



РУСТЭК-ЕСУ

Руководство по установке и настройке РУСТЭК-ЕСУ

Версия 3.4.4

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 РУСТЭК-ЕСУ	19
5. Настройка сегментов	22
5.1. Настройка сегмента РУСТЭК/KVM	22
5.1.1. Настройка сетевых зон для KVM сегмента.....	22
5.1.2. Настройка Openstack-раннера.....	24
5.1.3. Настройка ресурсного пула для KVM-сегмента	26
5.1.4. Создание шаблонов VM для сегмента РУСТЭК/KVM	29
5.2. Настройка сегмента VMware vSphere.....	33
5.2.1. Создание management-сети.....	33
5.2.2. Создание директории для ВЦОДов клиентов.....	35
5.2.3. Настройка сетевых зон для сегмента VMware vSphere	36
5.2.4. Настройка vSphere-раннера РУСТЭК-ЕСУ	38
5.2.5. Настройка ресурсного пула для сегмента VMware vSphere	40
5.2.6. Развёртывание Edge-роутера.....	44
5.2.7. Создание шаблонов VM для сегмента VMware vSphere	46
6. Добавление ресурсных пулов партнёру.....	56
7. Создание ВЦОДов в сегментах.....	57
8. Настройка РУСТЭК-ЕСУ для работы с кластерами Kubernetes	60
8.1. Создание шаблонов Kubernetes для сегмента VMware vSphere.....	60
8.2. Создание шаблонов Kubernetes для сегмента РУСТЭК/KVM	70
8.3. Создание кластеров Kubernetes в РУСТЭК-ЕСУ	78
8.4. Особенности и поддерживаемый функционал	80
9. Расширенная настройка	82
9.1. Настройка NGINX реверс-прокси.....	82
9.2. Настройка управления DNS-зонами в РУСТЭК-ЕСУ	83
9.3. Настройка сети для роутеров (edge) сегмента VMware vSphere.....	86
9.4. Универсальный скрипт развёртывания.....	94
9.5. Подготовка сервера с Veeam Backup&Replication для работы с РУСТЭК-ЕСУ.....	97
9.6. Подключение S3-хранилища на базе NetApp StorageGRID к РУСТЭК-ЕСУ.....	104
9.7. Подключение YooKassa к РУСТЭК-ЕСУ.....	106
9.8. Подключение Telegram-бота к РУСТЭК-ЕСУ для управления облачной инфраструктурой	108

9.9. Подключение Telegram-бота к РУСТЭК-ЕСУ для двухфакторной авторизации.....	111
10. Развёртывание на платформе виртуализации VMware vSphere.....	113
10.1. Системные требования	113
10.2. Порядок развёртывания	113
10.3. Примечания по установке и дальнейшей настройке.....	123
11. Подготовка инфраструктуры для получения обновлений РУСТЭК-ЕСУ	124
Приложение 1. Пример Auto DevOps-скрипта.....	126

1. Поставка РУСТЭК-ЕСУ

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

- .raw – для установки на РУСТЭК (KVM).
- .ova – для установки на VMware ESXi.

В качестве гостевой 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 Системы.

Минимальные требования для сервера ESU-box:

- vCPU 4 ядра.
- RAM 4 ГБ.
- Размер диска 20 ГБ.

2. Развёртывание на платформе виртуализации РУСТЭК

2.1. Системные требования

- РУСТЭК Wallaby.
- Одна маршрутизируемая сеть, минимально допустимая /27, с доступом до management-сети РУСТЭК

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

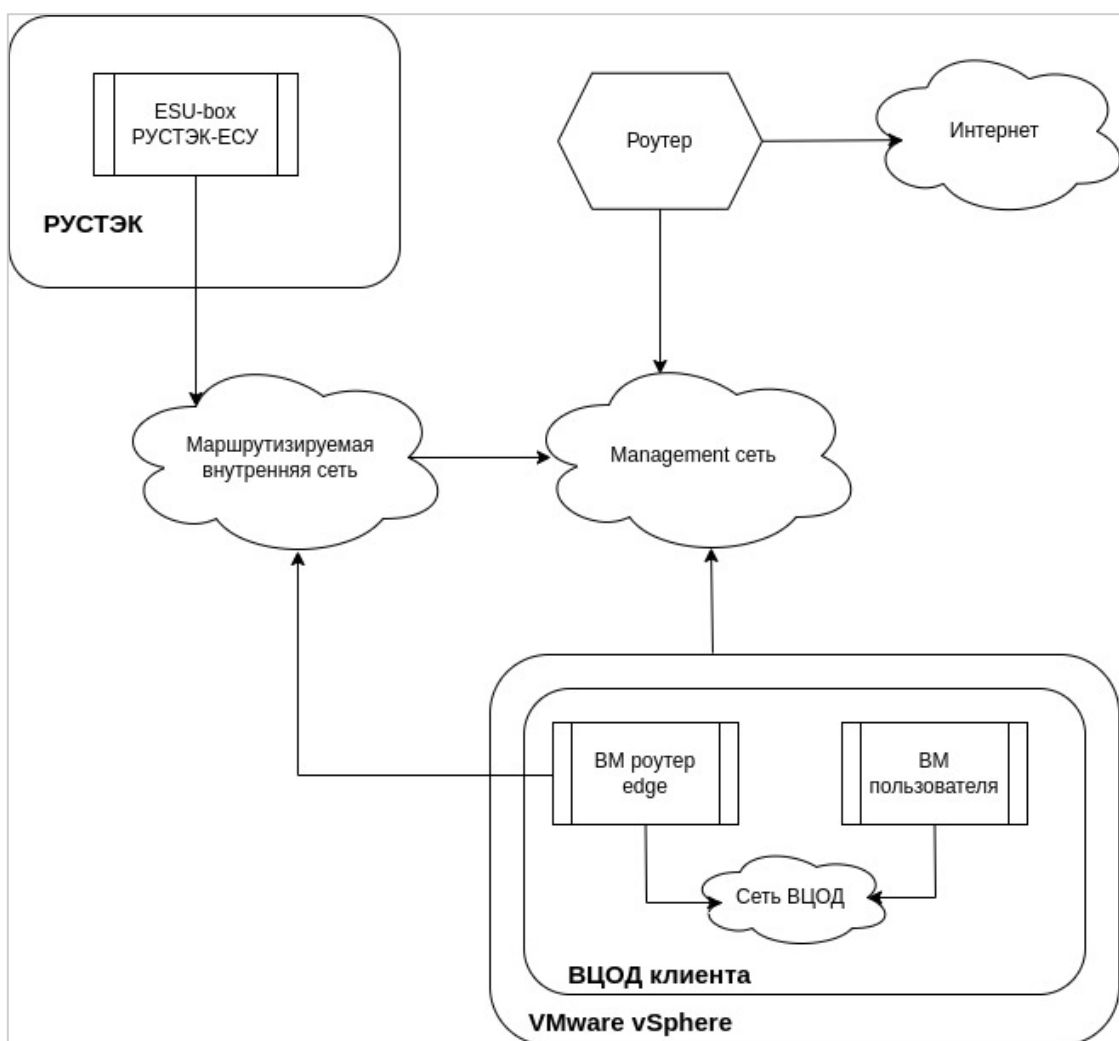


Рисунок 1

2.2. Порядок развёртывания

1. Зайти в Панель управления РУСТЭК по ссылке <https://<virtual ip>/New>
2. Создание образа (Рисунок 2, Рисунок 3):
Перейти в раздел «Копии и образы» – «Образы» и нажать кнопку «Создать».

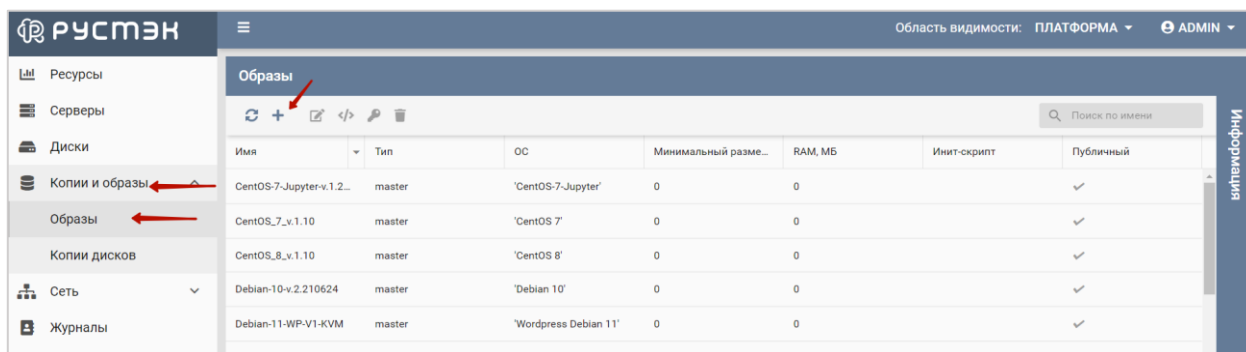


Рисунок 2

Откроется окно с параметрами образа, где необходимо заполнить поля:

- Имя – указывается «произвольное».
- Имя ОС – указывается «произвольное».
- Контейнер – оставить значение «bare».
- Формат диска – указать «raw».
- RAM(МБ) – указывается минимальное кол-во ОЗУ для будущих VM – указать 4096.
- Размер диска(ГБ) – указывается минимальный размер дисков для будущих VM – указать 20 ГБ.
- Сетевой адаптер – выбрать «virtio».
- Дисковый контроллер – выбрать «virtio-scsi».
- Публичный – снять чек-бокс.
- Метод загрузки – выбрать «Файл».

И нажать «Создать».

Создание нового образа ✕

Имя	Rustack-ESU-image ✕
Проект	admin ▼
Имя ОС	Debian-rustack ✕
Контейнер	bare ▼
Формат диска	raw ▼
RAM, МБ	4096 ✕ ▲ ▼
Размер диска, ГБ	20 ✕ ▲ ▼
Сетевой адаптер	virtio ▼
Дисковый контролер	virtio-scsi ▼
Публичный	<input type="checkbox"/>
Защищенный	<input type="checkbox"/>
Улучшения Windows	<input type="checkbox"/>
Загрузчик UEFI	<input type="checkbox"/>
QEMU агент	<input type="checkbox"/>
Метод загрузки	<input type="radio"/> URL <input checked="" type="radio"/> Файл
Метадата	Вводить через запятую

СОЗДАТЬ
ОТМЕНА

Рисунок 3

3. Загрузка образа (Рисунок 4, Рисунок 5)

Найти в списке новый образ, выбрать его и нажать на кнопку «Загрузить образ».

Имя	Тип	ОС	Минимальный ра...	RAM, МБ	Инит-скрипт	Публичный	Проект
<input checked="" type="checkbox"/>	Rustack-ESU-image	master	Debian-rustack	20	4096		admin

Рисунок 4

Нажать «Добавить файл» и выбрать предоставленный дистрибутив в формате raw. Далее нажать «Загрузить». Начнется процесс загрузки образа.

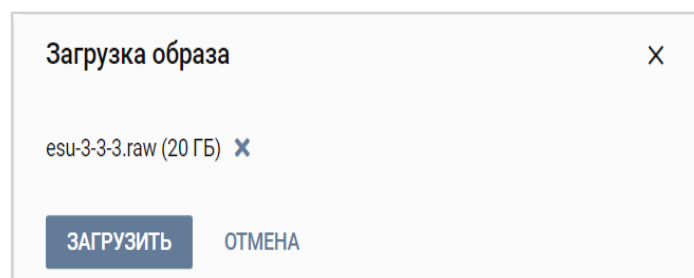


Рисунок 5

4. Создание маршрутизируемой сети (Рисунок 6, Рисунок 7)

По окончании загрузки вам необходимо создать сеть для будущей Единой системы управления. Для этого необходимо перейти в раздел «Сеть» – «Сети» и нажать «Создать».

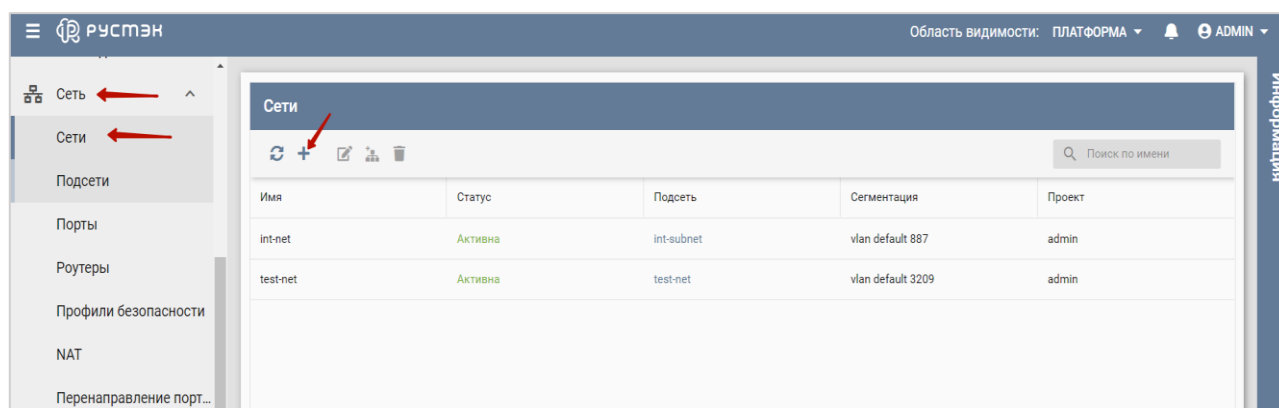


Рисунок 6

Заполнить необходимые поля:

- Имя – указывается произвольное.
- Тип сегментации – VLAN.
- Номер VLAN – номер выделенного влана для менеджмент-сети Единой системы управления.
- Безопасность портов – отключаем.
- Внешняя — ставим галочку.

Создание сети		✕
Имя	ESU-Rustack	✕
Описание		
MTU		⬆
DNS		
Тип сегментации	VLAN	▼
Номер VLAN	3058	✕ ⬆
Внешняя	<input checked="" type="checkbox"/>	
Безопасность портов	<input type="checkbox"/>	
Проект	admin	▼
Общая	<input type="checkbox"/>	
Теги		
СОЗДАТЬ		ОТМЕНА

Рисунок 7

5. Создание подсети для маршрутизируемой сети (Рисунок 8)

После создания сети необходимо создать подсеть. Для этого перейдите в раздел «Сети» – «Подсеть» и нажмите «Создать», далее необходимо заполнить поля:

- Имя – указывается произвольное.
- Сеть – выбрать сеть, созданную на предыдущем этапе.
- Версия протокола – Ipv4.
- Адрес сети – указать cidr.
- Шлюз – указать шлюз.
- DHCP – снять чек-бокс.

Нажать «Создать».

Создание подсети [X]

Имя: Rustack-ESU-subnet [X]

Описание: _____

Сеть: ESU-Rustack [v]

Версия IP: IPv4 [v]

Адрес сети: 10.11.14.0/24 [X]

Шлюз: 10.11.14.1 [X]

Проект: admin [v]

DHCP:

DNS-серверы: Вводить через запятую _____

Публикация IP в DNS:

Теги: _____

Диапазоны IP

+ ДОБАВИТЬ

Маршруты

+ ДОБАВИТЬ

СОЗДАТЬ ОТМЕНА

Рисунок 8

!!!Важно!!! Из создаваемой сети для будущей VM ESU_box должен быть организован доступ до менеджмент-сети хостов виртуализации.

6. Создание конфигурации VM (Рисунок 9)

Перейдите в раздел **Конфигурация – Конфигурации** и нажмите «Создать». После чего необходимо заполнить поля будущей конфигурации:

- Имя – указывается произвольное.
- vCPU – количество CPU.
- RAM, МБ – количество ОЗУ. Обратите внимание, что размер указывается в Мбайт.

Нажать «Создать».

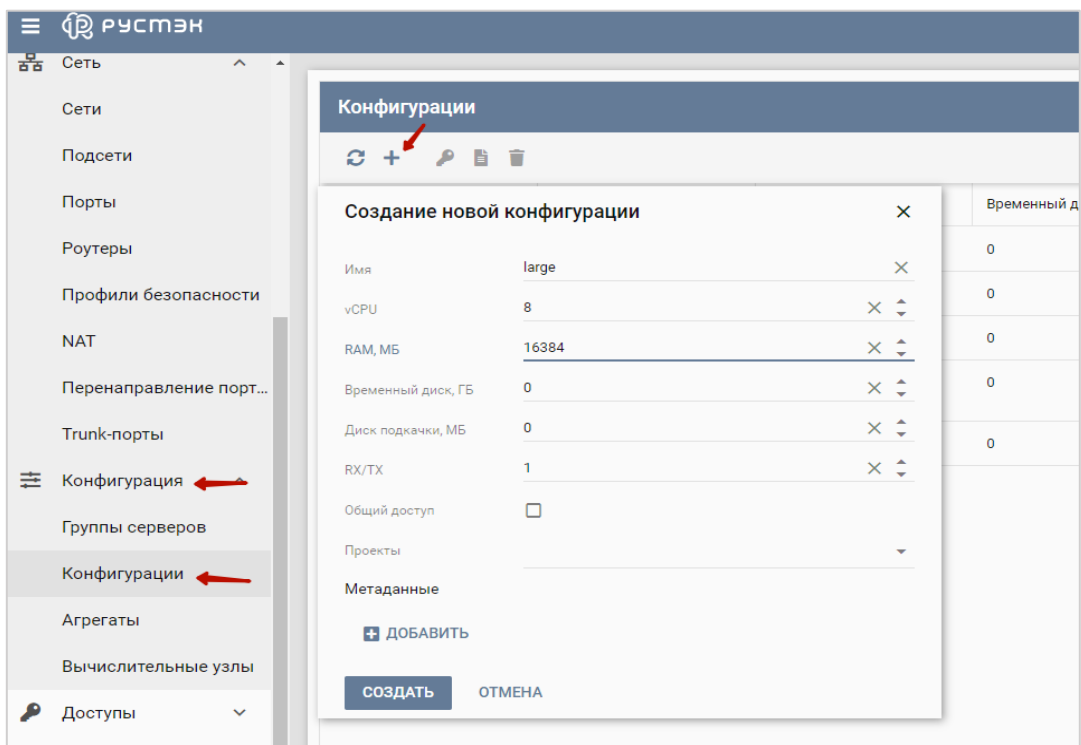


Рисунок 9

7. Создание VM (Рисунок 10)

Необходимо перейти во вкладку «Серверы» и нажать «Создать» в появившейся форме требуется заполнить поля:

- Имя – указывается произвольное.
- ОС – выбрать ранее загруженный образ.
- Конфигурация – указать необходимую конфигурацию (минимальная 4 CPU, 4 ГБ RAM).
- Размер диска – указать размер диска VM (минимальный размер 20 Гб).
- Чек-бокс «Удалять диск вместе с сервером» – рекомендуем снять.
- Сети – выбрать ранее созданную маршрутизируемую сеть.

Нажать «Создать».

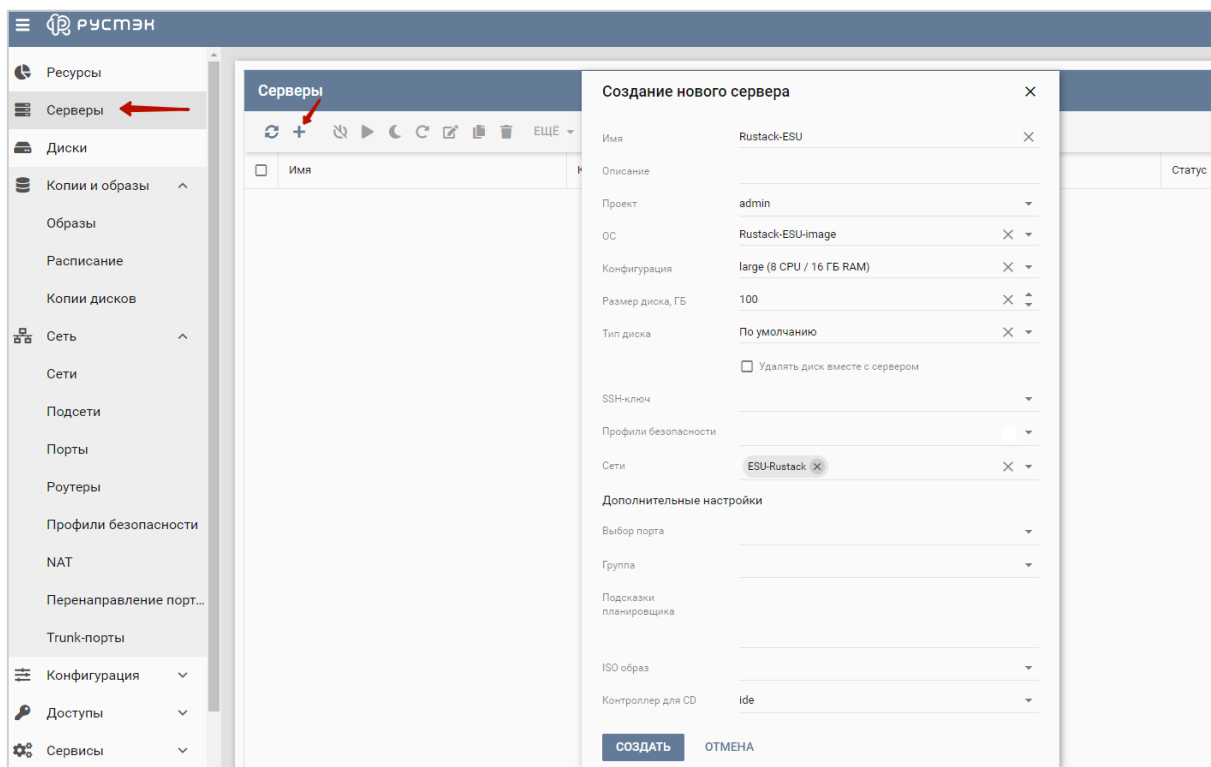


Рисунок 10

Дождаться окончания создания сервера (статус изменится на «Запущен»).

8. Открываем VNC-консоль для созданной VM (Рисунок 11)

Для открытия консоли сервера переходим в меню «Серверы». Выбираем созданный сервер, затем нажимаем «Ещё» и либо сразу открываем консоль сервера, нажав «Открыть консоль», либо получаем ссылку, нажав на «Ссылка на консоль сервера» и открываем её в новой вкладке.

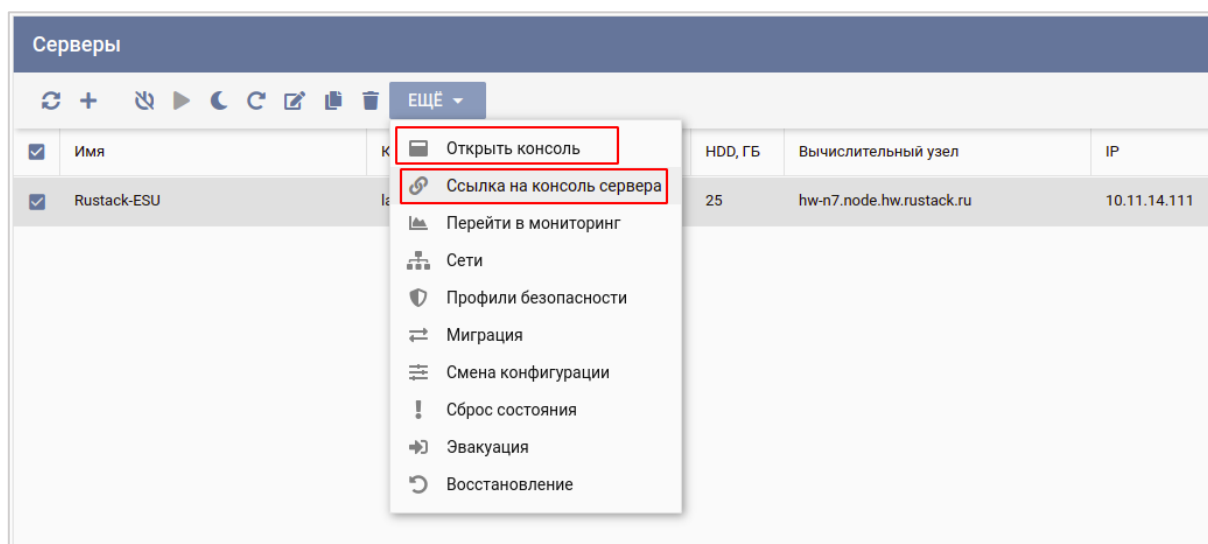


Рисунок 11

Стандартная учётная запись на сервере с РУСТЭК-ЕСУ (ESU-box): **deploy:1-qpALzm/**

3. Установка РУСТЭК-ЕСУ

Установка запускается автоматически при запуске ВМ с РУСТЭК-ЕСУ.

Сначала произойдет распаковка контейнеров. Нужно дождаться завершения процесса (Рисунок 12 и Рисунок 13):

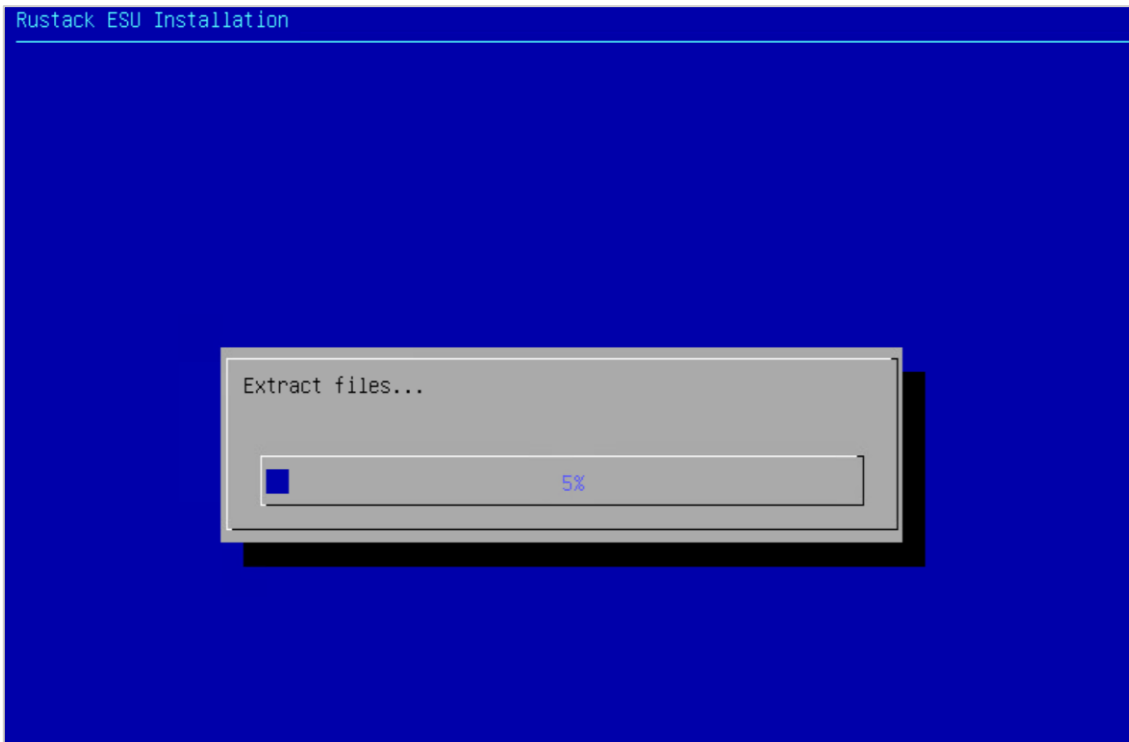


Рисунок 12



Рисунок 13

Далее будет задано несколько вопросов относительно сетевой конфигурации:

Сначала нужно указать какой IP был назначен ВМ ESU-box внутри РУСТЭК и какой подсеть будет располагать (Рисунок 14 и Рисунок 15).

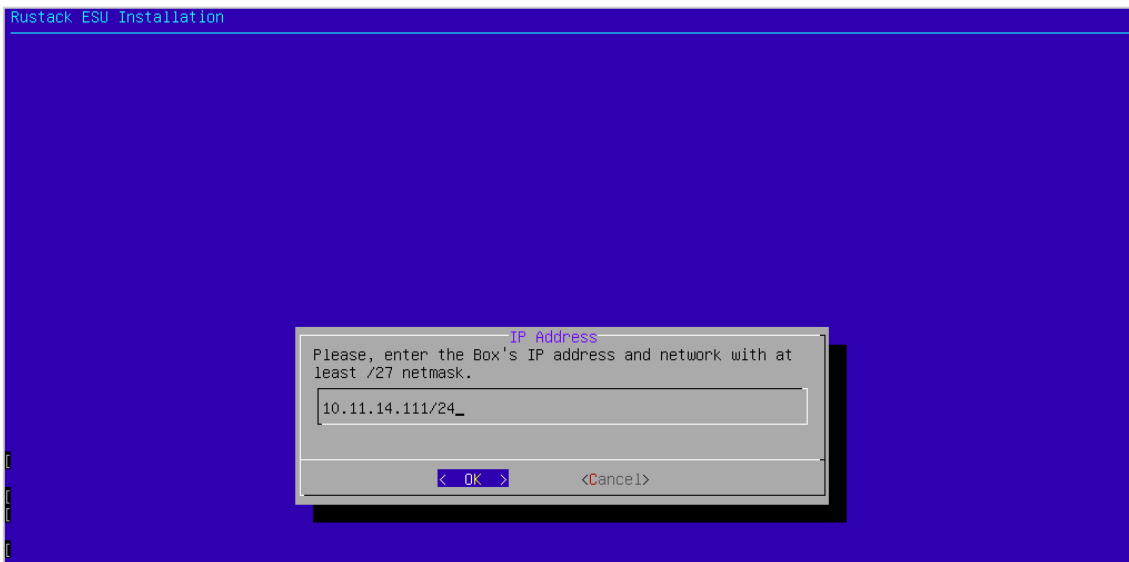


Рисунок 14

Серверы							
<input checked="" type="checkbox"/>	Имя	Конфигурация	vCPU	RAM, ГБ	HDD, ГБ	Вычислительный узел	IP
<input checked="" type="checkbox"/>	Rustack-ESU	large	8	16	25	hw-n7.node.hw.rustack.ru	10.11.14.111

Рисунок 15

Далее необходимо ввести шлюз подсети (Рисунок 16).

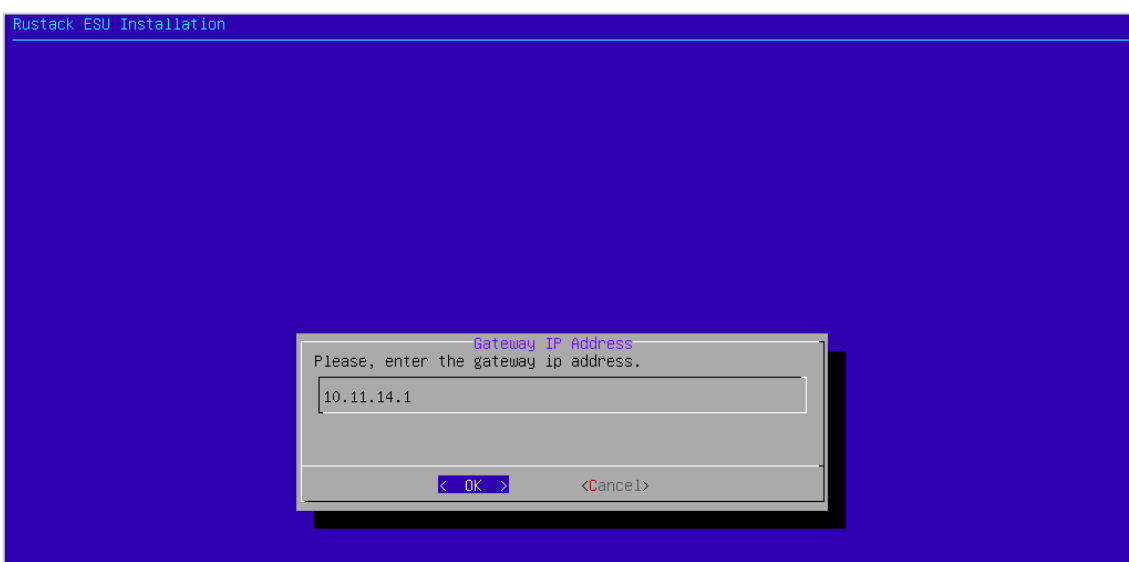


Рисунок 16

В следующем окне инсталлятора необходимо ввести VLAN ID, если на ESU-box подана сеть с несколькими VLAN. В нашем случае подан один VLAN, а значит данное поле заполнять не нужно (Рисунок 17).



Рисунок 17

На вопрос «Хотите ли вы включить DHCP-сервер в ESU-box?» надо ответить **Yes**, поскольку в нашей сети его нет. Для выбора опции (Yes) используйте кнопку пробел (Рисунок 18).

!!!Важно!!! Запуск DHCP-сервера на ESU-box обязателен.

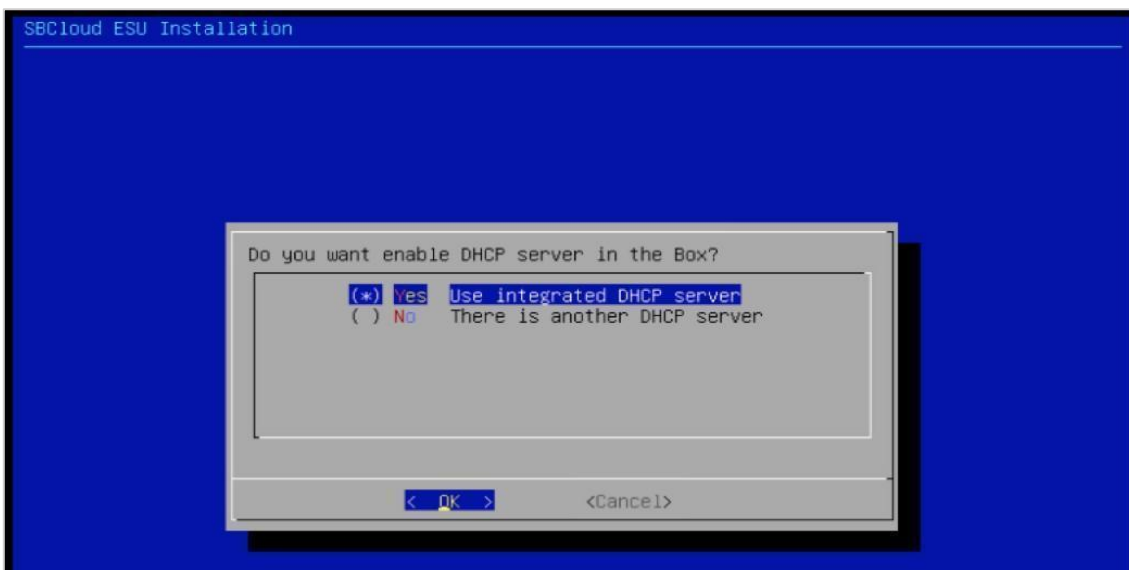


Рисунок 18

Затем нужно ввести адрес DNS-сервиса (Рисунок 19).



Рисунок 19

Далее нужно указать адрес SMTP-сервера. Он должен поддерживать подключение без авторизации. Можно оставить значение по умолчанию для использования встроенного SMTP-сервера (Рисунок 20).

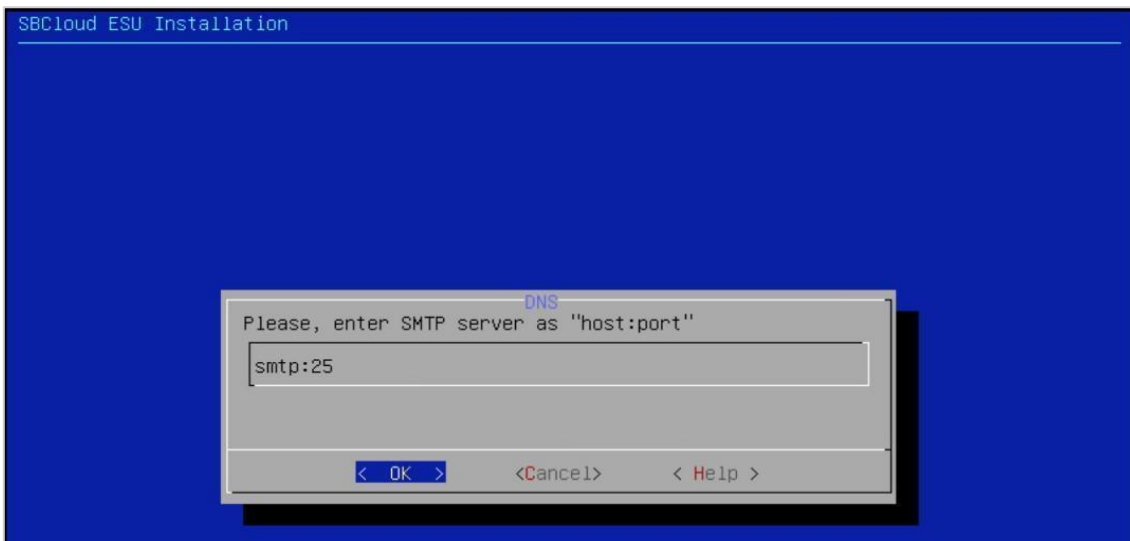


Рисунок 20

Теперь указываем пароль, который будет установлен для пользователя admin с правами администратора платформы (Рисунок 21).

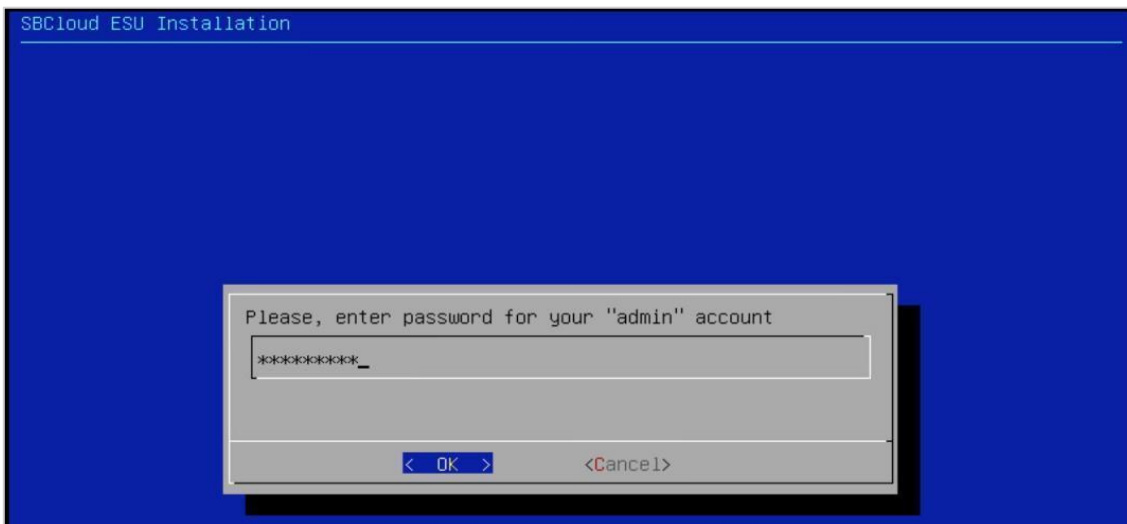


Рисунок 21

После всего этого необходимо дождаться завершения процесса настройки (Рисунок 22–Рисунок 24).



