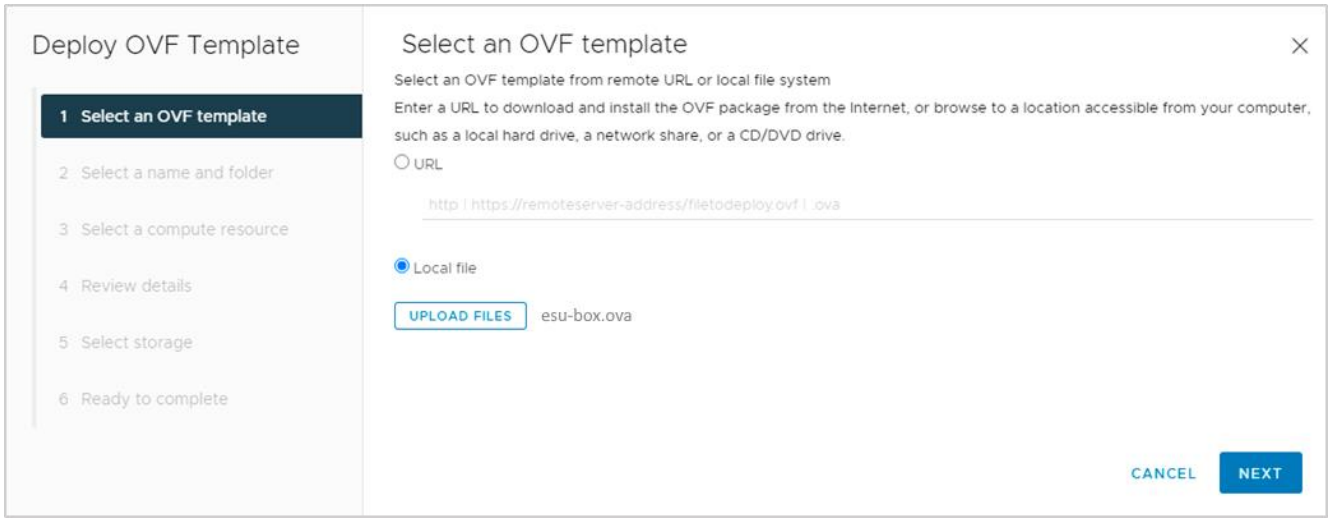

Рисунок 155

Выберите созданную папку Management, где будет развёрнута ВМ (Рисунок 156).

