База знаний РЕД Виртуализация

- РЕД Виртуализация
  - Описание программного продукта
  - Документация
  - Системные требования
    - Аппаратная часть
    - Аппаратное и программное оснащение клиентов
    - Гипервизор
    - Хранилище
    - Ограничения РЕД Виртуализации
  - Подготовка сетевого хранилища: NFS
  - Установка РЕД Виртуализации
    - Установка в режиме Standalone
    - Установка в режиме Host
    - Установка в режиме Gluster Hyperconverged для одного узла
    - Установка в режиме Gluster Hyperconverged для нескольких узлов
    - Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Standalone с помощью стороннего центра сертификации
    - Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Hosted Engine с помощью стороннего центра сертификации
  - Инструмент для смены доменного имени Engine
  - Хосты со статусом «Non Responsive»
  - Настройка параметров расширения "тонких" дисков ВМ
  - Часто задаваемые вопросы (FAQ)
  - Информация об обновлениях

Описание программного продукта

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

РЕД Виртуализация позволяет управлять виртуальными машинами через веб-интерфейс, используя для администрирования библиотеку **libvirt**.

В состав *РЕД Виртуализации* входит реализация веб-интерфейса и служб, необходимых для управления виртуальными машинами. *РЕД Виртуализация* представляет собой образ ОС на основе РЕД ОС, в состав которого включены необходимые пакеты и репозиторий для установки и функционирования системы виртуализации.

РЕД Виртуализация позволяет создавать масштабируемую кластерную систему виртуализации с распределенной системой контроля ресурсов оборудования и полномочий пользователей.

Функции управления виртуальными машинами включают в себя выбор приоритета высокой доступности, живую миграцию, мгновенные снимки в реальном времени, клонирование виртуальных машин из моментальных снимков, создание шаблонов виртуальных машин, использование **cloud-init** для автоматической настройки во время подготовки и развертывания виртуальных машин. Поддерживаемые гостевые операционные системы включают *GNU* / *Linux*, *Microsoft Windows* и *FreeBSD*.

РЕД Виртуализация представляет собой программный продукт, состоящий из следующих компонентов:

- программные средства, предназначенные для установки на аппаратный сервер: гипервизор, базовую операционную систему, вспомогательные компоненты и утилиты;
- система управления виртуализацией *РЕД Виртуализация*;
- документация;
- драйверы паравиртуализации;
- клиентская часть для ОС Windows (версий от XP SP3 и выше);
- инструментарий для построения отчётов по журналам событий;
- утилиты и служебные программы;
- подсистема идентификации и аутентификации.

Документация

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

База знаний по **РЕД Виртуализации** периодически дополняется статьями, которые не были включены в основную документацию.

Полная и актуальная документация включает в себя следующие руководства:

- Руководство по установке и первичной настройке;
- Руководство по администрированию РЕД Виртуализации;
- Руководство по администрированию виртуальных машин РЕД Виртуализации;
- Руководство по созданию и восстановлению резервных копий системы управления РЕД Виртуализация.

Аппаратная часть

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Минимальные и рекомендуемые требования к оборудованию, описанные здесь, основаны на типичной установке малого и среднего размера. Точные требования по конкретной конфигурации различаются в разных случаях в зависимости от её размера и нагрузки.

Требования к оборудованию указаны в таблице 1.

Таблица 1. Минимальные и рекомендуемые требования к оборудованию

Конфигурация	Минимальная	Рекомендуемая
Процессор	Двухядерный процессор	Четырехъядерный процессор или несколько двухъядерных процессоров
Оперативная память	16 Гб установленной оперативной памяти	32 Гб установленной оперативной памяти
Жесткий диск	80 Гб доступного дискового пространства	100 Гб доступного дискового пространства
Сетевой интерфейс	1 сетевой интерфейс с пропускной способностью 1 Гбит/с	1 сетевой интерфейс с пропускной способностью 10 Гбит/с

Минимальных и рекомендуемых требований достаточно только для установки системы виртуализации, в которой управляющее ядро engine расположено непосредственно на хосте виртуализации. Дальнейшая работа системы виртуализации требует дополнительных ресурсов, в случае запуска кластера – отдельного сетевого хранилища.

Для расчета дополнительных ресурсов необходимых для работы системы виртуализации можно использовать следующие базовые единицы:

- 1 физическое ядро на каждую виртуальную машину;
- 4 ГБ оперативной памяти на каждую виртуальную машину;
- 30 ГБ свободного дискового пространства для каждой виртуальной машины.

При организации кластера необходимо подключать сетевое хранилище отдельным сегментом высокоскоростной сети.

ВАЖНО!

Для корректной работы РЕД Виртуализации требуется:

- физический сервер (установка РЕД Виртуализации в виртуальной машине также возможна, но не гарантируется ее корректная работа);
- готовое хранилище (программное или аппаратное);
- во время установки должен быть подключен только один сетевой интерфейс,

управление которым будет передано гипервизору РЕД Виртуализации.

Аппаратное и программное оснащение клиентов

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Доступ к управлению виртуальными машинами можно получить с помощью веб-браузера. Имеется **портал администрирования** и **портал виртуальных машин**. Рекомендуется использовать одну из последних версий **Mozilla Firefox** или **Chromium**.

Доступ к консолям виртуальных машин можно получить с помощью поддерживаемых клиентов удаленного просмотра (**Virtual viewer**) в системах Linux и Windows. Рекомендуется использовать протокол **SPICE**. SPICE в настоящее время поддерживает максимальное разрешение **2560x1600** пикселей.

Для доступа к виртуальным машинам с терминальных клиентов используется специальный клиент, поставляемый в комплекте с программным обеспечением.

Гипервизор

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Центральный процессор

Все процессоры должны иметь поддержку расширений процессоров **Intel® 64** или **AMD64**, а также включенные расширения аппаратной виртуализации **AMD-V™** или **Intel VT®**. Также требуется поддержка настройки **No eXecute** (NX).

Поддерживаются следующие модели процессоров **AMD**:

- Opteron G1-G5;
- EPYC.

Поддерживаются следующие модели процессоров **Intel**:

- Nehalem;
- Westmere;
- SandyBridge;
- IvyBridge;
- Haswell;
- Broadwell;
- Cascadelake;
- Skylake;
- Icelake.

Поддерживаются следующие модели процессоров **AArch64**:

- Huawei Kunpeng 920.

Проверка, поддерживает ли процессор требуемые флаги, приведена далее.

Необходимо включить виртуализацию в BIOS, выключите питание и перезагрузите хост после этого изменения, чтобы убедиться, что оно применено. Далее:

1. Загрузитесь в операционную систему и зарегистрируйтесь под пользователем, имеющим административные права;

2. В командной строке определите, что ваш процессор имеет необходимые расширения и что они включены, выполнив эту команду:

```
grep -E 'svm|vmx' /proc/cpuinfo
```

Если отображается какой-либо вывод, то процессор поддерживает аппаратную виртуализацию. Если выходные данные не отображаются, процессор может по-прежнему поддерживать аппаратную виртуализацию, но она заблокирована в BIOS. Обратитесь к BIOS системы и руководству по материнской плате, предоставленному производителем.

Оперативная память

Минимальная необходимая оперативная память - **8 ГБ**. Максимальная поддерживаемая оперативная память составляет **4 ТБ**.

Однако объем требуемой оперативной памяти зависит от требований гостевой операционной системы, требований гостевых приложений, активности и использования гостевой памяти. **KVM** также может перерасходовать физическую оперативную память для виртуальных пользователей, позволяя вам предоставлять таким пользователям требования к оперативной памяти, превышающие те, что физически присутствуют, при условии, что пользователи не все работают одновременно при пиковой нагрузке. *KVM* делает это, только выделяя ОЗУ для пользователей по мере необходимости и перемещая контент неактивных пользователей в **swap** (файл подкачки, расположен на локальном физическом носителе хоста).

Жёсткие диски

Хосты требуют локального хранилища для хранения конфигурации, журналов, дампов ядра и для использования в качестве пространства подкачки.

Это минимальные требования к хранилищу для установки хоста РЕД Виртуализации. Мы рекомендуем использовать значения, превышающие те, что указаны ниже:

- /(root) - **6 ГБ**;
- /home - **1 ГБ**;
- /tmp - **1 ГБ**;
- /boot - **1 ГБ**;
- /var - **15 ГБ**;
- /var/crash - **10 ГБ**;
- /var log - **8 ГБ**;
- /var/log/audit- **2 ГБ**;
- swap - **1 ГБ**;
- резерв **20%** размера пула в группе томов для будущего расширения метаданных.

Минимальный общий объем - **75 ГБ**.

PCI устройства

Хосты должны иметь по крайней мере один сетевой интерфейс с минимальной пропускной способностью **1 Гбит/с**. Рекомендуется, чтобы каждый узел имел два сетевых интерфейса с одним выделенным для поддержки интенсивных сетевых действий, таких как миграция виртуальных машин. Производительность таких операций ограничена доступной пропускной способностью.

Требования к назначению устройств

Если вы планируете реализовать назначение устройств и передачу данных **PCI**, чтобы виртуальная машина могла использовать определенное устройство **PCI-e** с хоста, убедитесь, что выполнены следующие требования:

1. Процессор должен поддерживать **IOMMU** (например, VT-d или AMD-Vi);

2. Прошивка должна поддерживать перепрошиваемый модуль и использование IOMMU;

3. Корневые порты процессора должны поддерживать ACS или ACS-эквивалентные возможности;

4. PCI-e устройства должны поддерживать ACS или ACS-эквивалентные возможности.

Рекомендуется, чтобы все коммутаторы PCI-e и мосты между устройством PCI-e и корневым портом поддерживали ACS. Например, если коммутатор не поддерживает ICS, все устройства за этим коммутатором используют одну и ту же группу IOMMU и могут быть назначены только одной виртуальной машине.

Для поддержки графических процессоров используется назначение устройств PCI для **NVIDIA K-Series Quadro** (модель 2000 серии или выше), **GRID** и **Tesla** на основе PCIe в качестве графических устройств без **VGA**. В настоящее время к виртуальной машине может быть подключено до двух графических процессоров в дополнение к одному из стандартных эмулируемых интерфейсов VGA. Эмулируемая VGA используется для предварительной загрузки и установки, а графический процессор NVIDIA начинает работать после загрузки графических драйверов NVIDIA. Обратите внимание, что **NVIDIA Quadro 2000** не поддерживается, равно как и карта **Quadro K420**.

Требования к vGPU

Если вы планируете настроить узел, чтобы разрешить виртуальным машинам на этом узле устанавливать **vGPU**, необходимо выполнить следующие требования:

1. vGPU-совместимый графический процессор;

2. Ядро хоста с поддержкой GPU;

3. Установленный графический процессор с драйверами;

4. Предварительно заданный тип mdev_type соответствует одному из типов mdev, поддерживаемых устройством;

5. Драйверы с поддержкой vGPU, установленны на каждом узле кластера;

6. vGPU-поддерживается операционной системой виртуальной машины с установленными графическими драйверами.

Требования к сети

Система управления и все хосты должны иметь **полное доменное имя** и **полное прямое и обратное разрешение имен**. Настоятельно рекомендуется использовать **DNS**; использование файла **/etc/hosts** для разрешения имен обычно требует больше работы и большую вероятность ошибки.

Из-за широкого использования DNS в среде «РЕД Виртуализация» запуск службы DNS в качестве виртуальной машины, размещенной в среде, не поддерживается. Все службы DNS, используемые средой «РЕД Виртуализация» для разрешения имен, должны размещаться вне этой среды.

Хранилище

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

«РЕД Виртуализация» использует централизованную систему хранения для образов дисков виртуальных машин, файлов ISO и снимков. Сеть хранения данных может быть реализована с использованием:

- сетевой файловой системы **NFS**;
- **GlusterFS**;
- других POSIX-совместимые файловые системы;
- **iSCSI**;
- протокола Fibre Channel (**FCP**);
- параллельной NFS (**pNFS**).

Настройка хранилища является обязательным условием для нового центра обработки данных, поскольку центр обработки данных не может быть инициализирован, если домены хранения не подключены и не активированы.