Рисунок 22

```
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 23

```
Debian GNU/Linux 10 localhost tty1
localhost login: [ OK ] Started ESU Firstboot Kickstart Service.
```

Рисунок 24

На этом установка РУСТЭК-ЕСУ завершена.

4. Настройка РУСТЭК-ЕСУ

После завершения установки, по IP адресу порта созданного сервера ESU-box (также указывался при инсталляции) будет доступен web-интерфейс РУСТЭК-ЕСУ. В нашем случае это <https://10.11.14.111/cp> (обратите внимание, что нужно использовать <https://>).

Авторизуйтесь с логином `admin` и паролем, заданным при инсталляции (Рисунок 25).

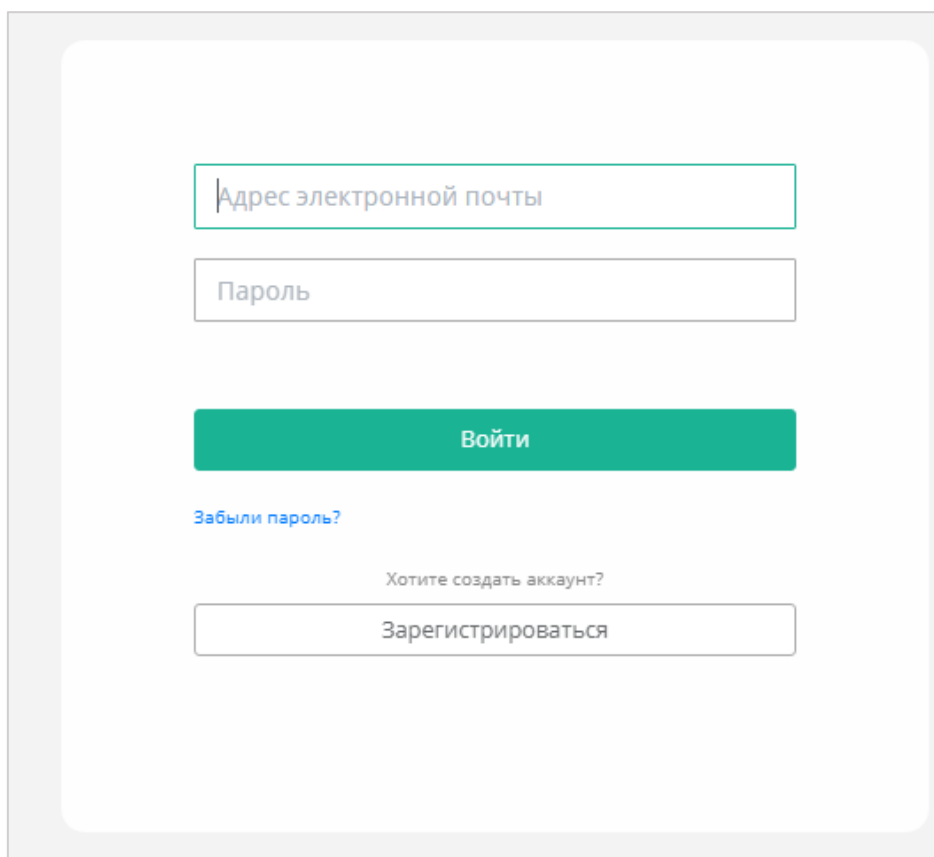


Рисунок 25

В меню **Администрирование – Тарифные планы** создаётся тарифный план – достаточно ввести только название (Рисунок 26).

Создание тарифного плана

Главная / Администрирование / Тарифные планы / Создание тарифного плана

Помощник по SKU

Основные настройки

Имя: Тарифный план

Отменить Далее >

Рисунок 26

В меню **Администрирование – Партнёры**, создается партнёр – необходимо указать тарифный план (Рисунок 27).

Добавление партнера

Главная / Администрирование / Партнёры / Добавление партнера

Основные настройки | Настройки клиентов по умолчанию

Имя: Партнёр

Тарифный план: default

Отменить Далее >

Рисунок 27

В меню **Администрирование – Домены**, партнёр привязывается к домену, и также производятся настройки домена – задаются/изменяются шаблоны писем (Рисунок 28).

Изменение домена

Главная / Администрирование / Домены / **Изменение домена**

Имя	<input type="text" value="default"/>
Домены	<input type="text" value="default"/> x
DNS зона	<input type="text" value="Отключена"/> Выбрать
Связанный партнер	<input type="text" value="Отсутствует"/> Выбрать

	Логотип Favicon Фон
Логотип	<input type="text" value="Выберите файл..."/>

	Авторизация Регистрация Персональные данные
Текст, который показывается на форме авторизации	<div style="border: 1px solid #ccc; height: 100px;"></div>

Рисунок 28

5. Настройка сегментов

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

5.1. Настройка сегмента РУСТЭК/KVM

В случае если для управления РУСТЭК-ЕСУ необходимо добавить несколько сегментов РУСТЭК, то для каждого из них нужно выполнить все нижеперечисленные настройки.

5.1.1. Настройка сетевых зон для KVM сегмента

В меню **Инсталляция** → **Ресурсы** → **Сетевые зоны** создаётся и настраивается сетевая зона. Для создания сетевой зоны нажмите кнопку **Создать сетевую зону** (Рисунок 29).

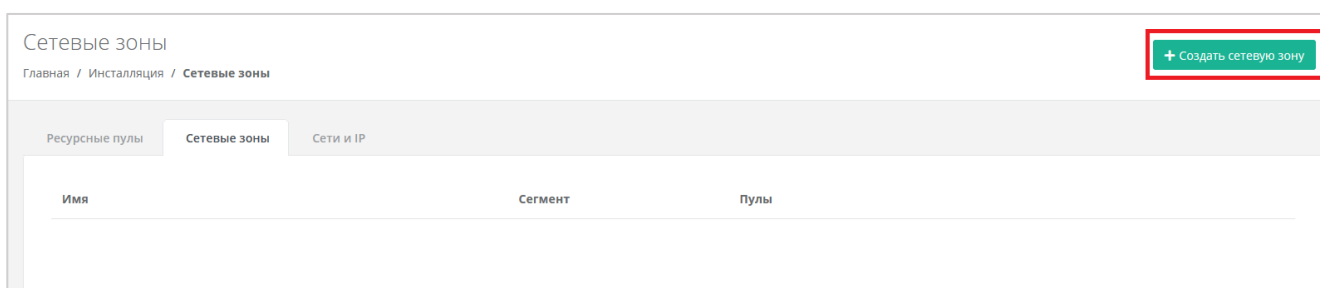


Рисунок 29

Введите название сетевой зоны, выберите сегмент VLAN и нажмите кнопку **Далее** (Рисунок 30).

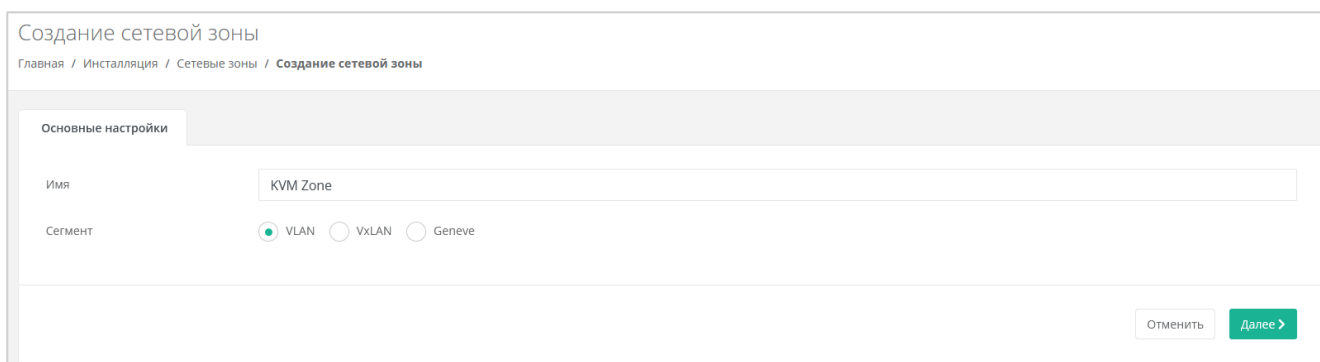


Рисунок 30

После нажатия кнопки **Далее** появится возможность добавления пулов. Необходимо указать диапазон VLAN для пользовательских проектов: 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 31).

Изменение сетевой зоны

Главная / Установка / Сетевые зоны / Изменение сетевой зоны

Основные настройки

Имя: KVM Zone

Сегмент:
 VLAN
 VXLAN
 Geneve

Пулы:

Начало диапазона	Конец диапазона	Действия
701	1000	

+ Добавить пул

Удалить Отменить Сохранить

Рисунок 31

Аналогично создаём **вторую** сетевую зону для *внешней* сети (Рисунок 32).

Вводим диапазон для external-сети: один и тот же VLAN указывается и в начале, и в конце диапазона, в данном случае — 41.

Изменение сетевой зоны

Главная / Установка / Сетевые зоны / Изменение сетевой зоны

Основные настройки

Имя: KVM Zone ext

Сегмент:
 VLAN
 VXLAN
 Geneve

Пулы:

Начало диапазона	Конец диапазона	Действия
41	41	

+ Добавить пул

Удалить Отменить Сохранить

Рисунок 32

В меню **Установка** → **Ресурсы** → **Сети и IP** создаем external-сеть нажатием кнопки **Создать сеть**. В открывшейся форме заполните следующие поля настроек (Рисунок 33):

- Название — любое.
- Сетевая зона — созданная ранее для *внешней* сети KVM-сегмента.
- VID/VNID — VLAN внешней сети: в нашем случае — 41.
- Тип сети — внешняя.

Рисунок 33

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

Добавляем подсеть с конфигурацией сети с помощью кнопки **Добавить подсеть**. DHCP должен быть **выключен**, CIDR надо указывать полный. Если нужно уменьшить диапазон выдаваемых IP-адресов, можно указать произвольный диапазон (Рисунок 34).

Рисунок 34

Данная внешняя сеть автоматически будет создана при первом создании ВЦОД в KVM.

5.1.2. Настройка Openstack-раннера

Следующим этапом в меню **Установка** → **Система** → **Раннеры** конфигурируется OpenStack-раннер для KVM-сегмента. Указывается IP-адрес РУСТЭК, логин администратора и пароль для авторизации посредством Keystone и Содержимое

файла `clouds.yml`, который находится по следующему пути: `/etc/openstack/clouds.yml` на контроллер-ноде РУСТЭК (Рисунок 35).

Изменение раннера

Главная / Установка / Раннеры / Изменение раннера

Основные настройки

ID: default-openstack-runner

Тип: OpenStack

Callback URL: http://openstack_runner:5000

Включен: Снять флажок можно запретить API взаимодействовать с раннером

Пароль: 886Lset3

URL, на котором расположена служба Keystone. Может быть http://1.2.3.4 или https://1.2.3.4: http://10.11.3.10

Имя пользователя: admin

Содержимое файла `clouds.yml`, описывающее параметры подключения к OpenStack Identity:

```
---
clouds:
  rustack:
    auth:
      auth_url: http://10.11.3.10/keystone/v3/
      username: admin
      password: 886Lset3
      domain_id: default
      project_name: admin
      identity_api_version: 3
```

Удалить Отменить Сохранить

Рисунок 35

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» (Рисунок 36).

Включить Octavia

Включить Cinder Backup

Рисунок 36

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

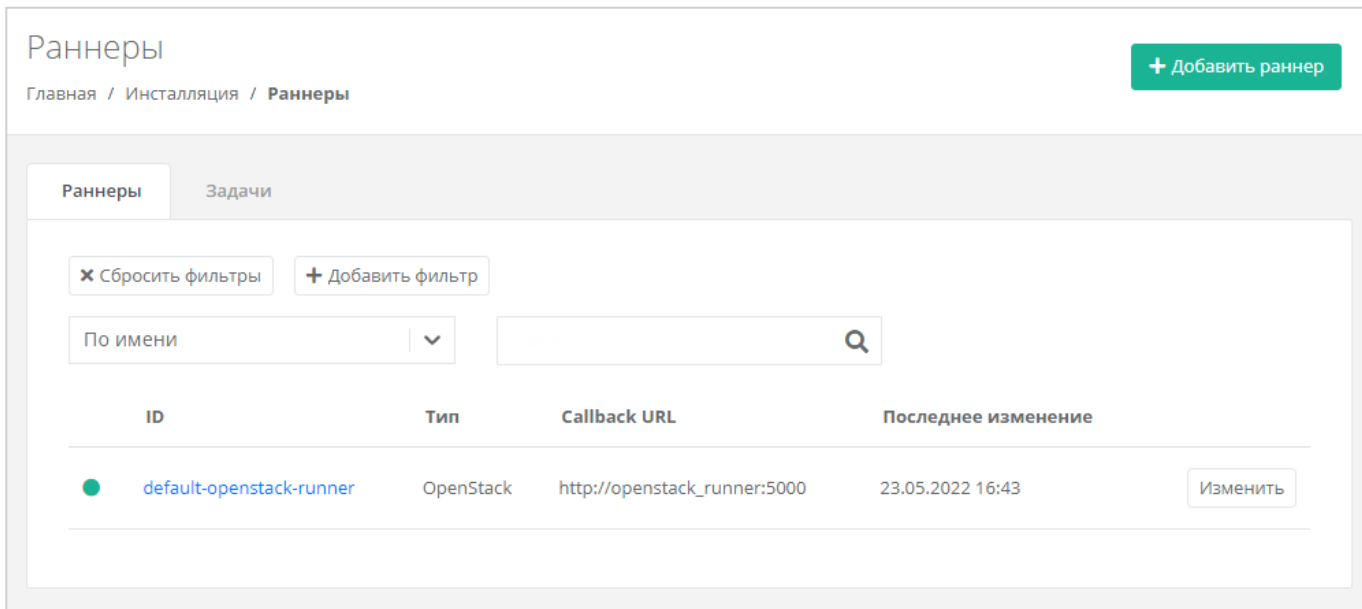


Рисунок 37

5.1.3. Настройка ресурсного пула для KVM-сегмента

Далее в меню **Установка** → **Ресурсы** → **Ресурсные пулы**, конфигурируется ресурсный пул – необходимо указать соответствующий раннер (в данном случае – default-openstack-runner), сетевую зону и внешнюю сеть (Рисунок 38).

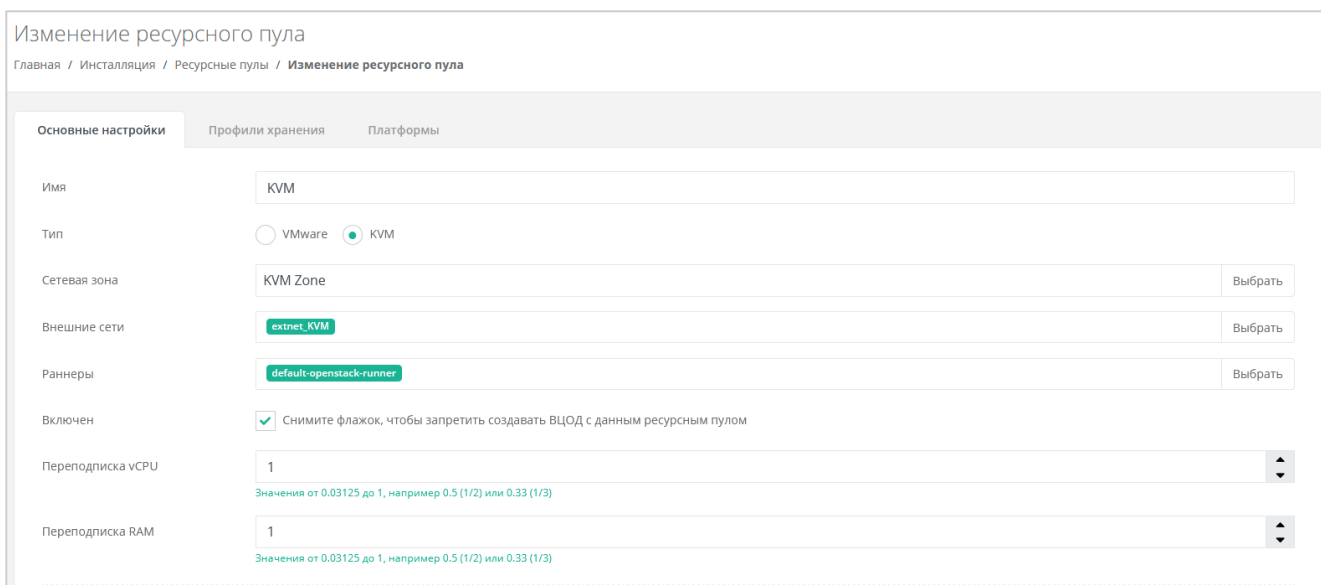


Рисунок 38

Далее необходимо настроить переподписку vCPU и RAM (Рисунок 39).

Изменение ресурсного пула

Главная / Установка / Ресурсные пулы / Изменение ресурсного пула

Основные настройки | Профили хранения | Платформы

Имя:

Тип: VMware KVM

Сетевая зона: Выбрать

Внешние сети: Выбрать

Раннеры: Выбрать

Включен: Снимите флажок, чтобы запретить создавать ВЦОД с данным ресурсным пулом

Переподписка vCPU: Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Переподписка RAM: Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Рисунок 39

После этого необходимо настроить ограничения на один сервер (Рисунок 40)

Раннеры: Выбрать

Включен: Снимите флажок, чтобы запретить создавать ВЦОД с данным ресурсным пулом

Переподписка vCPU: Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Переподписка RAM: Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Ограничения на один сервер

vCPU: шт.

RAM: ГБ

Диски: шт.

Подключения: шт. Распространяется также и на роутеры

Рисунок 40

Для KVM-сегмента заполнять поля ниже не нужно.

При необходимости можно задать логотип для ресурсного пула – кнопка «Выберите файл...» напротив поля «Иконка» в нижней части вкладки.

После сохранения новых настроек ресурсного пула РУСТЭК-ЕСУ должна забрать адреса сервисных портов РУСТЭК в свою БД. В этом можно убедиться, запустив в консоли VM 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 41).

```
In [1]: Port.objects.table('id', 'type', 'network_id', 'ip_address')
...:
```

id	type	network_id	ip_address
a1444fb8-5e72-4c9e-af43-f6ff8474f1a2	service	3c31f9fc-3e5f-43b5-aaa2-27b434b38917	185.17.143.89
884627df-feaa-4b44-b859-1fe00317726b	service	3c31f9fc-3e5f-43b5-aaa2-27b434b38917	185.17.143.75
6db921b9-91f6-4bbd-b108-ca2cf20588e8	service	3c31f9fc-3e5f-43b5-aaa2-27b434b38917	185.17.143.76
a47b37ac-bc68-4b4e-803d-48b105334256	service	3c31f9fc-3e5f-43b5-aaa2-27b434b38917	185.17.143.87

Рисунок 41

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 external-сети – она должна называться openstack network list-external.**

Далее конфигурируются профили хранения ресурсного пула (Рисунок 42).

- Имя – в соответствии с подсказкой (SSD, SATA, SAS).
- Отображаемое имя – любое.
- Имя вольюм тайпа – в соответствии с доступными volume type в РУСТЭК.
- Биллинг-класс – выбираем необходимый.

Добавление профиля хранения ✕

Имя	<input type="text" value="SATA"/>
Имя вольюм тайпа	<input type="text" value="nfs"/>
Биллинг класс	<input type="text" value="Предоставление дискового пространства уровня SATA ..."/>
Макс. размер диска	<input type="text" value="ГБ 32768"/> <div style="font-size: 0.8em; color: #0070c0; margin-top: 5px;"> Пользователь не сможет создать диск больше указанного размера. Для дисков большего размера (уже существующих или создаваемых административно) будет отключен функционал снапшотов. </div>
Позиция	<input type="text" value="1"/>

Рисунок 42

Имя volume type в РУСТЭК можно получить, выполнив на одном из контроллеров РУСТЭК команду:

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

Будет выведен приблизительно следующий список (Рисунок 43):

```
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 43

В качестве вольюм тайпа в панели управления РУСТЭК-ЕСУ необходимо указать значение поля «Name». В нашем случае это nfs.

Далее необходимо проверить правильность заполнения вкладки «Платформа». Если настройки отсутствуют или не совпадают – нужно нажать кнопку «Добавить платформу» и в открывшемся окне указать имя агрегата из РУСТЭК.

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

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

Будет выведен приблизительно следующий список (Рисунок 44):

```
aio ~ # OS_CLOUD=rustack_system openstack aggregate list
+-----+-----+-----+
| ID | Name          | Availability Zone |
+-----+-----+-----+
| 1  | production   | None              |
+-----+-----+-----+
```

Рисунок 44

5.1.4. Создание шаблонов VM для сегмента РУСТЭК/KVM

Для создания шаблона VM 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 VM с операционной системой Ubuntu 18.04 LTS.

Заходим по SSH (root:rustack) на один из контроллеров РУСТЭК и скачиваем целевой образ, после чего создаем 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 – имя образа в РУСТЭК, его необходимо записать или запомнить.

Создаём шаблон в РУСТЭК-ЕСУ через веб-интерфейс, для этого переходим в меню **Инсталляция** → **Шаблоны** → **Серверы** и нажимаем кнопку **Создать шаблон**, после чего открывается форма где необходимо указать сегмент (в данном случае – KVM), название шаблона, группу (Рисунок 45).

Создание шаблона

Главная / Инсталляция / Серверы / Создание шаблона

Основные настройки Дополнительные

Доступен для VMware KVM

Имя

Группа шаблонов

Включен Снимите флажок, чтобы шаблон не показывался в витрине

Windows лицензия Если флажок установлен, с пользователя будет списываться стоимость лицензии Windows

Имя шаблона

- Один и тот же образ (шаблон) должен одновременно присутствовать на всех гипервизорах этого типа!
- vSphere: шаблон должен иметь уникальное название и быть шаблоном (без сетей, снапшотов, LSI Logic SCSI, один диск на scsi 0:0)

Рекомендации до деплоя

Рекомендации после деплоя

Иконка ✕

Рисунок 45

Нажимаем на имя шаблона – откроется список образов РУСТЭК, в котором необходимо выбрать ранее созданный образ (Рисунок 46).

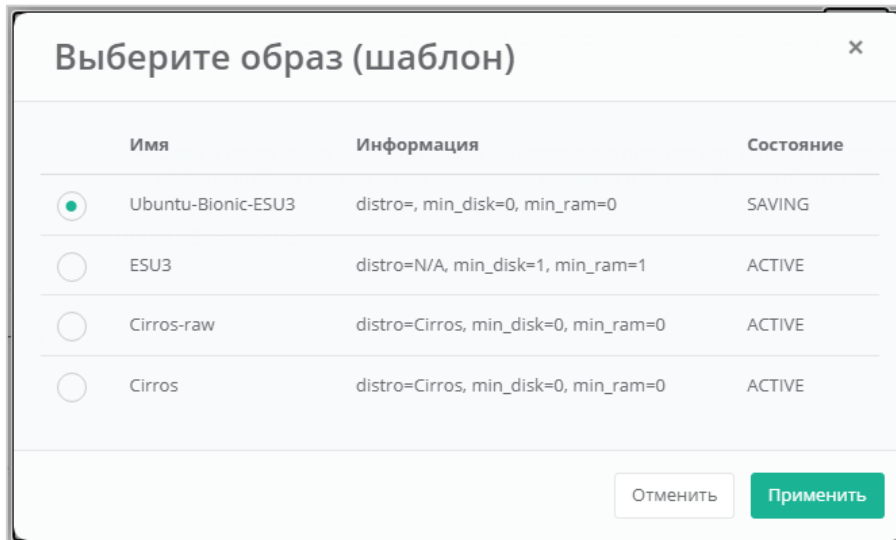


Рисунок 46

Указываем минимальное число ядер CPU (минимум 1 ядро) и объем RAM (минимум 2 Гб – Рисунок 47).

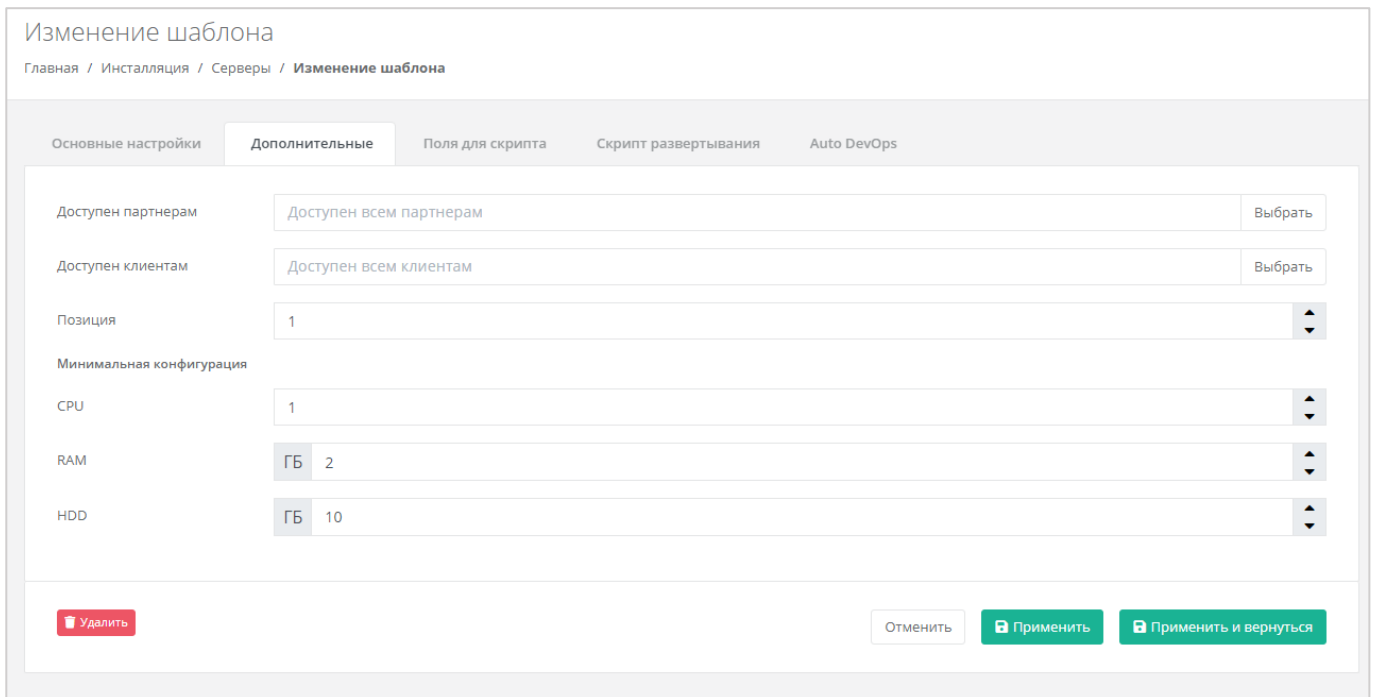


Рисунок 47

Переходим во вкладку поля для скрипта. Рекомендуем заполнить поля, указанные на скриншоте (Рисунок 48).

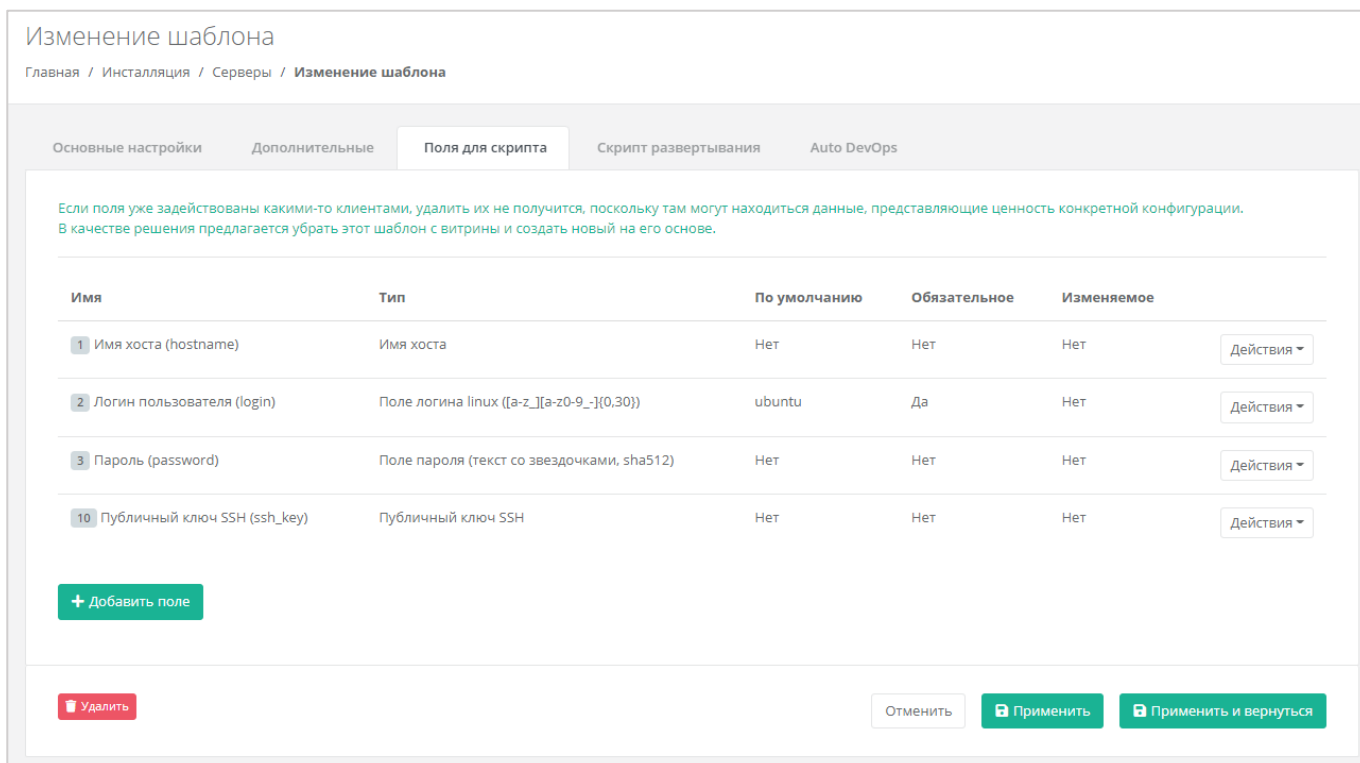


Рисунок 48

Далее во вкладке **Скрипт развёртывания** необходимо добавить скрипт развёртывания.

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

Примечание: универсальный скрипт развёртывания для Linux OS приложений ниже в документации в разделе 9.4.

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.

!!!Важно!!! 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 VM появится в списке шаблонов и из него можно будет создавать VM.

5.2. Настройка сегмента VMware vSphere

В случае если для управления РУСТЭК-ЕСУ необходимо добавить несколько инсталляций VMware vSphere (сегментов), то для каждого из них нужно выполнить 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 dvSwitch, под которым будут создаваться пользовательские сети (порт-группы).

5.2.1. Создание management-сети

Создаем management-сеть, в которой развёрнута и работает ВМ с РУСТЭК-ЕСУ – ESU-box (настройки сети должны совпадать с настройками маршрутизируемой сети внутри РУСТЭК), она же портгруппа на dvSwitch в vSphere (требуется один VLAN). Необходимо учитывать, что в эту сеть будут подключены пользовательские роутеры для сегмента VMware (в разделе «*Настройка сети для роутеров (edge) сегмента VMware vSphere*» этого документа описана процедура, позволяющая изменить такое поведение, создав отдельную сеть для роутеров).

Таким образом, размер подсети напрямую влияет на максимальное число ВЦОДов. ВМ ESU-box с РУСТЭК-ЕСУ станет DHCP-сервером в этой подсети (также возможна установка в сеть, где уже присутствует DHCP сервер). В данном примере сеть называется vlan3058 (*Создание*: Рисунок 49, Рисунок 50, *Редактирование*: Рисунок 51 и Рисунок 52).

New Distributed Port Group

- 1 Name and location
- 2 Configure settings
- 3 Ready to complete

Name and location

Specify distributed port group name and location.

Name

Location

CANCEL NEXT

Рисунок 49

New Distributed Port Group

- 1 Name and location
- 2 Configure settings
- 3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Port allocation ⓘ

Number of ports

Network resource pool

VLAN

VLAN type

VLAN ID

Advanced

Customize default policies configuration

CANCEL BACK NEXT

Рисунок 50

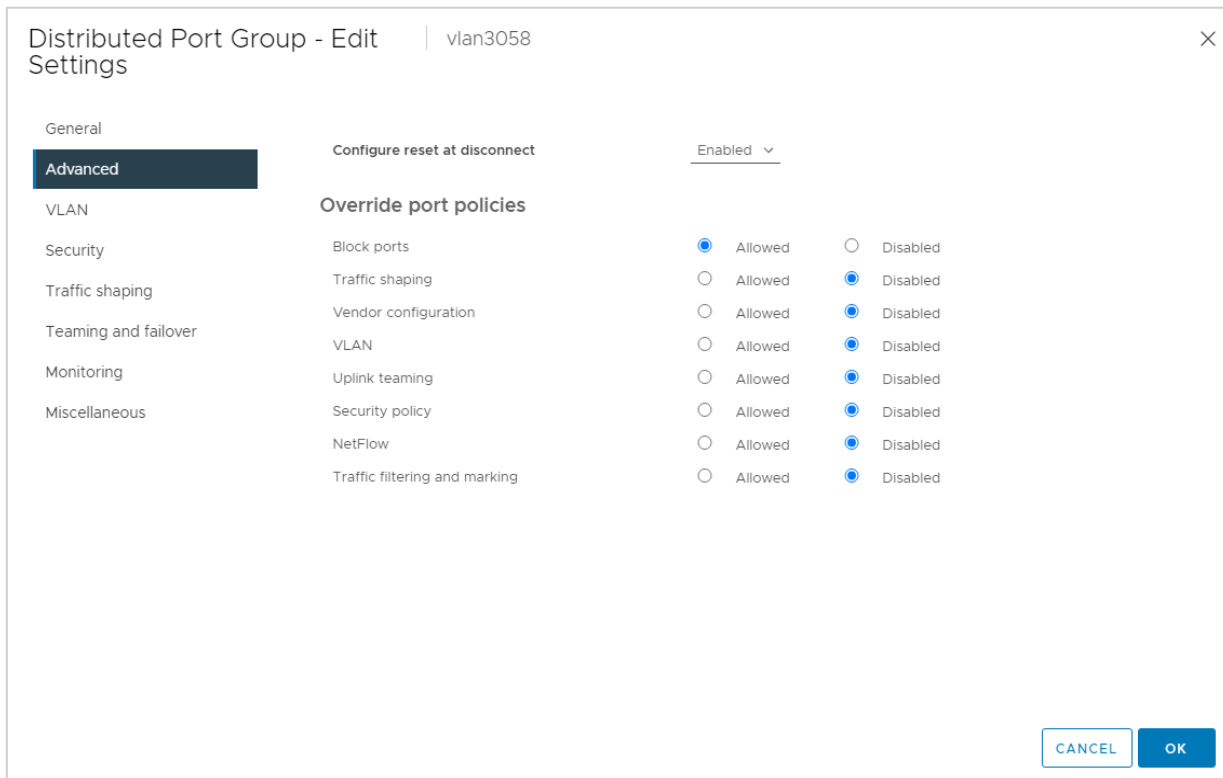


Рисунок 51

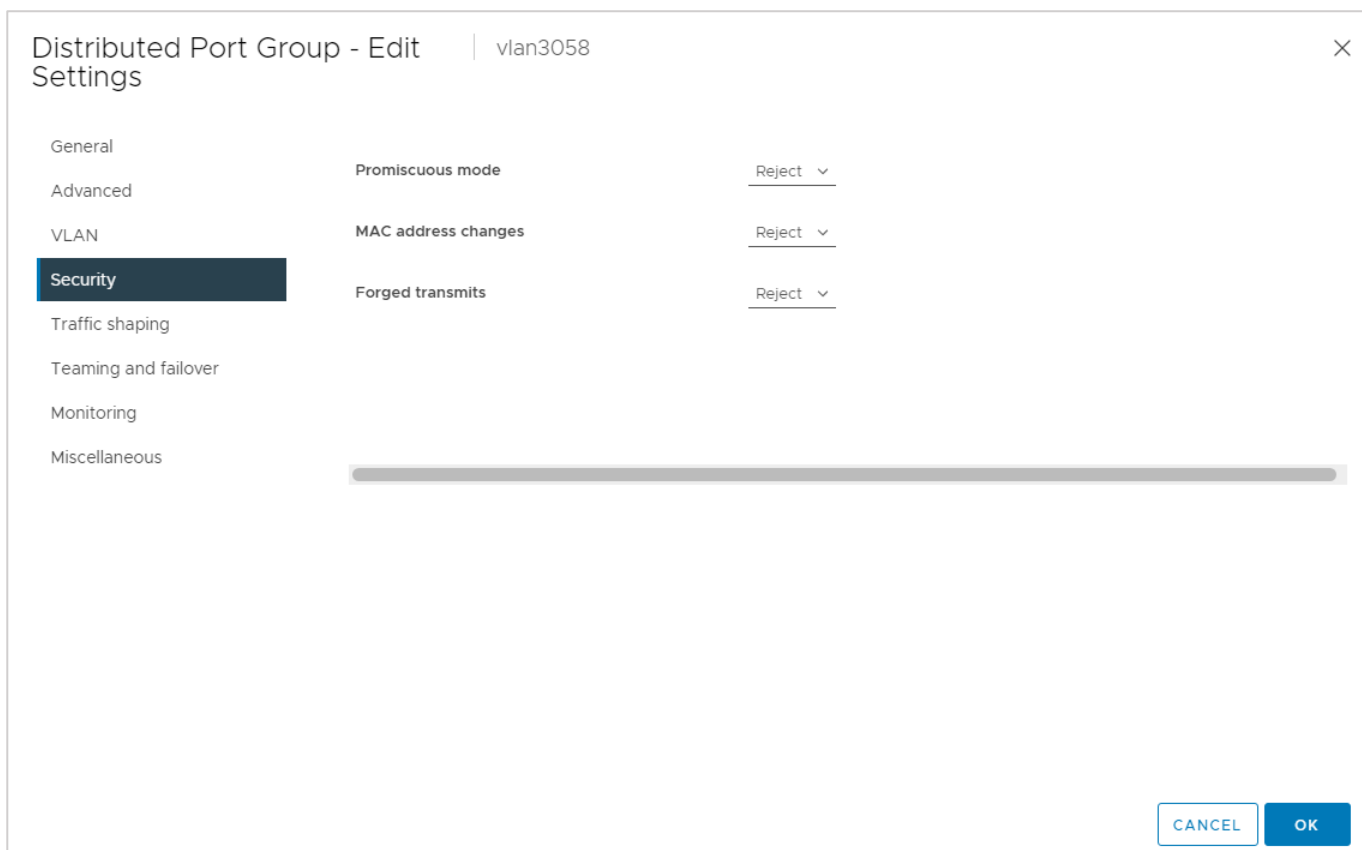


Рисунок 52

5.2.2. Создание директории для ВЦОДов клиентов

Создаем директорию, в которой будут располагаться ВЦОДы клиентов. Например, ESU3-Test, а в ней директорию Management (Рисунок 53):

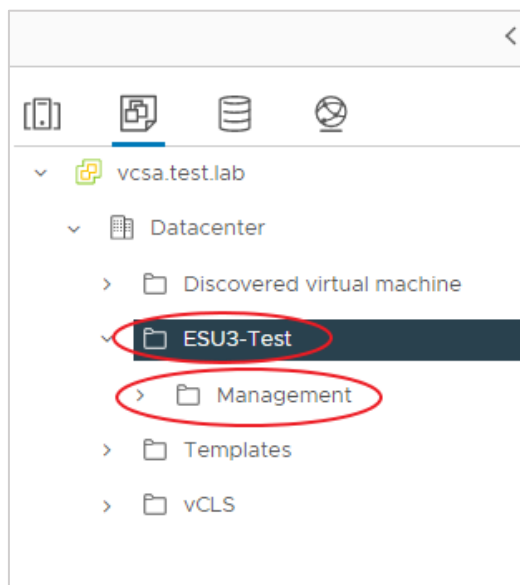


Рисунок 53

5.2.3. Настройка сетевых зон для сегмента VMware vSphere

Для создания сетевой зоны в панели управления РУСТЭК-ЕСУ переходим в меню **Инсталляция** → **Ресурсы** → **Сетевые зоны**, нажимаем кнопку **Создать сетевую зону**.

Введите название сетевой зоны, выберите сегмент VLAN и нажмите кнопку **Далее** (Рисунок 54).

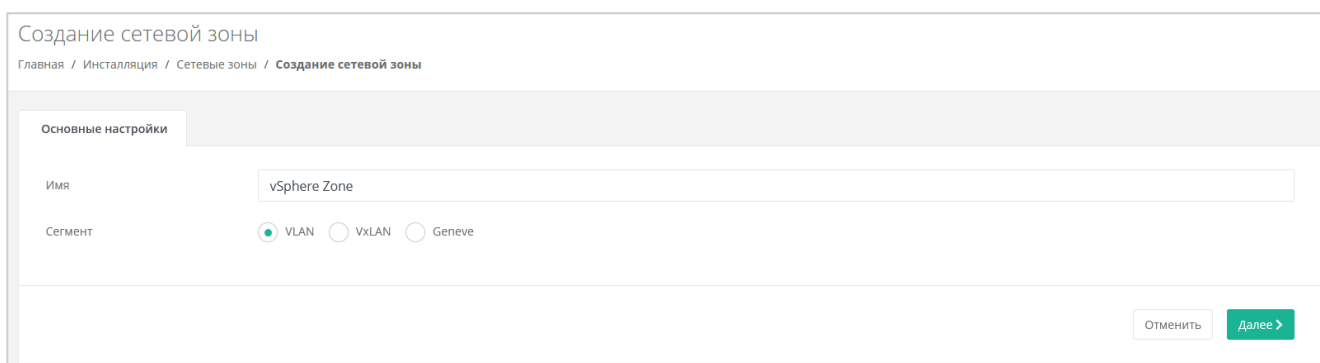


Рисунок 54

После нажатия кнопки **Далее** появится возможность добавления пулов. Необходимо указать диапазон VLAN для локальных пользовательских IP-адресов: 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 55).

Основные настройки

Имя: vSphere Zone

Сегмент: VLAN VxLAN Geneve

Пулы:

Начало диапазона	Конец диапазона	Действия
3060	3090	

+ Добавить пул

Удалить Отменить Сохранить

Рисунок 55

Аналогично создаём **вторую** сетевую зону для *внешней* сети (Рисунок 56).

VLAN 3227 будем использовать для публичных IP-адресов пользовательских ВЦОДов — устанавливаем его в начало и конец диапазона.

Основные настройки

Имя: vSphere Zone ext

Сегмент: VLAN VxLAN Geneve

Пулы:

Начало диапазона	Конец диапазона	Действия
3227	3227	

+ Добавить пул

Удалить Отменить Сохранить

Рисунок 56

Заводим внешнюю сеть для сегмента VMware vSphere.

Переходим в меню **Инсталляция** → **Ресурсы** → **Сети и IP**. Нажимаем кнопку **Создать сеть**. В открывшейся форме заполните следующие поля настроек (Рисунок 57):

- Название — любое.
- Сетевая зона — созданная ранее для внешней сети VMware-сегмента.
- VID/VNID — VLAN внешней сети: в нашем случае — 3227.
- Тип сети — внешняя.

Создание сети

Главная / Установка / Сети и IP / Создание сети

Основные настройки

Имя: ext-3227

Сетевая зона: vSphere Zone ext Выбрать

VID / VNID: 3227

Тип сети: Внешняя

Имя на платформе виртуализации: ext3227

Отменить Далее >

Рисунок 57

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

Нажимаем кнопку **Добавить подсеть**. DHCP должен быть **выключен**, CIDR необходимо указывать полный. Если нужно уменьшить диапазон выдаваемых IP-адресов, можно указать произвольный диапазон (Рисунок 58).