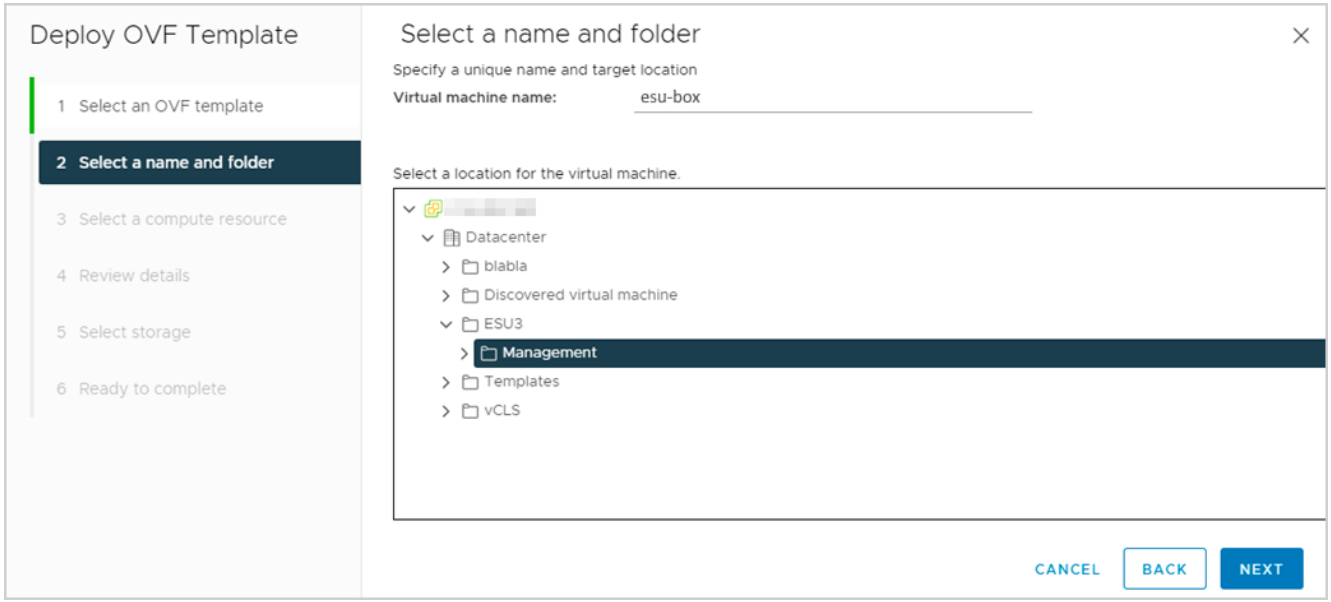

Рисунок 156

Выберите кластер, где будет развёрнута ВМ (Рисунок 157).

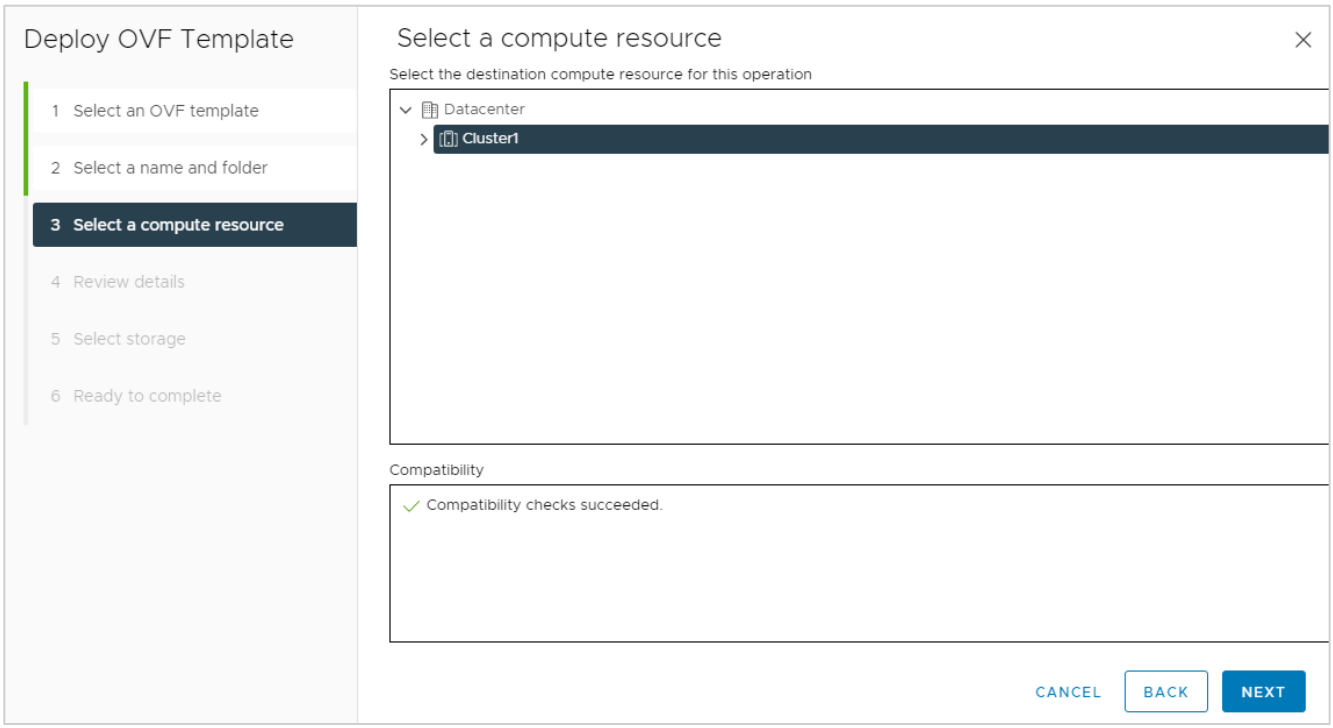

Рисунок 157

Подтвердите дальнейшие действия (Рисунок 158).