Ограничения РЕД Виртуализации

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

На основе тестирования производительности РЕД Виртуализации как крупномасштабной среды определены также **максимальные рекомендуемые значения** для системы.

Для логических объектов РЕД Виртуализации предусмотрены следующие **ограничения**:

- *Дата-центр*:
  - максимальное количество одновременно работающих виртуальных машин на одном Engine с несколькими центрами обработки данных: **4000**;
  - максимальное количество центров обработки данных: **400**;
  - максимальное количество хостов: **250** на один центр обработки данных;
  - максимальное количество ВМ: **4000**.

- *Кластер*:
  - максимальное количество кластеров: **400** (400 кластеров в одном центре обработки данных либо по одному кластеру в каждом из 400 центров обработки данных);
  - максимальное количество ВМ: **4000**.

- *Сеть*:
  - на один хост: **200**;
  - на один кластер: **300**;
  - максимальное общее количество сетей: **100** на 150 хостах либо **60** на кластер с 250 хостами.

- *Место хранения*:
  - максимальное количество доменов на центр обработки данных: **50**. Однако каждый дополнительный домен хранения может приводить к некоторому снижению производительности.

    Рекомендуется использовать только необходимое для работы количество доменов хранения.
  - количество хостов на домен: **без ограничений**;
  - логических томов на блочный домен: **1500**;
  - максимальное количество LUN: **300**;
  - максимальный размер диска: **500 ТБ** (по умолчанию ограничен размером **8 ТБ**).

- *Хосты*:
  - максимальное количество хостов: **400**;
  - количество хостов на один центр обработки данных: **250**.

- *Виртуальные машины* (ВМ):
  - максимальное количество ВМ: **4000**.

  Общее количество ВМ зависит от оборудования хоста и потребляемых ресурсов.

Подготовка сетевого хранилища: NFS

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Чтобы **Engine** мог хранить данные в доменах хранения, представленных экспортируемыми каталогами, в них должны быть определенные учетные записи системных пользователей и их группы.

Дальнейшие действия выполняются на сервере с операционной системой РЕД ОС, который используется в качестве сетевого хранилища данных.

Если не установлен пакет NFS, его необходимо установить командой:

```
dnf install nfs-utils nfs4-acl-tools
```

Приведенная ниже процедура устанавливает разрешения для одного каталога (в примере **/data**). Вам необходимо повторить `chown` и `chmod` шаги для всех каталогов, которые вы собираетесь использовать в качестве доменов хранения в РЕД Виртуализации.

1. Создайте каталог **data**:

```
mkdir /data
```

2. Создайте группу **kvm**:

```
groupadd kvm -g 36
```

3. Создайте пользователя **vdsm** в группе **kvm**:

```
useradd vdsm -u 36 -g 36
```

4. Установите право собственности на экспортированный каталог на **36:36**, что дает **vdsm:kvm** право владения:

```
chown -R 36:36 /data
```

5. Измените режим каталога, чтобы права на чтение и запись были предоставлены владельцу, а права на чтение и выполнение были предоставлены группе и другим пользователям:

```
chmod 0755 /data
```

6. Все настройки сервера хранятся в файле **/etc/exports**. Откройте его на редактирование:

```
nano /etc/exports
```

и добавьте в конец файла строки вида (строк может быть произвольное количество):

```
/data
192.168.1.1/255.255.255.0(rw,insecure,nohide,all_squash,anonuid=36,anongid=36,no_subtree_check)
```

где:

- **/data** – путь к папке, для которой раздается доступ;
- **192.168.1.1** – IP-адрес, которому раздается доступ к папке (можно указать всю сеть, тогда запись примет вид **192.168.1.0/24**).

Чтобы запустить службу и добавить её в автозагрузку, выполните команду:

```
systemctl enable nfs-server.service --now
```

Примечание.

Если в системе, где происходит развёртывание хранилища **NFS** установлен и запущен **firewall**, внесите в него необходимые изменения:

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

Установка в режиме Standalone

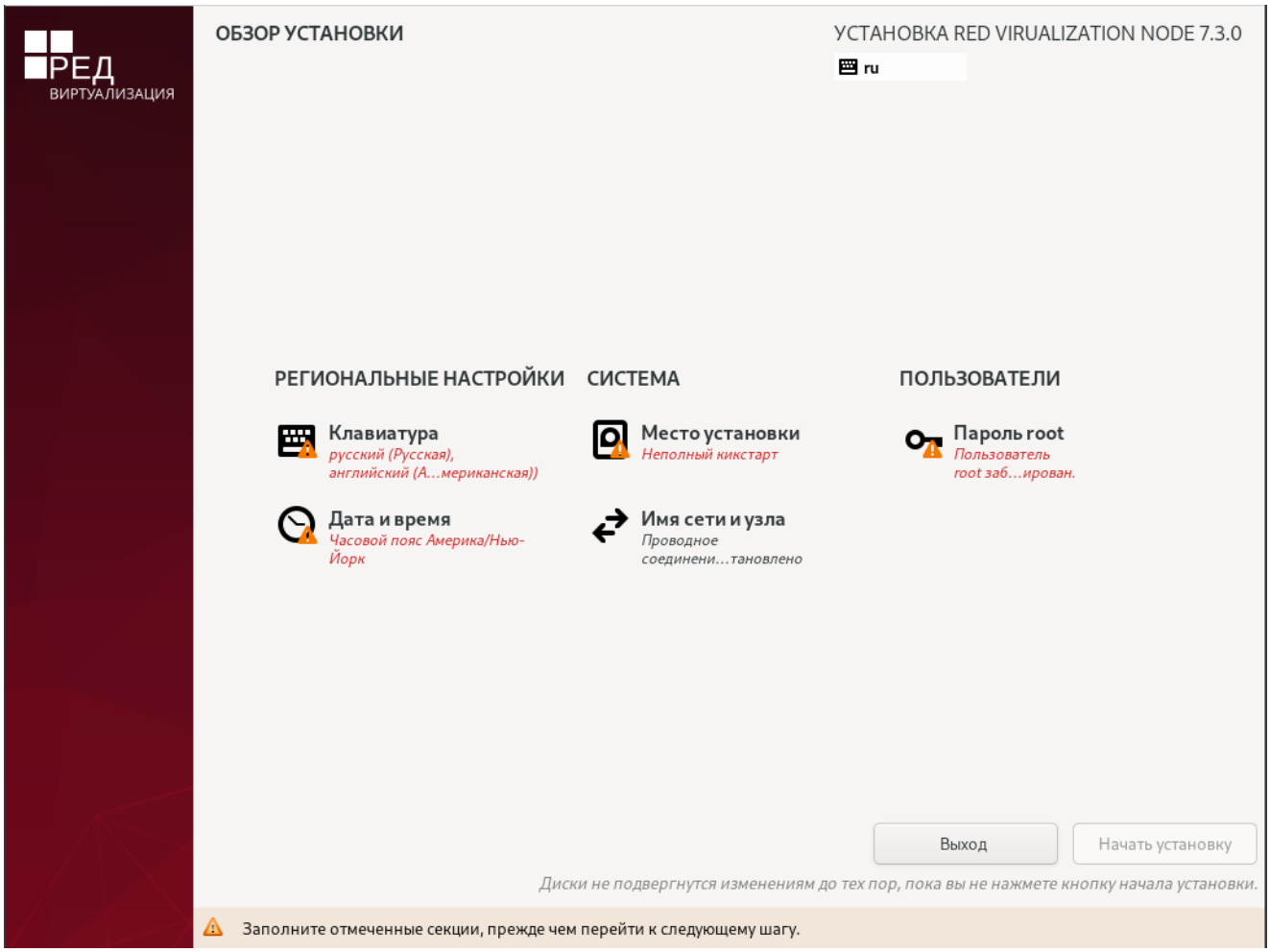
В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Примечание.

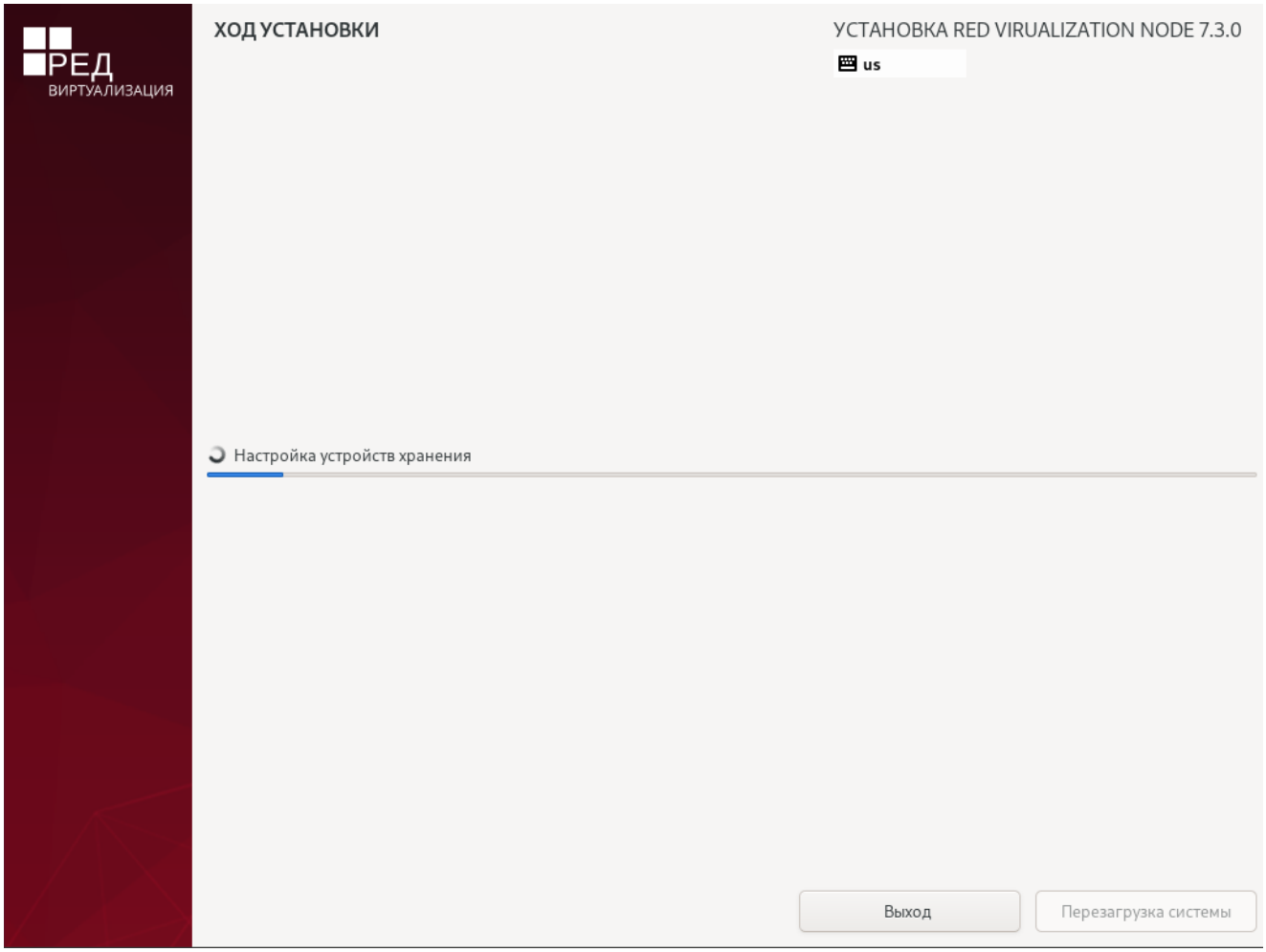
При установке в режиме **standalone** расширение до кластера невозможно.

Для установки РЕД Виртуализации в режиме **standalone** после загрузки образа в меню установщика необходимо выбрать пункт «**Install RED Virtualization 7.3.0 Standalone Engine**».