Добавление подсети

CIDR: 10.11.6.0/24

DHCP: Включить

Шлюз подсети: 10.11.6.1

Диапазон адресов: 10.11.6.200 (Начальный адрес) - 10.11.6.254 (Конечный адрес)

DNS серверы: Например, 8.8.8.8

Маршруты: + Добавить маршрут

Отменить Принять

Рисунок 58

5.2.4. Настройка vSphere-раннера РУСТЭК-ЕСУ

В настройках веб-интерфейса переходим в **Установка** → **Система** → **Раннеры** и конфигурируем vSphere-раннер РУСТЭК-ЕСУ (Рисунок 59). Указываем:

- IP-адрес сервера vCenter;
- имя пользователя и пароль для доступа к vCenter (учётная запись должна быть с правами администратора);

- название дата-центра – название должно соответствовать фактическому названию в vSphere (например, Datacenter, см. Рисунок 60);
- название DVSwitch, на котором будут создаваться пользовательские сети (порт-группы).

Изменение раннера

Главная / Инсталляция / Раннеры / Изменение раннера

Основные настройки

ID: default-vsphere-runner

Тип: vSphere

Callback URL: http://vsphere_runner:8010

Включен: Сняв флажок можно запретить API взаимодействовать с раннером

Название датацентра. Например: MyDatacenter: Datacenter

IP адрес хоста vCenter. Например: 10.10.10.1: 10.11.14.10

Имя пользователя для взаимодействия с vCenter: administrator@vcsa.test.lab

Пароль от vCenter: fhwsefhweshr3oi

Имя dsvswitch под которым будут создаваться сети. Например: DSwitch0: DSwitch

Рисунок 59

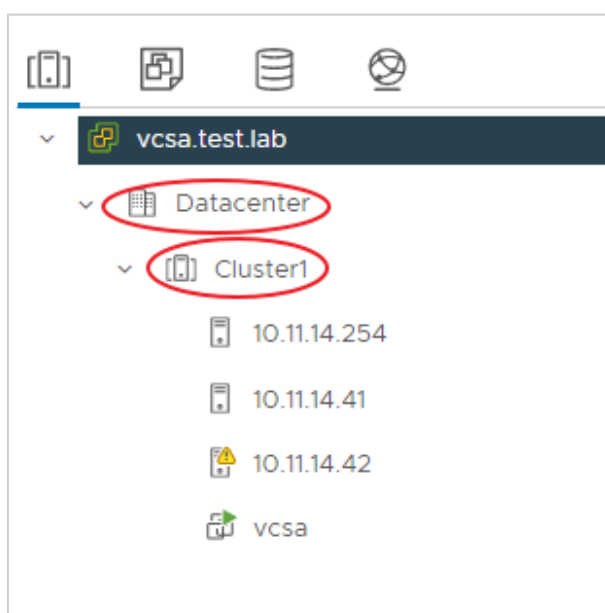


Рисунок 60

Если настройки введены правильно, индикатор vSphere-раннера должен быть зелёным (Рисунок 61).

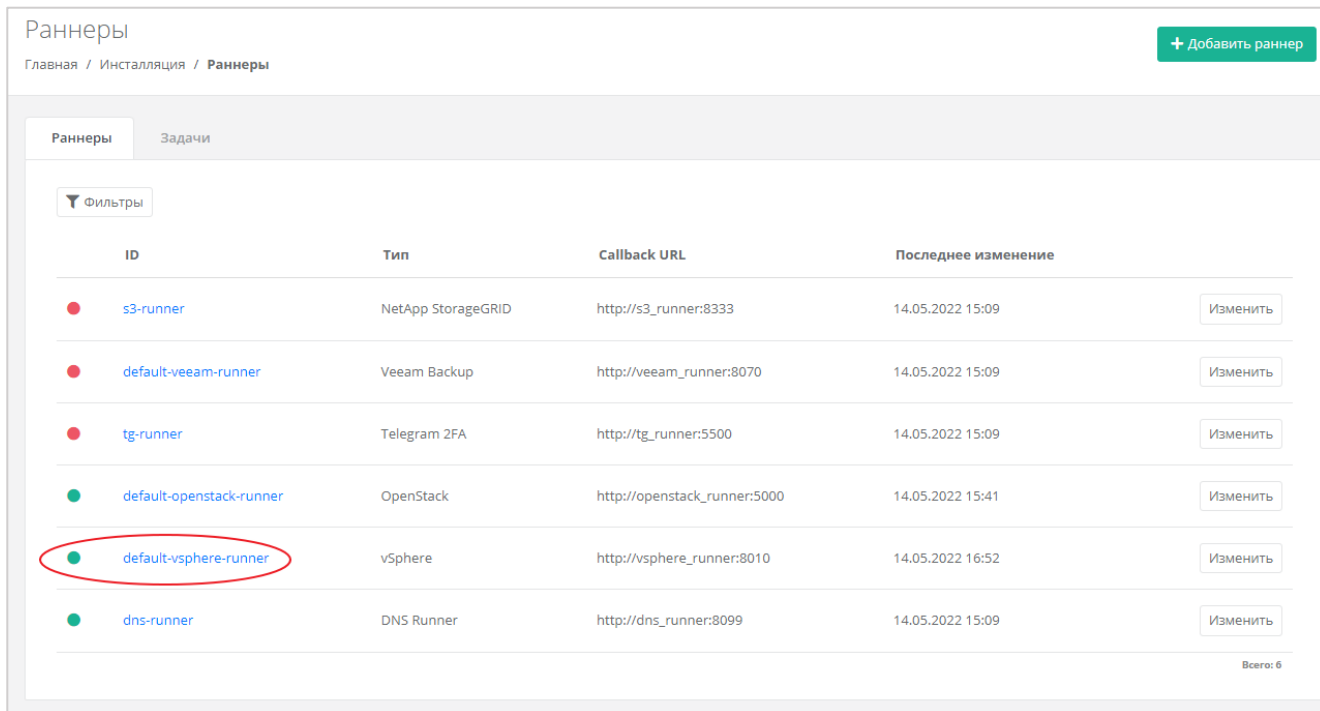


Рисунок 61

Создадим новый токен для пользователя runner – он понадобится для дальнейших настроек (Рисунок 62).

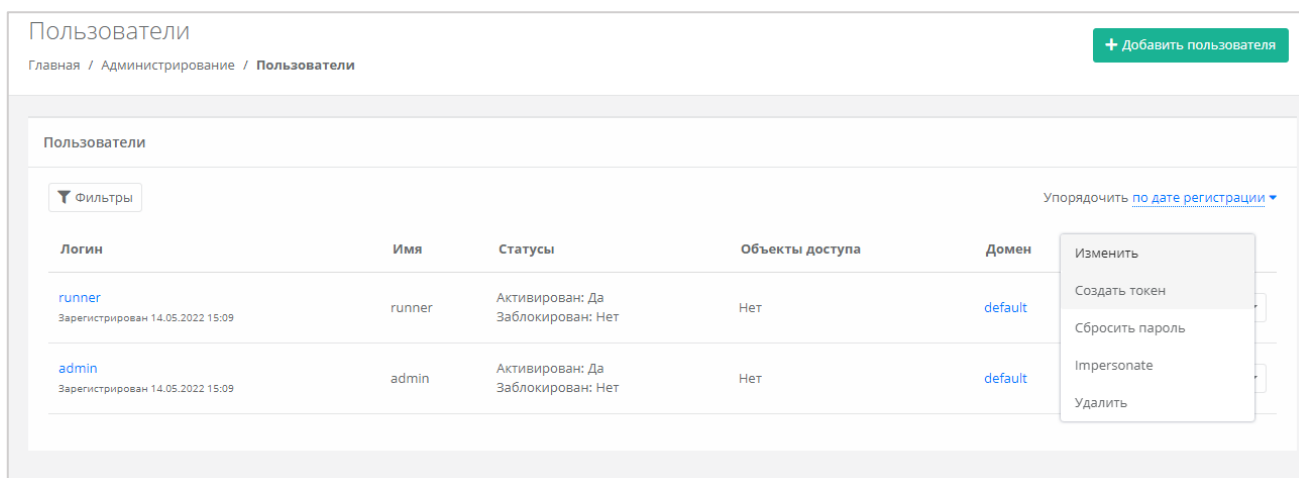


Рисунок 62

5.2.5. Настройка ресурсного пула для сегмента VMware vSphere

Далее необходимо изменить настройки ресурсного пула (Рисунок 63).

Переходим в [Инсталляция](#) → [Ресурсы](#) → [Ресурсные пулы](#).

На вкладке **Основные настройки** выбираем VMware Hypervisor.

Указываем:

- Тип – VMware.
- Раннер (в нашем случае – default-vsphere-runner).
- Сетевую зону (в нашем случае – vSphere Zone).
- Внешнюю сеть (в нашем случае ext-3227).
- Устанавливаем чек-бокс «Включен».

Изменение ресурсного пула

Главная / Установка / Ресурсные пулы / Изменение ресурсного пула

Основные настройки Профили хранения Платформы

Имя: VMware

Тип: VMware KVM

Сетевая зона: vSphere Zone Выбрать

Внешние сети: ext-3227 Выбрать

Раннеры: default-vsphere-runner Выбрать

Включен: Снимите флажок, чтобы запретить создавать ВЦОД с данным ресурсным пулом

Переподписка vCPU: 0.165
Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Переподписка RAM: 0.33
Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Рисунок 63

Далее необходимо настроить переподписку vCPU и RAM (Рисунок 64).

Изменение ресурсного пула

Главная / Установка / Ресурсные пулы / Изменение ресурсного пула

Основные настройки Профили хранения Платформы

Имя: VMware

Тип: VMware KVM

Сетевая зона: vSphere Zone Выбрать

Внешние сети: ext-3227 Выбрать

Раннеры: default-vsphere-runner Выбрать

Включен: Снимите флажок, чтобы запретить создавать ВЦОД с данным ресурсным пулом

Переподписка vCPU: 0.165
Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Переподписка RAM: 0.33
Значения от 0.03125 до 1, например 0.5 (1/2) или 0.33 (1/3)

Рисунок 64

После этого необходимо настроить ограничения по vCPU, RAM, дискам и подключениям на один сервер (Рисунок 65).

Раннеры	<input type="text" value="default-vsphere-runner"/>	<input type="button" value="Выбрать"/>
Включен	<input checked="" type="checkbox"/> Снимите флажок, чтобы запретить создавать ВЦОД с данным ресурсным пулом	
Переподписка vCPU	<input type="text" value="0.165"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>
Переподписка RAM	<input type="text" value="0.33"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>
Ограничения на один сервер		
vCPU	шт. <input type="text" value="32"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>
RAM	ГБ <input type="text" value="132"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>
Диски	шт. <input type="text" value="20"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>
Подключения	шт. <input type="text" value="7"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>
<small>Распространяется также и на роутеры</small>		

Рисунок 65

Ниже на той же странице указываем следующие настройки (Рисунок 66):

- название шаблона роутера – укажем «edge»;
- название management-сети (порт-группы), в которой работает РУСТЭК-ЕСУ;
- название служебного датастора, на котором будут размещаться пользовательские роутеры и служебные сервисы;
- адрес РУСТЭК-ЕСУ в management-сети, по которому будет доступно API;
- токен, который будет использоваться Edge-роутерами для работы с РУСТЭК-ЕСУ (был создан шагом выше).
- при необходимости можно задать логотип для ресурсного пула – кнопка «Выберите файл...» напротив поля «Иконка».

Название шаблона роутера, который будет использоваться при создании новых ВЦОД у клиентов. Например: edge-1.2.3	<input type="text" value="edge"/>
Название management сети, в которой работает ЕСУ и ее компоненты, включая пользовательские роутеры. Например: Toochka_mgmt	<input type="text" value="vlan3058"/>
Название служебного датастора, на котором будут размещаться пользовательские роутеры и служебные сервисы. Обычно этот тот же датастор, в котором размещена сама ЕСУ. Например: DS_Management	<input type="text" value="DatastoreCluster"/>
Адрес ЕСУ в management сети, по которому будет доступно API. Это значение используется при автоматическом развертывании роутеров EDGE в клиентских ВЦОДах. Например: http://192.168.20.5	<input type="text" value="http://10.11.14.111"/>
Токен, который будет использоваться роутерами EDGE при их автоматическом развертывании в клиентских ВЦОДах.	<input type="text" value="76d4cafd5482b3d383f80041a9878bede1e14ff"/>
Название директории, в которой будут расположены ВЦОДы клиентов.	<input type="text" value="ESU3-test"/>
DSN службы мониторинга Zabbix. Например: http://username:password@example.com?timeout=10	<input type="text"/>
Адрес к сервису LBaaS в K8s-инфраструктуре вида 1.2.3.4:12345	<input type="text"/>
Позиция	<input type="text" value="2"/>
Примечание	<input type="text"/>
Иконка	<input type="button" value="Выберите файл..."/>
<input type="button" value="Удалить"/> <input type="button" value="Отменить"/> <input type="button" value="Изменить"/>	

Рисунок 66

На вкладке **Профили хранения** добавляем профили хранения (Рисунок 67) – указываем имя, отображаемое название, название Storage DRS-кластера vSphere (Рисунок 68), который будет использоваться для хранения дисков VM и выбираем биллинг-класс.

Добавление профиля хранения

Имя: SSD

Имя SDRS-кластера: DatastoreCluster

Биллинг класс: Предоставление дискового пространства уровня SSD (...)

Макс. размер диска: ГБ 32768

Позиция: 1

Пользователь не сможет создать диск больше указанного размера. Для дисков большего размера (уже существующих или создаваемых административно) будет отключен функционал снимков.

Отменить Принять

Рисунок 67

DatastoreCluster

Summary Monitor Configure Permissions Hosts VMs Datastores

Total Datastores: 1
Total VMDKs: 18
Snapshots: 0
Type: VMFS

Datastore Cluster Resources

Datastore Cluster Consumers

Custom Attributes

Attribute	Value
-----------	-------

No items to display

Edit...

Storage DRS

Storage DRS automation
I/O metrics
Space threshold
I/O latency threshold
Storage DRS recommendations
Storage DRS faults

Tags

Assigned Tag	Color
--------------	-------

Assign... Remove...

Рисунок 68

Далее переходим на вкладку **Платформы** (Рисунок 63) и нажимаем кнопку **Добавить платформу**, в открывшемся окне указываем имя созданного кластера – в нашем примере **Cluster1** (Рисунок 69).

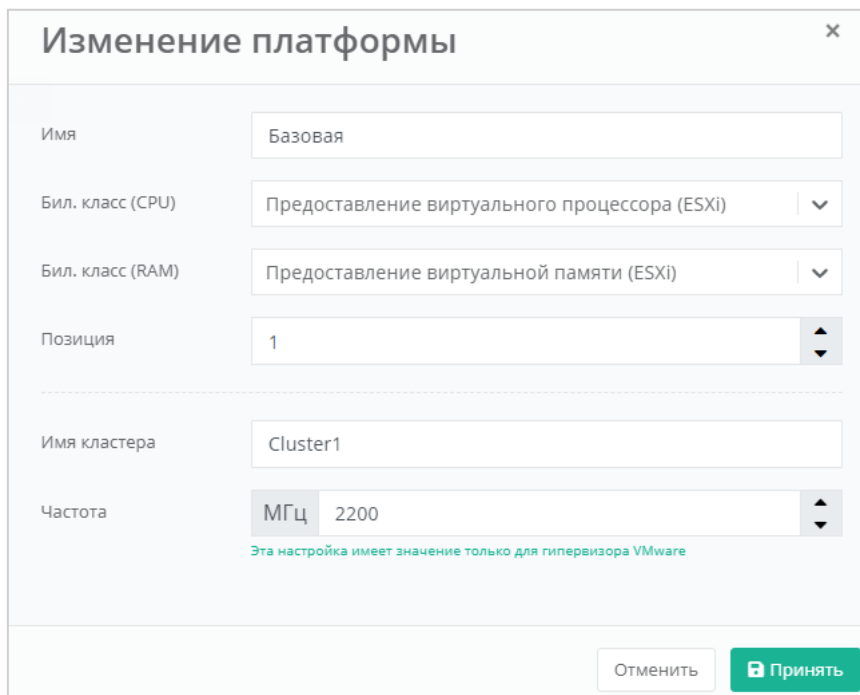


Рисунок 69

После того, как введены все настройки, в форме изменения ресурсного пула нажимаем кнопку **Принять**.

5.2.6. Развёртывание Edge-роутера

Теперь, когда vSphere runner и ресурсный пул настроены, необходимо произвести развёртывание Edge-роутера. Развёртывание будет произведено на все ресурсные пулы VMware, настроенные в системе.

Для развёртывания необходимо зайти по SSH на ESU-box (стандартная УЗ deploy:1-qpALzm/), посмотреть, какая последняя версия роутера доступна в данной версии (`ls -lah | grep edge*.ova`) и выполнить команду:

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

где **x.x.x** — последняя доступная версия.

!!!Важно!!! В целях безопасности настоятельно рекомендуем изменить логин и пароль учётной записи после настройки.

Инструмент `toochkactl` произведёт заливку и развёртывание шаблона роутера (в формате `.ova`) на ресурсных пулах (Рисунок 70).

```

deploy@localhost:~$ toochkactl edge-deploy --filename edge-1.2.7.ova
├
Toochka

config file: /opt/box/toochka.conf
Upload EDGE template...
sudo: unable to resolve host localhost: Name or service not known
[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 [deploy_edge : Deploy EDGE] *****
*****
[WARNING]: Skipping plugin (/usr/local/lib/python3.7/dist-packages/ansible/plugins/filter/core.py) as it seems to be invalid: cannot
import name 'environmentfilter' from 'jinja2.filters'
(/usr/local/lib/python3.7/dist-packages/jinja2/filters.py)
[WARNING]: Skipping plugin (/usr/local/lib/python3.7/dist-packages/ansible/plugins/filter/mathstuff.py) as it seems to be invalid: c
annot import name 'environmentfilter' from 'jinja2.filters'
(/usr/local/lib/python3.7/dist-packages/jinja2/filters.py)
changed: [localhost -> localhost]

PLAY RECAP *****
*****
localhost                : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

deploy@localhost:~$

```

Рисунок 70

Обратите внимание, что силу особенностей развёртывания шаблона у вас должна быть стандартная портгруппа с названием «VM Network».

После завершения развёртывания на vSphere появится выключенная VM с названием «edge-x.x.x», а в настройках ресурсного пула вместо «edge» будет прописана актуальная версия роутера (Рисунок 71).

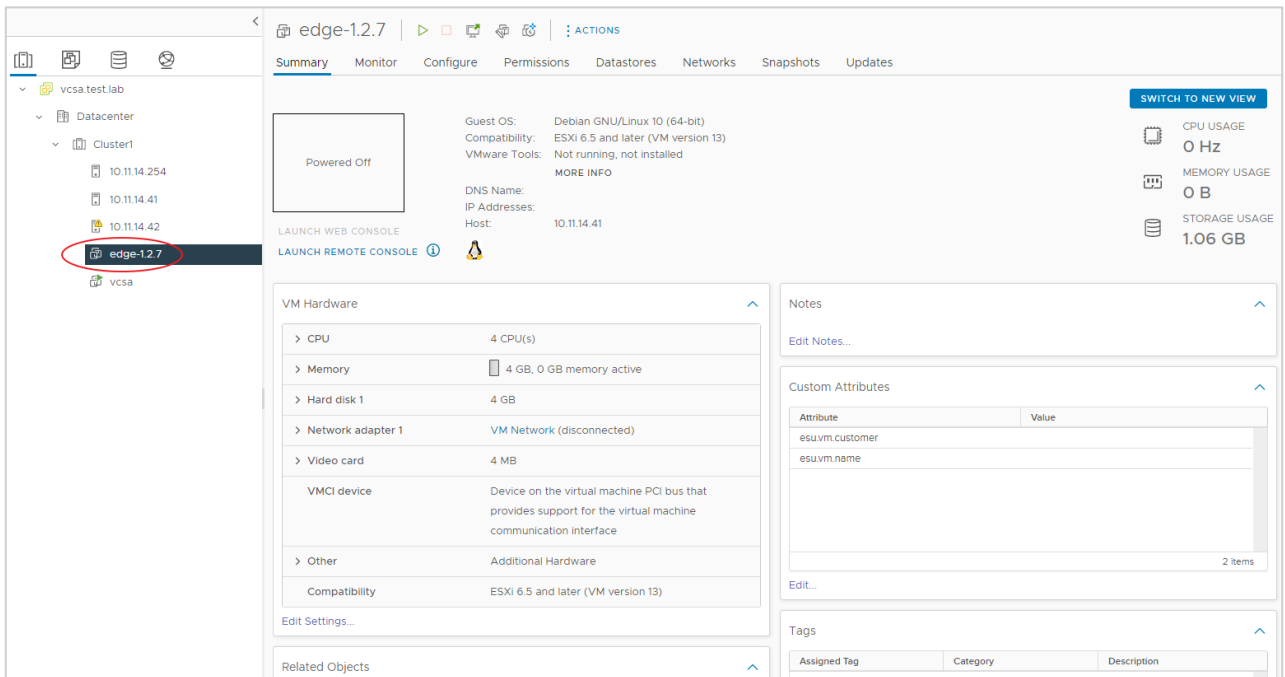


Рисунок 71

После этого Система будет готова к созданию ВЦОД в сегменте VMware.

5.2.7. Создание шаблонов VM для сегмента VMware vSphere

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

Далее будет рассмотрен пример создания шаблона VM 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>

Заходим в vSphere Client (Рисунок 72) и в целевом дата-центре производим развёртывание .ova-шаблона.

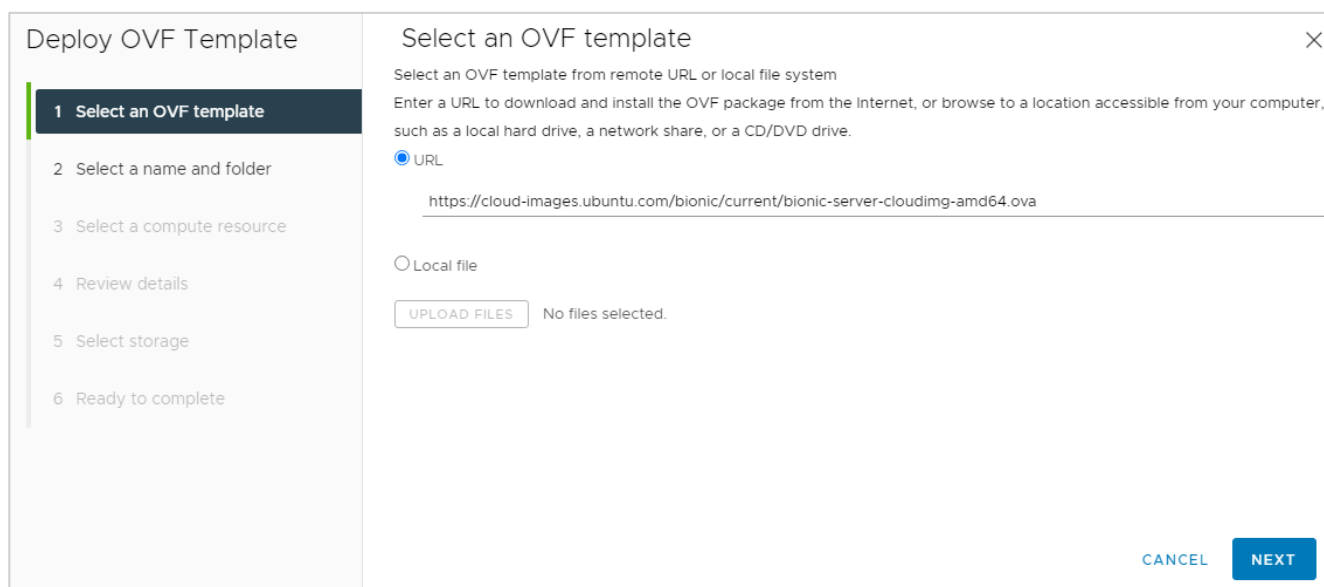


Рисунок 72

Далее в мастере деплоя (Рисунок 73 – Рисунок 78) необходимо указать имя создаваемой VM, кластер, на котором она будет развёрнута, хранилище, на котором будет лежать VM (при указании типа диска нужно указать «**Thin provision**»).

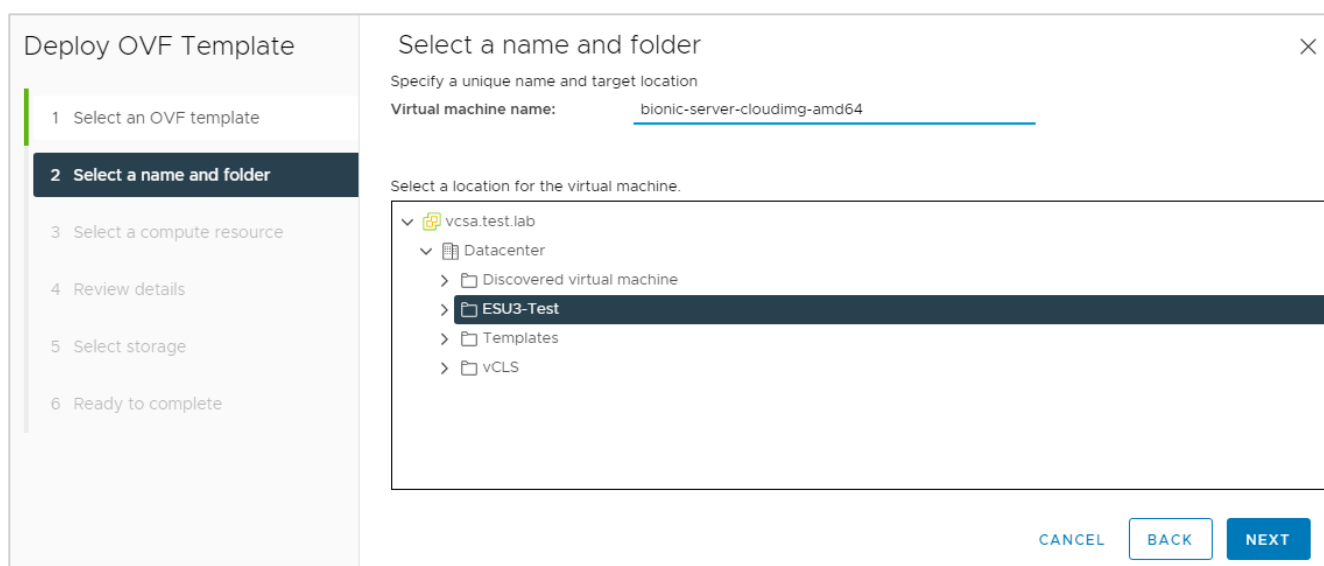


Рисунок 73

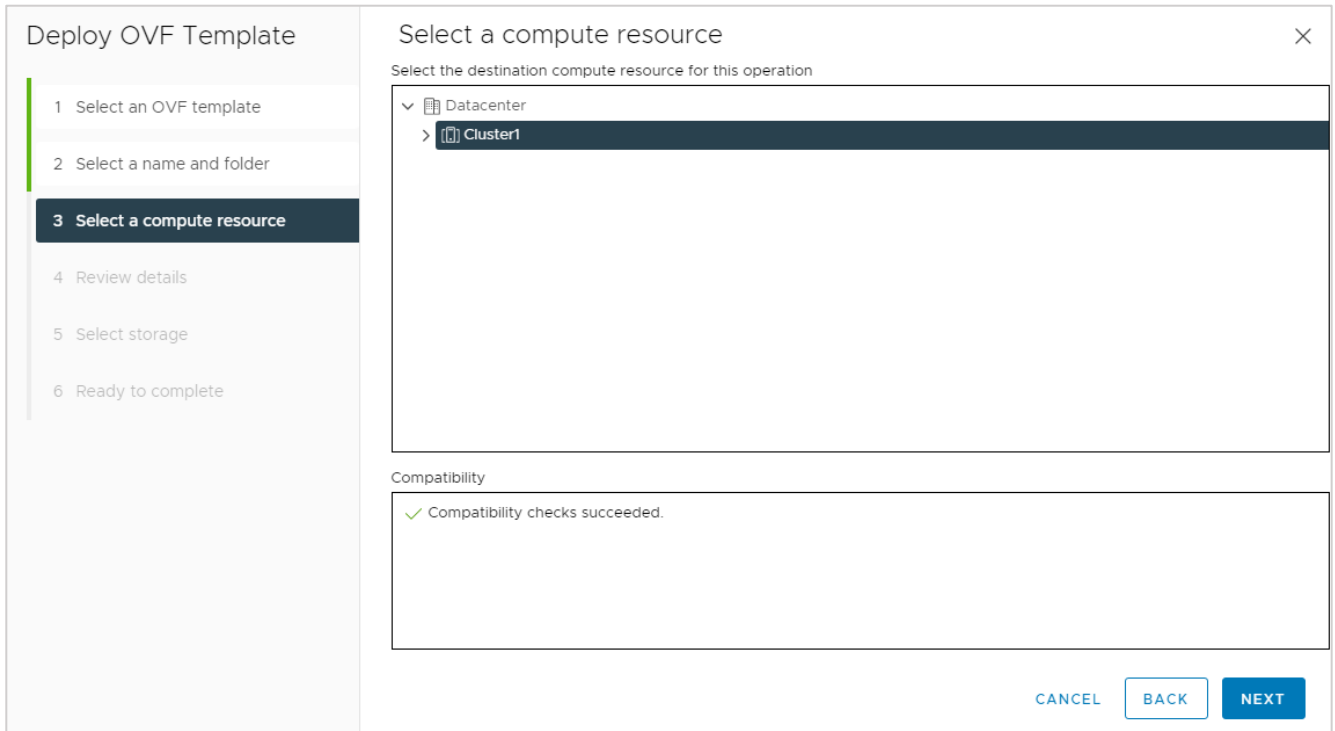


Рисунок 74

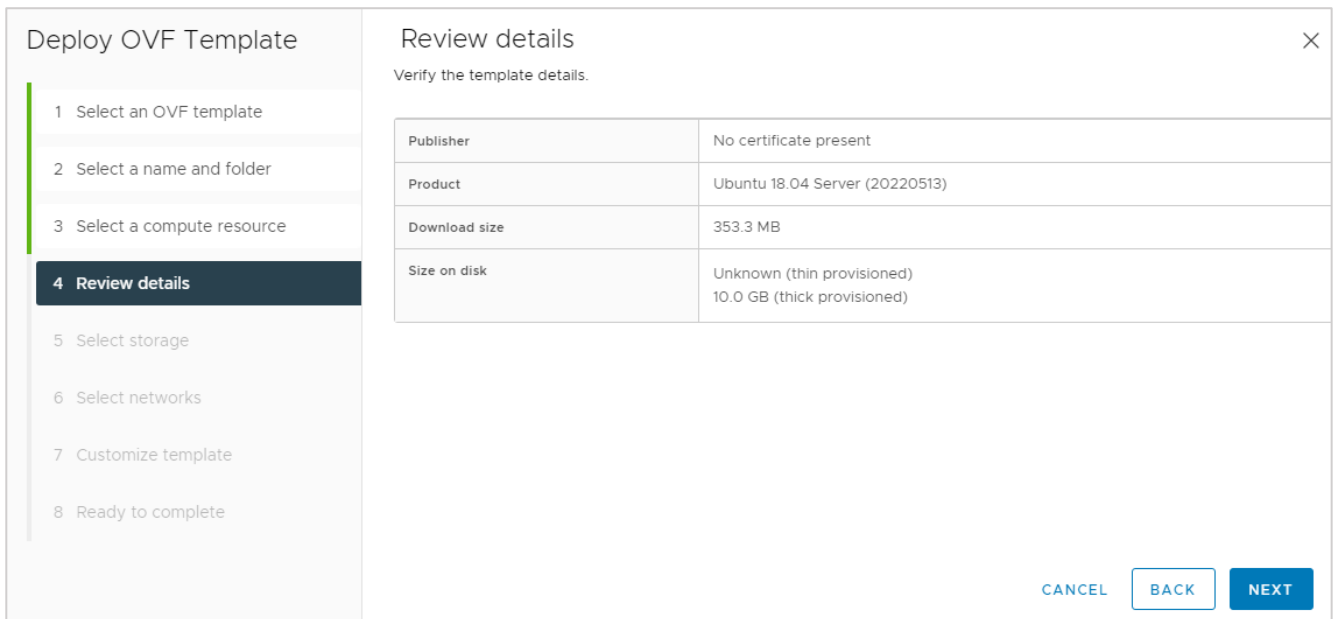


Рисунок 75

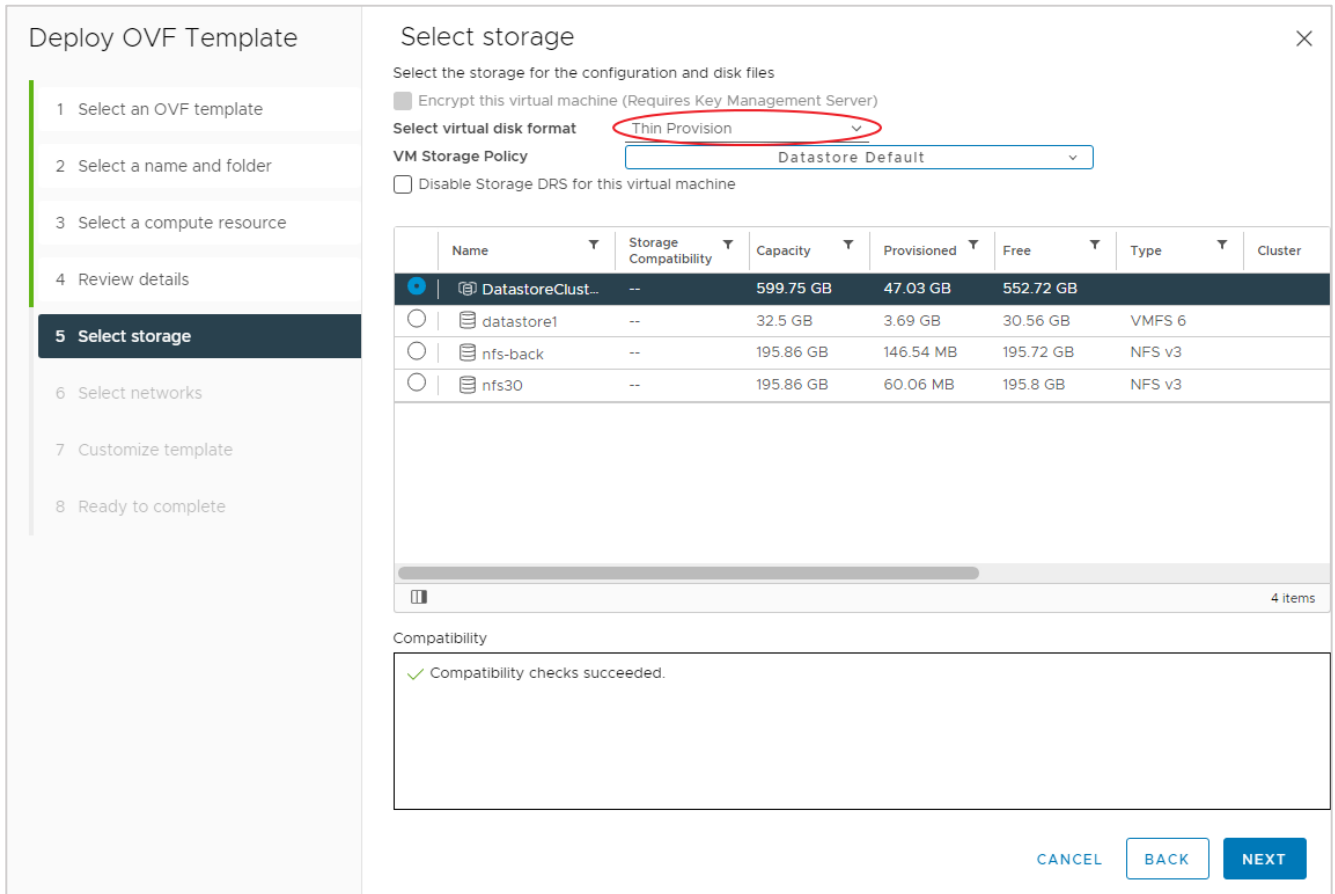


Рисунок 76

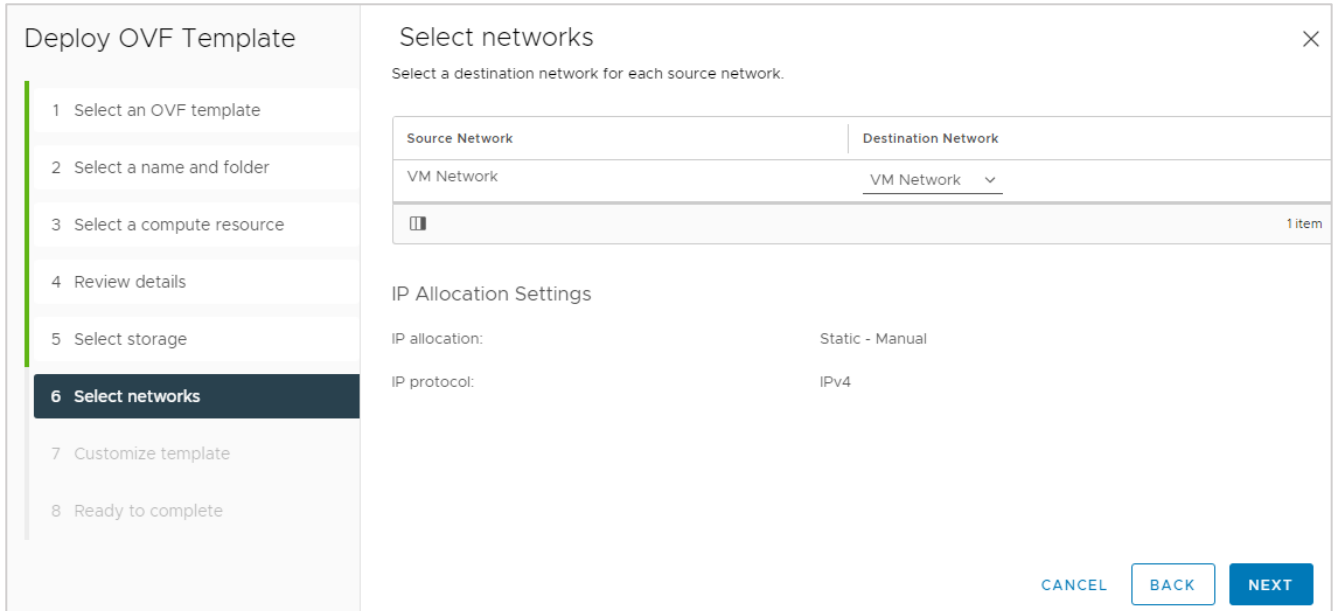


Рисунок 77

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 78

Дожидаемся завершения развёртывания .ova-шаблона. Ставим пароль на свое усмотрение (Рисунок 79).

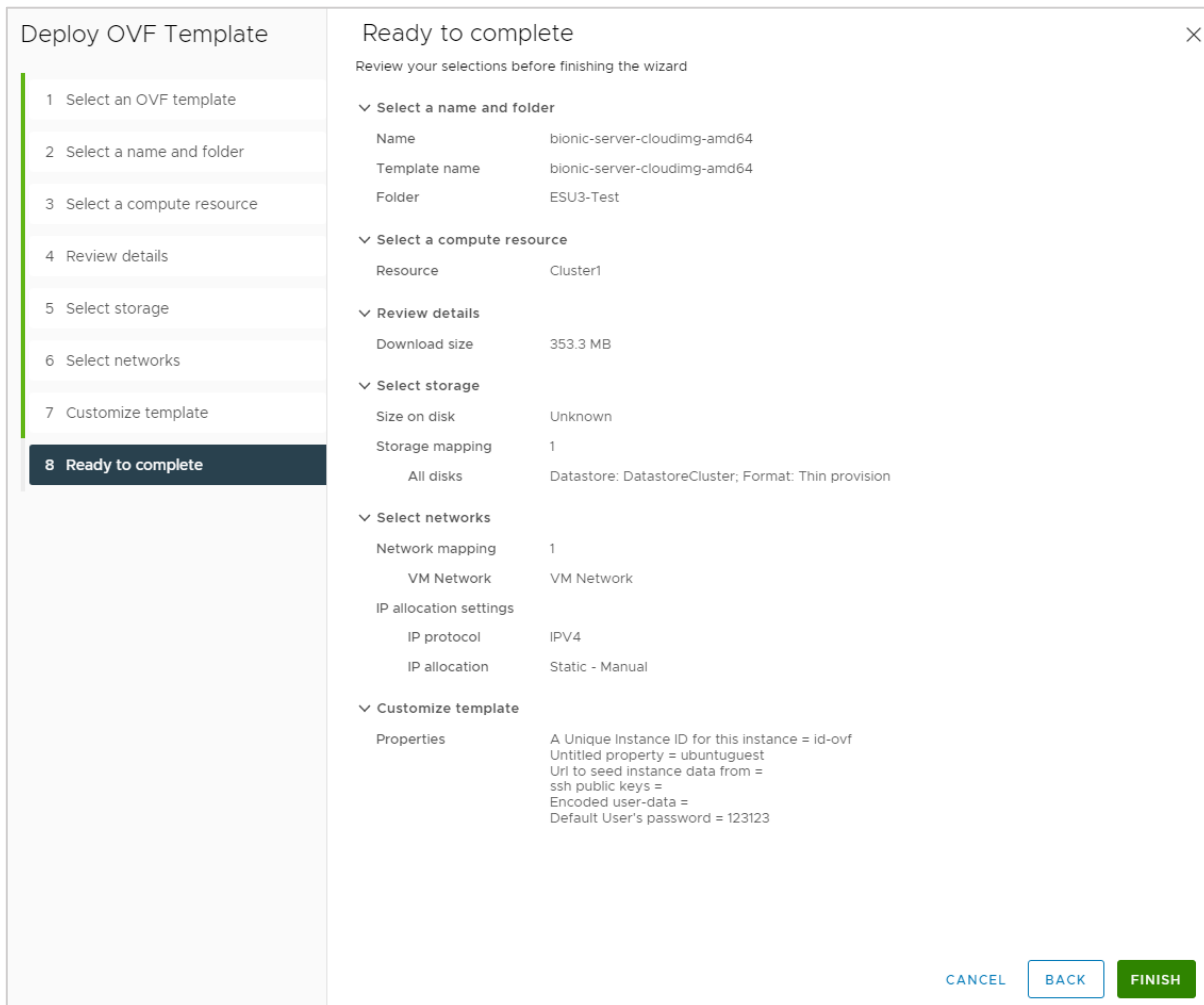


Рисунок 79

Далее необходимо отредактировать настройки ВМ (Рисунок 80) – выставляем необходимый нам тип SCSI-контроллера (VMware Paravirtual), удаляем сетевой адаптер, указываем для CD-ROM IDE 0:0 и проверяем у Hard Disk type Thin Provision.