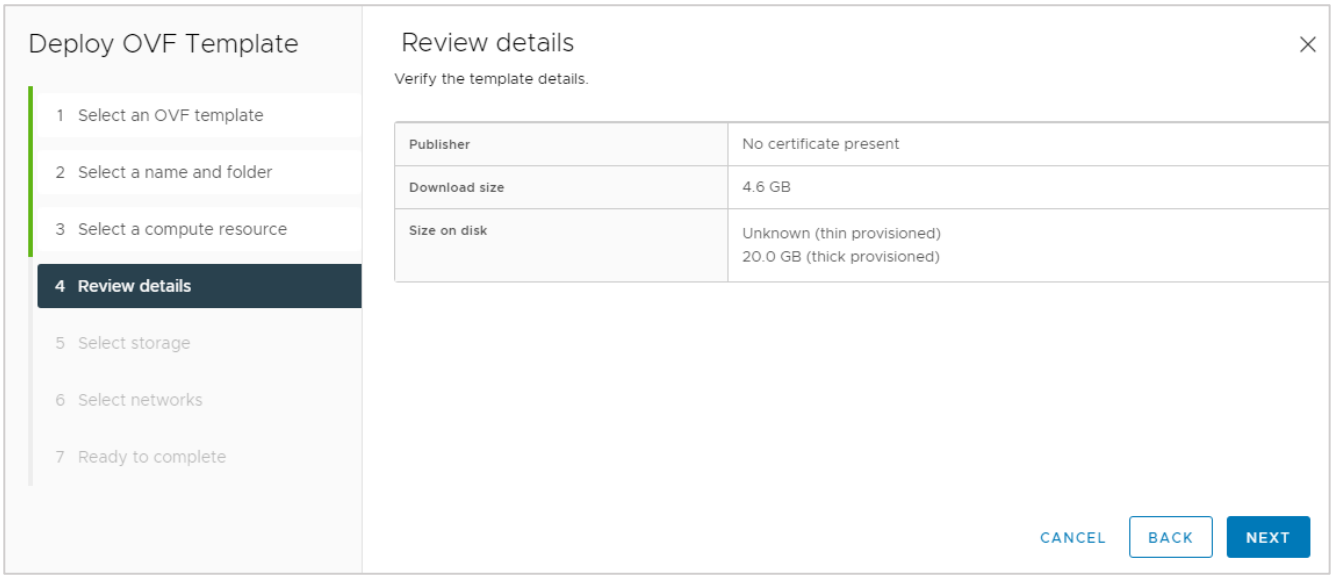

Рисунок 158

Выберите формат диска Thin Provision и датастор для диска сервера (Рисунок 159).

Thin Provision должен быть выбран обязательно!