Откроется стандартное окно установки РЕД Виртуализации, в котором необходимо настроить раскладку клавиатуры, установить дату и часовой пояс, выбрать устройства для установки системы виртуализации, активировать соединение с сетью и задать имя узла, а также задать пароль администратора **root**. Подробнее о необходимых настройках см. в статье «Установка РЕД Виртуализации в режиме Host».

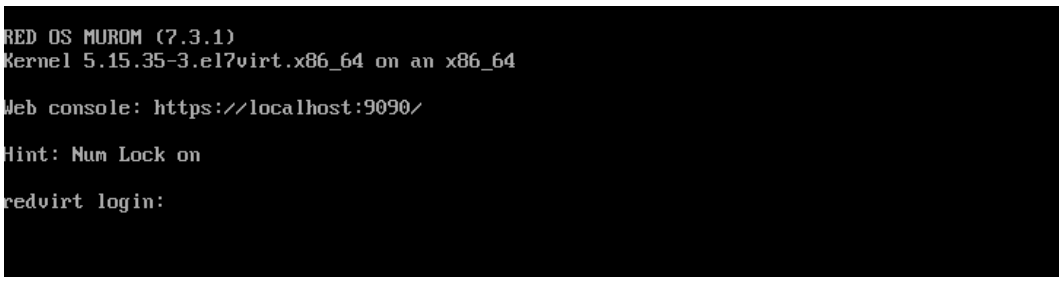


После определения всех необходимых настроек начинается этап установки РЕД Виртуализации. После данного шага программа установки будет работать с файлами только что установленной базовой системы.



После выполнения копирования файлов и настройки компонентов, пользователю будет предложено произвести перезагрузку кнопкой «**Перезагрузить систему**».

Затем откроется терминал установленной системы.



Далее необходимо настроить среду управления виртуализацией. Для этого войдите в систему под учетной записью **root**. Затем создайте каталог для хранилища и назначьте необходимые разрешения:

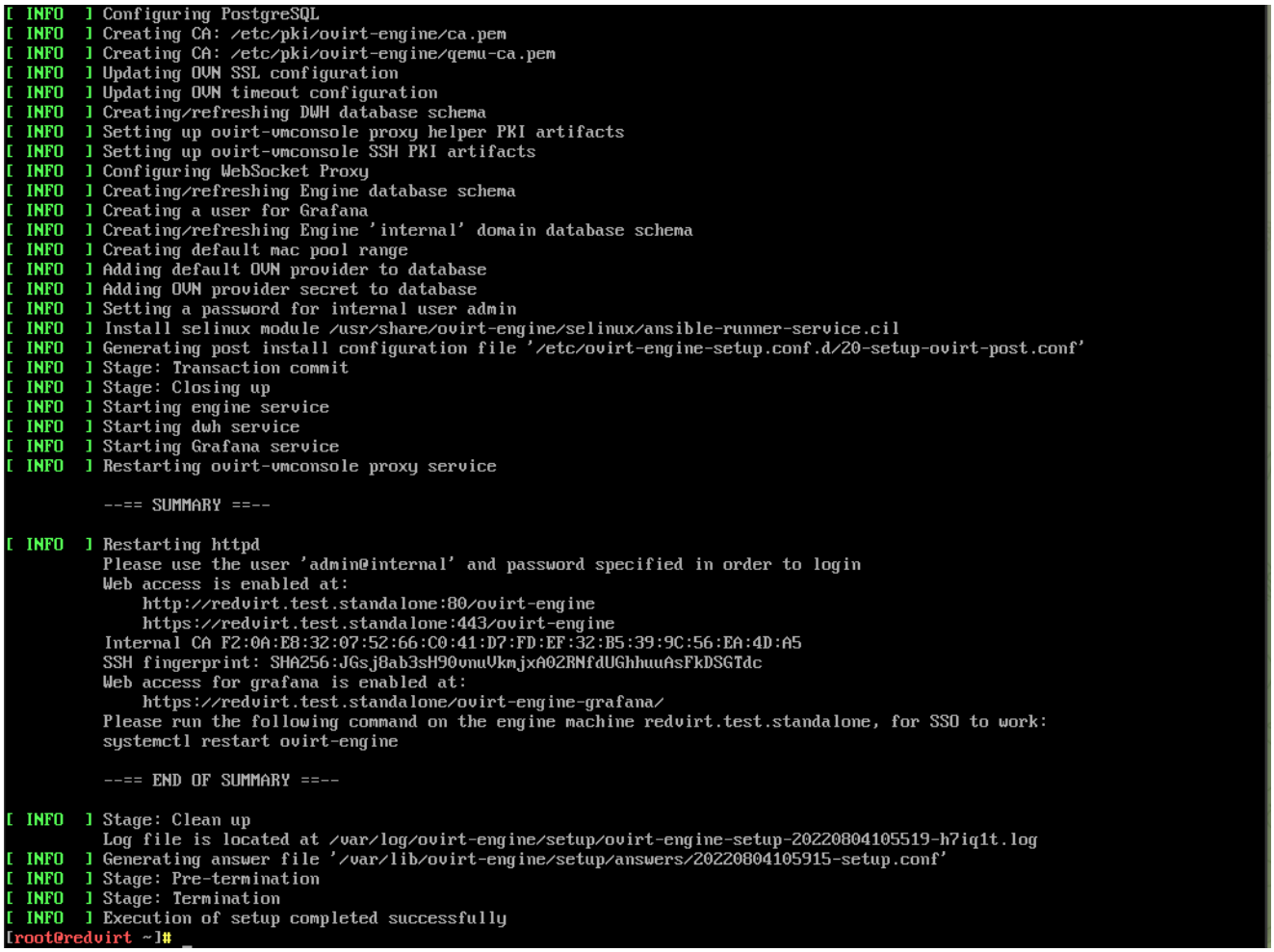
```
mkdir -p /srv/data
chown 36:36 /srv/data
chmod 0755 /srv/data
```

Далее запустите команду конфигурирования среды виртуализации:

```
engine-setup --accept-defaults
```

На запрос «**Engine admin password**» введите пароль администратора системы виртуализации, затем нажмите **Enter** и подтвердите его. Пароль должен иметь длину не менее 8 символов и содержать буквы, цифры и знаки.

После выполнения всех вышеуказанных действий будет произведена настройка среды управления виртуализацией.



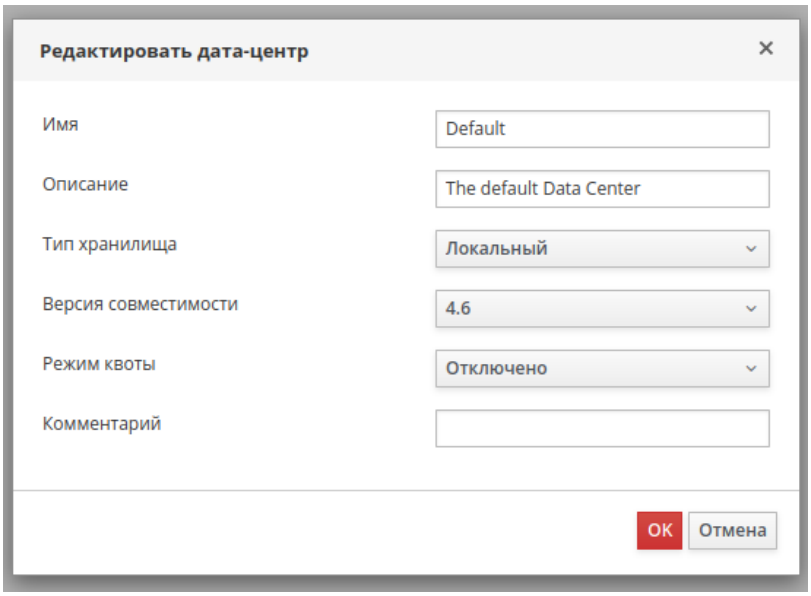
Затем необходимо произвести настройку возможности загрузки виртуальных дисков и iso-образов в систему РЕД Виртаулизации. Для этого выполните команды:

```
engine-config -s ImageTransferProxyEnabled=false
systemctl restart ovirt-engine
```

Теперь система управления средой виртуализации доступна для запуска в веб-интерфейсе.

После успешной авторизации на веб-портале необходимо настроить хранилище. Перейдите в настройки дата-центра для включения возможности добавления локальных хранилищ.

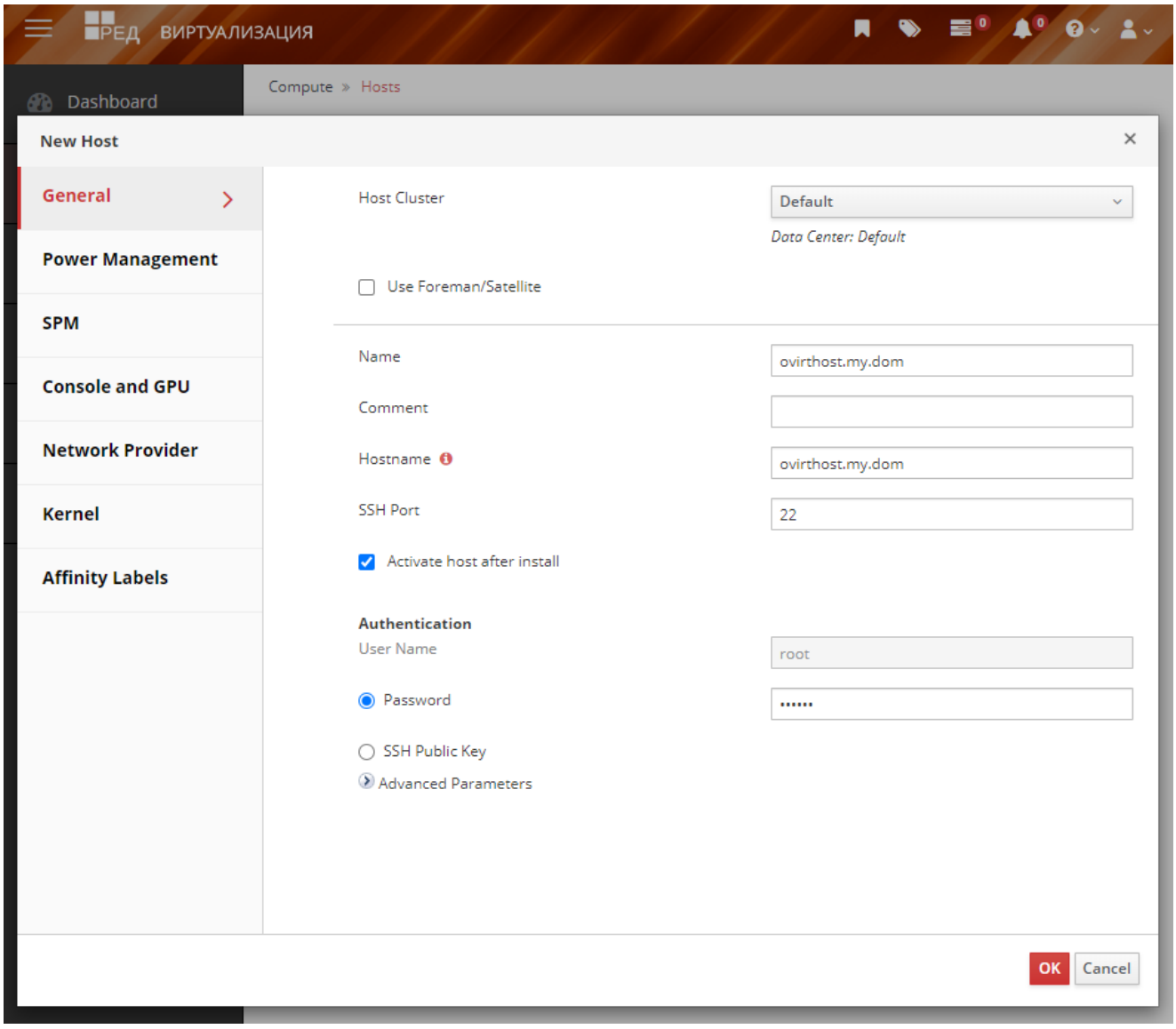
Откройте «**Виртуализация**» - «**Дата-центры**», нажмите «**Редактировать**» и в поле «**Тип хранилища**» выберите «**Локальный**». Нажмите «**ОК**».