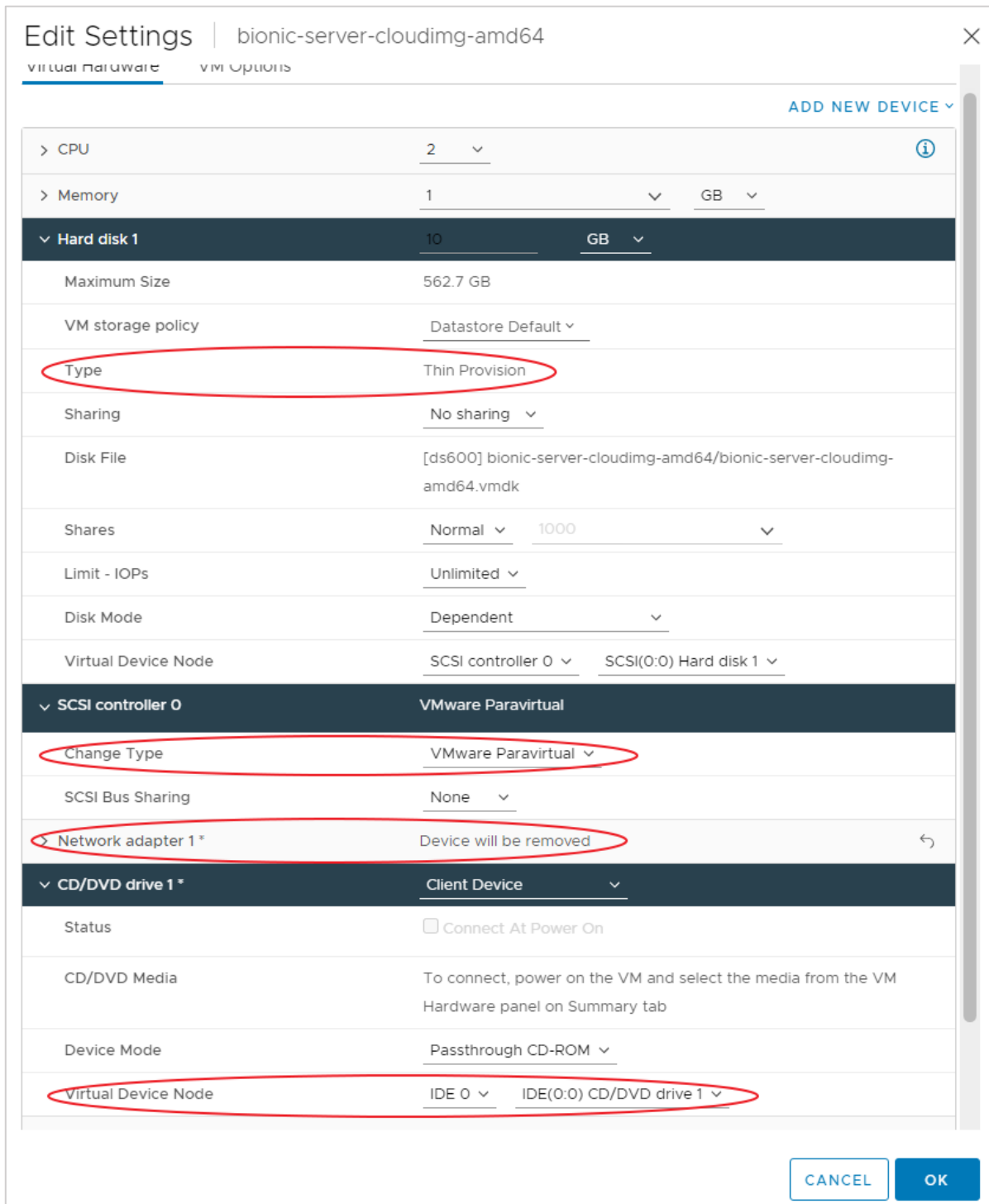


Рисунок 80

Запускаем получившуюся ВМ. Вводим установленный пароль (пользователь ubuntu), входим в систему. Потребуется сменить пароль. Меняем на любой.

Затем:

- изменяем файл cloud.cfg;

Cloud-init config может находиться в двух местах:

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

- закомментируем секцию users:

- внизу допишем секцию datasource (Рисунок 81);

```
datasource:
  Ec2:
    strict_id: false
    timeout: 10
    max_wait: 20
    metadata_urls:
      - http://169.254.169.254:80
```

Рисунок 81

- запустим команду `sudo dpkg-reconfigure cloud-init`. Запуск команды открывает интерфейс, в котором можно включить/отключить секции datasource;
- отключим всё, оставим EC2 (Рисунок 82):

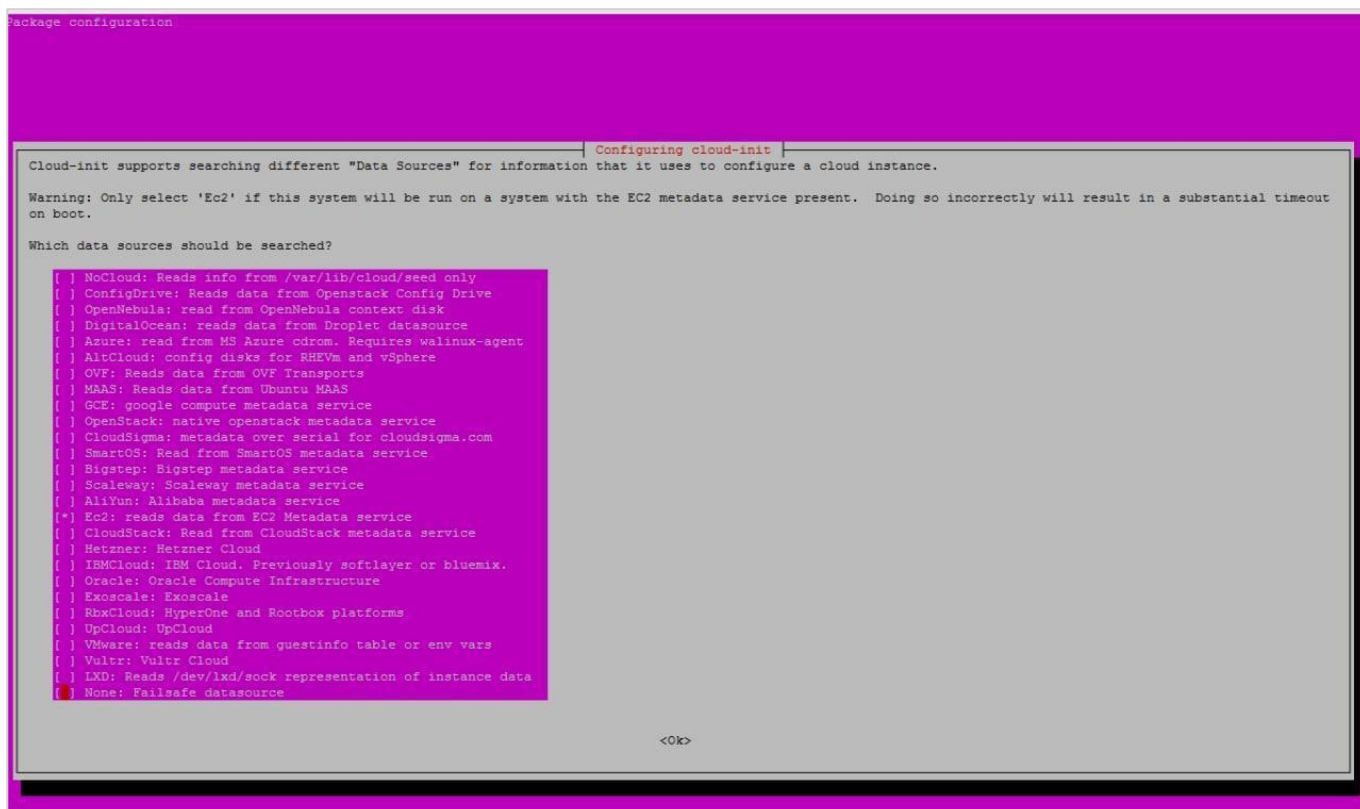


Рисунок 82

- выполняем команду `sudo cloud-init clean`;
- выполняем команду `sudo userdel -f ubuntu`;
- отключаем VM.

Конвертируем VM в шаблон (Рисунок 83).

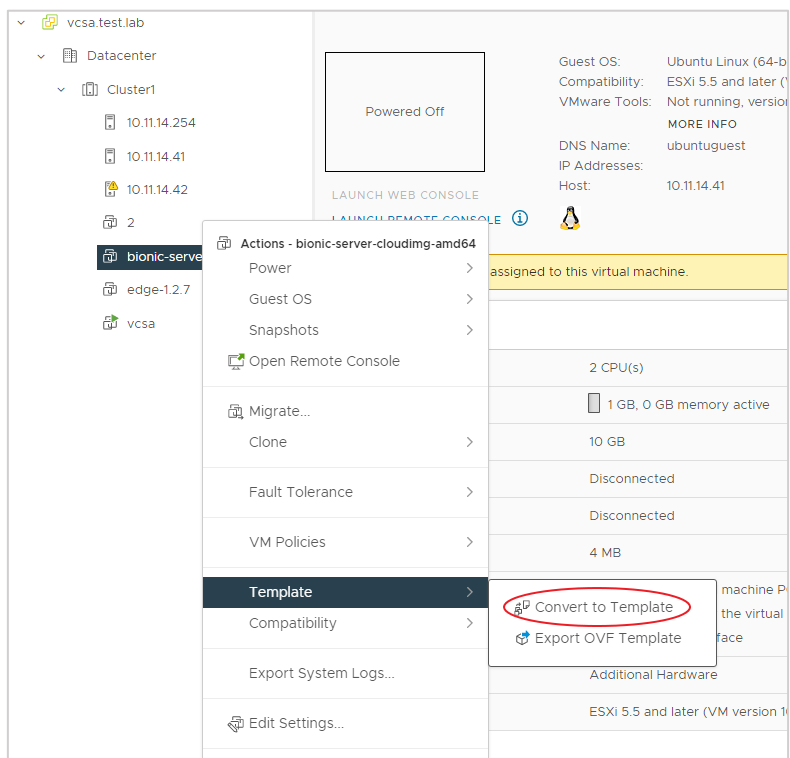


Рисунок 83

После этого необходимо завести шаблон в РУСТЭК-ЕСУ (Рисунок 84 – Рисунок 86). Процедура аналогична заведению шаблона для KVM-сегмента (см. раздел 5.1.4), необходимо только выбрать другой сегмент (VMware) и другой ID шаблона (выбрать созданный на предыдущих шагах шаблон из списка).

Создание шаблона

Главная / Установка / Серверы / **Создание шаблона**

Основные настройки | Дополнительные

Доступен для VMware KVM

Имя

Группа шаблонов Выбрать

Включен Снимите флажок, чтобы шаблон не показывался в витрине

Windows лицензия Если флажок установлен, с пользователя будет списываться стоимость лицензии Windows

Имя шаблона

- Один и тот же образ (шаблон) должен одновременно присутствовать на всех гипервизорах этого типа!
- vSphere: шаблон должен иметь уникальное название и быть шаблоном (без сетей, снапшотов, LSI Logic SCSI, один диск на scsi 0:0)

 Выбрать

Рекомендации до деплоя

Рекомендации после деплоя

Иконка ✕

Отменить Далее >

Рисунок 84

Изменение шаблона

Главная / Установка / Серверы / **Изменение шаблона**

Основные настройки | **Дополнительные** | Поля для скрипта | Скрипт развертывания | Auto DevOps

Доступен партнерам Выбрать

Доступен клиентам Выбрать

Позиция ▲▼

Минимальная конфигурация

CPU ▲▼

RAM ▲▼

HDD ▲▼

Удалить Отменить Применить Применить и вернуться

Рисунок 85

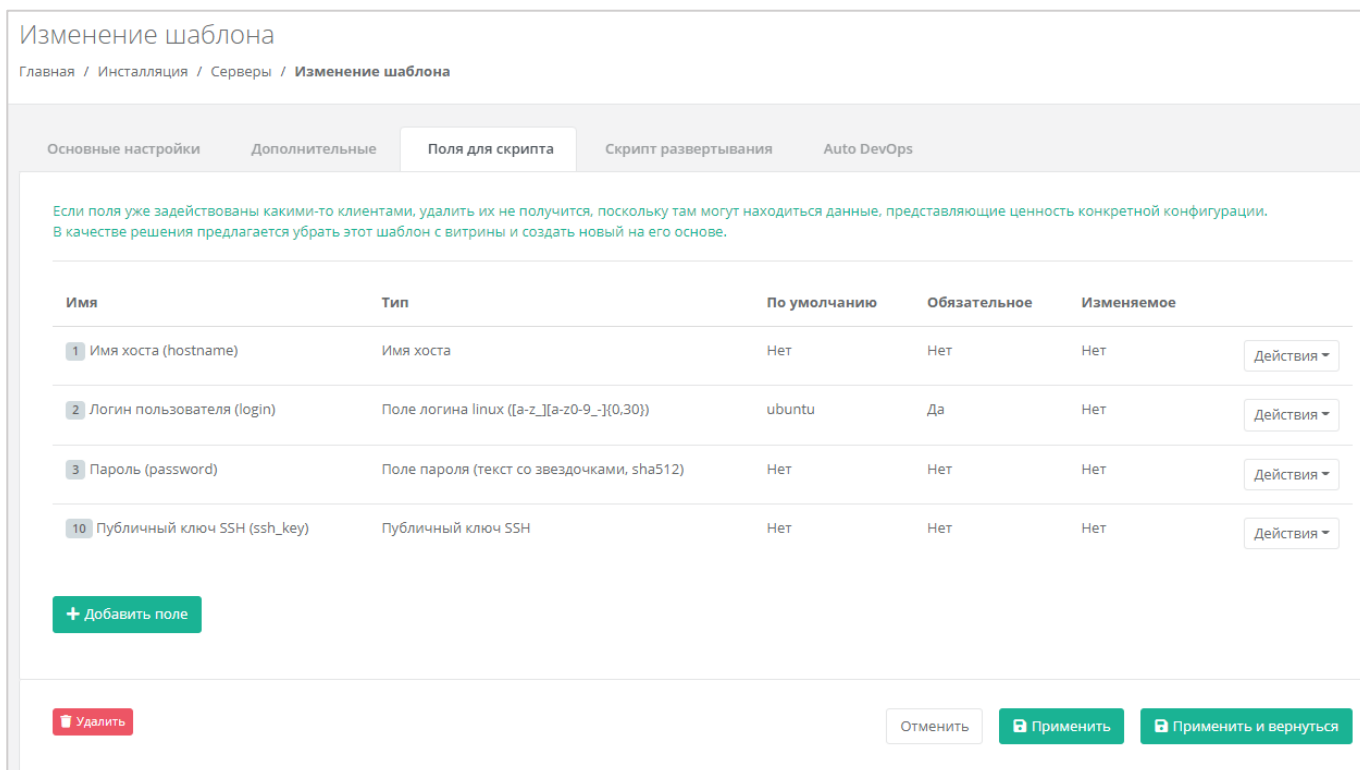


Рисунок 86

Далее во вкладке **Скрипт развёртывания** необходимо добавить 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 9.4.

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.

!!!Важно!!! 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 VM появится в списке шаблонов и из него можно будет создавать VM.

6. Добавление ресурсных пулов партнёру

После того как ресурсные пулы для обоих сегментов были настроены их необходимо добавить партнёру.

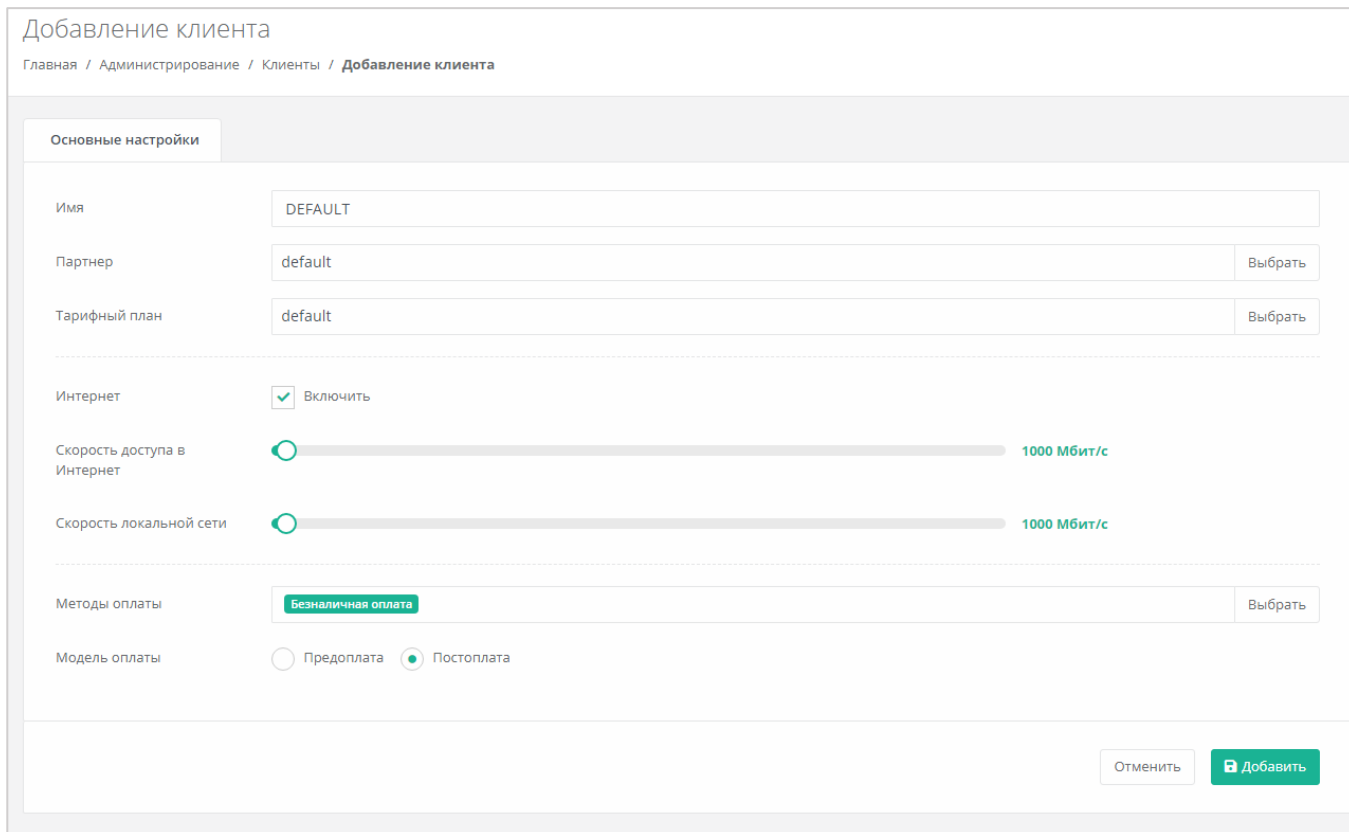
Переходим в **Администрирование** → **Партнёры**. Выбираем созданного партнёра, переходим на вкладку **Основные настройки**. В поле «Ресурсные пулы» выбираем необходимый ресурсный пул (Рисунок 87).

Рисунок 87

Для сохранения настроек нажимаем кнопку **Изменить**.

7. Создание ВЦОДов в сегментах

Теперь можно создать первые ВЦОДы в сегментах для проверки работоспособности Системы. Сначала в меню **Администрирование** → **Клиенты**, потребуется создать клиента (Рисунок 88).



The screenshot shows the 'Добавление клиента' (Add client) form. At the top, there is a breadcrumb trail: Главная / Администрирование / Клиенты / Добавление клиента. The form is divided into sections. The first section, 'Основные настройки' (Basic settings), includes fields for 'Имя' (Name) with the value 'DEFAULT', 'Партнер' (Partner) with 'default' and a 'Выбрать' (Select) button, and 'Тарифный план' (Tariff plan) with 'default' and a 'Выбрать' (Select) button. The second section, 'Интернет' (Internet), has a checked checkbox for 'Включить' (Enable), and two sliders for 'Скорость доступа в Интернет' (Internet access speed) and 'Скорость локальной сети' (Local network speed), both set to 1000 Мбит/с. The third section, 'Методы оплаты' (Payment methods), has a dropdown menu set to 'Безналичная оплата' (Cashless payment) with a 'Выбрать' (Select) button. The fourth section, 'Модель оплаты' (Payment model), has radio buttons for 'Предоплата' (Prepayment) and 'Постоплата' (Postpayment), with 'Постоплата' selected. At the bottom right, there are 'Отменить' (Cancel) and 'Добавить' (Add) buttons.

Рисунок 88

В горизонтальном меню нажимаем кнопку **Создать проект** (Рисунок 89) и создаём первый проект (Рисунок 90).

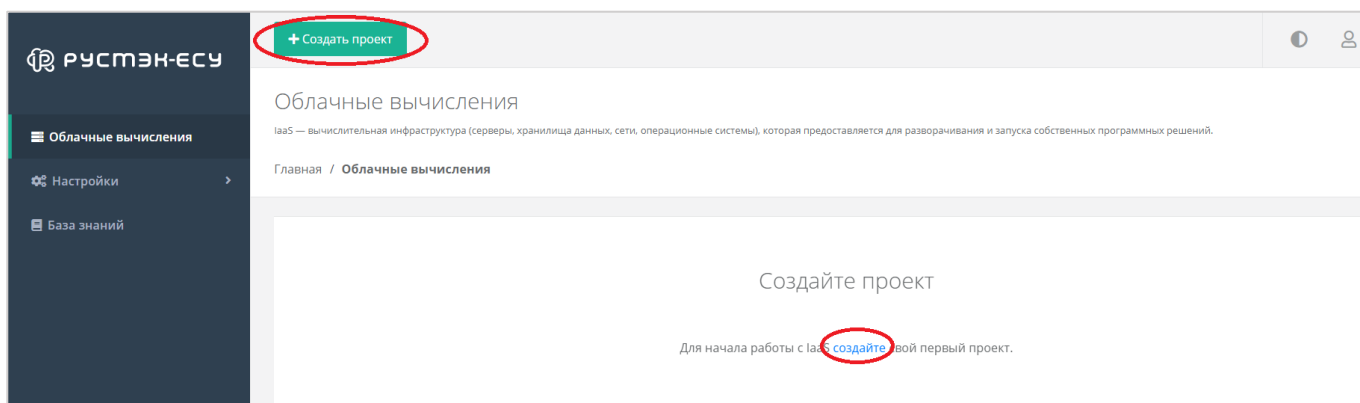


Рисунок 89

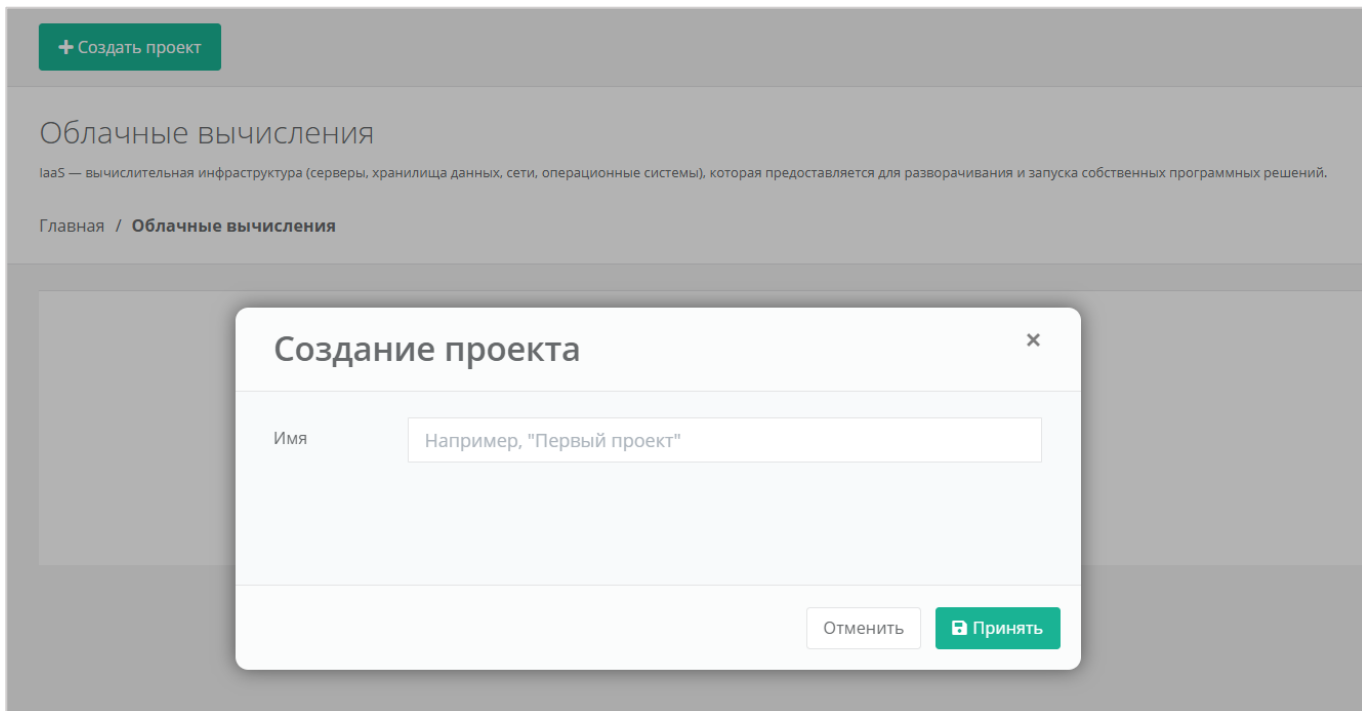


Рисунок 90

Далее переходим в раздел меню **Облачные вычисления** и активируем один из ВЦОДов, например VMware (Рисунок 91).

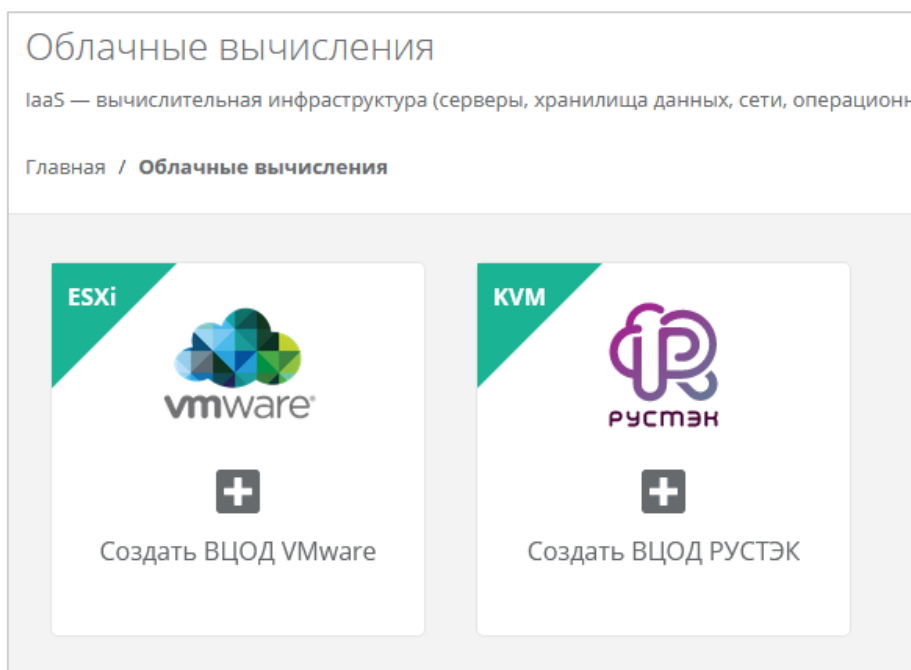


Рисунок 91

После некоторого времени ВЦОД будет готов и иметь статус «работает». В нем можно будет создать виртуальную машину (Рисунок 92).

В нашем примере создано по одному ВЦОД в каждом сегменте (VMware и РУСТЭК).

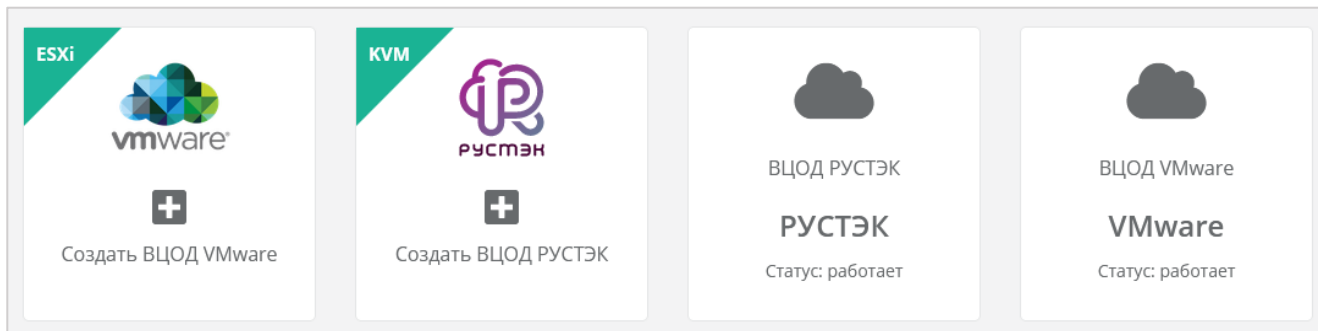


Рисунок 92

8. Настройка РУСТЭК-ЕСУ для работы с кластерами Kubernetes

8.1. Создание шаблонов Kubernetes для сегмента VMware vSphere

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

Сначала необходимо скачать подготовленные нашей командой шаблоны в архивах.

Master-нода:

<https://ncl.sbcloud.ru/s/EtYnDbQgoe2xPMF/download/k8s-1.22.1.master.zip>

Нода:

<https://ncl.sbcloud.ru/s/HHQwGfJQso3M7ZR/download/k8s-1.22.1.node.zip>

Распаковываем архивы.

Заходим в панель управления VMware vSphere. В панель управления необходимо загрузить распакованные образы. Для этого выбираем директорию, в которую будут загружены образы, в нашем случае это ESU3-Test, кликаем по ней правой кнопкой мыши и выбираем «Deploy OVF Template» (Рисунок 93).

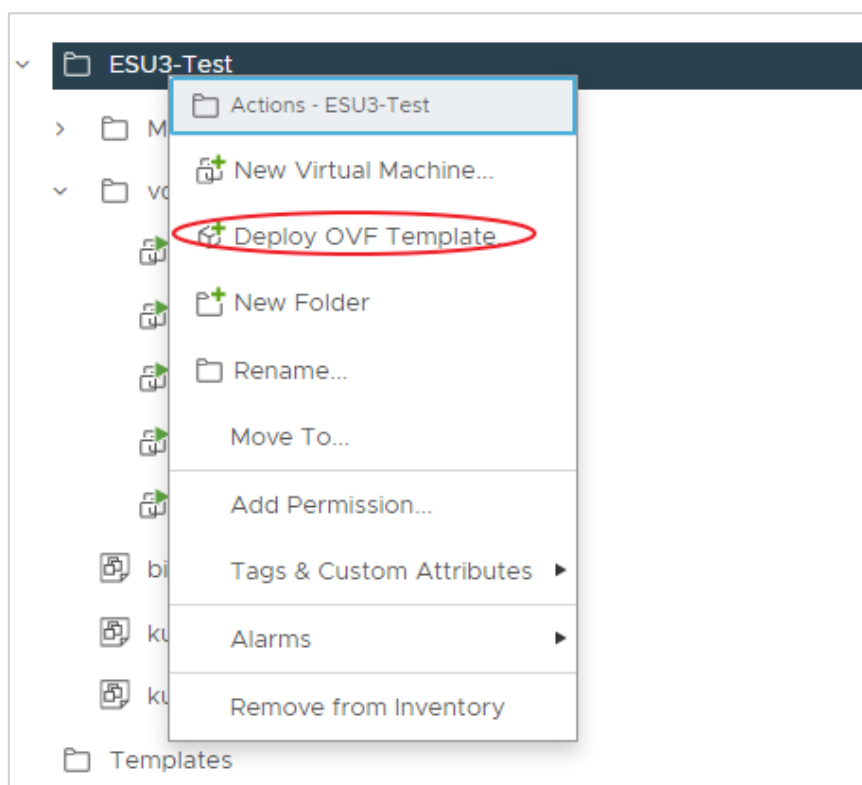


Рисунок 93

Далее выбираем загрузку файла с локального компьютера (Рисунок 94).

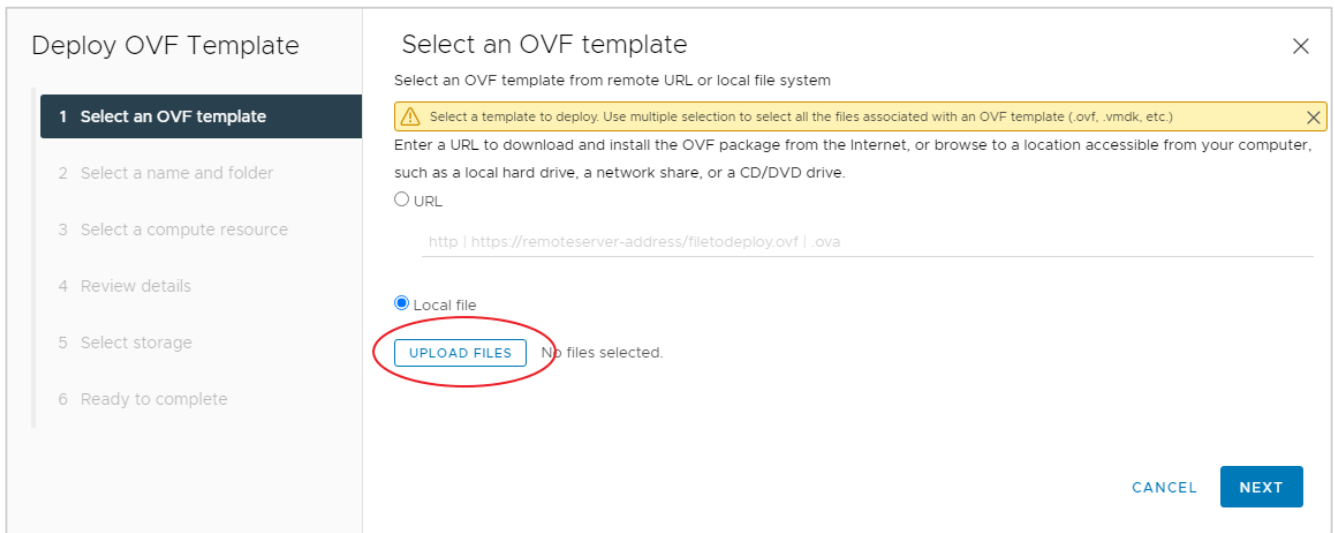


Рисунок 94

В открывшемся окне выбираем файлы нашего образа. После выбора файлов нажмём кнопку «Next» (Рисунок 95).

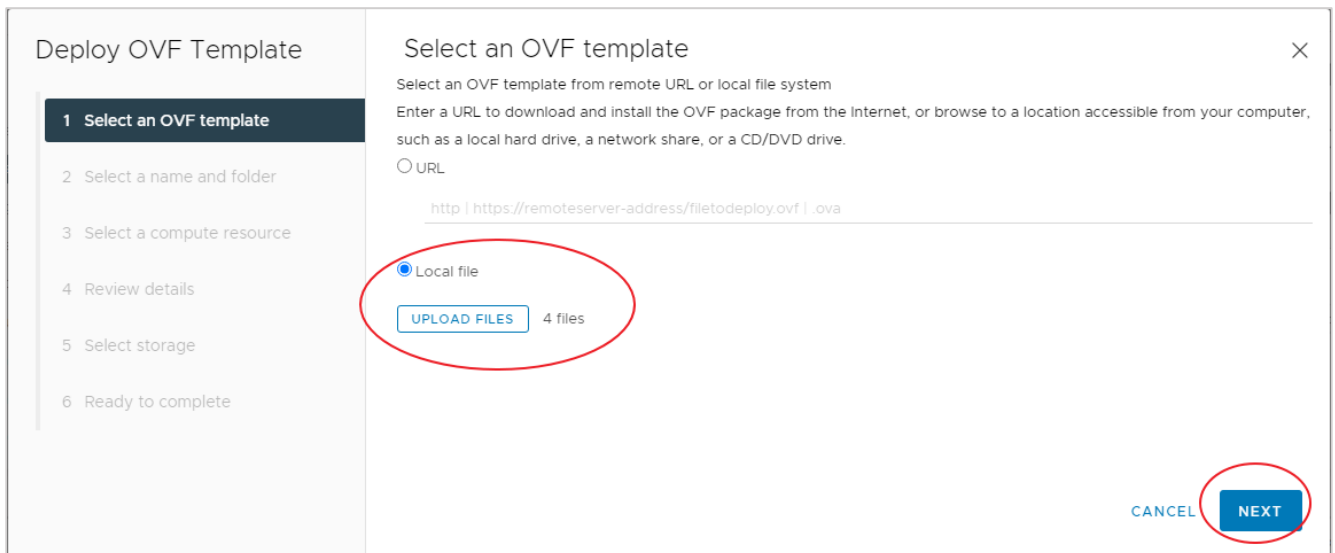


Рисунок 95

Выберем название шаблона и папку для хранения (Рисунок 96).

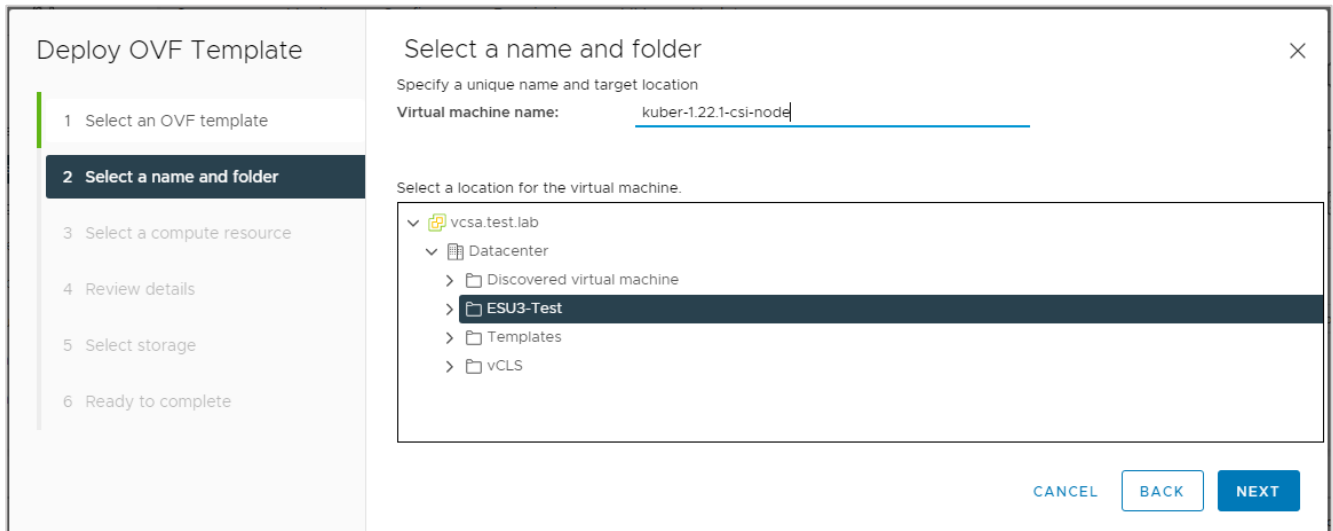


Рисунок 96

Выберем кластер, где будет храниться шаблон и нажимаем «NEXT» (Рисунок 97).