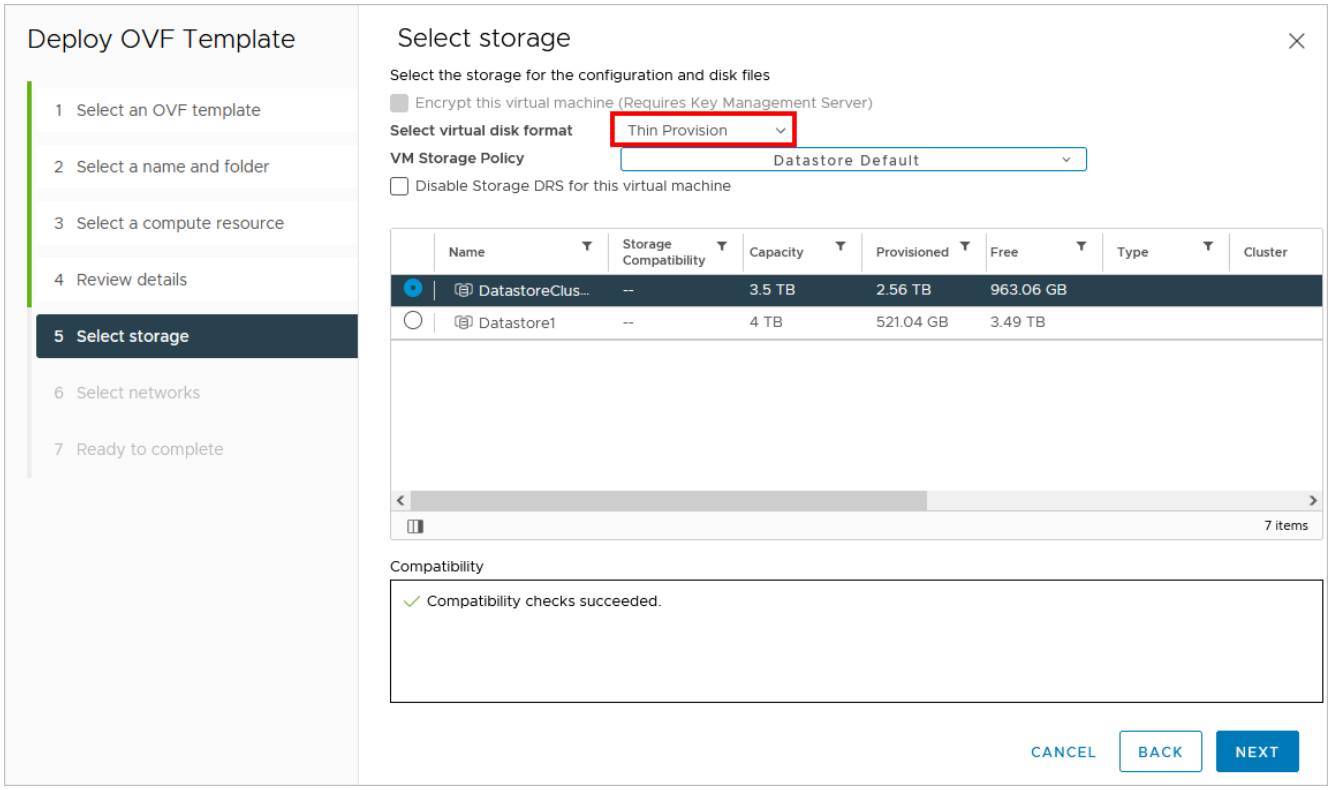

Рисунок 159

Выберите сеть, которая будет подключена к создаваемой ВМ. Выберите созданную ранее в vDS портгруппу, в следующем окне нажмите **FINISH** (Рисунок 160, Рисунок 161).