Далее необходимо создать вычислительный хост.

Для этого откройте «**Виртуализация**» - «**Узлы**» и нажмите кнопку «**Новый**». В открывшемся окне в полях «**Name**» и «**Hostname**» впишите имя машины, на которую производится установка. В примере это **ovirthost.my.dom**.

В поле «**Password**» впишите действующий пароль **root**-пользователя. Нажмите «**OK**».

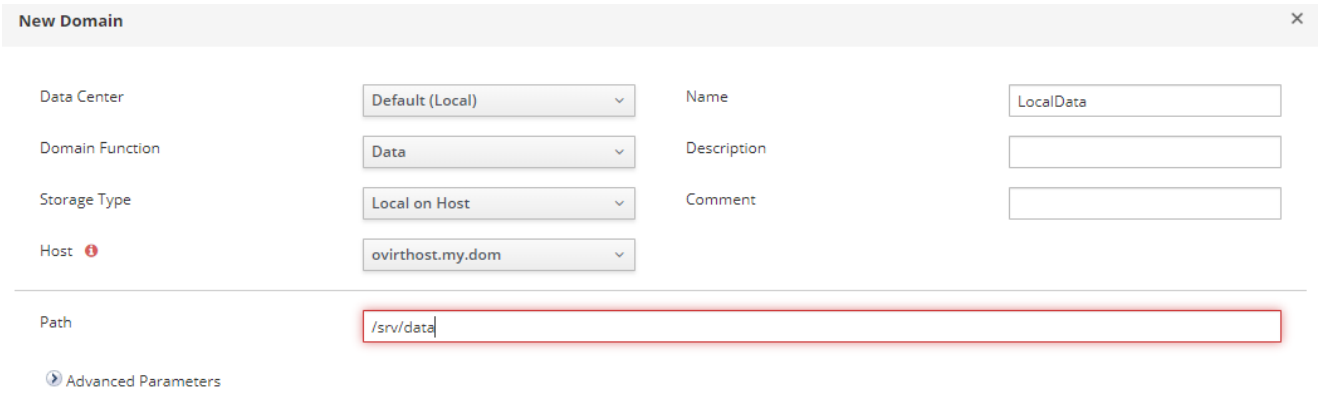


На вопрос «**You haven’t configured Power Management for this Host. Are you sure you want to continue?**» нажмите «**OK**». Вы можете настроить политику питания позже.

Далее начнется настройка хоста, следить за процессом настройки можно, нажав на создаваемый хост и выбрав вкладку «**Events**».

После успешного запуска хоста создайте локальный домен хранения.

Откройте «**Хранилище**» - «**Домен**» и нажмите кнопку «**Новый**». В открывшемся окне в поле «**Name**» впишите имя создаваемого домена, например, «**Local**». В поле «**Storage Type**» выберите «**Local on Host**». В поле «**Path**» впишите **путь** к каталогу, который вы указывали ранее в командах консоли. Нажмите «**OK**».



Установка в режиме Host

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Подготовка к установке

Для выполнения установки у Вас должен быть дистрибутив РЕД Виртуализации 7.3.

Оборудование должно соответствовать требованиям, описанным в разделе «Системные требования».

Подключите дистрибутив к одному из хостов и загрузитесь в программу установки, выбрав носитель дистрибутива в качестве загружаемого устройства.

Последовательность установки

Программа установки РЕД Виртуализации работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования хоста завершилась успешно, будет запущен графический интерфейс программы-установщика (anaconda). Процесс установки реализован в виде «мастера» установки, представляющий из себя интерактивный графический интерфейс, в котором пользователю предлагается отвечать на вопросы и указывать необходимые опции установки. Мастер установки разделен на шаги, каждый шаг посвящен настройке или установке определенного сервиса системы.

Если по каким-то причинам возникла необходимость прекратить установку, выполните **Reset** на хосте. Помните, что совершенно безопасно прекращать установку только до нажатия кнопки «**Установить**», поскольку до этого момента не производится никаких изменений на жестком диске.

Технические сведения о ходе установки можно посмотреть, нажав **Ctrl+Alt+F1**, вернуться к

программе установки - **Ctrl+Alt+F7**. По нажатию **Ctrl+Alt+F2** откроется отладочная виртуальная консоль.

Во время установки РЕД ОС выполняются следующие шаги:

- Установка предпочитаемой раскладки клавиатуры;
- Выбор типа накопителя хоста и подготовка разделов диска;
- Задание пароля администратора системы;
- Выбор часового пояса и установка даты и времени;
- Присвоение имени компьютера в сети и настройка сетевых интерфейсов;
- Сохранение настроек;
- Установка системы;
- Установка загрузчика;
- Перезагрузка системы;
- Завершение установки.

Язык системы

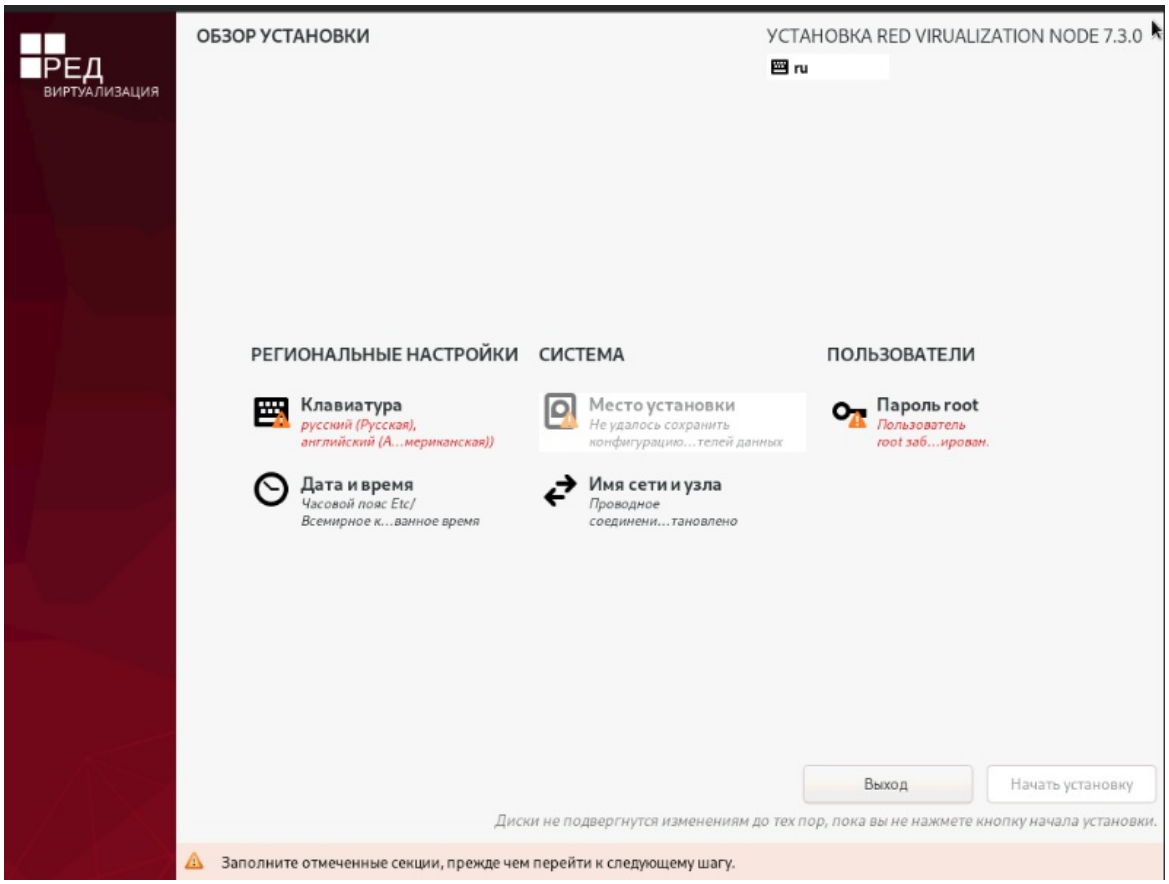
Язык интерфейса программы установки и графического интерфейса устанавливаемой системы виртуализации по умолчанию русский, не конфигурируется и не изменяется в процессе установки. Дополнительным языком является английский язык. Другие дополнительные языковые пакеты можно установить из репозитория после завершения установки системы.

Переключение раскладки клавиатуры при установке системы виртуализации выполняется нажатием комбинации функциональных клавиш **Alt** и **Shift** одновременно.

Обзор установки

После выбора языка необходимо произвести первоначальную конфигурацию установщика и параметров будущей системы виртуализации.

В этом окне необходимо задать региональные и системные настройки. Здесь и в последующих окнах установщика красным цветом выводятся подсказки у тех вкладок, которые должны быть обязательно заполнены до перехода к следующему шагу установки.



Клавиатура

В окне настройки клавиатуры можно выбрать используемые в системе раскладки.

В отдельном поле ввода можно проверить корректность отображения вводимых символов.

Первая раскладка в списке будет использоваться по умолчанию.

Здесь и далее возврат в предыдущее меню осуществляется с помощью кнопки «**Готово**».

Расположение установки

В меню выбора расположения установки можно выбрать устройство для установки хоста виртуализации.

Переход к этому шагу может занять некоторое время. Время ожидания может быть разным и зависит от производительности хоста, объёма и типов используемых накопителей, количества существующих разделов на них.

На этом этапе подготавливается площадка для установки хоста виртуализации, в первую очередь - выделяется свободное место на диске.

Можно выбрать и использовать профили разбиения диска. Профиль — это шаблон распределения места на диске для установки системы. Можно выбрать:

- создать разделы автоматически;

- настрою разделы;
- дополнительно (Blivet-GUI).

Первый профиль предполагает автоматическое разбиение диска. Будет выбрано оптимальное расположение.

Необратимые изменения разделов на жестком диске требуют подтверждения со стороны пользователя. После подтверждения внесенные изменения сохраняются на жестком диске/дисках хоста.

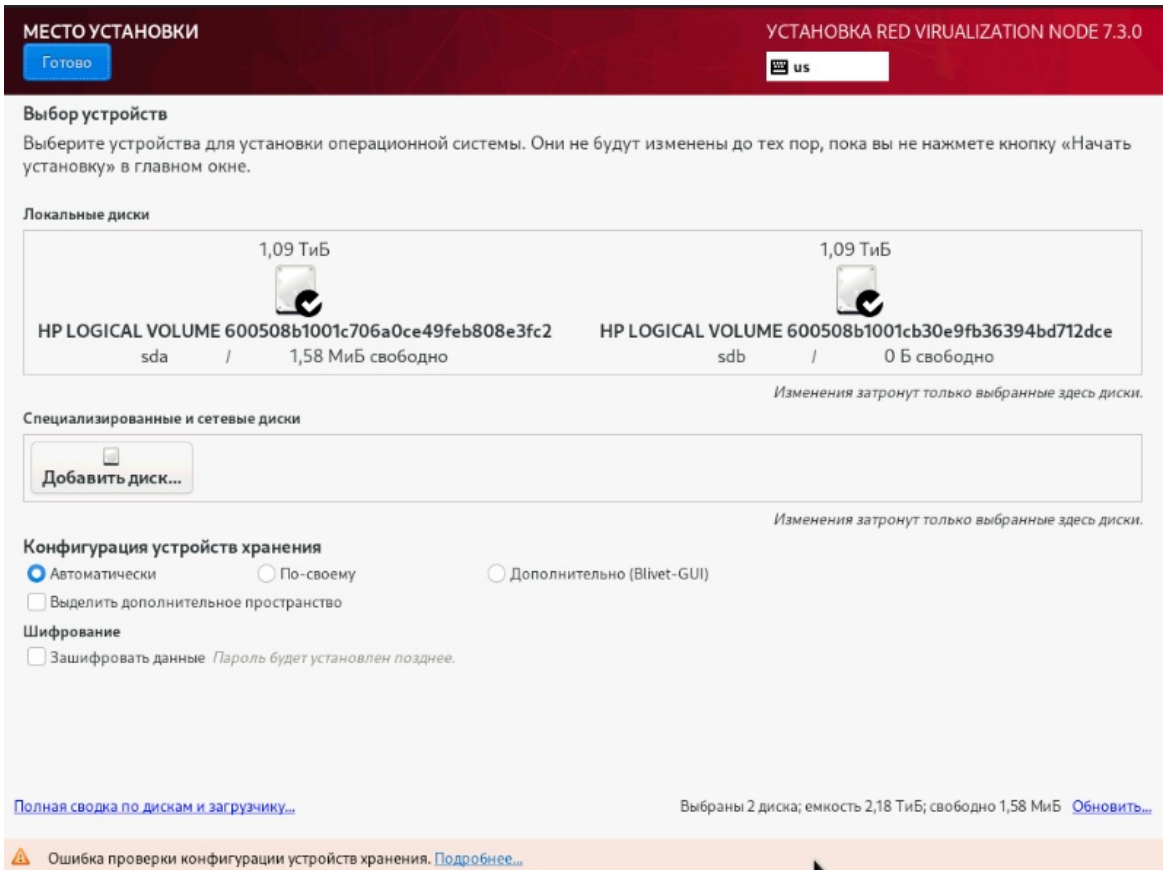
Если для применения одного из профилей автоматической разметки доступного места окажется недостаточно, будет выведено сообщение о невозможности выполнения операции разбиения диска.