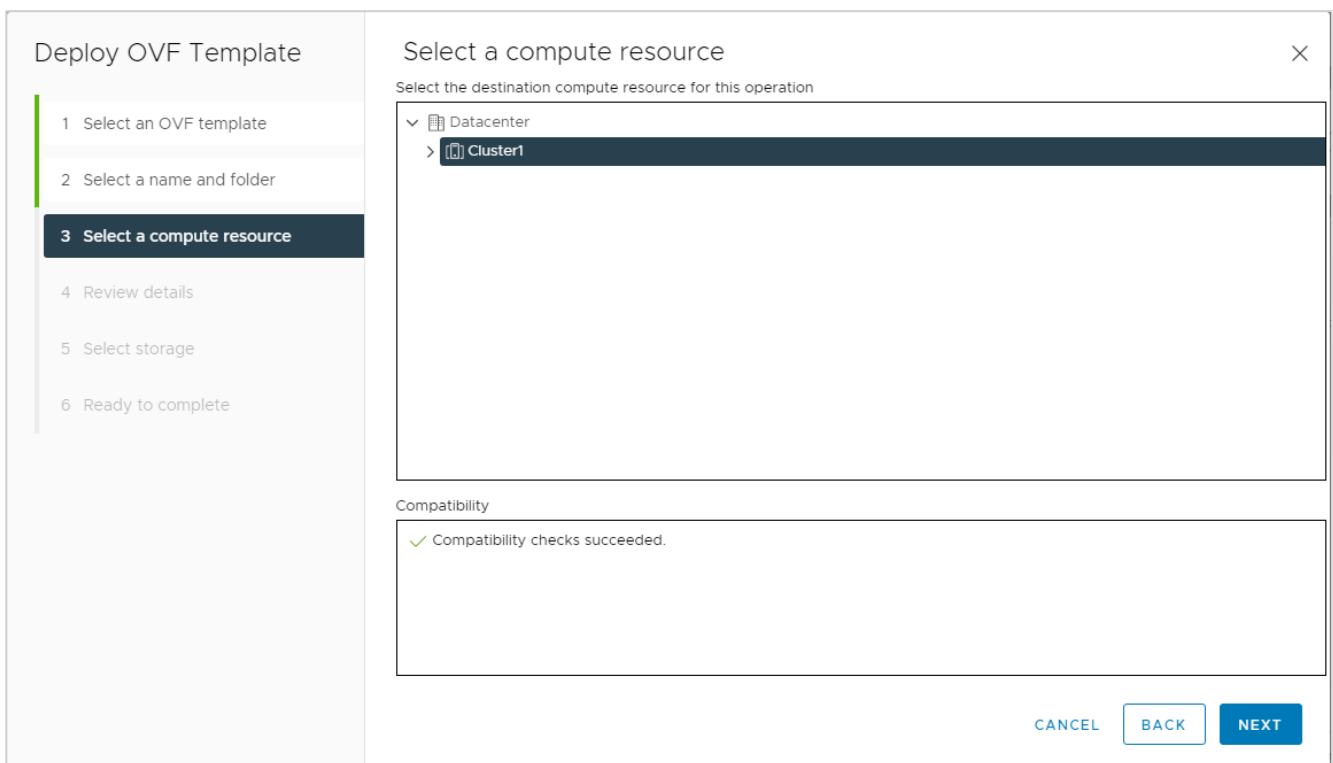


Рисунок 97

Нажимаем «NEXT» (Рисунок 98).

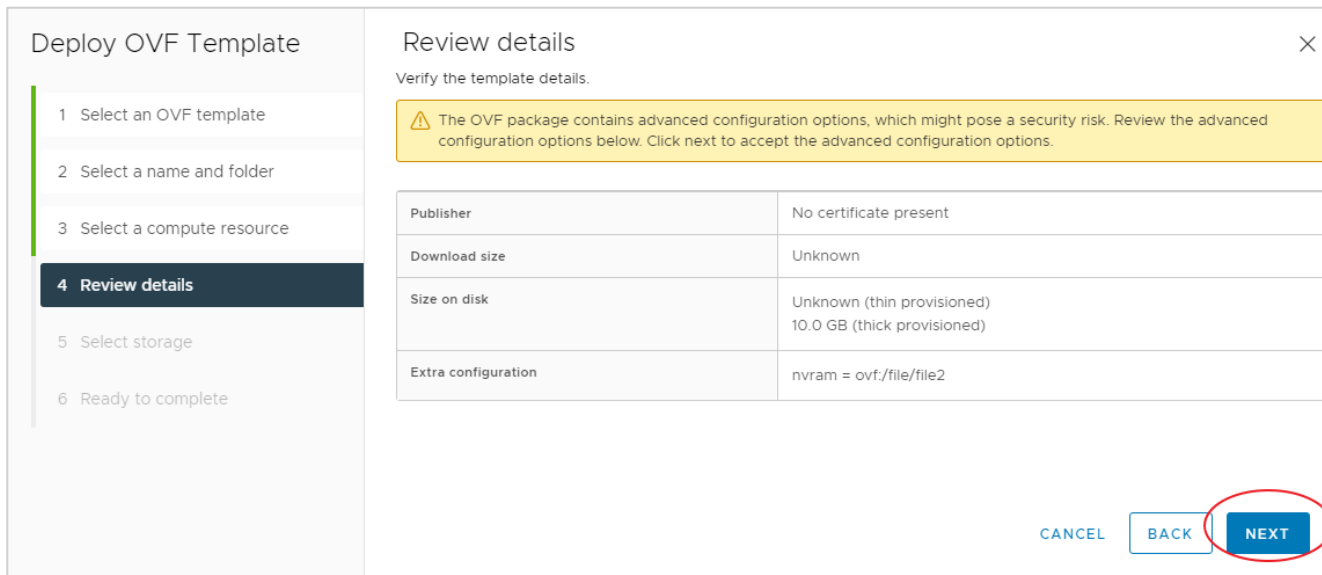


Рисунок 98

Выбираем датастор для хранения шаблона (Рисунок 99).

Обязательно выбираем формат диска Thin Provision!

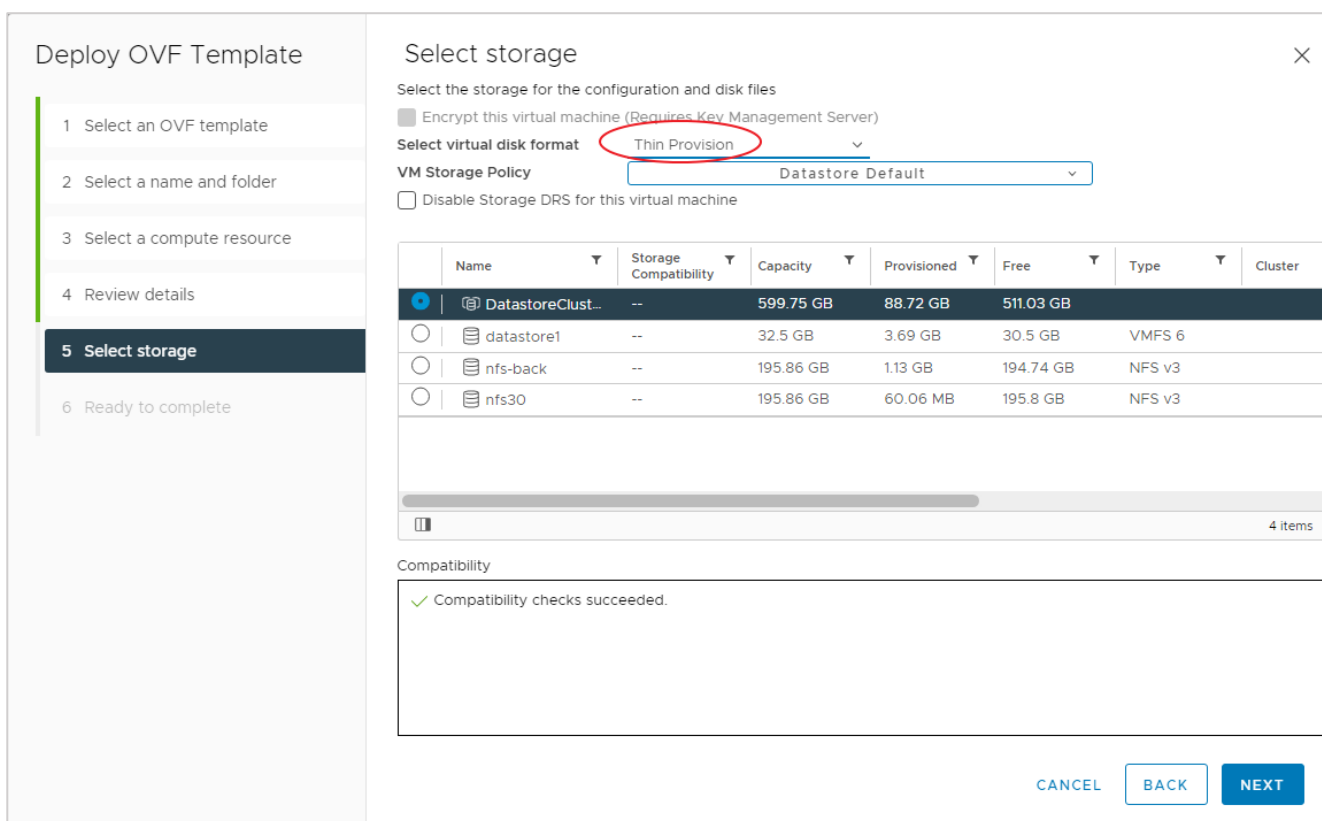


Рисунок 99

Завершаем процесс нажатием кнопки «FINISH» в открывшемся окне (Рисунок 100).

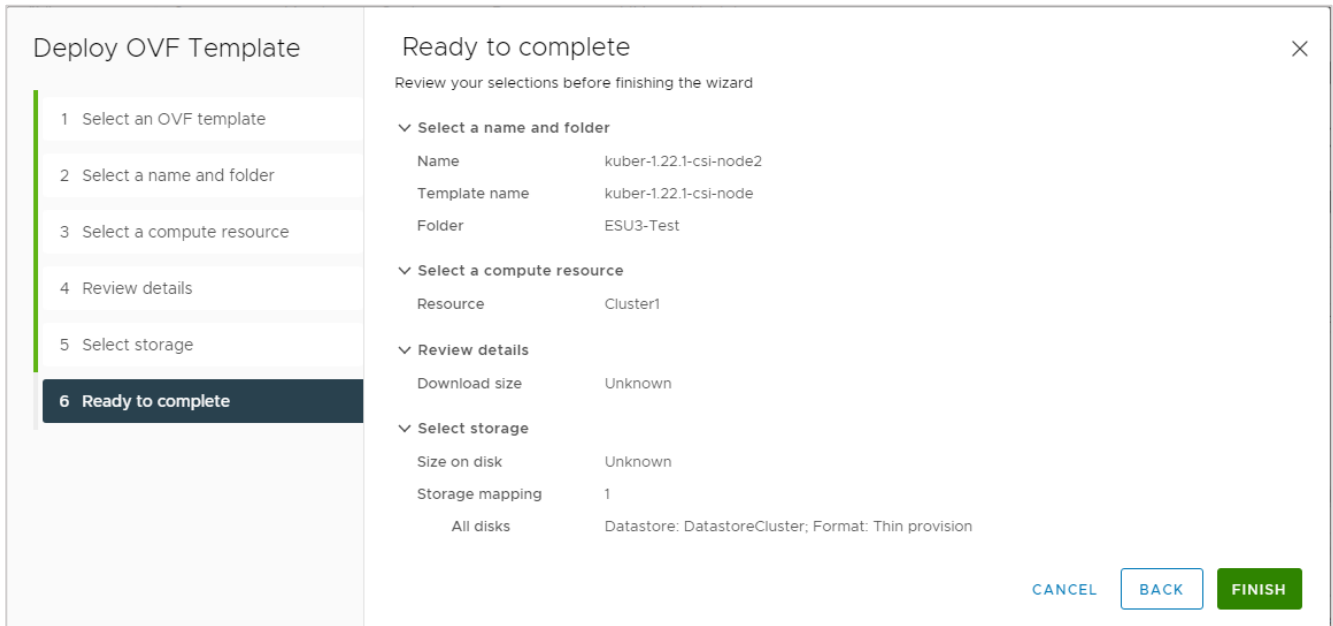


Рисунок 100

После успешной загрузки необходимо сконвертировать созданную таким образом ВМ в темплейт. Для этого нажмём по ней правой кнопкой мыши и выберем «Template» – «Convert to Template» (Рисунок 101).

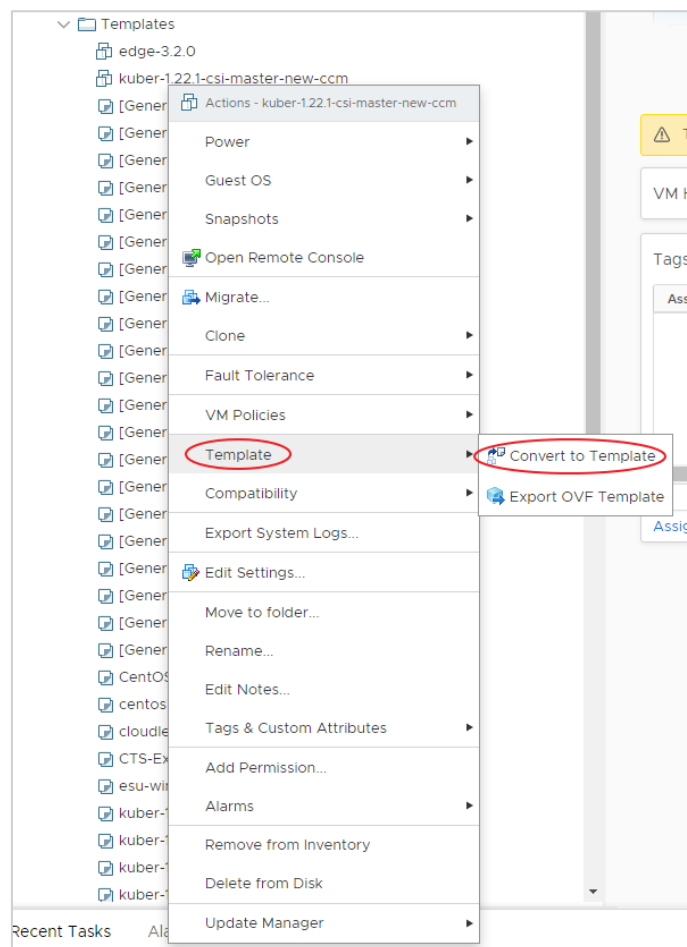


Рисунок 101

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

После успешной загрузки шаблонов в VMware vSphere необходимо настроить РУСТЭК-ЕСУ для работы с ними. Для этого в панели управления РУСТЭК-ЕСУ переходим в меню **Инсталляция** → **Шаблоны** → **Kubernetes** и нажимаем **Создать шаблон** (Рисунок 102).

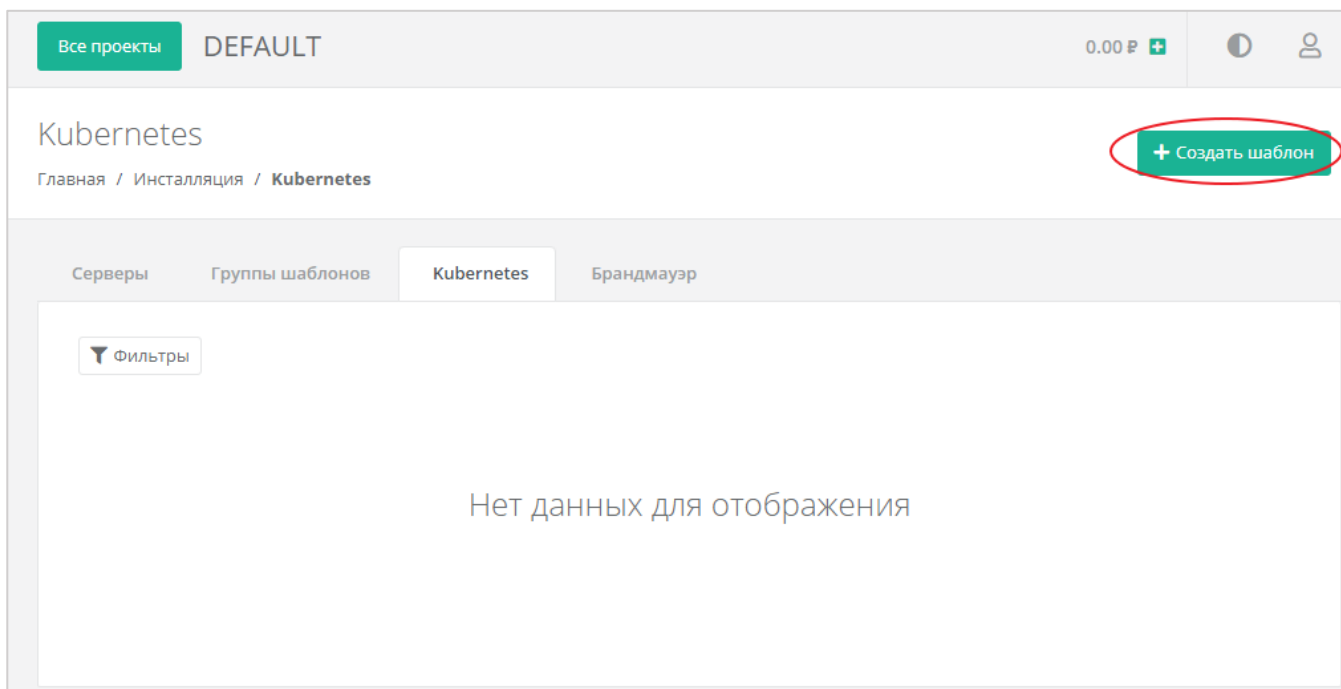


Рисунок 102

В открывшемся окне заполняем следующие параметры (Рисунок 103):

- Доступен для – выбираем сегмент VMware.
- Имя – произвольное имя.
- Включен – чек-бокс установлен.
- Темплейт мастера – выбираем шаблон мастера, загруженный в vSphere из выпадающего списка.
- Темплейт ноды – выбираем шаблон ноды, загруженный в vSphere из выпадающего списка.
- Видимый шаблон ОС – выбираем 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.

Нажимаем **Применить**.

Изменение шаблона

Главная / Инсталляция / Kubernetes / Изменение шаблона

Основные настройки | Скрипт развертывания

Доступен для VMware KVM

Имя

Включен Снимите флажок, чтобы шаблон не показывался в витрине

Позиция

Темплейт мастера

Темплейт ноды

Видимый шаблон ОС

Минимальная конфигурация

CPU

RAM

HDD

Рисунок 103

Далее во вкладке **Скрипт развёртывания** необходимо добавить скрипт.
Скрипт развёртывания:

```

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_uid="{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
AAAAB3NzaC1yc2EAAAADAQABAAQDKZnwLDIoHsfZukwf/QnHP8KR/diFMQgLFxG0Doe9qdZ/nE7xf3
bUF9WNXwMEemQv6Vo6Jdp0kTswT+ZuELlxcvd4OgnIBChdY8qym/4/BFMqFJz6IJ1Bhenp/+bvy/cWR2b
BKNiYb0Cw5dWU+0xbS7516jy0oH3zCwVTNGQ7ieB5cwJaq3w9LYuXGITUN6pko3mJKMhQ1JB7mre8ZGkz
KIwux5Eut4me1JCFfi/bGF1UUB/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 нажимаем **Применить** и **вернуться** (Рисунок 104).

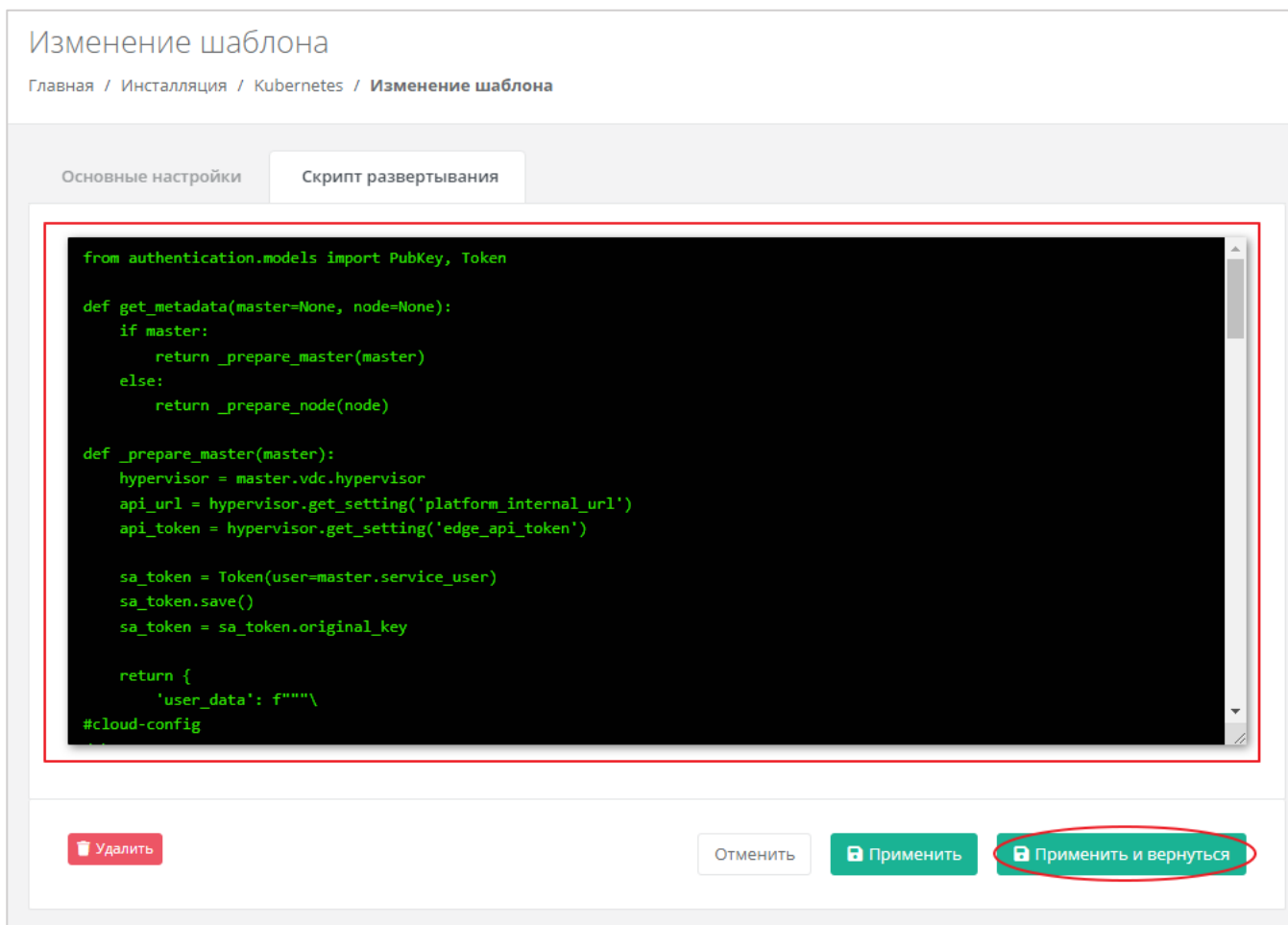


Рисунок 104

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).

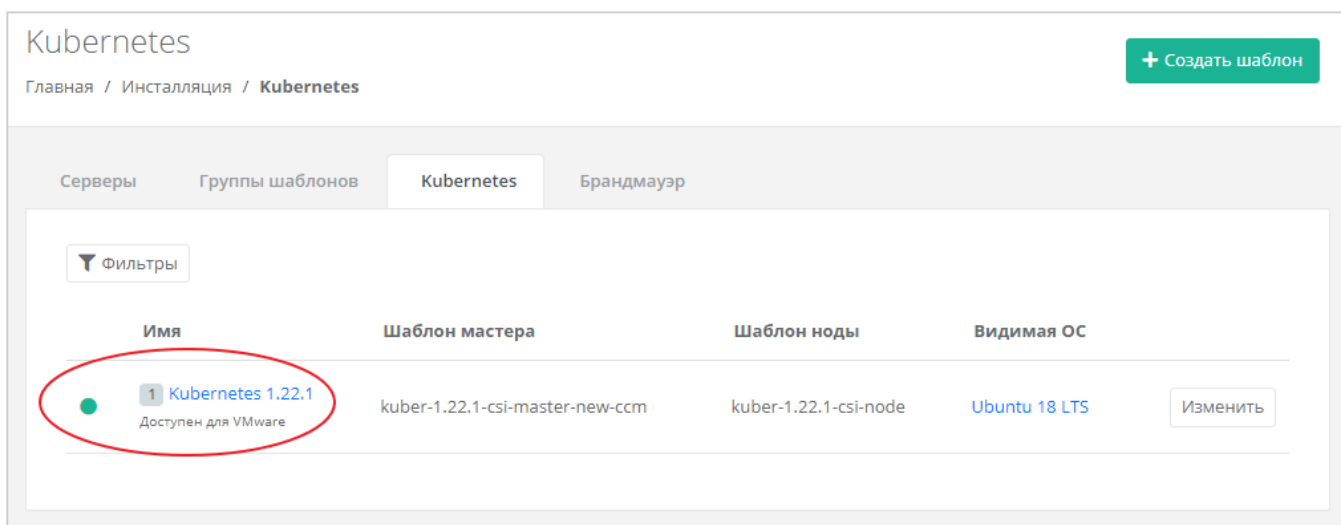


Рисунок 105

Создание кластера

Главная / Кластеры Kubernetes / Создание кластера

Основные настройки

Имя:

ВЦОД:

Версия:

Публичный IP:

Количество нод:

Конфигурация нод кластера

vCPU: 1 ядро

RAM: 1 ГБ

Диск: ГБ

Публичный ключ:

Рисунок 106

8.2. Создание шаблонов Kubernetes для сегмента РУСТЭК/KVM

Для создания шаблонов Kubernetes в сегменте РУСТЭК необходимо зайти по SSH (root:rustack) на один из контроллеров РУСТЭК, скачать .vmdk образы master-ноды и worker-ноды, конвертировать их в формат .raw и создать из них images.

Скачиваем образы в директорию **/tmp**, используя указанные в команде ссылки:

```
cd /tmp

curl -O -L https://ncl.sbcloud.ru/s/L3j8SNFKrkqcHjJ/download/kuber-1.22.1-csi-node-1.vmdk

curl -O -L https://ncl.sbcloud.ru/s/9HqHasftppNM4iq/download/kuber-1.22.1-csi-master-new-ccm-1.vmdk
```

Конвертируем образы в формат .raw:

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

qemu-img convert -p -O raw /tmp/kuber-1.22.1-csi-node-1.vmdk /tmp/kuber-1.22.1-
```

```
csi-node-1.raw
```

Удаляем исходники (.vmdk):

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

Создаём images (Рисунок 107):

```
openstack image create --disk-format raw --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 /tmp/kuber-1.22.1-csi-
master-new-ccm-1.raw kuber-1.22.1-csi-master-new-ccm
```

```
openstack image create --disk-format raw --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 /tmp/kuber-1.22.1-csi-
node-1.raw kuber-1.22.1-csi-node
```

```
alo /tmp # openstack image create --disk-format raw --container-format bare --public --property hw_disk_bus=scsi --property hw_scsi_model=virtio-scsi --prop
erty hw_vif_model=virtio --property image_type=master --file /tmp/kuber-1.22.1-csi-master-new-ccm-1.raw kuber-1.22.1-csi-master-new-ccm
-----
Field | Value
-----
container_format | bare
created_at | 2022-05-23T12:33:29Z
disk_format | raw
file | /v2/images/3f5d376d-d2fa-40c5-a2c1-2c8c7d90ea3a/file
id | 3f5d376d-d2fa-40c5-a2c1-2c8c7d90ea3a
min_disk | 0
min_ram | 0
name | kuber-1.22.1-csi-master-new-ccm
owner | f8f0379a9d3f426d9801a5296816c1b9
properties | hw_disk_bus='scsi', hw_scsi_model='virtio-scsi', hw_vif_model='virtio', image_type='master', os_hidden='False',
owner_specified.openstack.md5='', owner_specified.openstack.object='images/kuber-1.22.1-csi-master-new-ccm',
owner_specified.openstack.sha256=''
protected | False
schema | /v2/schemas/image
status | queued
tags |
updated_at | 2022-05-23T12:33:29Z
visibility | public

alo /tmp # openstack image create --disk-format raw --container-format bare --public --property hw_disk_bus=scsi --property hw_scsi_model=virtio-scsi --prop
erty hw_vif_model=virtio --property image_type=master --file /tmp/kuber-1.22.1-csi-node-1.raw kuber-1.22.1-csi-node
-----
Field | Value
-----
container_format | bare
created_at | 2022-05-23T12:37:09Z
disk_format | raw
file | /v2/images/6715ca9a-f363-413b-942e-12f969358b50/file
id | 6715ca9a-f363-413b-942e-12f969358b50
min_disk | 0
min_ram | 0
name | kuber-1.22.1-csi-node
owner | f8f0379a9d3f426d9801a5296816c1b9
properties | hw_disk_bus='scsi', hw_scsi_model='virtio-scsi', hw_vif_model='virtio', image_type='master', os_hidden='False',
owner_specified.openstack.md5='', owner_specified.openstack.object='images/kuber-1.22.1-csi-node', owner_specified.openstack.sha256=''
protected | False
schema | /v2/schemas/image
status | queued
tags |
updated_at | 2022-05-23T12:37:09Z
visibility | public
```

Рисунок 107

Удаляем образы (.raw):

```
rm /tmp/kuber-1.22.1-csi-node-1.raw
rm /tmp/kuber-1.22.1-csi-master-new-ccm-1.raw
```

После успешной загрузки шаблонов в РУСТЭК необходимо настроить РУСТЭК-ЕСУ для работы с ними. Для этого в панели управления РУСТЭК-ЕСУ переходим в

меню **Инсталляция** → **Шаблоны** → **Kubernetes** и нажимаем **Создать шаблон** (Рисунок 108).

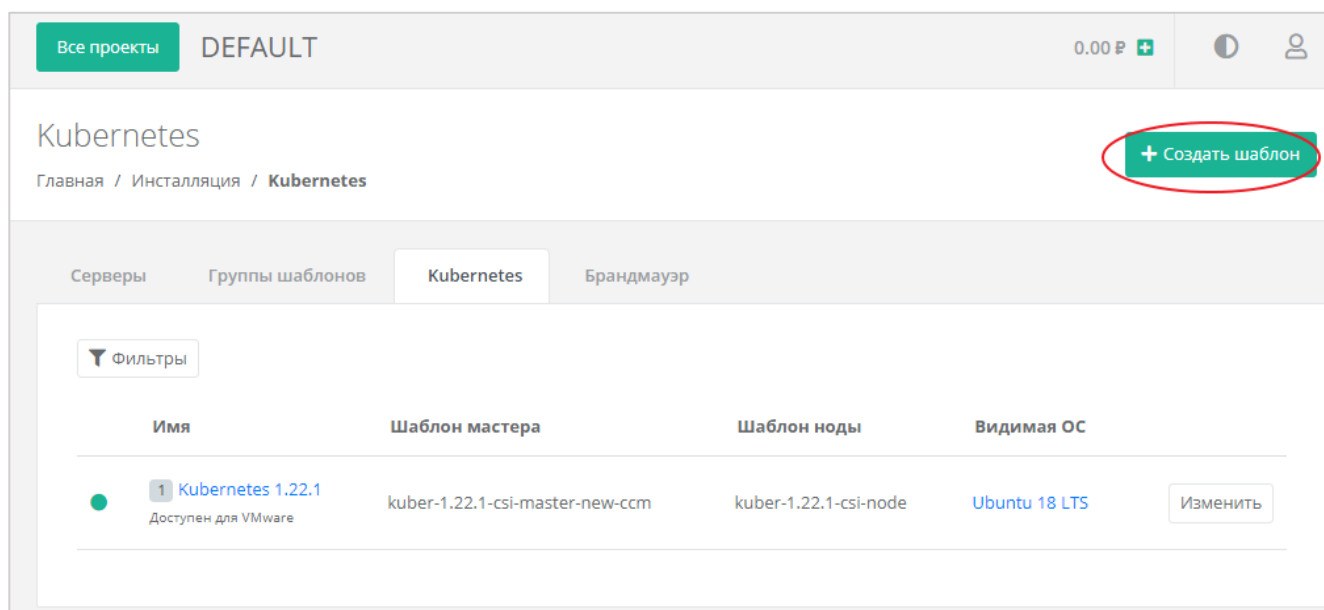


Рисунок 108

В открывшемся окне заполняем следующие параметры (Рисунок 109):

- Доступен для – выбираем сегмент KVM.
- Имя – произвольное имя.
- Включен – чек-бокс установлен.
- Темплейт мастера – выбираем шаблон мастера, загруженный в РУСТЭК из выпадающего списка.
- Темплейт ноды – выбираем шаблон ноды, загруженный в РУСТЭК из выпадающего списка.
- Видимый шаблон ОС – выбираем 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.

Нажимаем **Применить**.