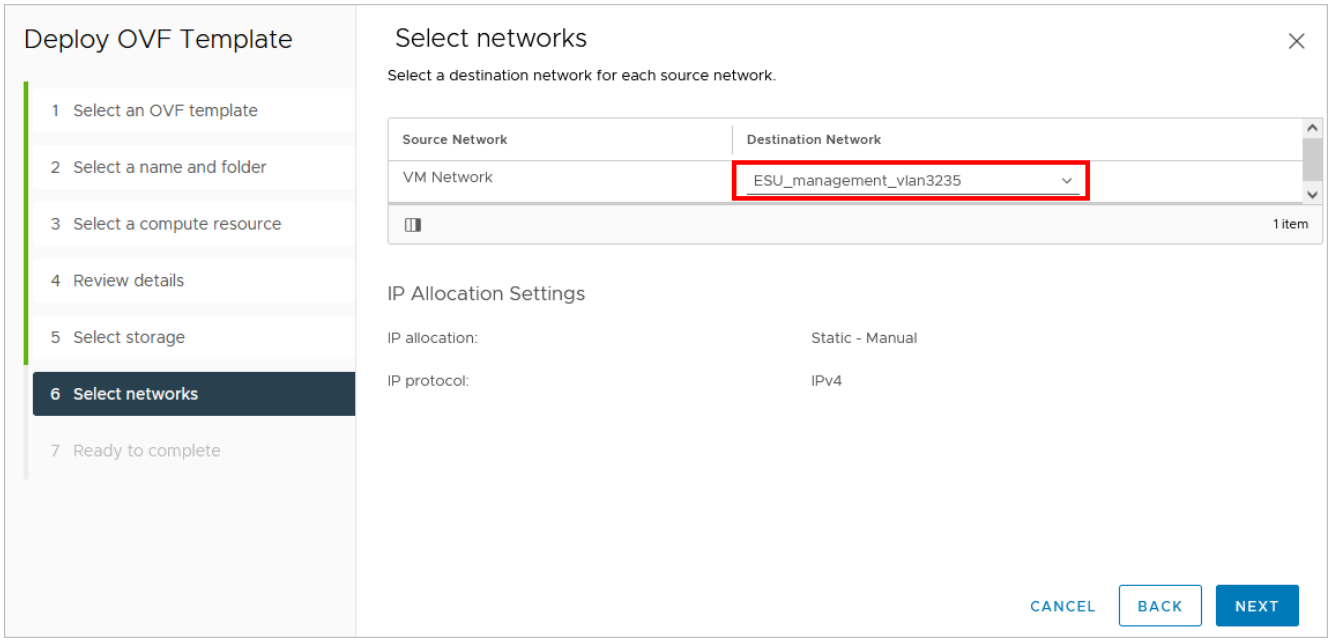

Рисунок 160

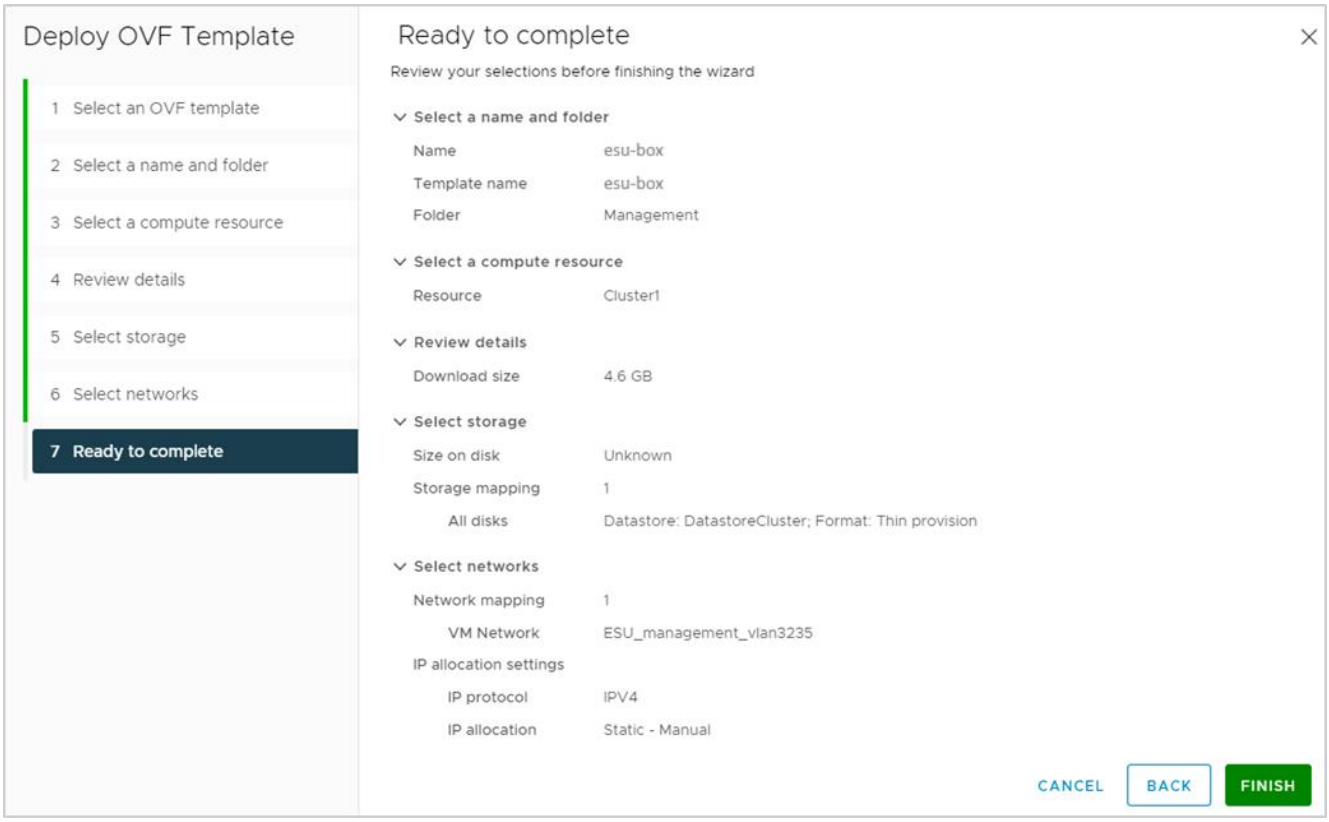

Рисунок 161

Начнётся процесс развёртывания (Рисунок 162).

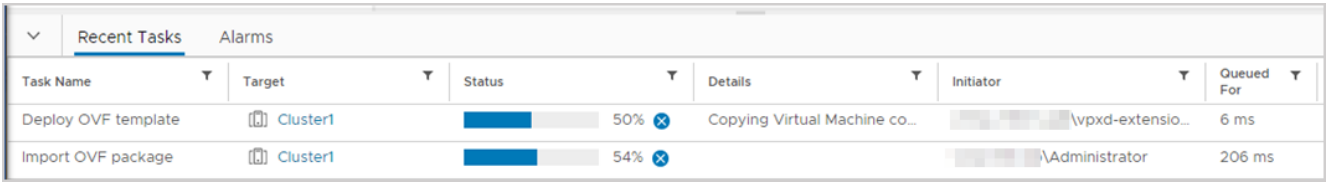

Рисунок 162