При необходимости освободить часть дискового пространства, следует воспользоваться профилем разбиения вручную. Можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «**Готово**» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке «**Файловая система**».

Не следует форматировать разделы с теми данными, которые необходимо сохранить, например, с пользовательскими данными (**/home**). С другой стороны, отформатировать можно любой раздел, который необходимо «очистить» (т.е. удалить все данные).

Blivet-gui является обособленной реализацией механизмов управления разделами и дисками, снабжённой привычным интерфейсом в стиле **GParted**. Программа поддерживает управление дисковыми разделами и хранилищами **LVM2** (включая шифрованные разделы LUKS, логические тома и группы томов). Так же как и в **GParted**, изменения в **blivet-gui** применяются не сразу, а после подтверждения внесённого набора изменений.



Задание пароля администратора системы

Далее необходимо настроить пароль локального администратора **root**.

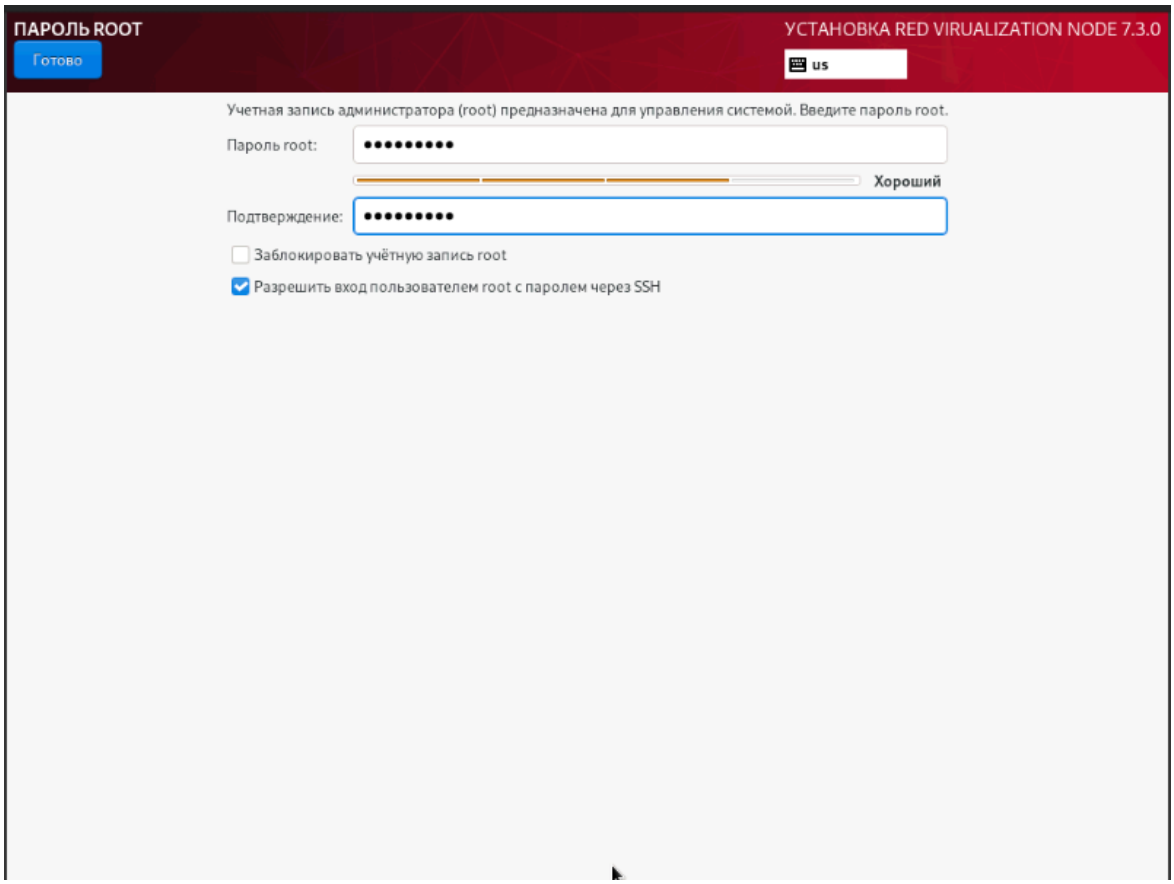
Необходимо запомнить пароль **root** - он необходим для авторизации и управления системой виртуализации.

Ввод пароля защищен, при наборе пароля вместо символов на экране отображаются специальные символы. Чтобы избежать опечатки при вводе пароля, его предлагается ввести дважды. К введенному паролю в режиме реального времени применяется политика сложности пароля, т.е. производится его проверка, и при слишком простом пароле или совпадении пароля с парольной последовательностью из словаря паролей системой будет предложено произвести смену пароля администратора.

ВАЖНО!

В поле «**Разрешить вход пользователем root с паролем через SSH**» должен быть установлен флажок, т.к. дальнейшая установка и настройка системы РЕД Виртуализации использует данную функцию в своей работе. Также данная функция требуется для доступа администратора к терминалу хоста.

Выбор пароля администратора - очень важный момент для безопасности: любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе.



Дата и время

В окне настройки даты и времени можно выбрать текущий регион и город и установить используемое локальное время, дату и формат времени.

Если установлена сеть, и есть доступ к глобальной сети, можно разрешить автоматическую настройку времени с помощью службы **ntp** — сетевое время.

Данную настройку можно изменить после завершения установки. По умолчанию устанавливается часовой пояс **UTC+03:00** (Европа/Москва).

Сеть и имя узла

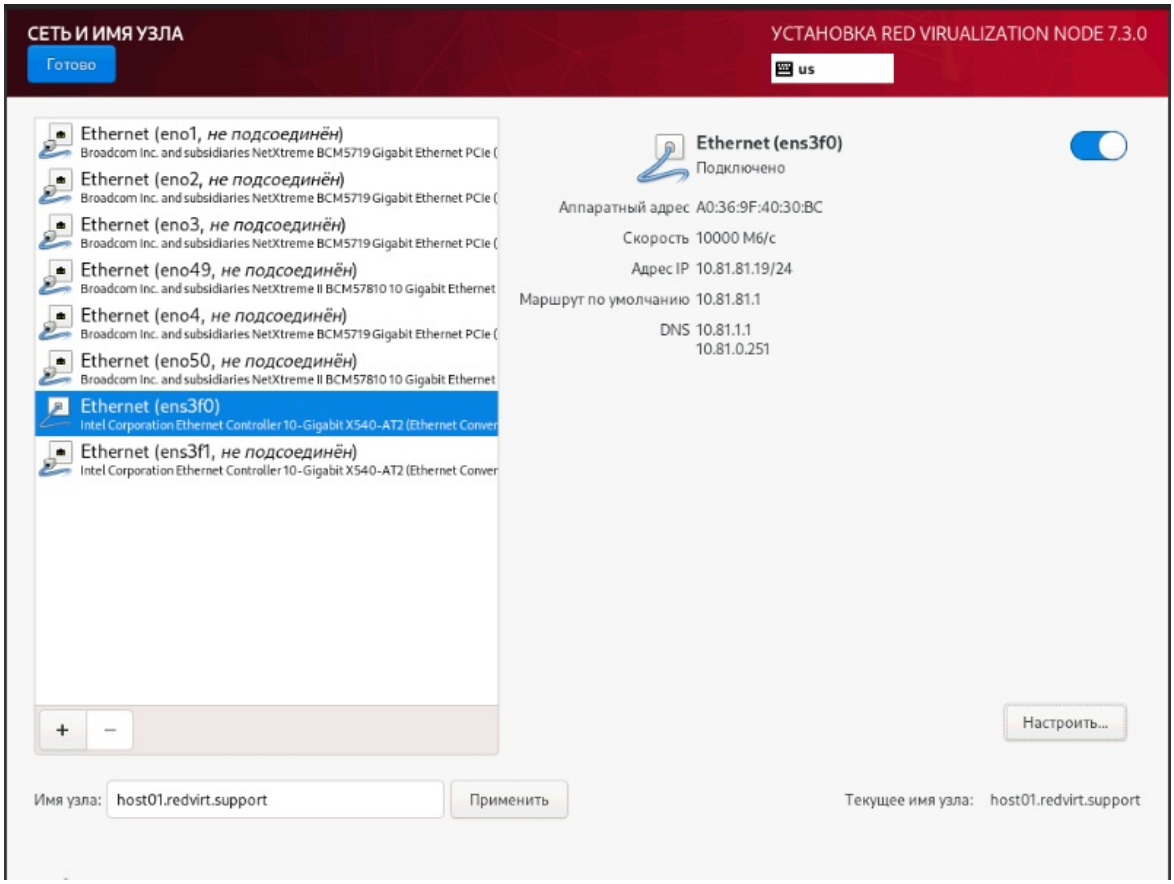
В меню выбора настройки сети можно активировать соединение с сетью и задать имя узла.

На данном этапе необходимо задать имя компьютера в сети (хоста). При наличии сети имя компьютера используется для однозначного определения каждого компьютера. Имя компьютера состоит непосредственно из имени компьютера и имени домена в сети, к которому принадлежит компьютер. Имя компьютера и имя домена разделяются знаком «**.**».

При наличии домена сети имя должно даваться полностью.