Создание шаблона

Главная / Инсталляция / Kubernetes / **Создание шаблона**

Основные настройки | Скрипт развертывания

Доступен для VMware KVM

Имя

Включен Снимите флажок, чтобы шаблон не показывался в витрине

Позиция

Темплейт мастера

Темплейт ноды

Видимый шаблон ОС

Минимальная конфигурация

CPU

RAM

HDD

Рисунок 109

Далее во вкладке **Скрипт развёртывания** необходимо добавить скрипт.
Скрипт развёртывания:

```

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_uid="{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
AAAAB3NzaC1yc2EAAAADAQABAAQDKZnwlDIoHsfZukwf/QnHP8KR/diFMQgLFxG0Doe9qdZ/nE7xf3
bUF9WNXwMEemQv6Vo6Jdp0kTswT+ZuELlxcvd4OgnIBChdY8qym/4/BFMqFJz6IJ1Bhenp/+bvy/cWR2b
BKNiYb0Cw5dWU+0xbS7516jy0oH3zCwVTNGQ7ieB5cwJaq3w9LYuXGITUN6pko3mJKMhQ1JB7mre8ZGkz
KIwux5Eut4me1JCFfi/bGF1UUB/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 нажимаем **Применить** и **вернуться** (Рисунок 110).

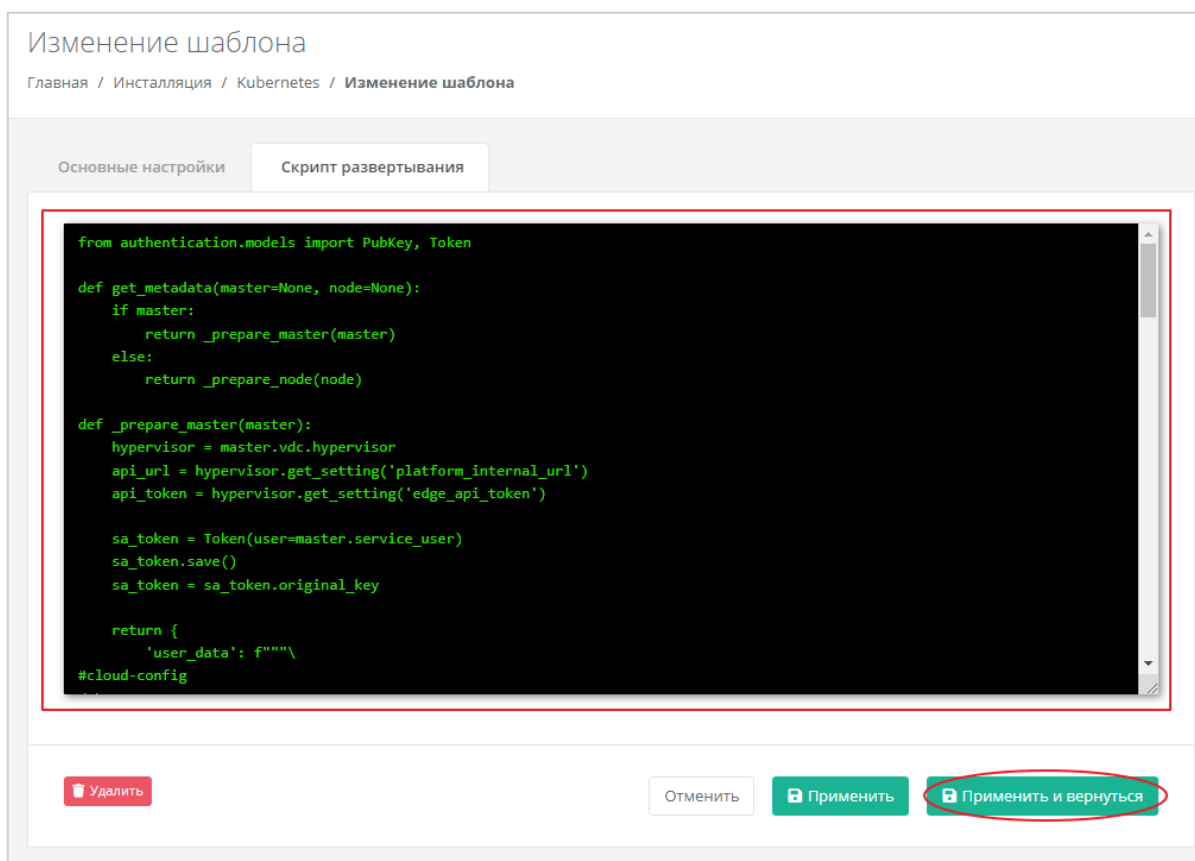


Рисунок 110

На этом настройка шаблона завершена, и он отобразится в списке шаблонов Kubernetes (Рисунок 111), а также будет доступен для создания в меню **Кластеры Kubernetes** для пользователя (Рисунок 112).

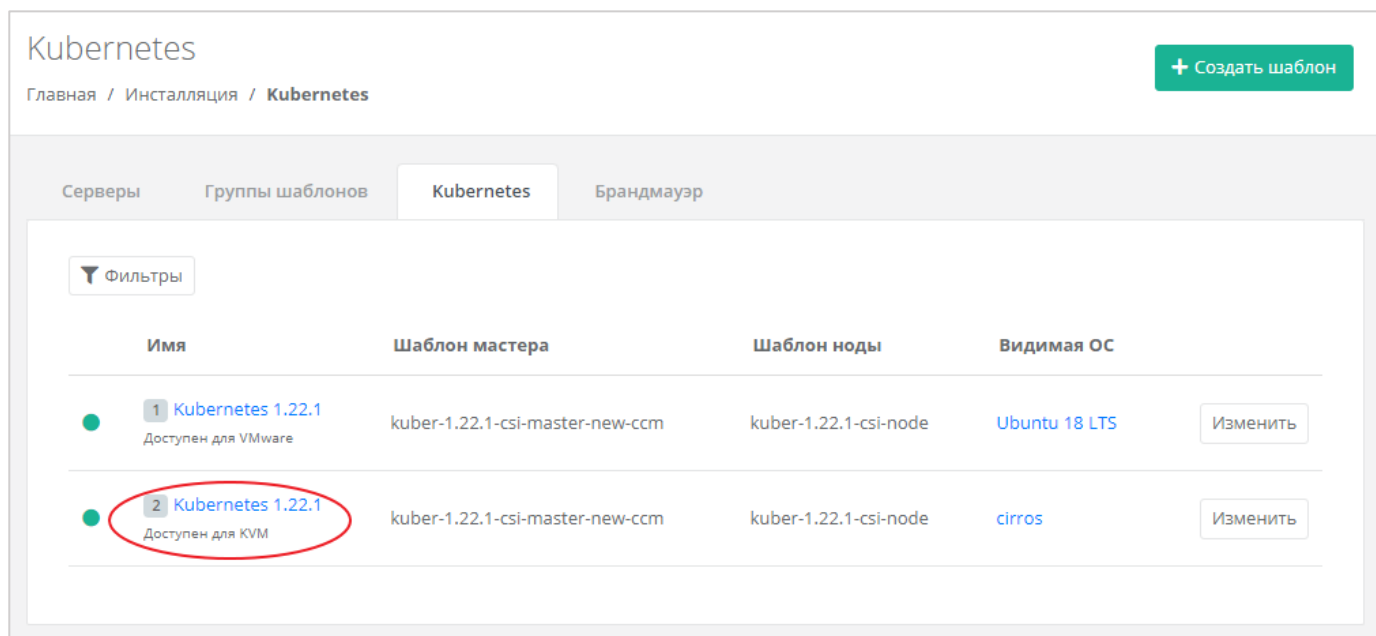


Рисунок 111

Создание кластера

Главная / Кластеры Kubernetes / Создание кластера

Основные настройки

Имя:

ВЦОД:

Версия:

- Kubernetes 1.22.1
- Kubernetes 1.19

Публичный IP:

Количество нод:

Конфигурация нод кластера

vCPU: 1 ядро

RAM: 1 ГБ

Диск: ГБ

Размер Тип

Публичный ключ:

Рисунок 112

Также для последующего развёртывания кластеров в сегменте РУСТЭК/KVM необходимо произвести донастройку ресурсного пула.

Для этого в главном меню панели управления переходим в **Инсталляция** → **Ресурсы** → **Ресурсные пулы**. Выбираем ресурсный пул KVM (Рисунок 113).

В открывшемся окне заполняем следующие параметры:

- Название management-сети, в которой работает ECU – название маршрутизируемой сети из пункта 2.2 инструкции.
- Адрес ECU в management-сети, по которому будет доступно API – адрес VM ESU-box в маршрутизируемой сети, выданный в пункте 2.2 (смотрим в панели РУСТЭК).
- Токен – токен пользователя (можно скопировать из настроек ресурсного пула vSphere).

Название management сети, в которой работает ECU и ее компоненты, включая пользовательские роутеры. Например: Toochka_mgmt	ESU-Rustack
Адрес ECU в management сети, по которому будет доступно API. Это значение используется при автоматическом развертывании роутеров EDGE в клиентских ВЦОДах. Например: http://192.168.20.5	http://10.11.14.111
Токен, который будет использоваться роутерами EDGE при их автоматическом развертывании в клиентских ВЦОДах.	977c9840912471ec90fbe7ed90e2290048cc1b2a

Рисунок 113

8.3. Создание кластеров Kubernetes в РУСТЭК-ЕСУ

После того, как шаблоны и ресурсный пул настроены, можно переходить к созданию кластеров Kubernetes.

Для этого в главном меню панели управления переходим в [Кластеры Kubernetes](#) и нажимаем **Создать кластер** (Рисунок 114).

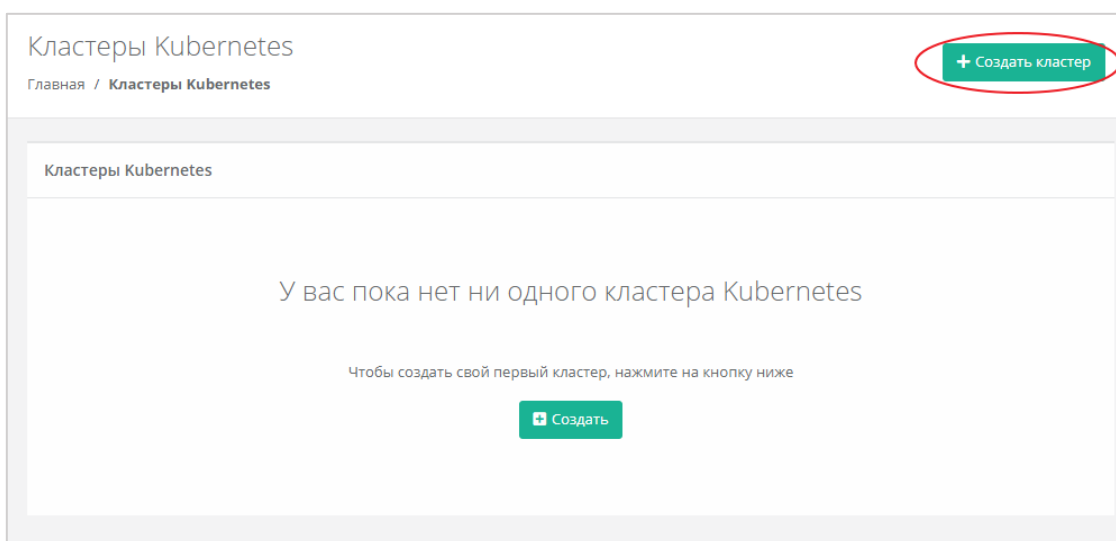


Рисунок 114

В открывшемся окне заполняем следующие параметры (Рисунок 115):

- Имя – произвольное наименование кластера.
- ВЦОД – выбор необходимого ВЦОД, либо создание нового.
- Версия – выбор версии Kubernetes.
- Публичный IP – выбор параметров 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:
 - CPU.
 - RAM.
 - Диск:

- Размер диска.
- Тип диска (SSD, SAS, SATA).
- Публичный ключ – выбор публичного ключа и возможность создания нового.

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

После заполнения всех полей нажимаем **Создать**.

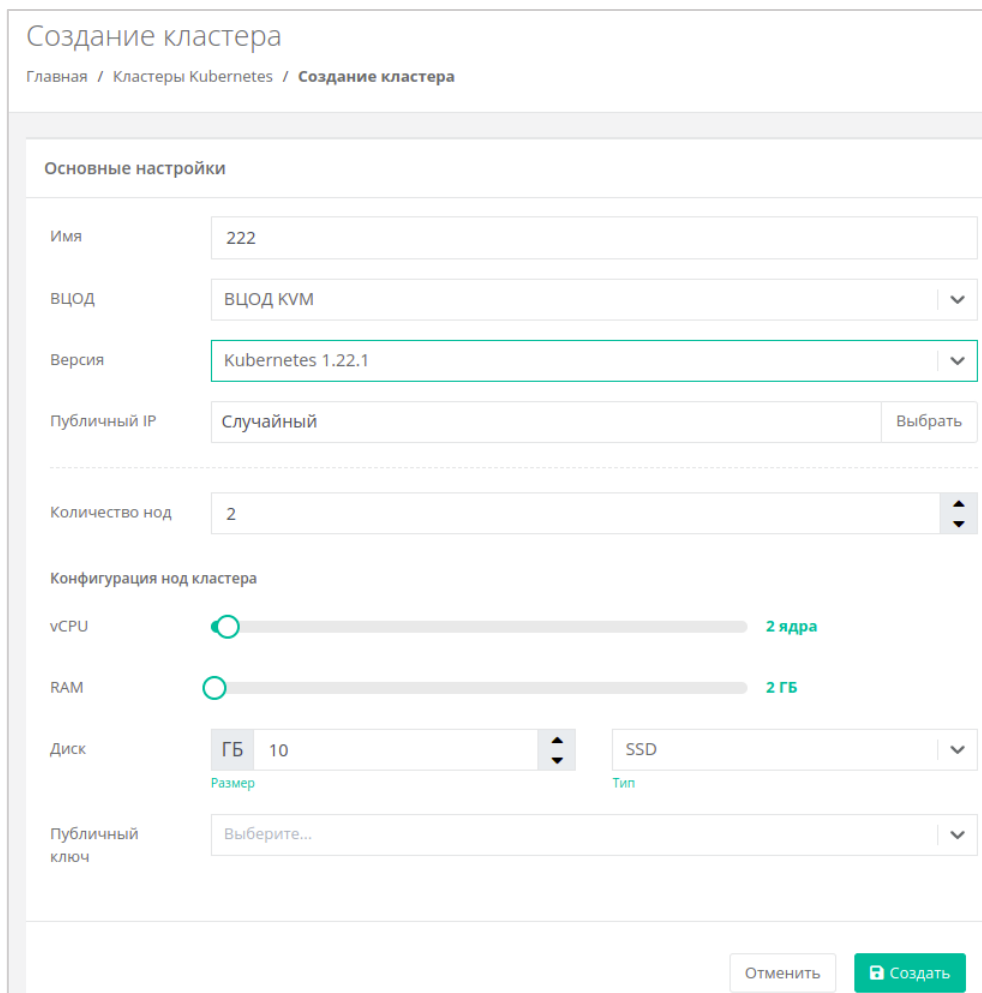


Рисунок 115

После создания кластер отобразится в панели управления (Рисунок 116).

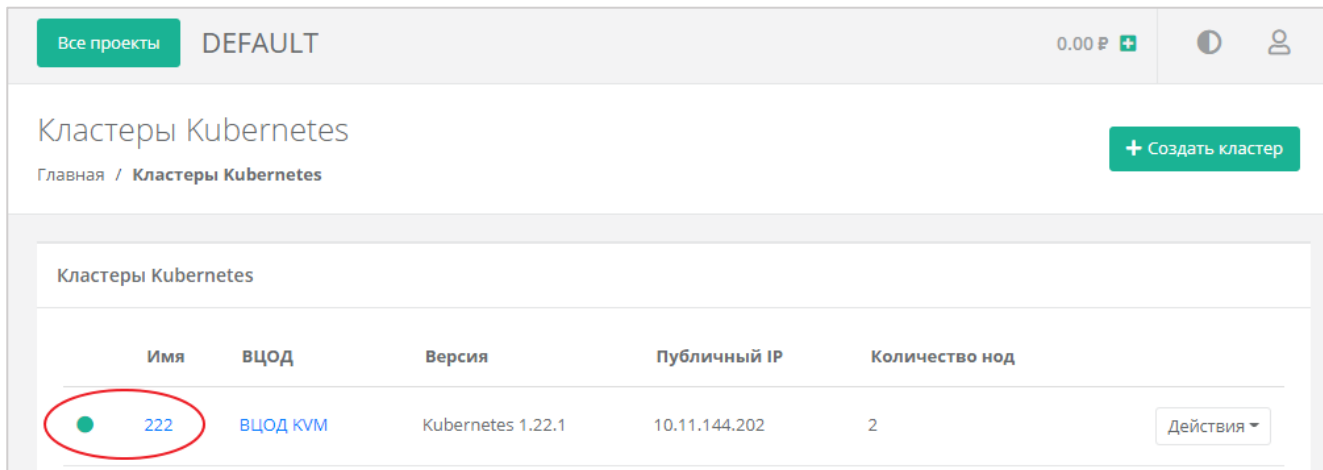


Рисунок 116

Ноды кластера также можно увидеть в меню **Облачные вычисления** → **ВЦОД** → **Серверы** и управлять ими как обычными серверами – изменять конфигурацию и управлять состоянием сервера (Рисунок 117).

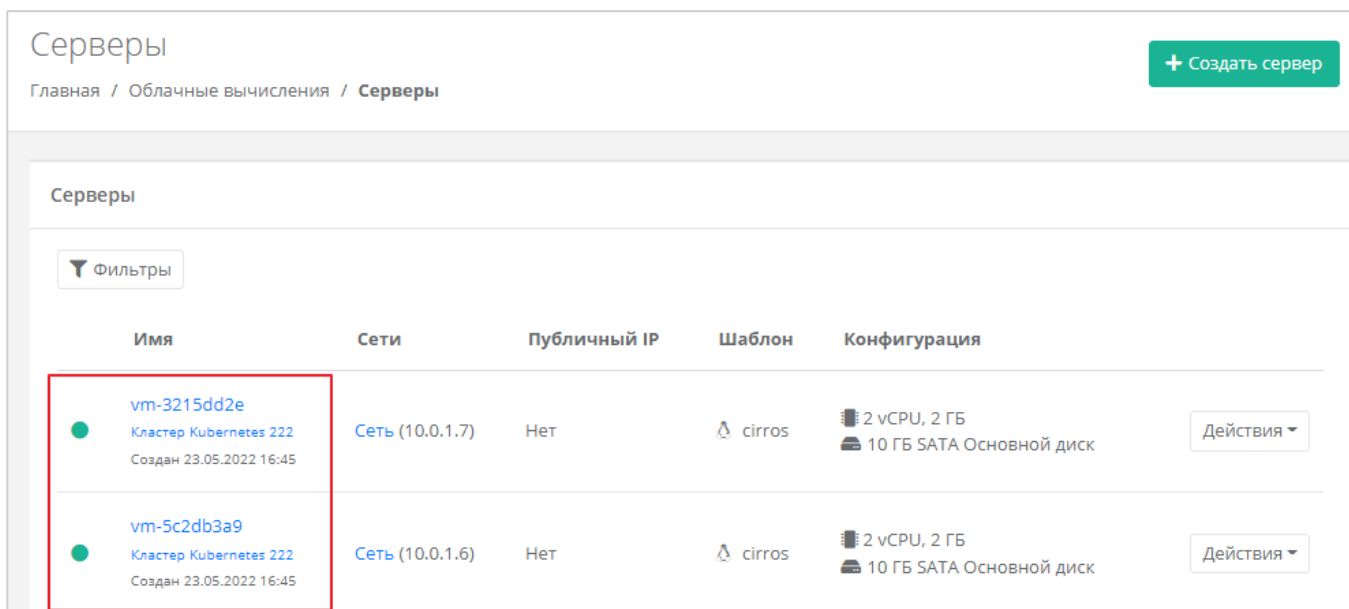


Рисунок 117

8.4. 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 VM. В случае ее «падения» кластер будет неуправляем до момента ее включения.

- Мастер-нода недоступна для управления пользователем и располагается в management-сети.

Поддерживаемый функционал:

- Балансировщики нагрузки в кластере Kubernetes (доступны только для сегмента VMware vSphere).
- Создание Persistence Volume Claims (доступны в обоих сегментах, но только создание – изменение недоступно).

9. Расширенная настройка

9.1. 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 nginx, который необходимо создать /etc/nginx/conf.d/<любое имя>.conf, где:

- <your_domain> – доменное имя сервера nginx.
- <ip_esu-box> – IP адрес по которому доступна панель управления.
- <path_to_cert> – 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_cert>/fullchain.pem;
    ssl_certificate_key <path_to_key>/<your_domain>/privkey.pem;
}
```

После создания файла конфигурации необходимо запустить службу nginx, для этого выполним команду:

```
systemctl start nginx
```

Затем необходимо добавить службу nginx в автозапуск, для этого выполним 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 кэширование на стороне реверс-прокси отключено. Замечено, что при использовании модуля modsecurity кэширование на стороне nginx может непреднамеренно включиться.

9.2. Настройка управления DNS-зонами в РУСТЭК-ЕСУ

РУСТЭК-ЕСУ имеет службу, позволяющую пользователям управлять ресурсными записями делегированных в неё доменов. Зоны, как водится, 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](#).

Обратите внимание, что нужна сетевая связность не только от BIND к РУСТЭК-ЕСУ, но и в обратную сторону.

Для примера в инсталляции РУСТЭК были развёрнуты два сервера на базе Ubuntu 18.04 LTS в той же сети, что и ESU-box. Также для наших серверов и ESU-box необходимо добавить дополнительные правила брандмауэра в созданный ранее профиль безопасности (Рисунок 118).

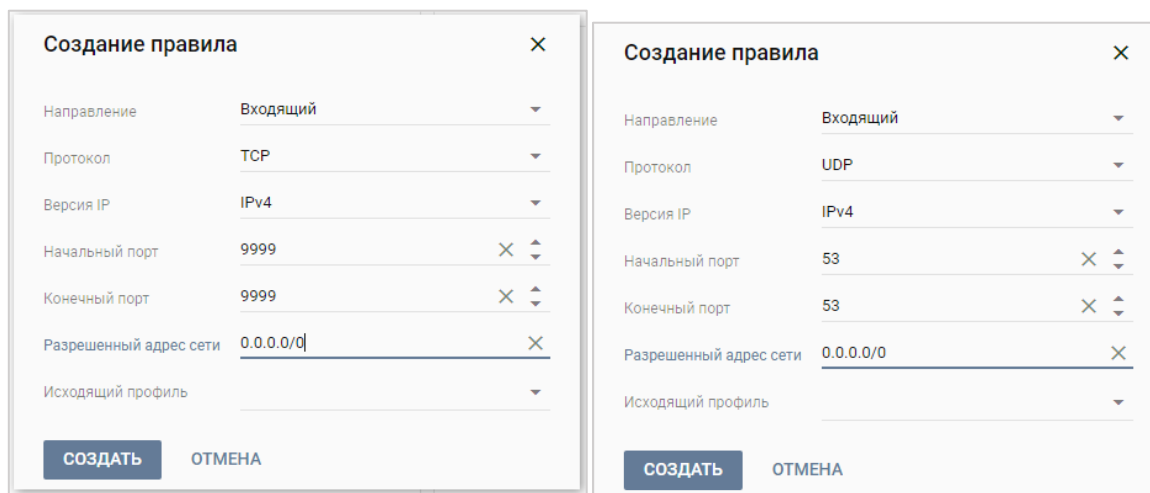


Рисунок 118

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

Пример конфигурации приведен на базе BIND из Ubuntu 18.04 LTS.

Устанавливаем:

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

Устанавливаем хостнейм на наши серверы командой:

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

Представим, что ESU-box расположена по адресу 10.11.14.111. 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 {
            10.11.14.111 port 9999;
        };
    };

    allow-notify {
        10.11.14.111;
    };
};
```

```
};

zone "catalog.local" {
    type slave;
    file "catalog.db";
    masters { 10.11.14.111 port 9999; };
};
```

Запускаем службу командой:

```
systemctl start bind9
```

Добавляем в автозапуск службу BIND:

```
systemctl enable bind9
```

Для созданных серверов необходимо добавить DNS записи (имена).

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

После произведённой настройки имена DNS-серверов, а также e-mail администратора, следует указать в самой РУСТЭК-ЕСУ на уровне провайдера в меню [Администрирование](#) → [Партнёры](#) (Рисунок 119).

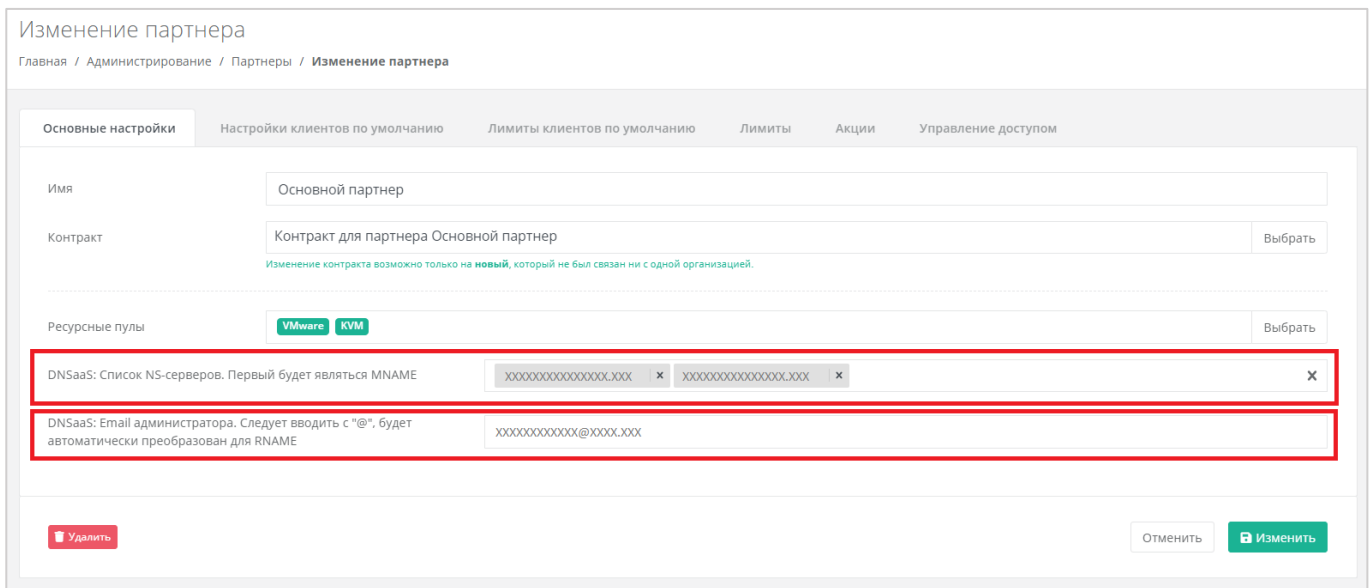


Рисунок 119

После успешной настройки в главном меню панели РУСТЭК-ЕСУ появится пункт **Доменные зоны**, из которого можно управлять доменными зонами и записями в них (Рисунок 120).

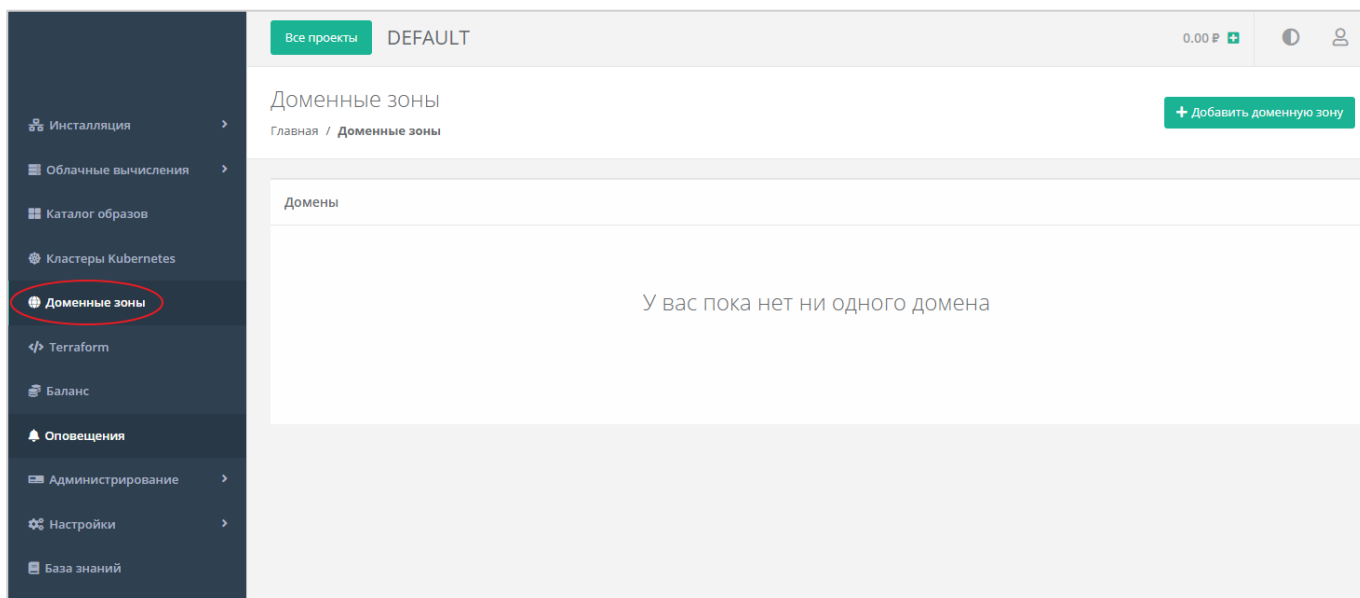


Рисунок 120

9.3. Настройка сети для роутеров (edge) сегмента VMware vSphere

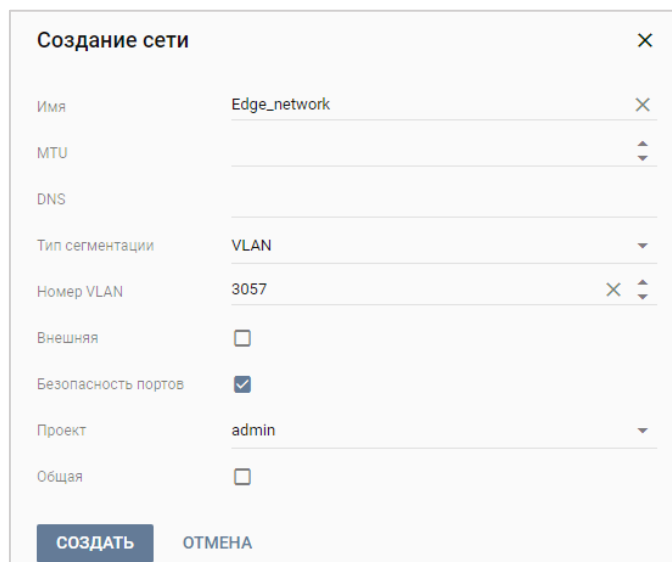
Базовая установка РУСТЭК-ЕСУ размещает пользовательские роутеры сегмента VMware в своей сервисной сети. Это удобно для быстрого запуска, но может вызывать проблемы при большом числе клиентов (размер сервисной сети ограничит количество клиентов сегмента VMware).

В таком случае необходимо создать отдельную сеть для роутеров внутри РУСТЭК, например, Edge_network (Рисунок 121).

Для этого в панели РУСТЭК необходимо перейти в раздел **Сеть – Сети** и нажать «Создать».

- Имя – указывается произвольное.
- Тип сегментации – VLAN.
- Номер VLAN – номер выделенного VLAN для внешней сети Единой системы управления.
- Внешняя – снять чек-бокс.
- Безопасность портов – указывается опционально. Данный функционал добавляет возможность использовать фаерволл на уровне порта виртуальной машины средствами ПАК.

После заполнения полей нажмите кнопку «Создать».



Имя	Edge_network
MTU	
DNS	
Тип сегментации	VLAN
Номер VLAN	3057
Внешняя	<input type="checkbox"/>
Безопасность портов	<input checked="" type="checkbox"/>
Проект	admin
Общая	<input type="checkbox"/>

СОЗДАТЬ ОТМЕНА

Рисунок 121

Далее необходимо создать подсеть для созданной сети (Рисунок 122).

Для этого перейдите в раздел **Сети – Подсеть** и нажмите «Создать», далее необходимо заполнить поля:

- Имя – указывается произвольное.
- Сеть – выбрать сеть, созданную на предыдущем этапе.
- Версия протокола – Ipv4.
- Адрес сети – указать cidr.
- Шлюз – указать шлюз.
- DHCP – снять чек-бокс.
- DNS-серверы – прописать по желанию.

После заполнения полей нажмите кнопку «Создать».

Создание подсети ✕

Имя	Edge_subnet ✕
Сеть	Edge_network ▾
Версия IP	IPv4 ▾
Адрес сети	192.168.100.0/24 ✕
Шлюз	192.168.100.1 ✕
Проект	admin ▾
DNCP	<input type="checkbox"/>
DNS-серверы	Вводить через запятую
Публикация IP в DNS	<input type="checkbox"/>

Диапазоны IP

+ ДОБАВИТЬ

Маршруты

+ ДОБАВИТЬ

СОЗДАТЬ
ОТМЕНА

Рисунок 122

Затем необходимо подключить ESU-box (сервер с РУСТЭК-ЕСУ) к этой сети.

Для этого перейдём в раздел **Серверы**, выберем сервер с установленной РУСТЭК-ЕСУ (ESU-box), правой кнопкой мыши раскроем меню действий и выберем «Сети», затем добавим новую созданную сеть (Рисунок 123, Рисунок 124).

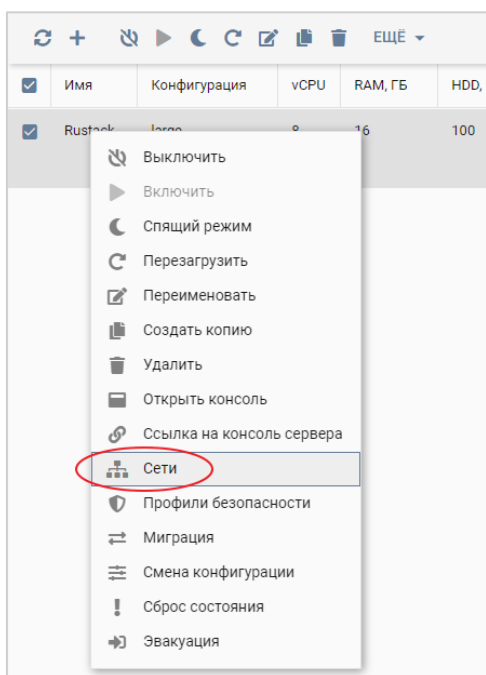


Рисунок 123

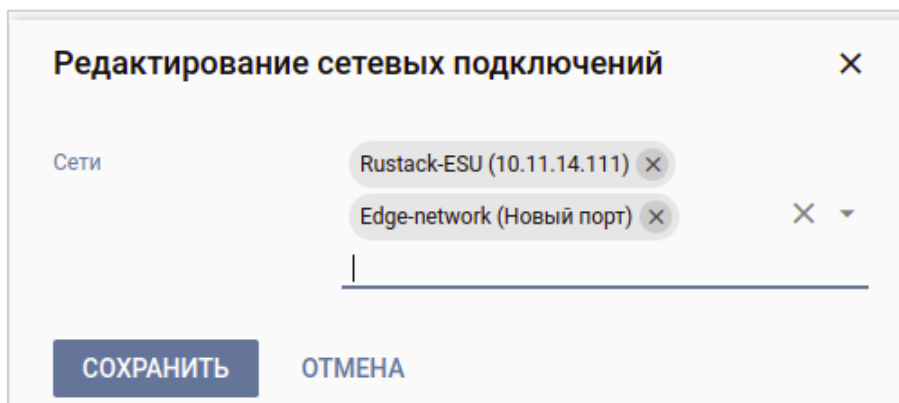


Рисунок 124

Теперь узнаём IP-адрес, назначенный для ESU-box в сети Edge_network, для этого обновим страницу в меню **Серверы** (Рисунок 125):

<input checked="" type="checkbox"/>	Имя	Конфигурация	vCPU	RAM, ГБ	HDD, ГБ	Вычи...	IP	Статус	Прое...
<input checked="" type="checkbox"/>	Rusta...	large	8	16	25	hw-n...	10.11.14.111 192.168.100.10	Запущен	admin

Рисунок 125

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

Сначала необходимо узнать имя нового сетевого интерфейса для этого выполняем команду:

```
ip a | grep en
```

В нашем случае имя нового сетевого интерфейса enp7s0.

Затем настраиваем этот интерфейс, для этого выполняем следующие команды:

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

В содержимое файла вставить и сохранить изменения:

```
auto enp7s0
iface enp7s0 inet static
address 192.168.100.10
netmask 255.255.255.0
gateway 192.168.100.1
```

Затем необходимо настроить DHCP-сервер на ESU-box, для нового сетевого интерфейса. Для этого выполним следующие команды:

Добавляем имя нового интерфейса в файл `/etc/default/isc-dhcp-server` (Рисунок 126).

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

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4=""
INTERFACESv6=""
# BEGIN ANSIBLE MANAGED BLOCK
INTERFACESv4="ens160 enp7s0"
# END ANSIBLE MANAGED BLOCK
```

Рисунок 126

Теперь производим настройку DHCP-сервера (Рисунок 127):

```
sudo vi /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 192.168.100.10 192.168.100.255;
    default-lease-time 600;
    max-lease-time 10800;
}
```

```
# BEGIN ANSIBLE MANAGED BLOCK
subnet 10.11.14.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option routers 10.11.14.1;
  option domain-name-servers 8.8.8.8;
  range 10.11.14.10 10.11.14.255;
  default-lease-time 600;
  max-lease-time 10800;
}
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 127

Перезагружаем службы DHCP-сервера и сети:

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

После этого необходимо создать и настроить сеть (portgroup на dvswitch) в VMware vSphere (Рисунок 128, Рисунок 129).

New Distributed Port Group

Name and location

Specify distributed port group name and location.

Name

Location

1 Name and location

2 Configure settings

3 Ready to complete

CANCEL NEXT

Рисунок 128

New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic ⓘ

Number of ports: 100

Network resource pool: (default)

VLAN

VLAN type: VLAN

VLAN ID: 3057

Advanced

Customize default policies configuration

CANCEL BACK NEXT

Рисунок 129

Далее необходимо указать через web-интерфейс в настройках ресурсного пула VMware данную сеть как management-сеть для роутеров.

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

Выберем ресурсный пул VMware vSphere и изменим следующие настройки (Рисунок 130):

- Название management-сети для пользовательских роутеров – укажем название нашей сети в VMware vSphere.
- Адрес ЕСУ в management-сети, в которой будут создаваться роутеры – указываем адрес сервера ESU-box в новой сети (Рисунок 125).

Изменение ресурсного пула

Главная / Установка / Ресурсные пулы / Изменение ресурсного пула

Основные настройки Профили хранения Платформы

Имя: VMware Hypervisor

Тип: VMware KVM

Сетевая зона: VMware Zone Выбрать

Раннеры: default-vmware-runner Выбрать

Включен

Название шаблона роутера, который будет использоваться при создании новых ВЦОД у клиентов. Например: edge-1.2.3: edge-1.2.7

Название management сети, в которой работает ECU и ее компоненты, включая пользовательские роутеры. Например: Toochka_mgmt: vlan3057

Название служебного датастора, на котором будут размещаться пользовательские роутеры и служебные сервисы. Обычно этот тот же датастор, в котором размещена сама ECU. Например: DS_Management: DatastoreCluster

Адрес ECU в management сети, по которому будет доступно API. Это значение используется при автоматическом развертывании роутеров EDGE в клиентских ВЦОДах. Например: http://192.168.20.5: http://192.168.100.10

Токен, который будет использоваться роутерами EDGE при их автоматическом развертывании в клиентских ВЦОДах: d336ac2b67ff18954e3e6b11b070e17dc9250055

Название директории, в которой будут расположены ВЦОДы клиентов: ESU3-Test

Рисунок 130

На этом настройка завершена.

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

Проверим это, создав новый ВЦОД в сегменте VMware vSphere (Рисунок 131).

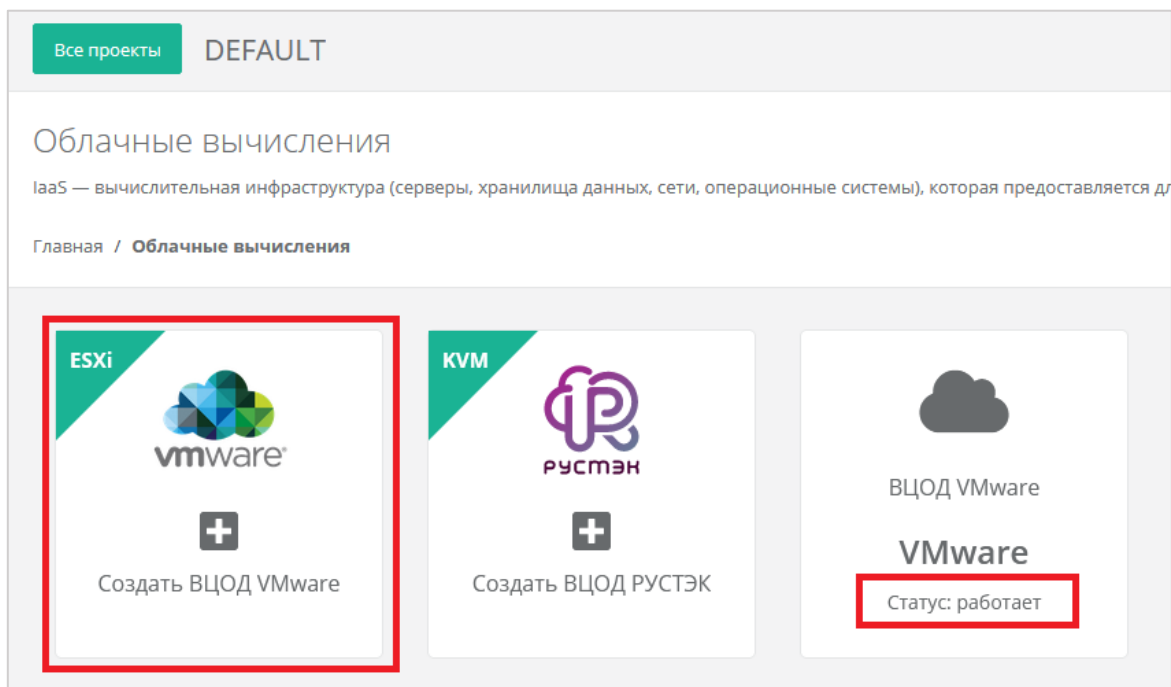


Рисунок 131

После создания ВЦОД перейдём в панель VMware vSphere и убедимся, что роутер (edge), созданный внутри нового ВЦОД, подключен к новой настроенной сети (Рисунок 132).

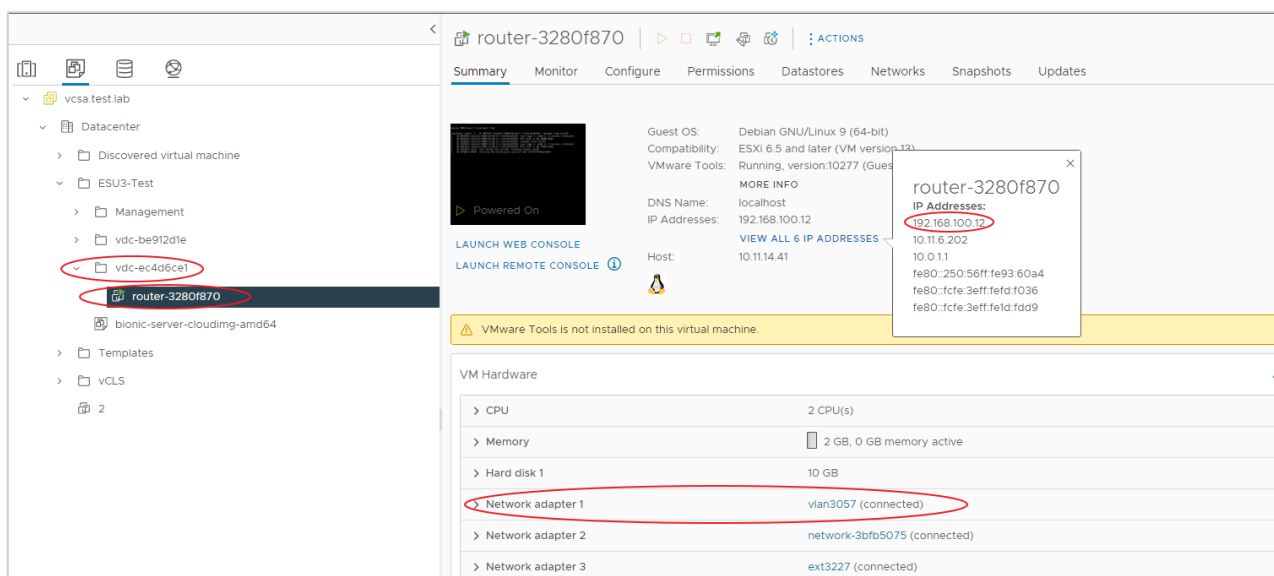


Рисунок 132

9.4. 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 5.1.4 (для сегмента РУСТЭК/KVM) и из раздела 5.2.7 (для сегмента VMware vSphere).

Сам скрипт пишется на языке JavaScript и должен содержать функцию `getMetadata(vmInfo, userData)`, возвращающую набор полей для передачи через EC2.

Вам понадобится добавить в меню **Инсталляция** → **Шаблоны** → **Серверы** к шаблонам ВМ следующие поля на вкладке **Поля для скрипта** при заведении шаблона (Рисунок 133):

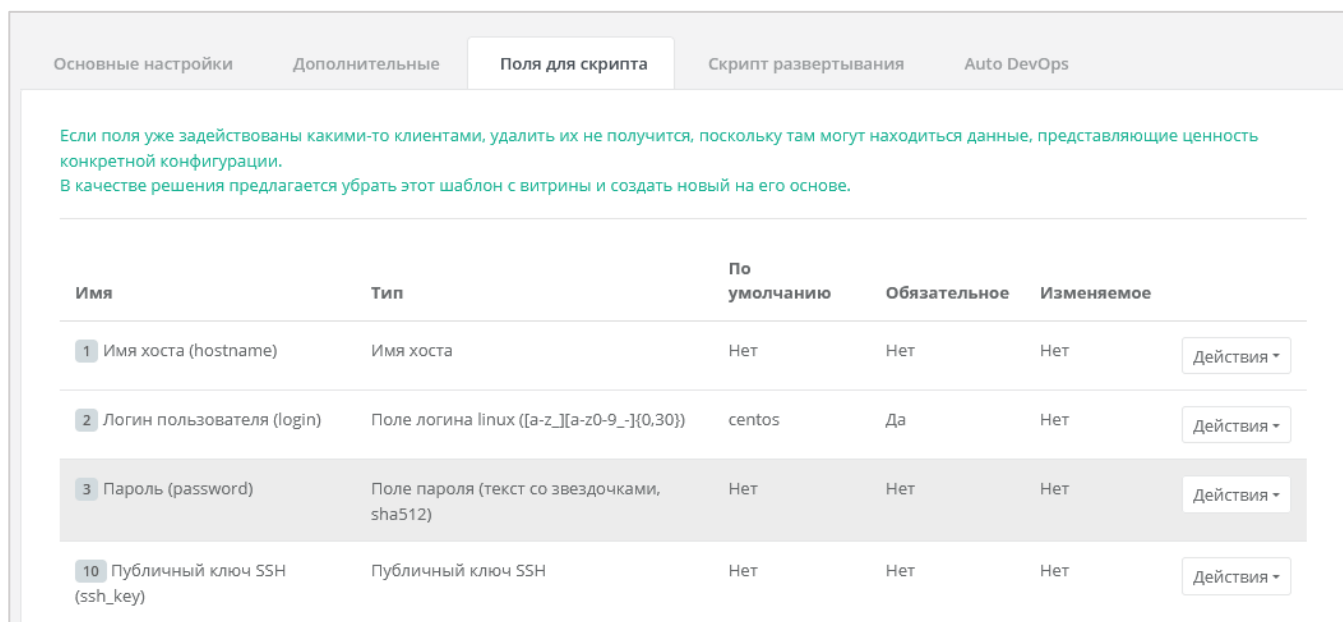


Рисунок 133

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: {}'.format(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
}

```

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

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

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

Пункты 1–3 выполняем согласно официальной документации:

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

Пункт 4 выполняем 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 стоять SSH-сервер.