5. После развёртывания включите ВМ и откройте консоль (Рисунок 163).

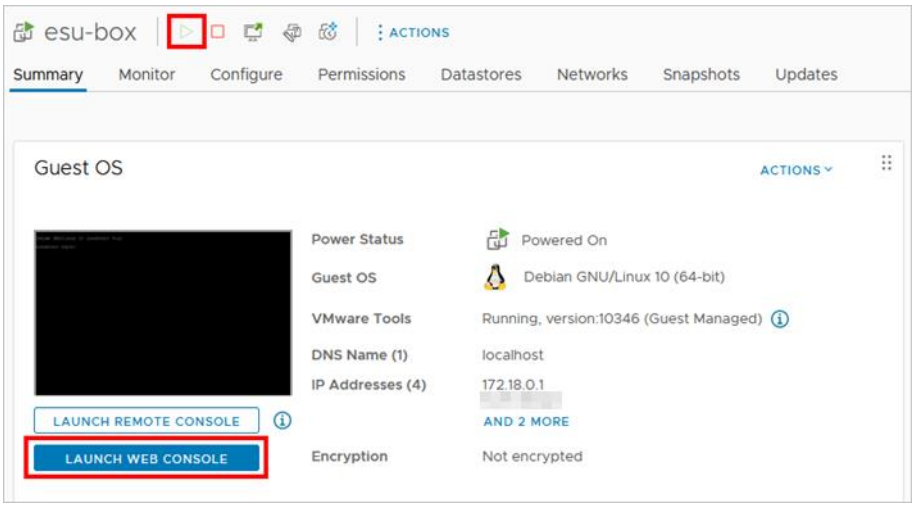

Рисунок 163

Стандартная учётная запись на ВМ с РУСТЭК-ЕСУ:
логин — **deploy**, пароль — **1-qpALzm/**.