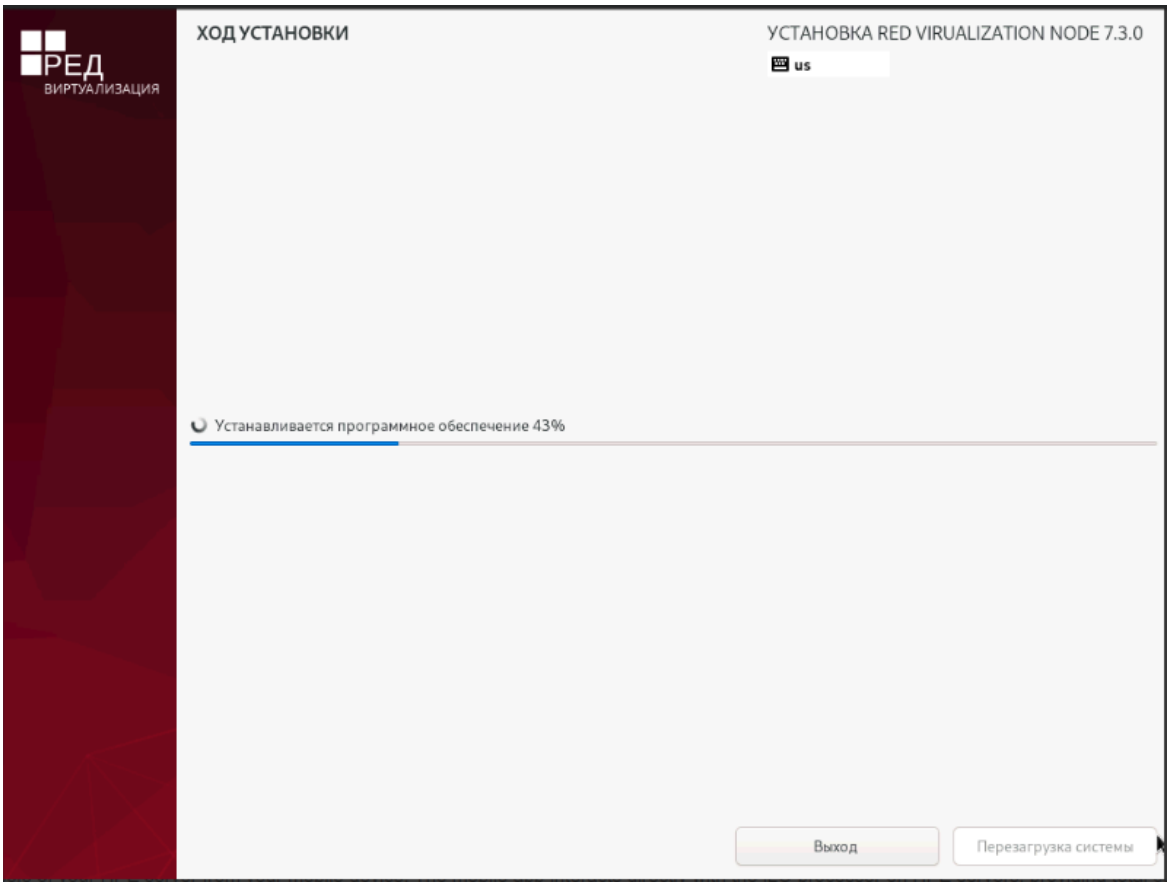
В качестве букв в имени компьютера разрешается только буквы латиницы. В имени компьютера не допускается использование заглавных букв, пробелов и специальных символов.

Также на данном этапе можно сконфигурировать параметры настройки сетевых интерфейсов: автоматическое включение интерфейсов, MAC-адреса сетевых интерфейсов, параметры сетевых протоколов.



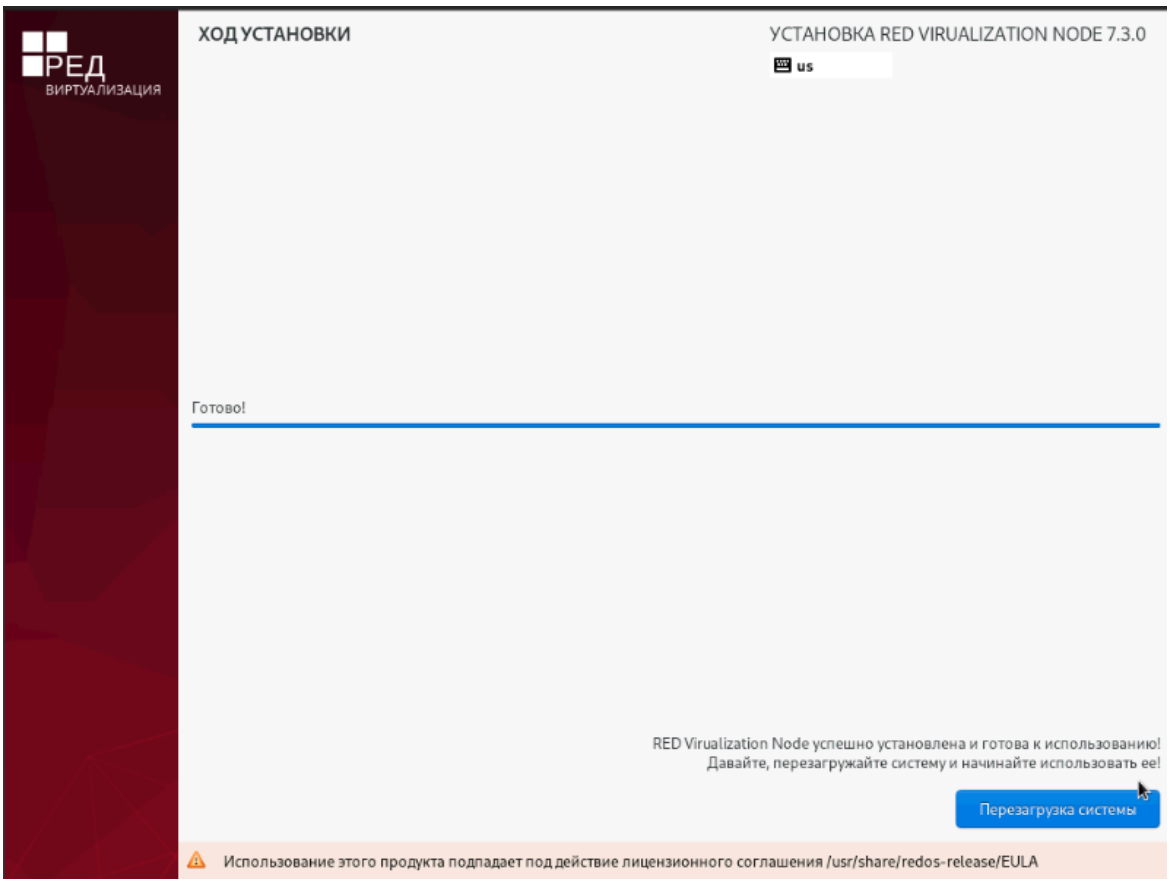
Установка системы виртуализации

После определения всех настроек начинается этап установки РЕД Виртуализации и представляет собой установку набора программ, необходимых для работы среды виртуализации.

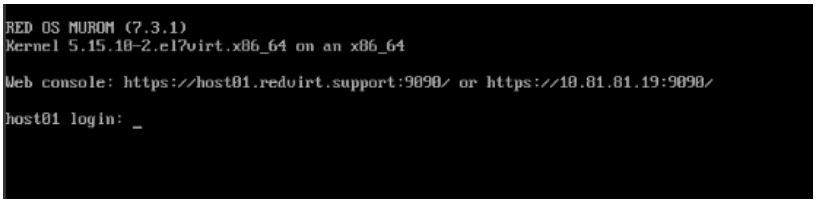


Начиная с этого шага, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить непосредственно на установленной ОС.

После выполнения копирования файлов и настройки компонентов, пользователю предлагается произвести перезагрузку кнопкой «**Перезагрузить систему**».



После перезагрузки откроется терминал установленной системы, где будет указан адрес веб-интерфейса, через который производится установка и настройка системы РЕД Виртуализация.



Примечание.

В случае, если во время установки системы вы по каким-то причинам не указали или указали неверно адрес хоста, необходимо выполнить следующие действия:

1. В открывшемся терминале установленной системы ввести логин (**root**) и *пароль* (созданный на этапе установки) для авторизации на сервере.

2. Установить имя хоста:

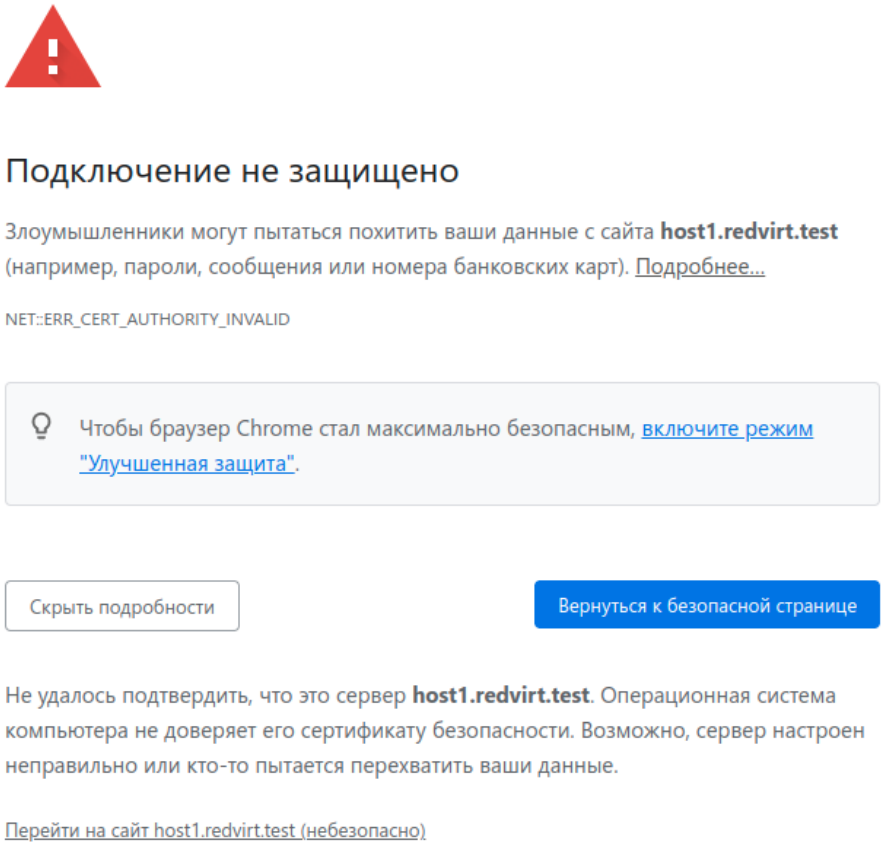
```
hostnamectl set-hostname host1.redvirt.test
```

3. Если DNS-сервер в сети не настроен, то в файле **/etc/hosts** нужно указать ip-адрес и имя будущей виртуальной машины управления системой РЕД Виртуализация. А также внести записи о самом хосте (хостах, если их несколько) и о хранилище.

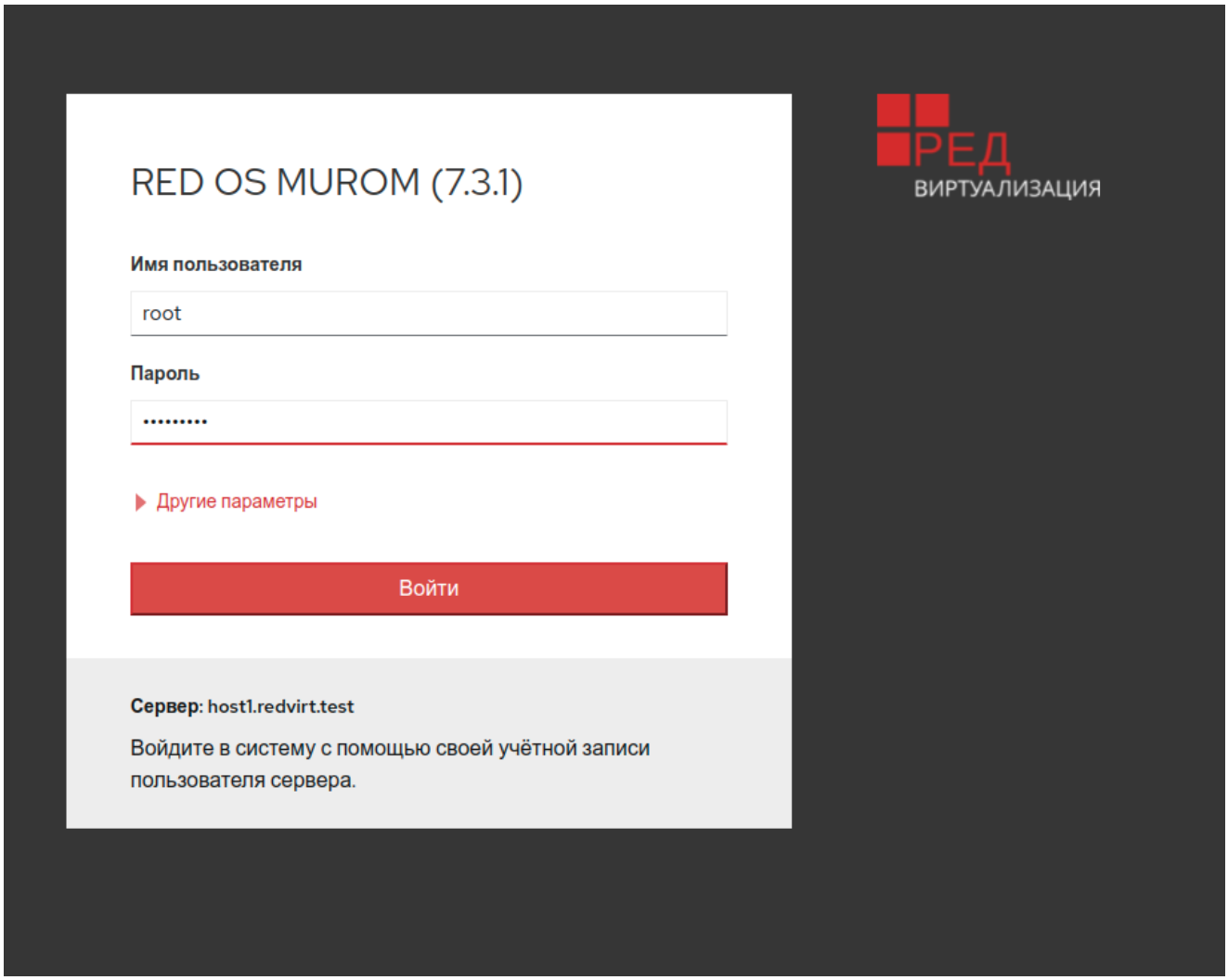
```
192.168.0.43 host1.redvirt.test *Хост*
192.168.0.44 nfs.redvirt.test *NFS-хранилище*
192.168.0.221 redvirt-engine1.test *Гипервизор РЕД Виртуализации*
```

После сохранения данных веб-интерфейс для установки и настройки системы РЕД Виртуализация будет доступен по адресу `https://<имя_хоста>:9090` либо `https://<IP-адрес_хоста>:9090`.