Порядок настройки SSH-сервера:

- Скачать OpenSSH-Win64.zip отсюда <https://github.com/PowerShell/Win32-OpenSSH/releases>

- Разархивировать в C:\Program Files\OpenSSH-Win64
- Перейти в панель управления / Система / Advanced System Settings / Advanced / Environmental Variables (Рисунок 134):

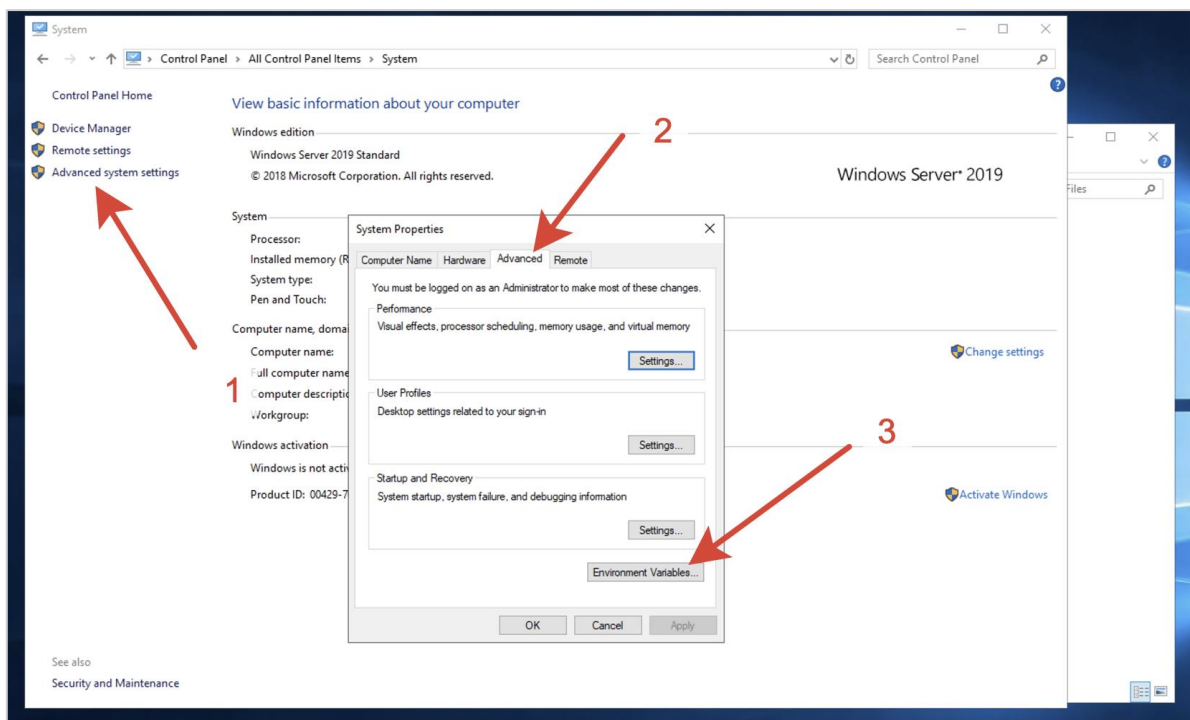


Рисунок 134

- В system variables (второй блок) выбрать Path, нажать редактировать (Рисунок 135):

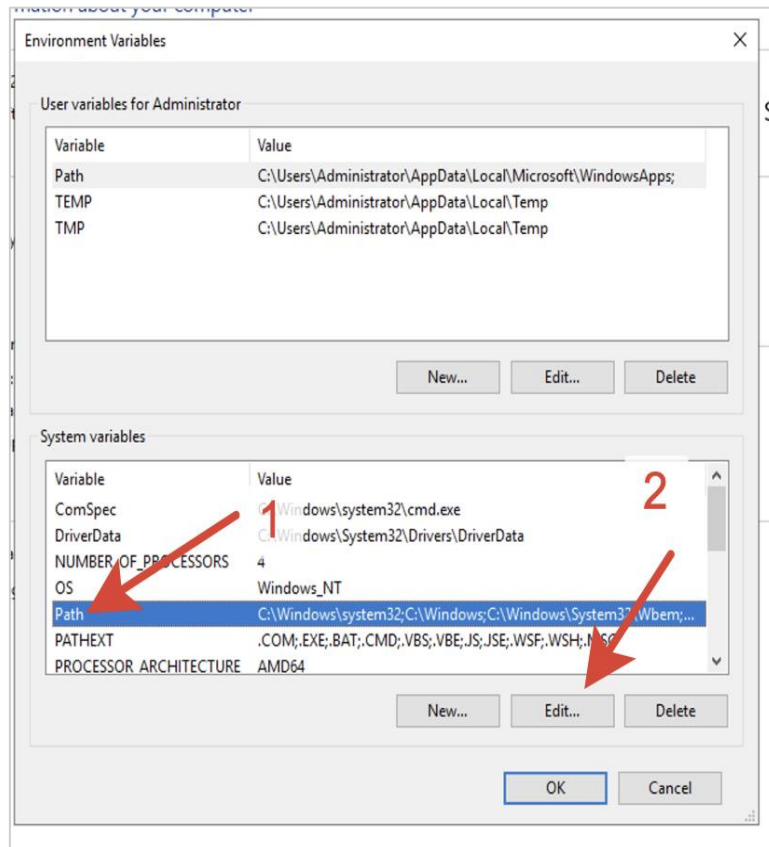


Рисунок 135

- Добавить туда C:\Program Files\OpenSSH-Win64 (Рисунок 136):

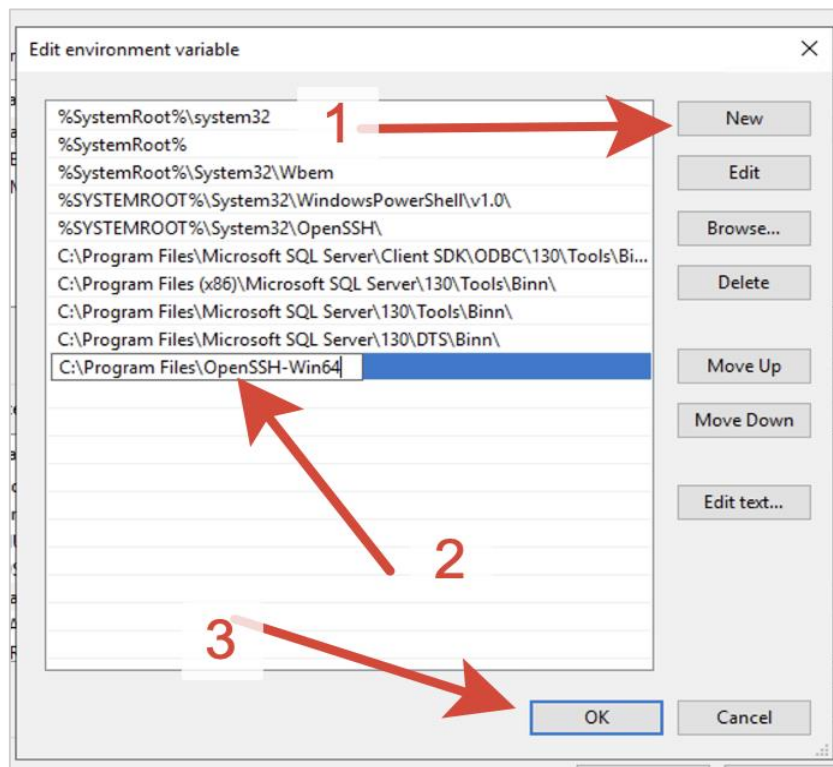


Рисунок 136

- Запустить PowerShell как администратор (Рисунок 137):

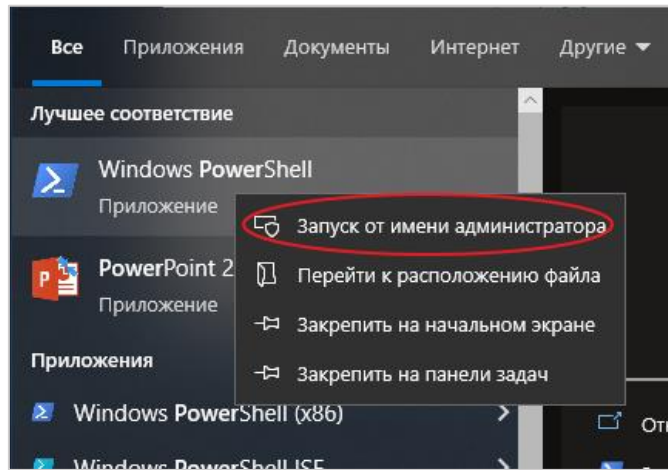


Рисунок 137

- Перейти в C:\Program Files\OpenSSH-Win64
- Запустить `.\install-sshd.ps1`.
- Если надпись "sshd and ssh-agent services successfully installed" появилась – всё верно (Рисунок 138):

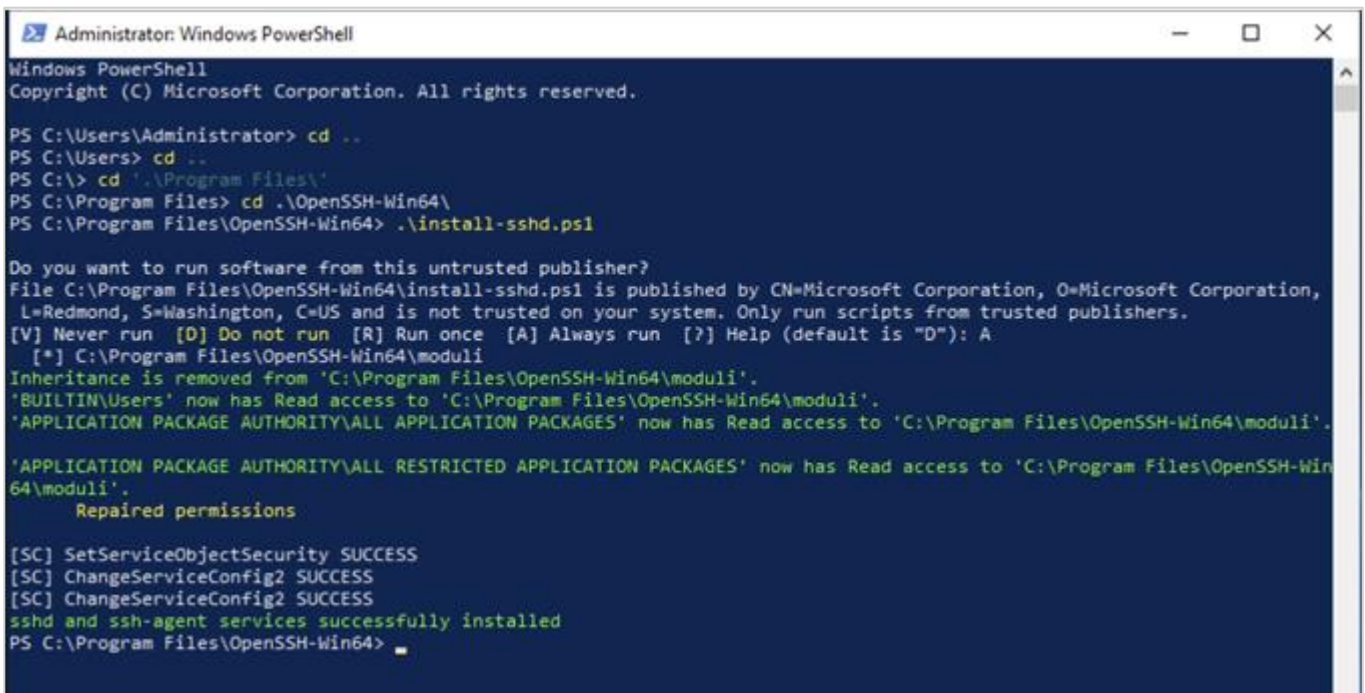


Рисунок 138

- Сгенерировать ключ хоста: `.\ssh-keygen.exe -A`.
- Зайти в сервисы, включить и настроить автозапуск сервису OpenSSH (Рисунок 139):

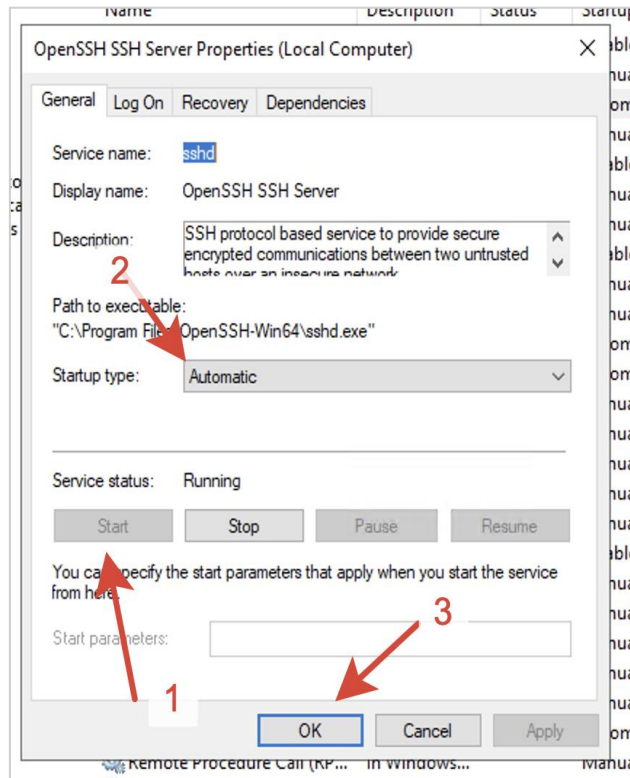


Рисунок 139

- Если сервис не включается, выполняем `.\FixHostFilePermissions.ps1` в директории с проектом.
- Делаем правило брандмауэра, пропускающее подключения на 22-й порт (Рисунок 140 – Рисунок 143).

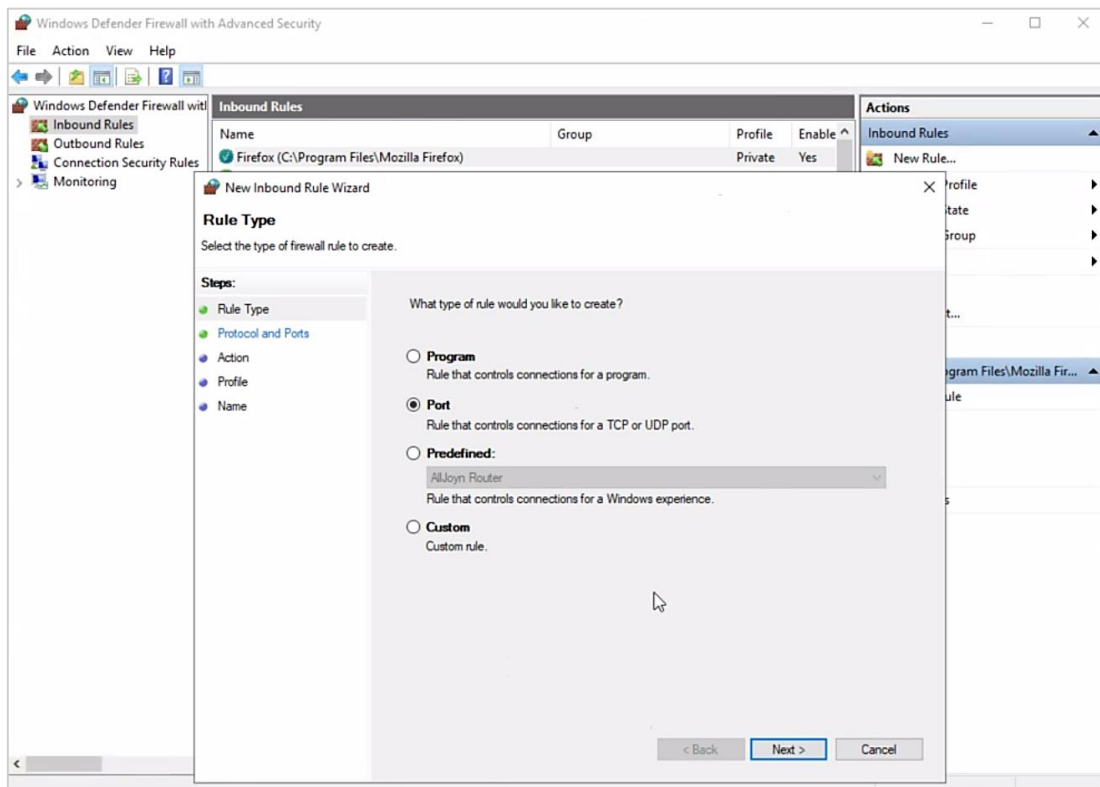


Рисунок 140

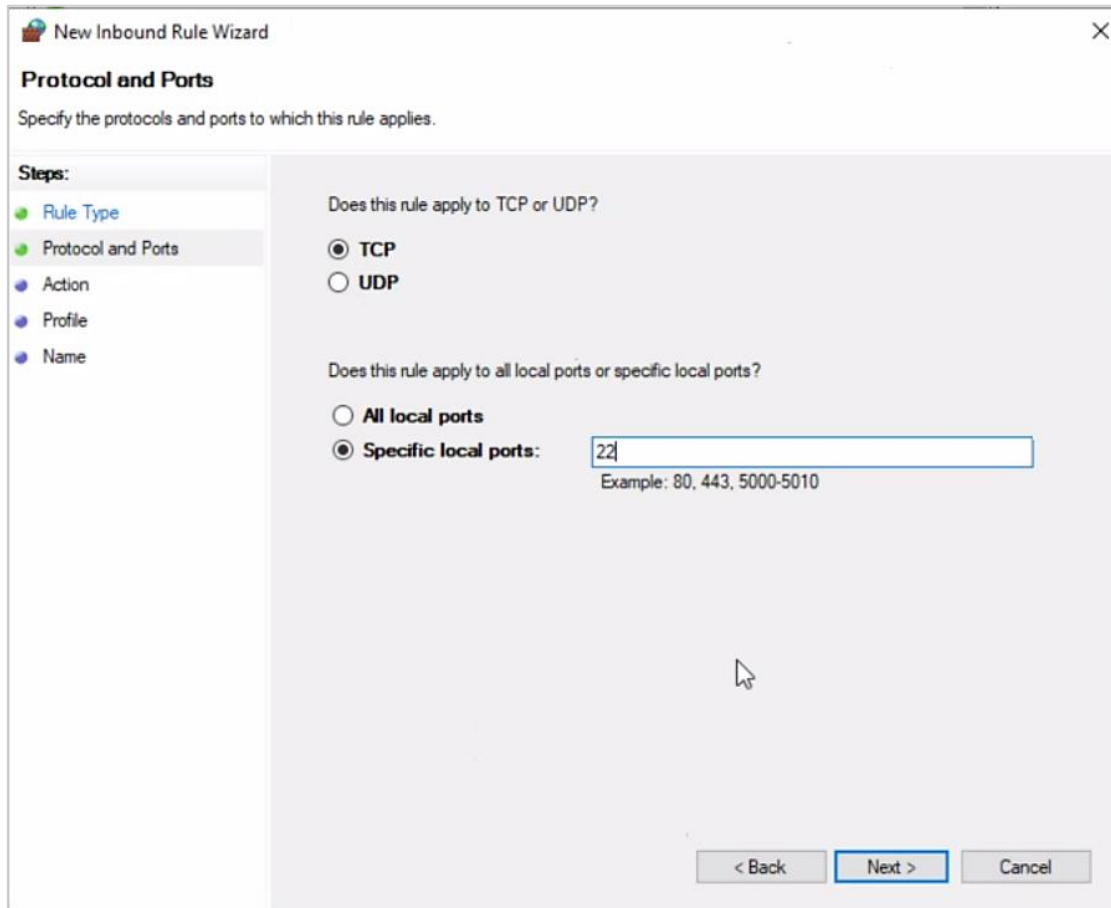


Рисунок 141

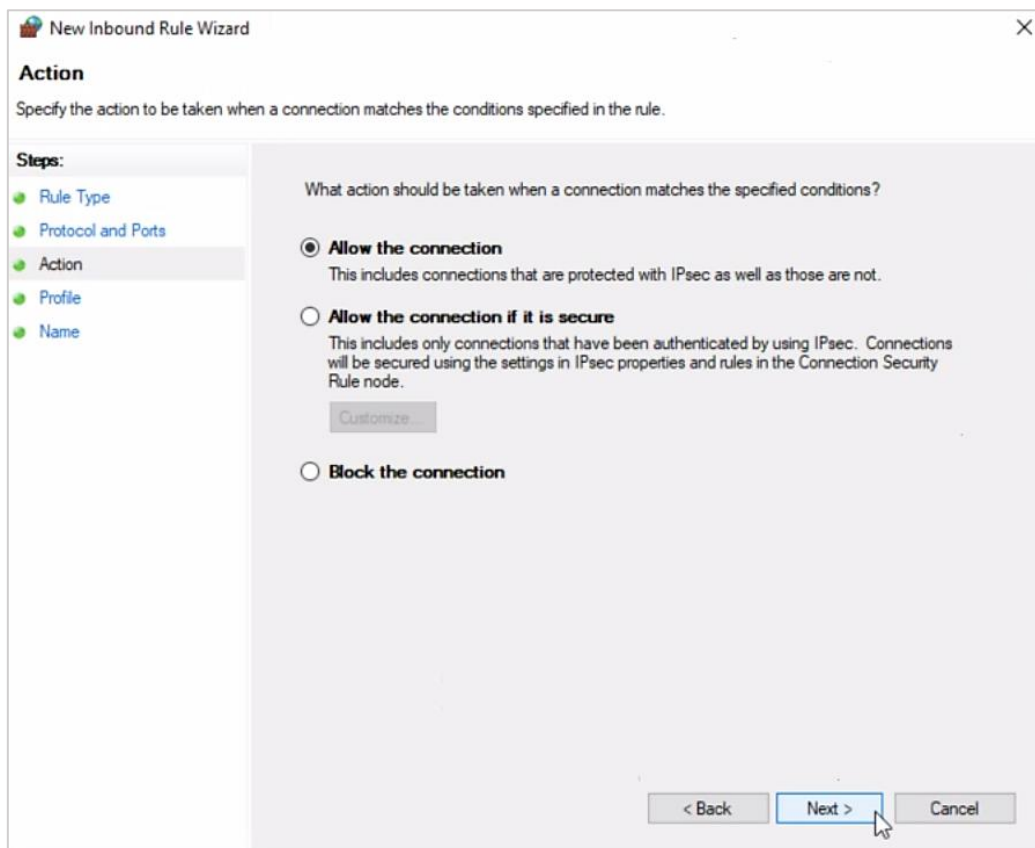


Рисунок 142

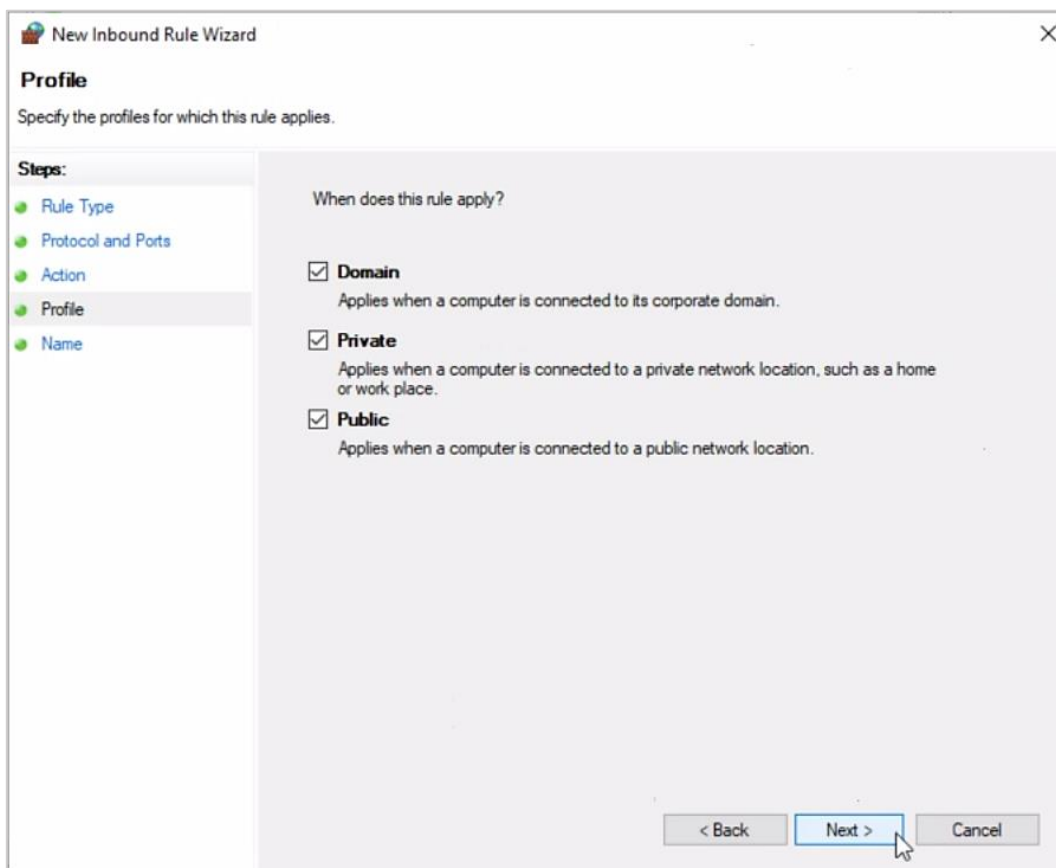


Рисунок 143

- Заходим с ESU-box по SSH на наш сервер и проверяем доступность PowerShell-плагина Veeam следующими командами (Рисунок 144):

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

```
~ $ ssh Administrator@10.11.145.251
Administrator@10.11.145.251's password:
Microsoft Windows [Version 10.0.17763.1397]
(c) 2018 Microsoft Corporation. All rights reserved.

administrator@VBR-01 C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin VeeamPSSnapin
PS C:\Users\Administrator> Get-PSSnapin VeeamPSSnapin

Name       : VeeamPSSnapin
PSVersion  : 5.1
Description : This is a PowerShell snap-in that includes the Veeam's cmdlet.
```

Рисунок 144

- Посмотрим, как называются обычные и ScaleOut репозитории, для этого выполним команду:

```
GET-VBRBackupRepository -ScaleOut
```


Примечание: NetApp Storage GRID должен быть развёрнут обязательно, с другими решениями РУСТЭК-ЕСУ интеграцию не поддерживает!

Чтобы подключить хранилище S3 к РУСТЭК-ЕСУ и использовать его из панели управления достаточно произвести настройку S3 раннера.

Для этого необходимо перейти в меню **Инсталляция** → **Система** → **Раннеры**, выбрать S3-runner и в открывшейся форме ввести информацию в соответствующие поля (Рисунок 147):

- Адрес API NetApp – указать адрес, по которому доступно API NetApp StorageGRID.
- Имя пользователя-администратора – указать логин администратора NetApp StorageGRID.
- Пароль пользователя-администратора – указать пароль администратора NetApp StorageGRID.
- URL к хранилищу S3 – указать URL по которому доступно S3 хранилище.

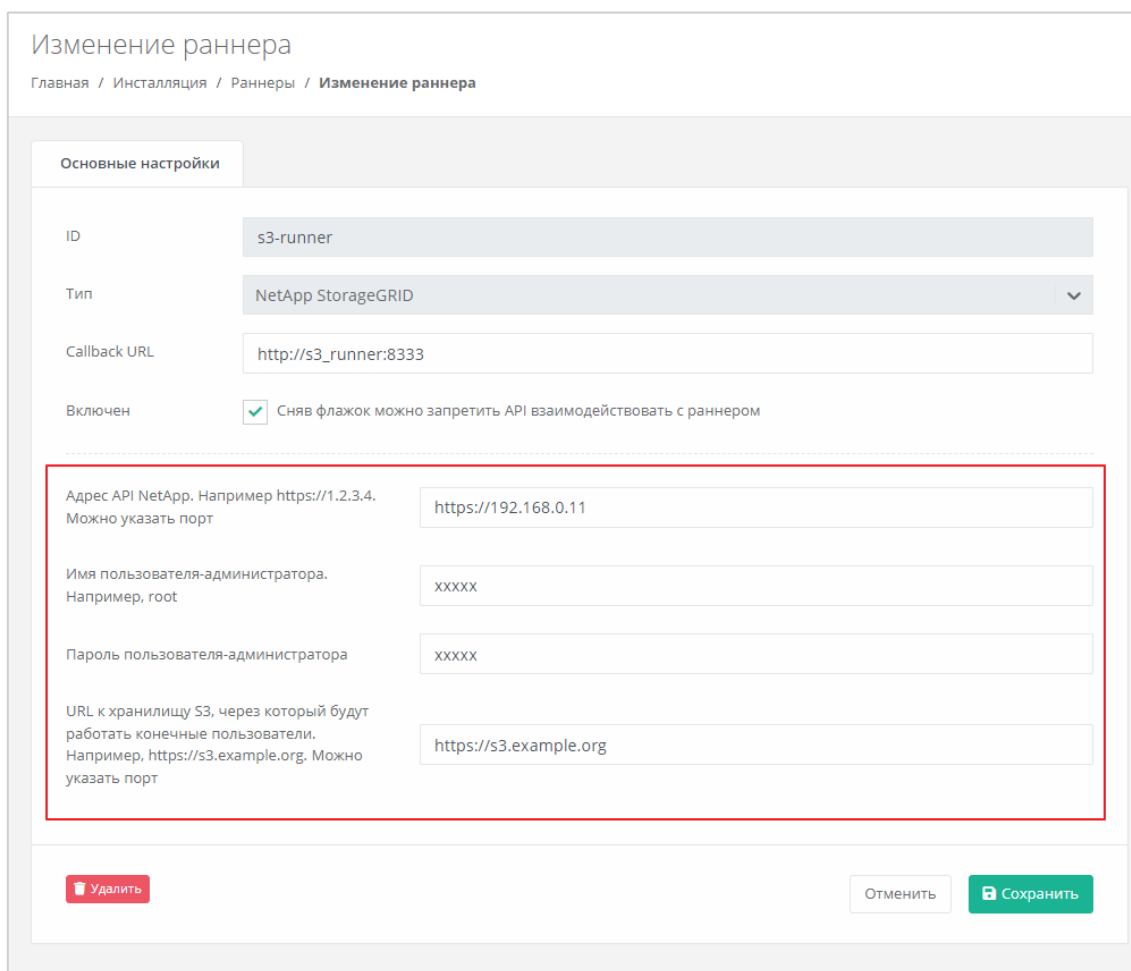


Рисунок 147

После сохранения изменений индикатор S3-раннера должен стать зелёным. После перезагрузки страницы появится пункт **Хранилище S3**.

9.7. Подключение YooKassa к РУСТЭК-ЕСУ

Зачастую, когда инсталляция РУСТЭК-ЕСУ используется в качестве публичного облака, необходимо подключить к ней способы оплаты, с помощью которых клиенты смогут оплачивать заказанные услуги.

Доступные методы оплаты можно задать при создании или изменении клиента в меню **Администрирование** → **Клиенты** (Рисунок 148, Рисунок 149).

Изменение клиента

Главная / Администрирование / Клиенты / Изменение клиента

Основные настройки | Примечания | Лимиты | Управление доступом

Имя: DEFAULT

Партнер: default [Выбрать]

Контракт: Контракт для клиента DEFAULT [Выбрать]
Изменение контракта возможно только на **новый**, который не был связан ни с одной организацией.

Интернет: Включить
Отключение **не приведет** к автоматическому изъятию публичных IP у клиента.

Скорость доступа в Интернет: 1000 Мбит/с
Изменение параметра **не приведет** к изменению скорости подключения к внешней сети на существующих роутерах и будет применено только на новых.

Скорость локальной сети: 1000 Мбит/с
Изменение параметра **не приведет** к изменению на существующих серверах и будет применено только на новых.

Методы оплаты: **Яндекс касса** [Выбрать]

Модель оплаты: Предоплата Постоплата

[Удалить] [Отменить] [Изменить]

Рисунок 148

Выберите

Яндекс касса

Безналичная оплата

[Отменить] [Применить]

Рисунок 149

РУСТЭК-ЕСУ «из коробки» поддерживает работу с сервисом YooKassa (бывшая ЯндексКасса), но для его работы необходимо произвести некоторые настройки, а именно: указать ID вашего магазина и ваш секретный ключ.

Как их получить описано в официальной документации сервиса: <https://yookassa.ru/developers/using-api/interaction-format>

После успешного получения ID магазина и секретного ключа можно переходить непосредственно к настройке РУСТЭК-ЕСУ.

Используя ssh, подключаемся по IP адресу к серверу с запущенной РУСТЭК-ЕСУ (ESU-box) и выполняем команду:

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

В открывшейся консоли вводим:

```
Setting.objects.create(setting_id='yandex_shop_id', target='paymentmethod-yandex', value='ваш_id_магазина')
Setting.objects.create(setting_id='yandex_secret_key', target='paymentmethod-yandex', value='ваш_секретный_ключ')
```

Выходим командой **exit**.

Выходим командой **exit**.

Далее необходимо произвести настройку HTTP уведомлений в личном кабинете YooKassa. Это необходимо для отправки уведомлений о пополнении в РУСТЭК-ЕСУ (Рисунок 150).

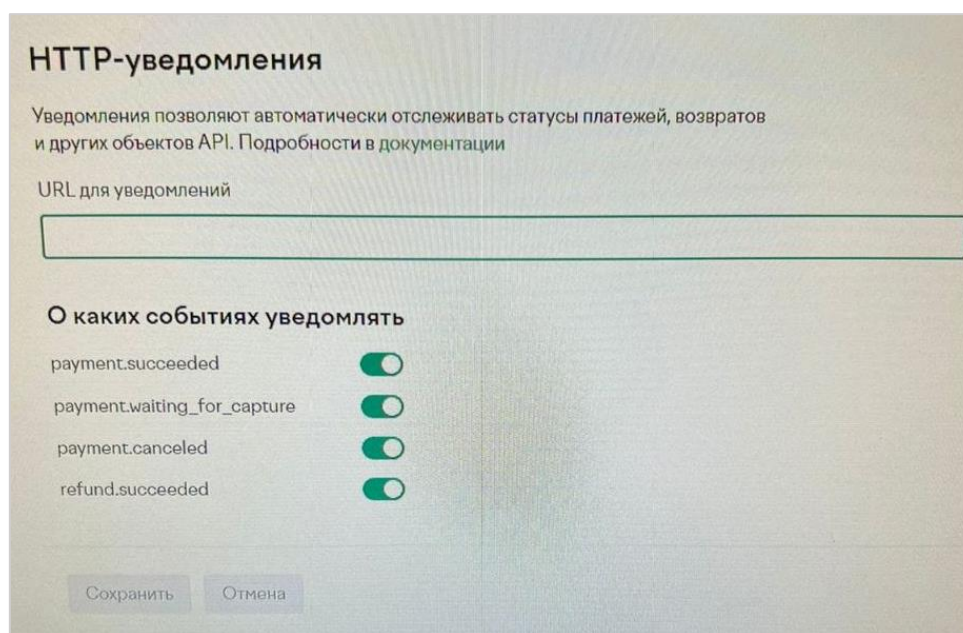


Рисунок 150

URL для уведомлений: https://адрес_API/v1/payment/yandex_payment_callback

На этом настройка завершена.

Примечание: пополнение баланса через сервис YooKassa, возможно только в том случае, если в качестве логина пользователя указан действительный e-mail, в противном случае РУСТЭК-ЕСУ сообщит об ошибке.

Обратите внимание на требования для доставки HTTP уведомлений на официальной странице сервиса: <https://yookassa.ru/developers/using-api/webhooks#configuration>

Для проверки интеграции настоятельно советуем сначала подключить тестовый магазин:

<https://yookassa.ru/developers/payment-acceptance/testing-and-going-live/testing>

9.8. 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.

```
[api]
database_url = postgres://toochka_new:toochka_new@postgres:5432/toochka_new
secret_key = stAizkeCqzmlKituJNb6Ywq3IVoPg4

[runners]
token = f0fcdfa63d087155adebaa95cbdd867f88c216e3

[smtp]
host = smtp
port = 25

[box]
nameserver = 8.8.8.8
ip = 10.11.12.110
gateway = 10.11.12.1
vlan =
monitoring_bot = botiiiiii:xxxxxxxxxxxx:-groupid
vrli_url =

[extras]
esu_bot = 1234567890:token-uuid
website_url =
```

Рисунок 151

Измените выделенные строки (Рисунок 151) на:

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

Сохраните изменения в конфигурационном файле `toochka.conf`.