8.3. Примечания по установке и дальнейшей настройке

- Процесс установки аналогичен установке на платформе виртуализации РУСТЭК (см. раздел 3). Но на этапе выбора IP-адреса необходимо выбрать адрес внутри заведённой в vDS портгруппы. Адрес должен быть выделен заранее (см. Рисунок 16).
- Панель управления РУСТЭК-ЕСУ будет доступна по адресу, указанному при установке.
- Сервер с РУСТЭК-ЕСУ (ESU-box) будет доступен по SSH по адресу, указанному при установке.
- До настройки ресурсного пула РУСТЭК в панели управления РУСТЭК-ЕСУ необходимо завести внешнюю сеть и подсеть для неё в платформе виртуализации РУСТЭК. Процесс создания внешней сети и подсети описан в пунктах 5–6 раздела 2.2.
- Для создания кластеров Kubernetes в сегменте РУСТЭК (см. раздел 6.2) в панели РУСТЭК необходимо завести сеть аналогичную портгруппе в vDS. Далее процесс настройки одинаков для обоих случаев. Процесс создания сети и подсети в РУСТЭК описан в пунктах 5–6 раздела 2.2. Безопасность портов и DHCP должны быть отключены.

Остальные настройки производятся аналогично ситуации, когда РУСТЭК-ЕСУ развёрнута на платформе виртуализации РУСТЭК.

9. Обновление РУСТЭК-ЕСУ

Чтобы обновить РУСТЭК-ЕСУ, доставьте пакет обновления на виртуальную машину с РУСТЭК-ЕСУ (ESU-box).

Если у ESU-box есть доступ к сети Интернет:

1. С помощью SSH подключитесь к ESU-box.

2. Скачайте архив с обновлением с помощью команды:

```
curl -O -u SHARE_ID:SHARE_PASSWORD https://file.rustack.ru/public.php/webdav/esu-update.tar.xz
```

Здесь `SHARE_ID` — идентификатор ссылки `https://file.rustack.ru/s/`**`SHARE_ID`**, `SHARE_PASSWORD` — пароль для доступа к скачиванию.

3. Распакуйте архив:

```
tar -xvf esu-update.tar.xz
```

Будут распакованы два файла — `toochka_ctl-3.5.0-py3-none-any.whl` и `esu-3-5-0-upgrade.esu`.

4. Выполните команду:

```
sudo pip install -U toochka*.whl
```

При успешном выполнении команды в консоли должно отобразиться сообщение `Successfully installed toochka-ctl-3.5.0`.

5. Запустите процесс обновления с помощью команды:

```
sudo toochkactl upgrade --filename esu-3-5-0-upgrade
```

6. Через некоторое время откроется окно мастера обновления, в котором нужно подтвердить установку обновлений.

7. Дождитесь завершения процесса обновления. Выберите **Continue**.

Если у ESU-box нет доступа к сети Интернет:

1. Скачайте архив с обновлением на сервер или компьютер, который имеет доступ к сети Интернет и ESU-box, подключенному к локальной сети (см. шаг 2 из инструкции выше).

2. Перенесите архив на ESU-box:

```
scp esu-update.tar.xz deploy@<ip_ESU-box>:/opt/box
```

Потребуется ввести пароль от ESU-box. Перемещение файла займёт некоторое время.

3. С сервера, на который было скачано обновление, с помощью SSH подключитесь к ESU-box.

4. Проверьте наличие архива с помощью команды `ls`.

Дальнейшие действия по установке обновления аналогичны шагам 3–7 из инструкции выше.

Приложение 1. Пример Auto DevOps-скрипта

Скрипт для включения правила брандмауэра «Разрешить WEB» для портов сервера.

```
from vdc.models import FirewallTemplate, FirewallRule
from rest_framework import serializers


def check(vm):
    if not vm.floating:
        raise serializers.ValidationError('Для правильного запуска необходимо
назначить публичный IP для этого сервера')


def on_start(vm):
    # Force to enable "Allow Web" rule
    allow_web_rule = FirewallTemplate.objects.get_or_none(name='Разрешить WEB',
vdc=None)
    if allow_web_rule and vm.floating:
        for port in vm.ports.filter(type='vm_int'):
            port.fw_templates.add(allow_web_rule)
```