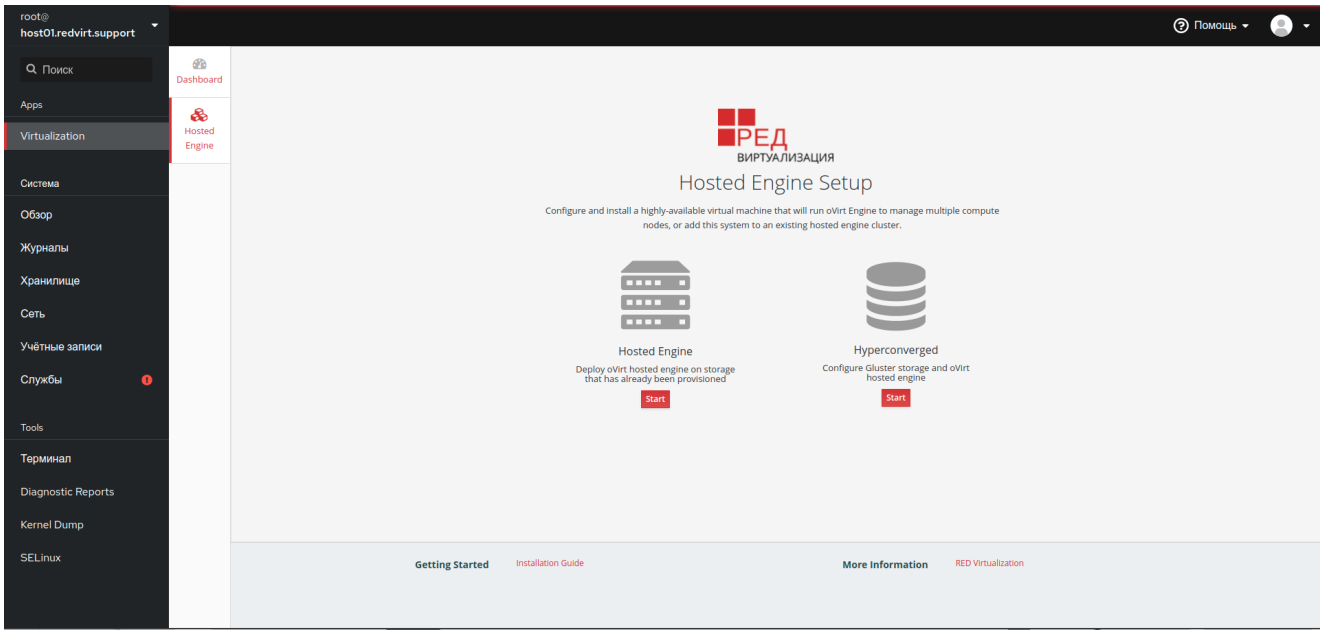
При попытке подключения к серверу будет выведено предупреждение о небезопасном соединении. Нажмите «**Перейти на сайт host1.redvirt.test (небезопасно)**» внизу страницы.



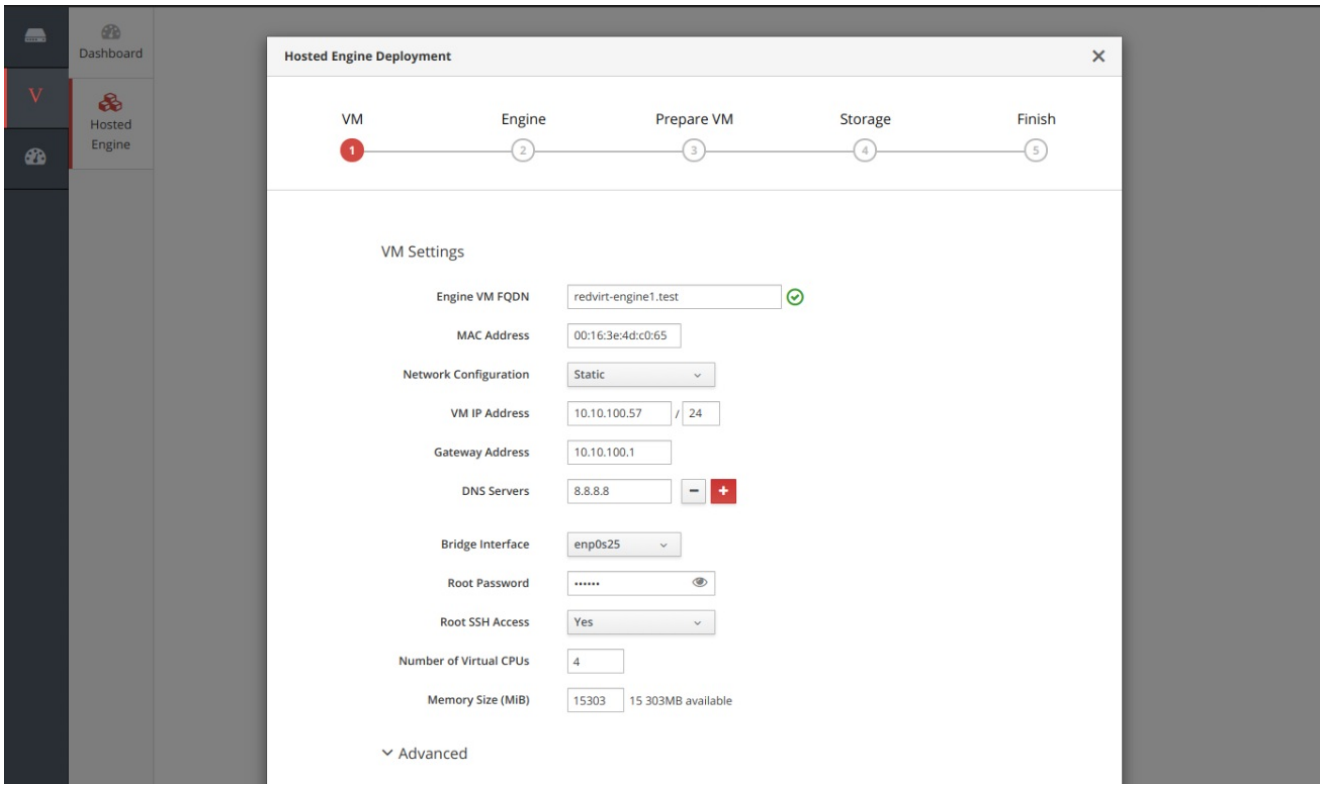
В окне авторизации введите имя пользователя - **root** и *пароль*, который был создан при установке системы.

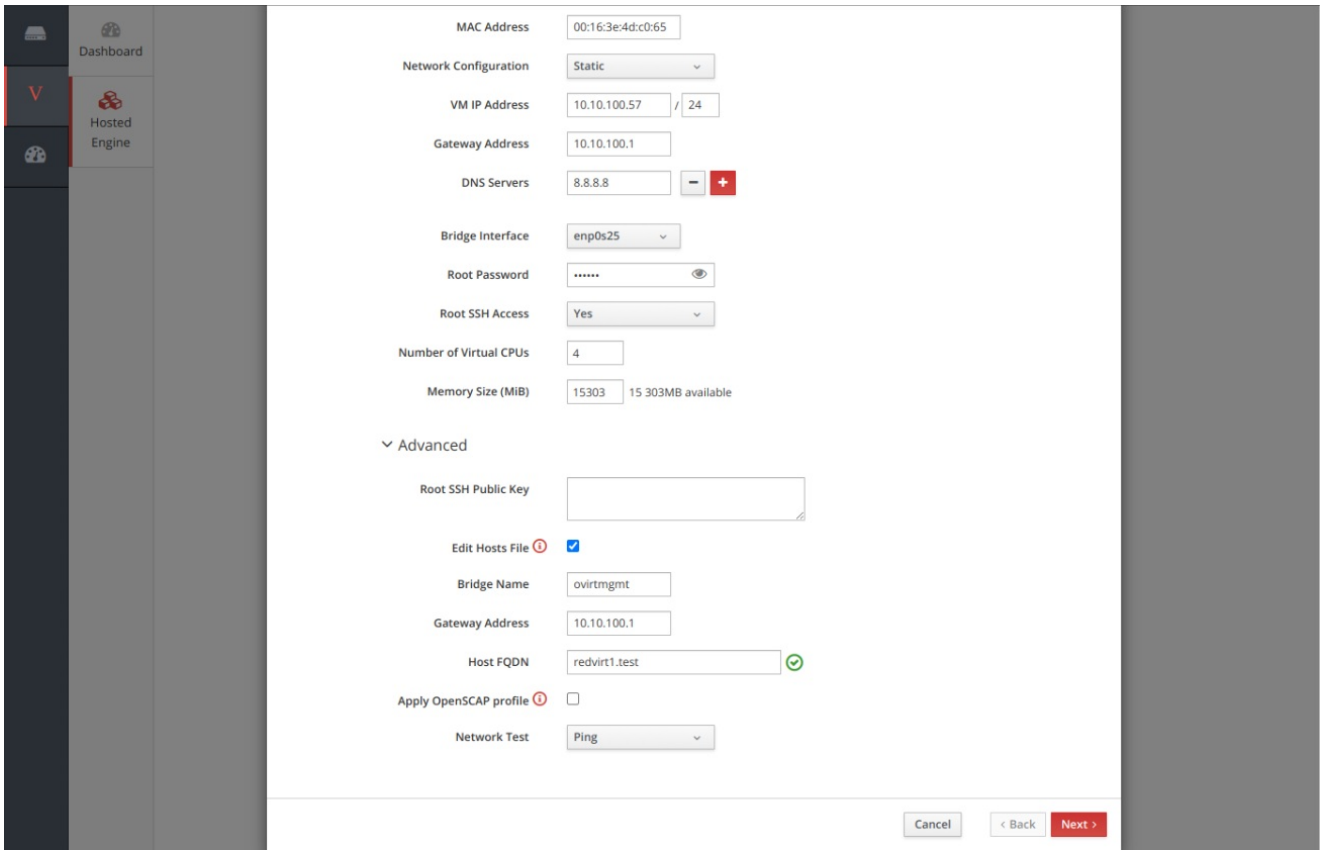


Перейдите во вкладку **Virtualization** – **Hosted Engine**.