7. Выполните команду:

```
sudo toochkactl configure
```

В результате в консоль будет выведен процесс конфигурации.

```
deploy@localhost:~$ sudo toochkactl configure
sudo: unable to resolve host localhost: Name or service not known

TooChka

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] *****ok: [localhost]

TASK [box_configure : Fix docker conf] *****
ok: [localhost]

TASK [box_configure : Set timezone to Europe/Moscow] *****
ok: [localhost]

TASK [box_configure : Restart services] *****
changed: [localhost] => (item=ntp)

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

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

Рисунок 152

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

Версия соглашения	<input type="text"/>
Минимальный остаток по умолчанию для пользователей домена	<input type="text" value="1000"/>
Имя бота Telegram для управления платформой клиентами	<input type="text" value="test_bot"/>
URL базы знаний. Доступна переменная {query}	<input type="text" value="https://kb.rustack.ru/ru/products/rustack-esu"/>

Рисунок 153

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 154).

Профиль

Главная / Профиль

Профиль | Публичные ключи | Сессии

ФИО: admin

Логин: admin

Телефон: +7 () - - - -

Минимальный остаток: ₪ 1000
Для предоплаченных клиентов — минимальный остаток на счете, при котором будет отправлено уведомление о низком балансе.

Уведомления о серверах: Отправлять уведомления о созданных виртуальных серверах

Уведомления о резервных копиях: Отправлять уведомления о созданных автоматически или вручную резервных копиях

Telegram аккаунт:

Telegram бот:
@esu88888888_bot предоставляет ограниченное управление вашей облачной инфраструктурой через Telegram

Двухфакторная авторизация: Отключена Телефон E-mail Telegram Одноразовый пароль

[Изменить пароль](#) [Паспортные данные](#)

Рисунок 154

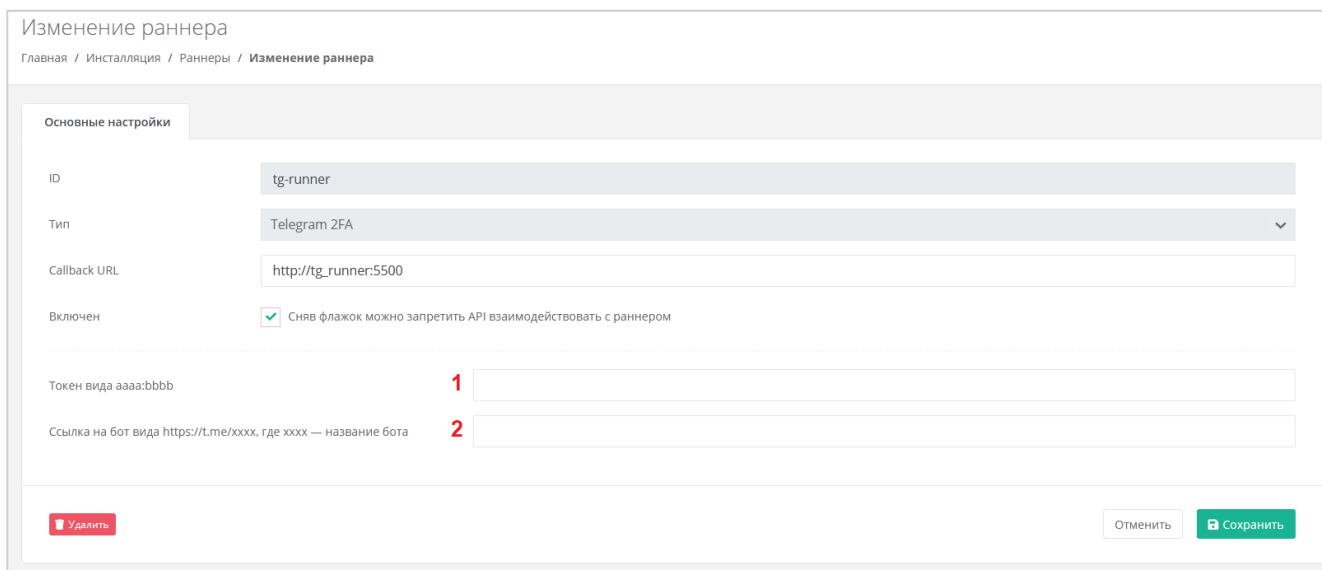
9.9. Подключение Telegram-бота к РУСТЭК-ЕСУ для двухфакторной авторизации

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 аааа:bbbb» (Рисунок 155, 1) введите (вставьте) токен, полученный от @botfather на шаге 5.
8. В поле «Ссылка на бот вида https://t.me/xxxx» (Рисунок 155, 2) введите **https://t.me/xxxx**, где **xxxx** — username бота, который вы вводили на шаге 4.



Изменение раннера

Главная / Установка / Раннеры / Изменение раннера

Основные настройки

ID: tg-runner

Тип: Telegram 2FA

Callback URL: http://tg_runner:5500

Включен: Сняв флажок можно запретить API взаимодействовать с раннером

Токен вида аааа:bbbb **1**

Ссылка на бот вида https://t.me/xxxx, где xxxx — название бота **2**

Удалить Отменить Сохранить

Рисунок 155

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

10. Развёртывание на платформе виртуализации VMware vSphere

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

10.1. Системные требования

Для развёртывания на платформе виртуализации VMware vSphere необходимы:

- VMware vSphere (6.7, 7.0);
- dvSwitch и сервисная портгруппа, одна маршрутизируемая подсеть не меньше /27 с доступом до сетей хостов VMware и Vcenter

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 VM 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 dvSwitch, под которым будут создаваться пользовательские сети (порт-группы).

10.2. Порядок развёртывания

Создаём management-сеть РУСТЭК-ЕСУ – портгруппу на dvSwitch в vSphere (требуется один VLAN). Необходимо учитывать, что в эту сеть будут подключены пользовательские роутеры для сегмента VMware и что сеть должна быть маршрутизируемой.

Таким образом, размер подсети напрямую влияет на максимальное число ВЦОДов. Сервер с установленной РУСТЭК-ЕСУ (ESU-box) станет DHCP-сервером в этой подсети.

Заводим маршрутизируемую сеть внутри dvSwitch в vSphere, в данном примере она называется ESU_management_vlan3235_n10.11.14.0m24, VLAN ID 3235 (Рисунок 156 – Рисунок 159).

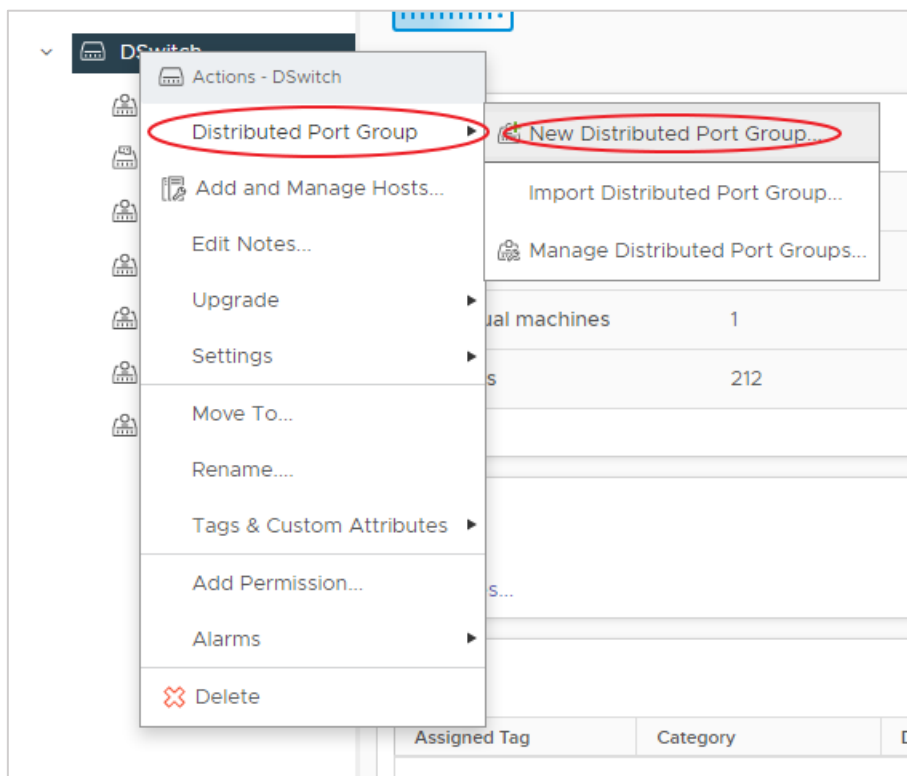


Рисунок 156

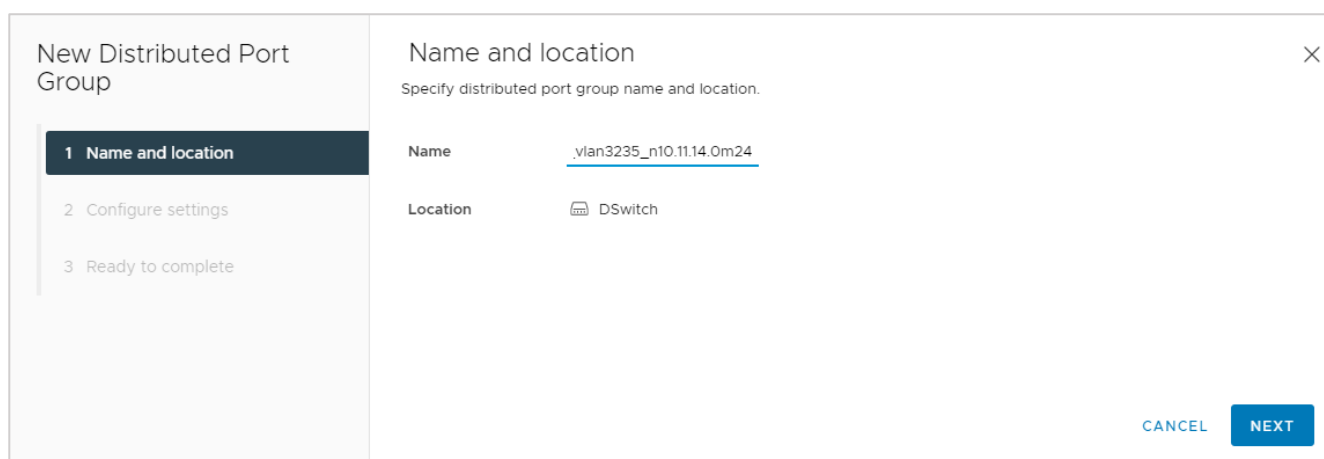


Рисунок 157

New Distributed Port Group

- 1 Name and location
- 2 Configure settings
- 3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding ▼
Port allocation	Elastic ▼ ⓘ
Number of ports	250
Network resource pool	(default) ▼

VLAN

VLAN type	VLAN ▼
VLAN ID	3235

Advanced

Customize default policies configuration

CANCEL
BACK
NEXT

Рисунок 158

New Distributed Port Group

- 1 Name and location
- 2 Configure settings
- 3 Ready to complete

Ready to complete

Review the changes before proceeding.

Distributed port group name	ESU_management_vlan3235_n10.11.14.0m24
Port binding	Static binding
Number of ports	250
Port allocation	Elastic
Network resource pool	(default)
VLAN ID	3235

CANCEL
BACK
FINISH

Рисунок 159

Переходим в редактирование созданной портгруппы и удостоверимся, что параметры указаны в соответствии с указанными ниже (Рисунок 160 – Рисунок 161).

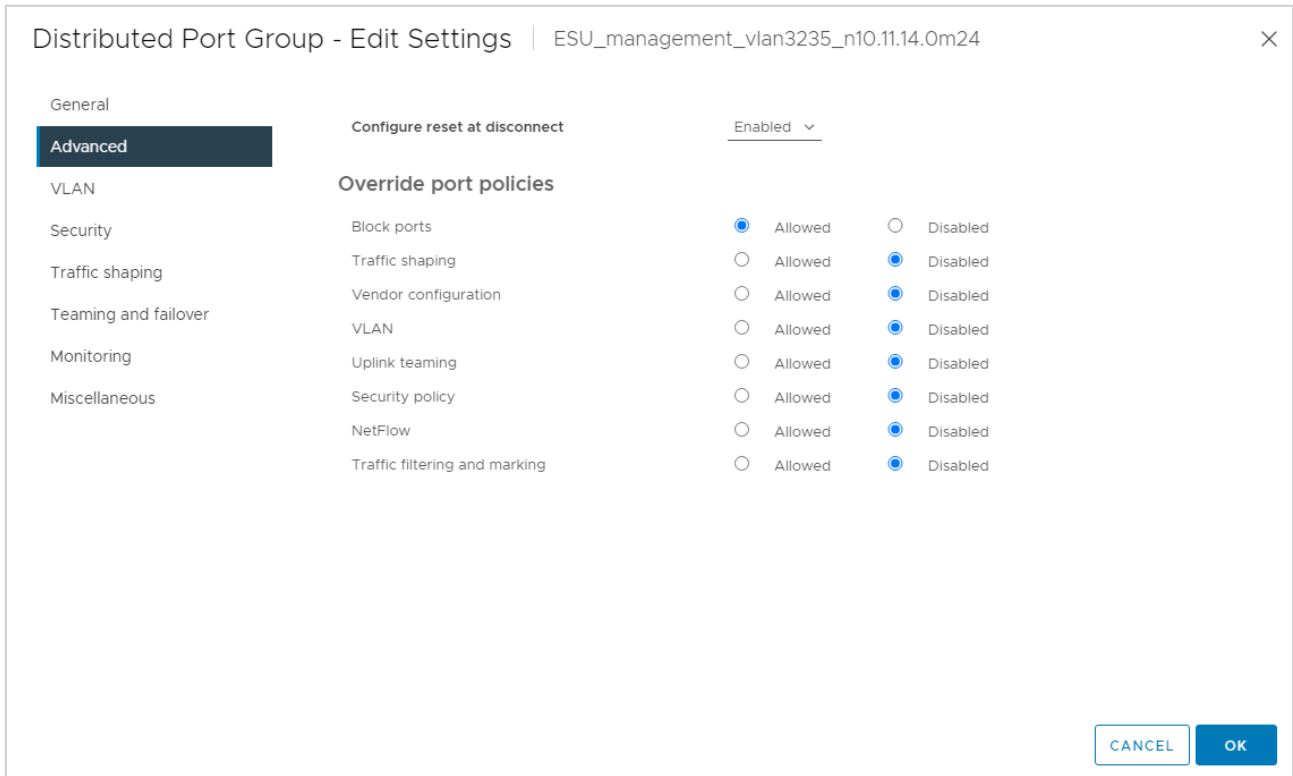


Рисунок 160

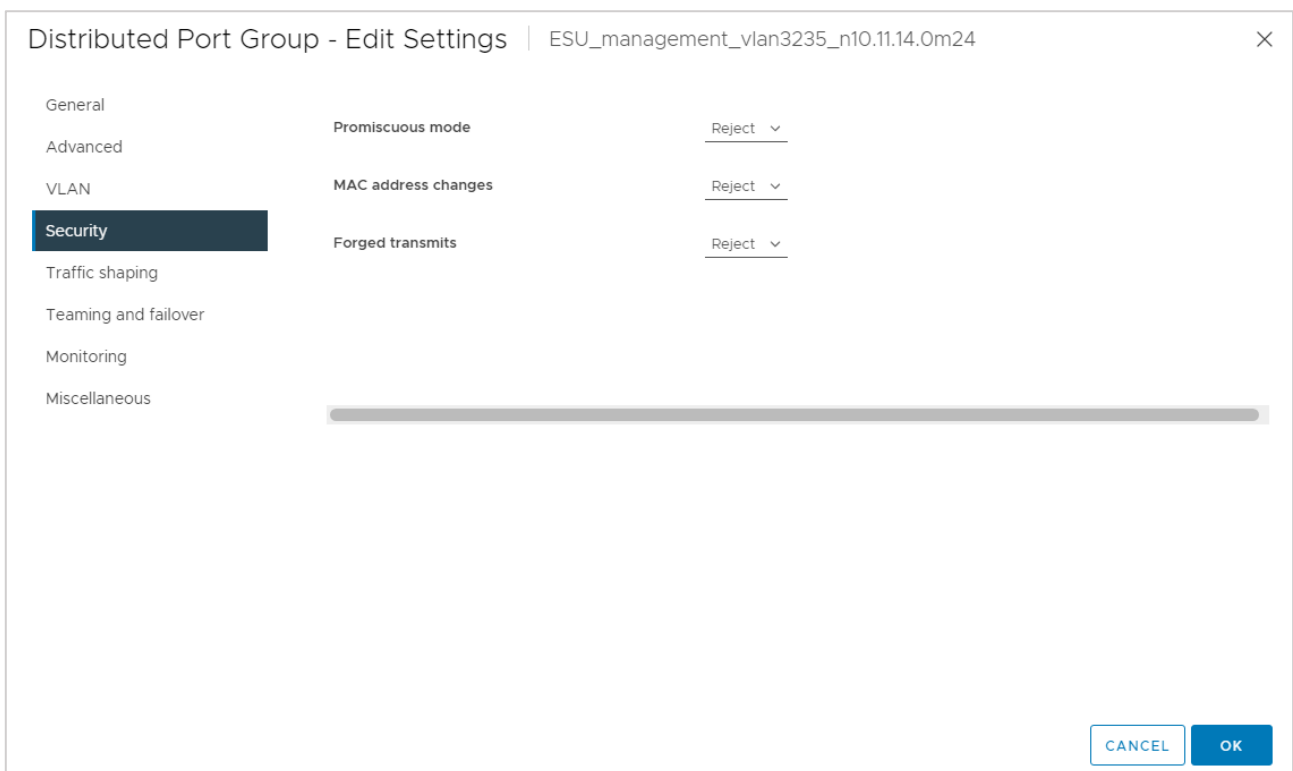


Рисунок 161

Создаём директорию, в которой будут расположены ВЦОДы клиентов и сама РУСТЭК-ЕСУ (ESU-box). Например, ESU3, а в ней создадим папку Management (Рисунок 162 – Рисунок 165):

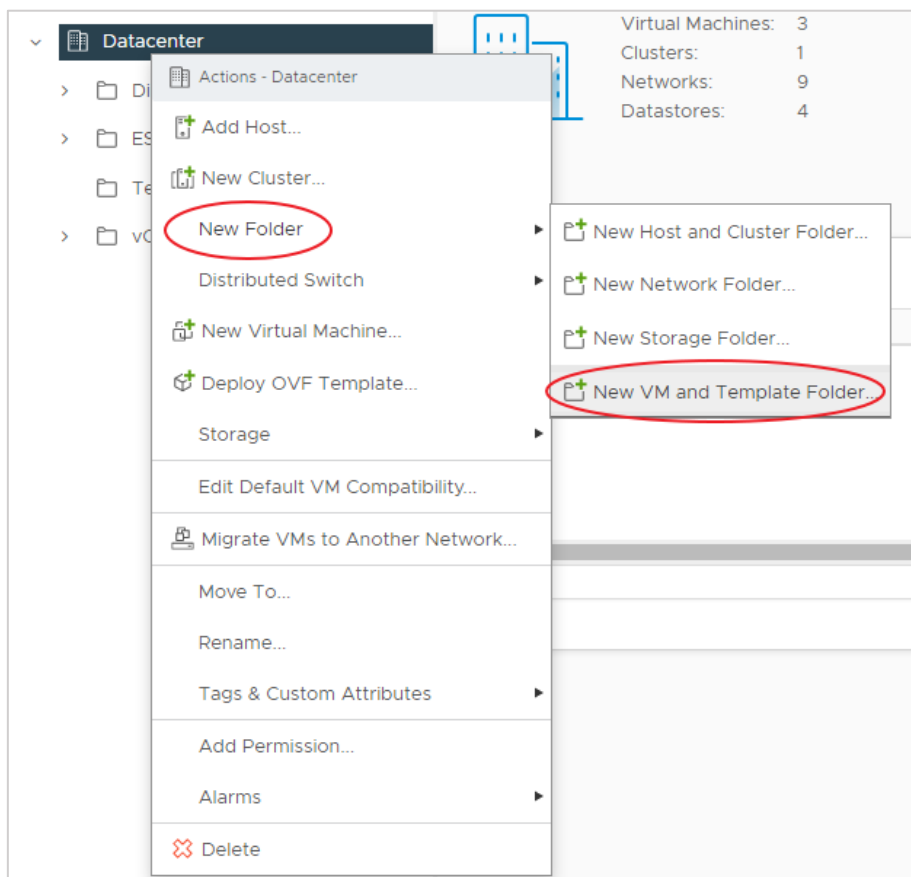


Рисунок 162



Рисунок 163

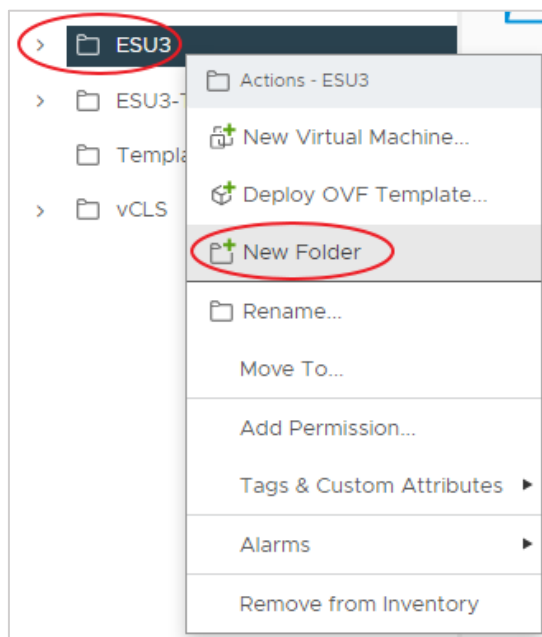


Рисунок 164

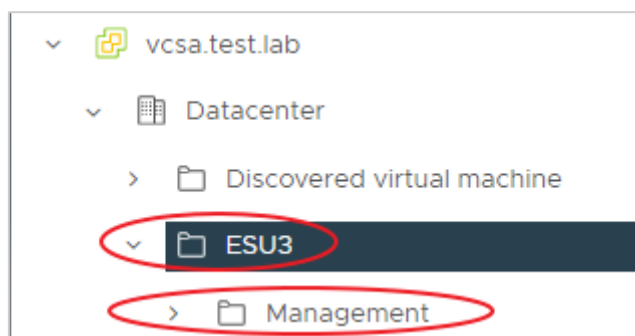


Рисунок 165

Далее необходимо загрузить предоставленный образ сервера с РУСТЭК-ЕСУ (ESU-box) в vSphere. Для этого выбираем папку Management и нажимаем «Deploy OVF Template» (Рисунок 166).

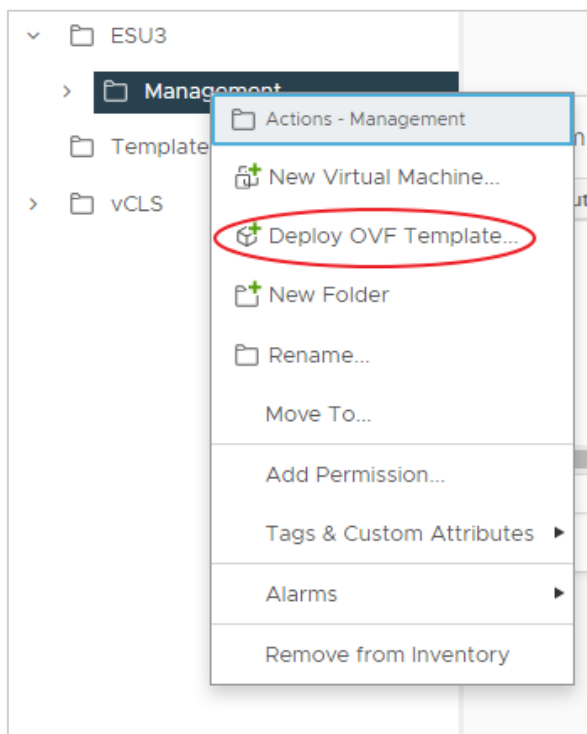


Рисунок 166

Далее выбираем предоставленный .ova-образ (Рисунок 167).

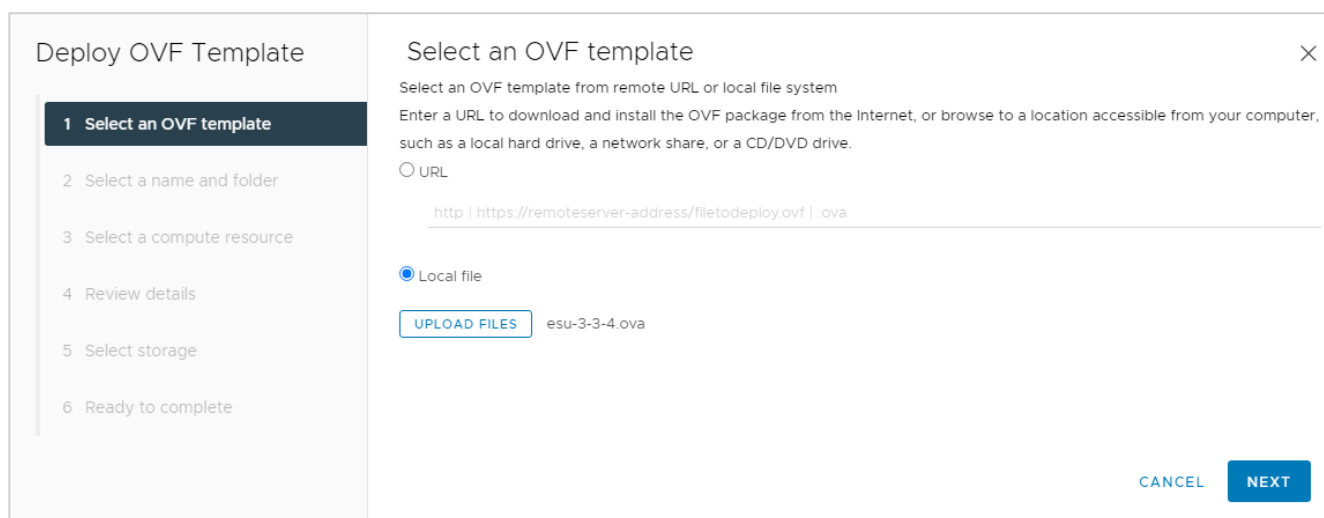


Рисунок 167

Выбираем созданную папку Management, где будет развёрнут сервер (Рисунок 168).

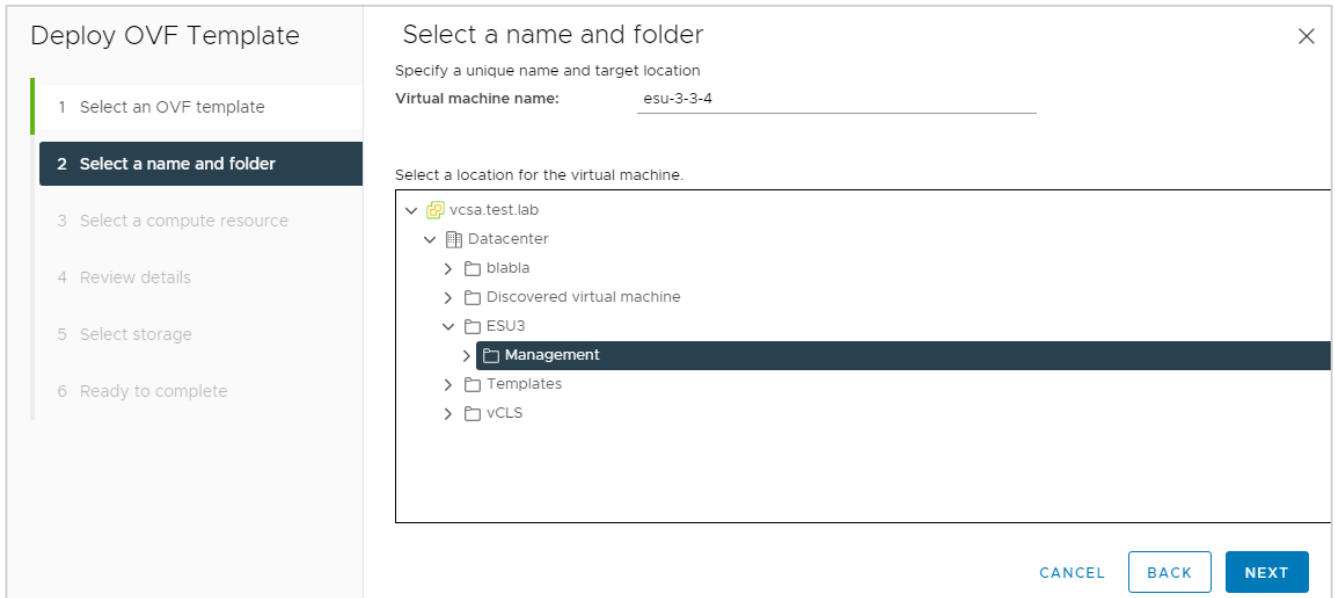


Рисунок 168

Выбираем кластер, где будет развёрнут сервер (Рисунок 169).

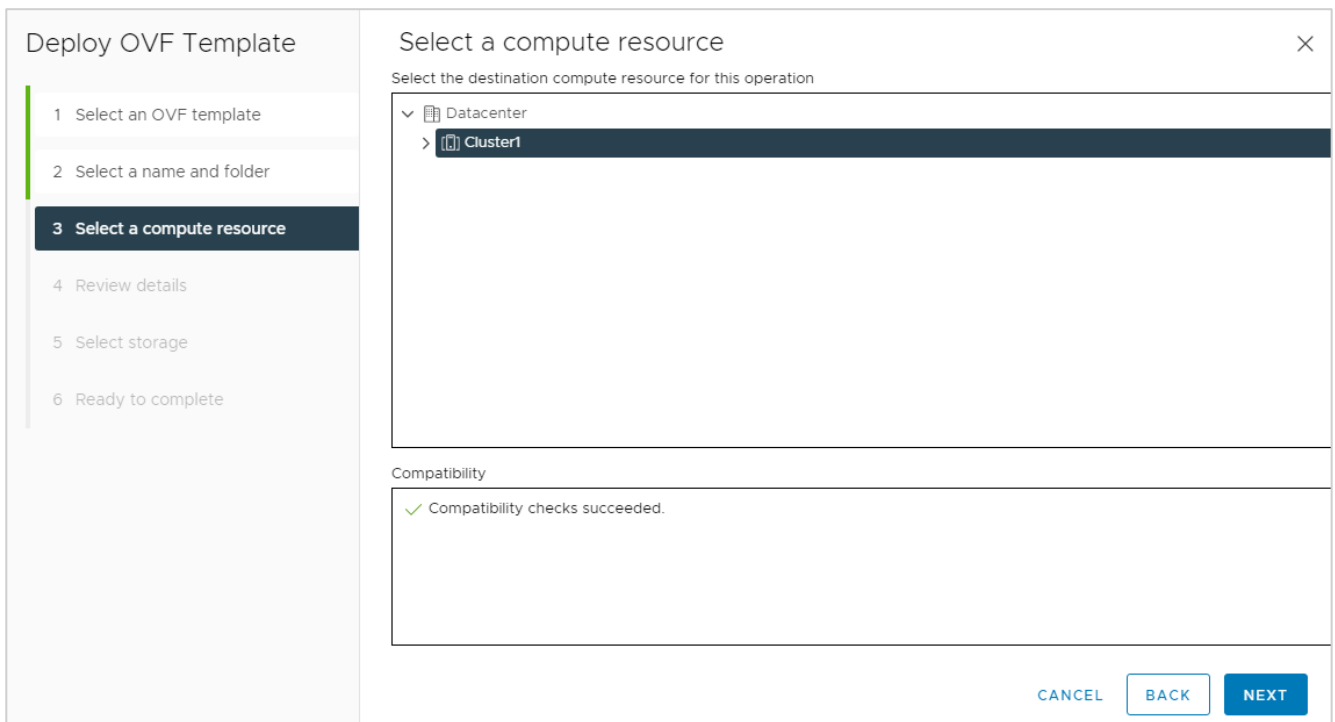


Рисунок 169

Подтверждаем дальнейшие действия (Рисунок 170).

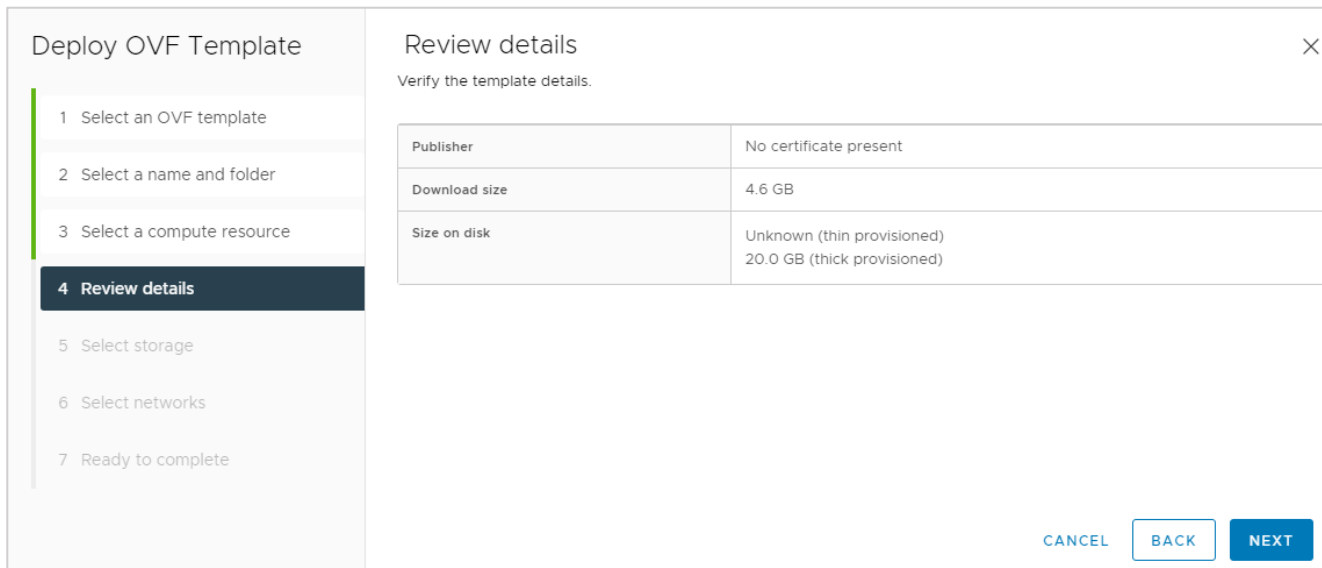


Рисунок 170

Выбираем формат диска Thin Provision и датастор для диска сервера (Рисунок 171).

Thin Provision должен быть выбран обязательно!

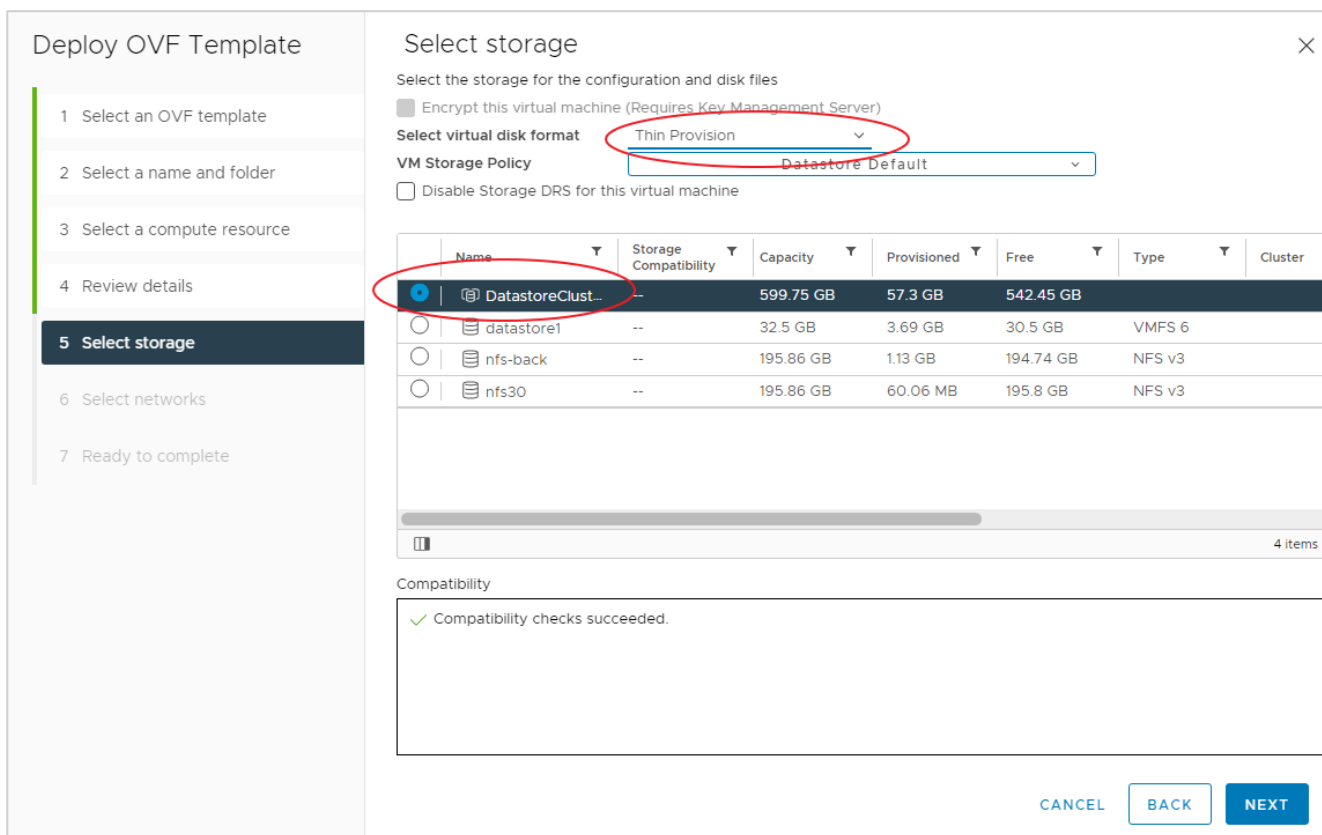


Рисунок 171

Выбираем сеть, которая будет подключена к нашему серверу. Выбираем созданную ранее и заведённую в dvSwitch портгруппу, в следующем окне жмём «FINISH» (Рисунок 172, Рисунок 173).

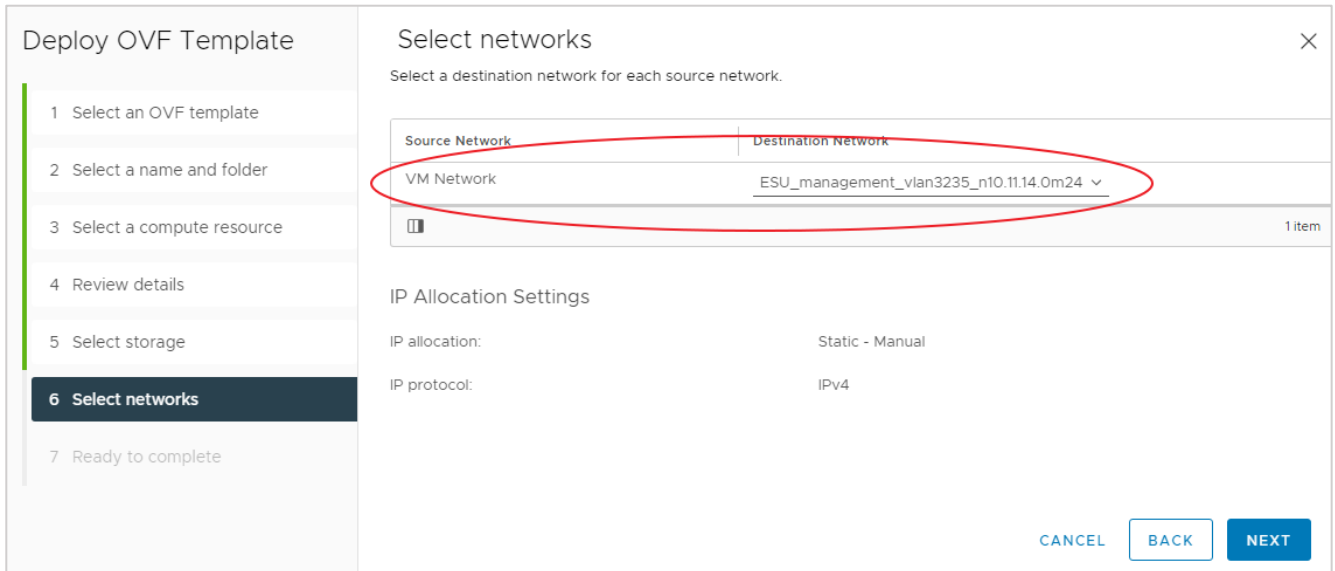


Рисунок 172

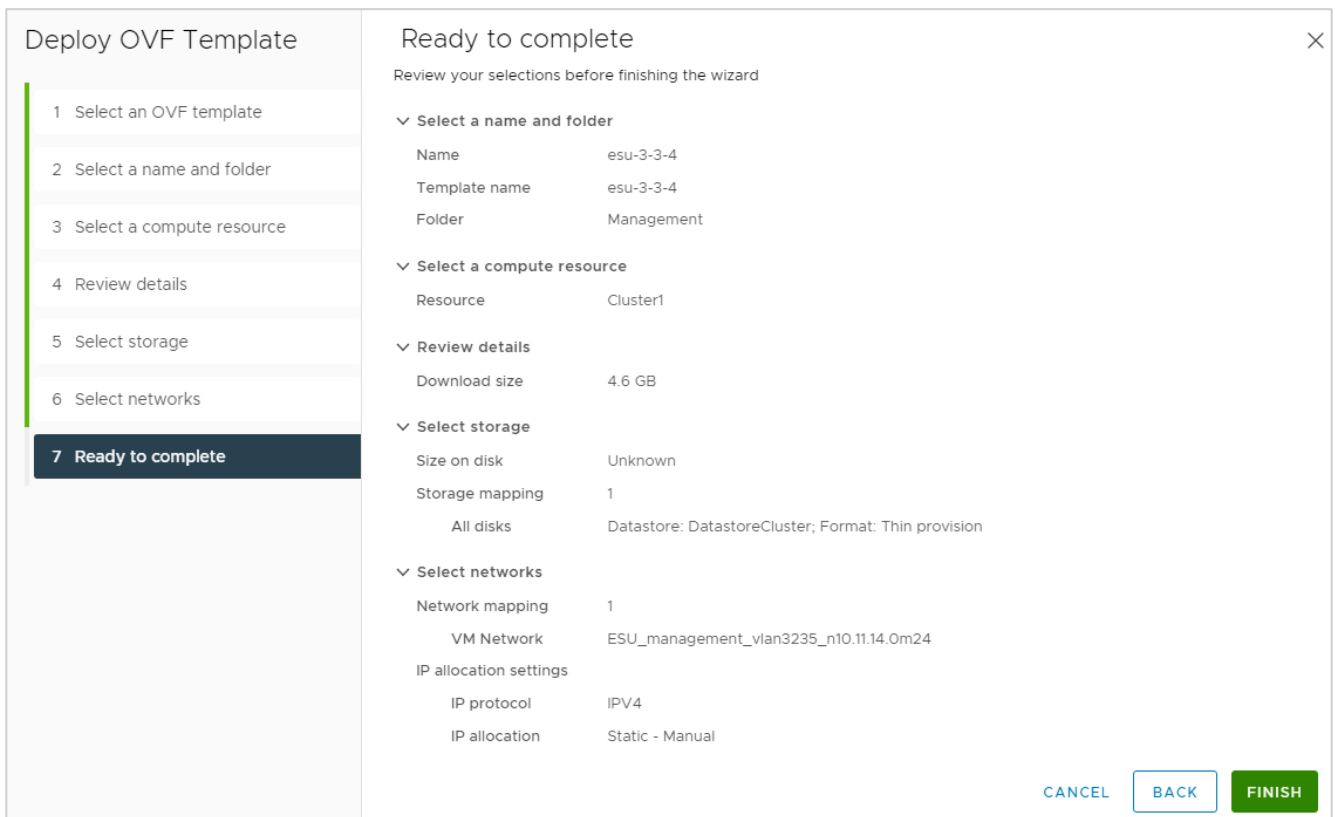


Рисунок 173

Начнётся процесс развёртывания (Рисунок 174).

Task Name	Target	Status	Details	Initiator	Queued For
Deploy OVF template	Cluster1	50%	Copying Virtual Machine co...	VCSA.TEST.LAB\vpvxd-extensio...	6 ms
Import OVF package	Cluster1	54%		vcsa.test.lab\Administrator	206 ms

Рисунок 174

После развёртывания включаем сервер и открываем консоль (Рисунок 175).

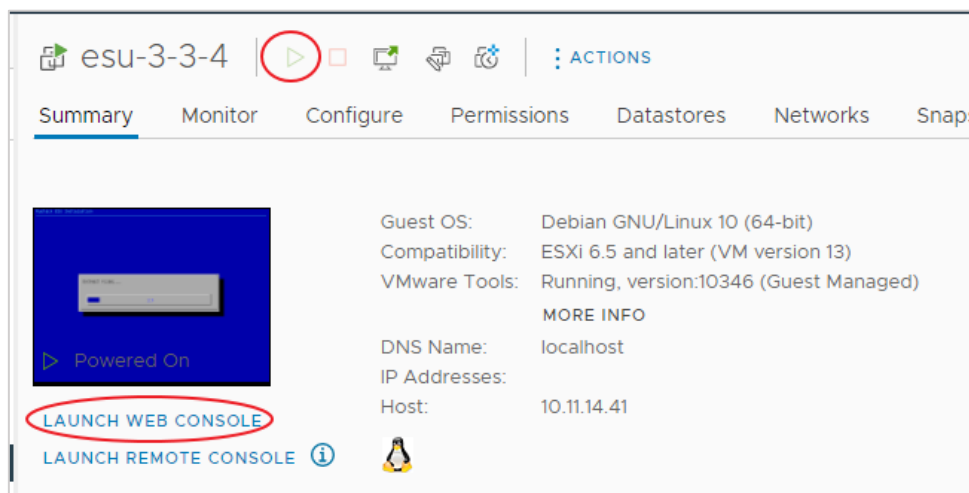


Рисунок 175

Стандартная учётная запись на сервере с РУСТЭК-ЕСУ (ESU-box): **deploy:1-qpALzm/**

10.3. 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 dvSwitch портгруппы. Адрес должен быть выделен заранее (см. Рисунок 14).
- 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/KVM в панели управления РУСТЭК-ЕСУ необходимо завести внешнюю сеть и подсеть для неё в платформу виртуализации РУСТЭК. Процесс создания внешней сети и подсети описан в пунктах (см. раздел 2.2, пункты 4, 5).
- Для создания кластеров Kubernetes в сегменте РУСТЭК/KVM (см. раздел 8) в панели РУСТЭК необходимо завести сеть аналогичную портгруппе в dvSwitch. Далее процесс настройки одинаков для обоих случаев. Процесс создания сети и подсети в РУСТЭК описан в пунктах (см. раздел 2.2, пункты 4, 5). Безопасность портов и DHCP должны быть отключены.

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

11. Подготовка инфраструктуры для получения обновлений РУСТЭК-ЕСУ

Обновления РУСТЭК-ЕСУ выпускаются примерно раз в месяц.

Для получения обновлений и использования актуальной версии необходимо настроить свою инфраструктуру для возможности доставки этих обновлений.

Обновление производится службой поставщика продукта с помощью Gitlab-раннера, установленного на стороне заказчика по согласованию с ним.

- Gitlab-раннер может быть установлен на сервер с РУСТЭК-ЕСУ (ESU-box) или на отдельный сервер на базе OS Linux, с которого по SSH доступен ESU-box.
- Сервер с установленным Gitlab-раннером должен иметь исходящий доступ во внешнюю сеть Интернет по протоколу HTTPS – это необходимо для установки связи между Gitlab на стороне поставщика продукта и Gitlab-раннером для доставки обновлений.

Сценарий подготовки к получению обновлений:

- Установить Gitlab-раннер согласно официальной документации: <https://docs.gitlab.com/runner/install/>.
- Предоставить доступ по SSH к серверу ESU-box и к серверу с установленным Gitlab-раннером для проведения процедуры регистрации Gitlab-раннер и авторизации ESU-box в Docker Registry.
- Инженерная служба поставщика продукта осуществляет процедуру регистрации Gitlab-раннера с помощью сгенерированного токена. Процедура описана в официальной документации: <https://docs.gitlab.com/runner/register/>.
- Инженерная служба поставщика продукта осуществляет процедуру авторизации ESU-box в Docker Registry с помощью сгенерированной пары login/password.
- Выполнить команду:

```
sudo docker login -u [user] -p [password] docker.vds2b.com
```

- После проведения процедуры регистрации раннера и авторизации сервера ESU-box (сценарий авторизации ESU-box описан ниже), SSH-доступ можно отключить.
- Дальнейшие настройки для получения обновлений производятся службой поставщика продукта на стороне Gitlab.

Сценарий авторизации ESU-box:

- Установка Gitlab-раннера на стороне заказчика в ESU-box / сервер рядом.
- Генерация токена для регистрации раннера и пары логин/пароль для авторизации ESU-box в Docker Registry на нашей стороне.
- Выдача этих пар заказчику.
- Регистрация раннера с выданной парой логин/пароль на стороне заказчика.

- Авторизация ESU-box в Docker Registry с выданной парой логин/пароль на стороне заказчика.

Приложение 1. Пример Auto DevOps-скрипта

```
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)
```