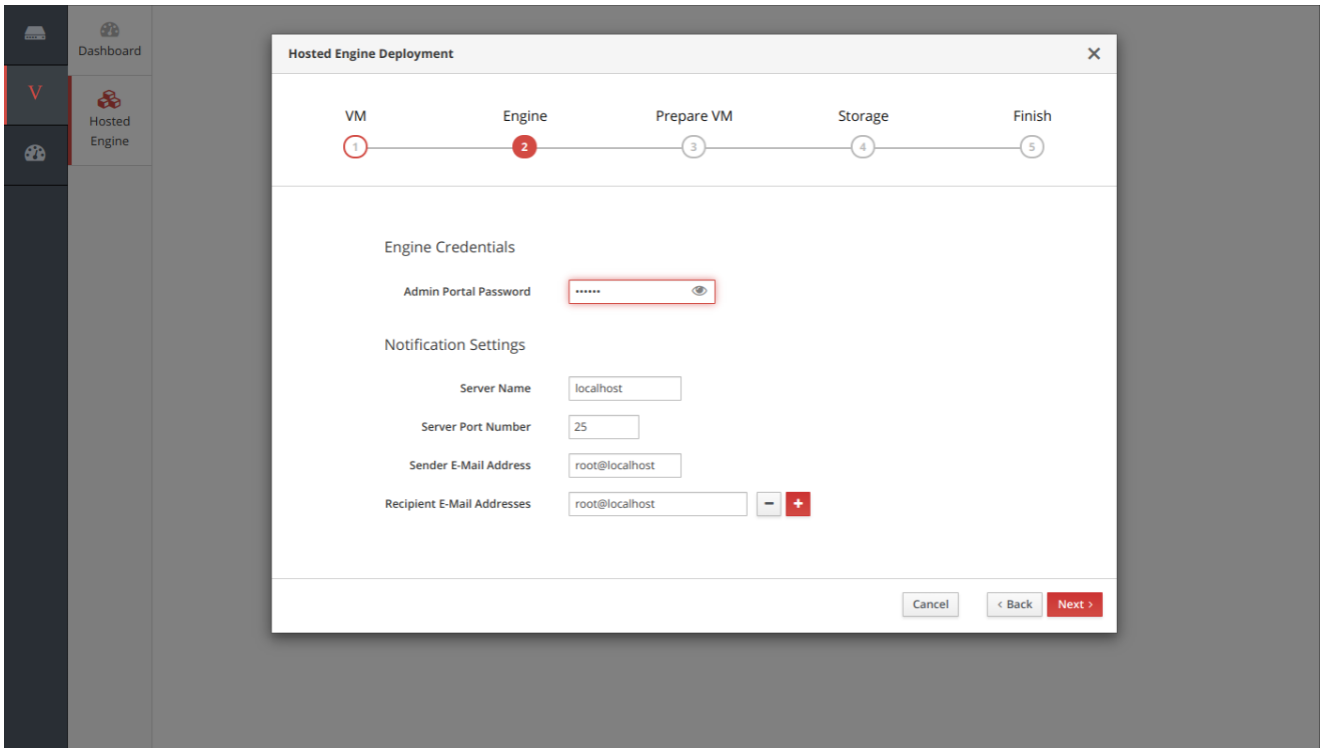
Нажмите **Hosted Engine** – **Start** и заполните поля на вкладке VM в соответствии с вашими параметрами сети.



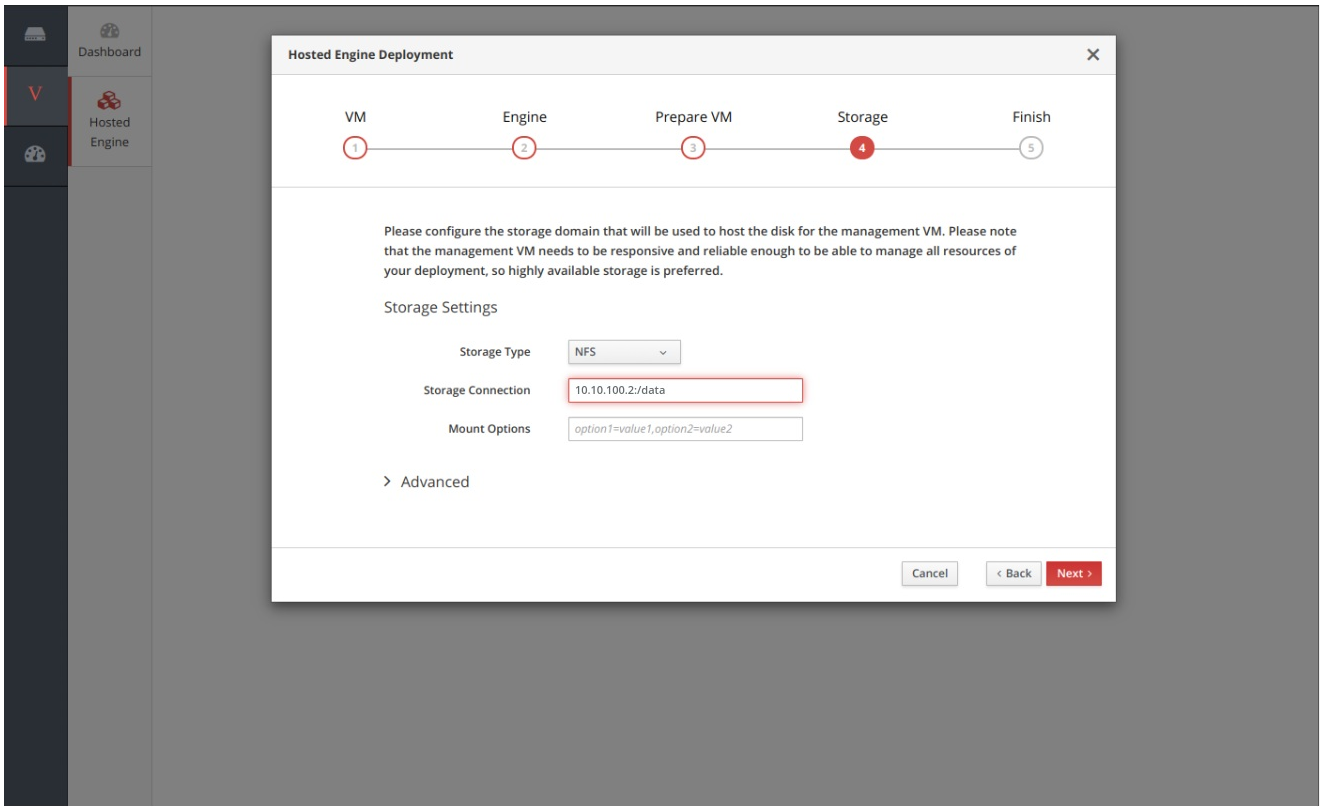


Нажмите **Next**.

Во вкладке **Engine** назначьте пароль администратору портала, а также настройте службу уведомлений.

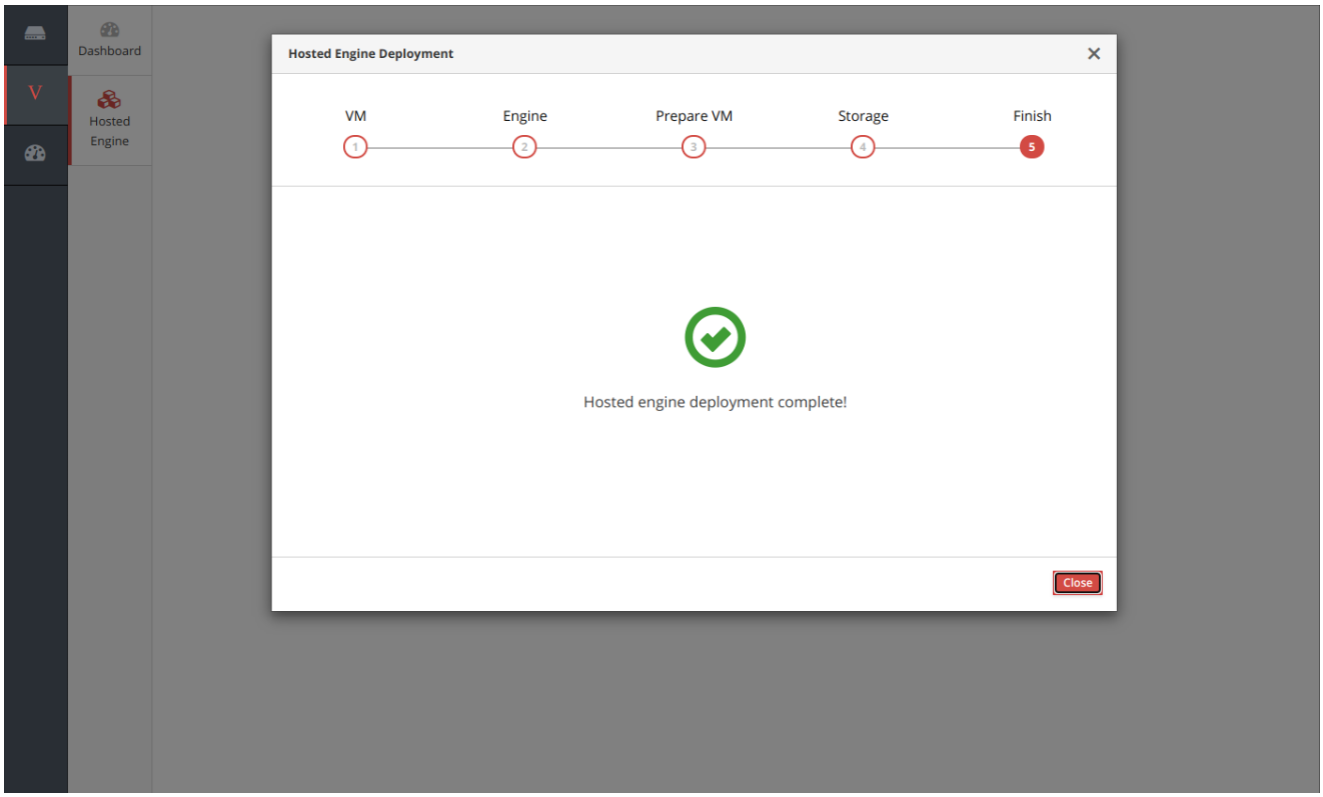


Во вкладке **Storage** добавьте хранилище.



Нажмите **Next**.

После успешной установки нажмите **Close**.


Dashboard
Hosted Engine
Hosted Engine Deployment
VM
Engine
Prepare VM
Storage
Finish
1
2
3
4
5
Hosted engine deployment complete!
Close

Установка в режиме Gluster Hyperconverged для одного узла

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Предварительные требования

Предварительные требования:

1. Хост РЕД Виртуализации, содержащий минимум один неразмеченный жесткий диск, на котором в процессе развёртывания будут созданы необходимые разделы **Gluster**.

2. На хосте должно быть как минимум 2 интерфейса, чтобы можно было разделить трафик на внешний (**frontend**) и внутренний (**backend**).

Наличие только одной сети приведет к тому, что мониторинг **Engine**, клиентский трафик, трафик ввода-вывода **Gluster** будут работать вместе и мешать друг другу. Чтобы разделить сеть **backend**, кластер **Gluster** формируется с использованием адресов сети **backend**, а узлы добавляются к **Engine** с использованием адресов сети **frontend**.

3. Подготовленное полное доменное имя для вашего **Engine** и хоста. В DNS должны быть установлены записи прямого и обратного поиска. **Engine** должен использовать ту же подсеть, что и сеть управления.

4. Беспарольный **ssh** от хоста к самому себе, так как роль **ansible** должна удаленно выполнять команды — обязательное условие. Для настройки выполните следующие действия на хосте, на котором планируется проведение установки кластера:

4.1. Сгенерируйте ключ доступа, выполнив следующую команду :

```
# ssh-keygen
```

ВАЖНО!

При генерации ключа нельзя использовать парольную фразу.

4.2. Скопируйте ключ на каждый хост кластера. Также выполните копирование на хост, на

котором производится настройка беспарольного доступа. Для копирования ключа выполните следующую команду :

```
# ssh-copy-id root@<fqdn_адрес_хоста>
```

Развертывание на узле РЕД Виртуализации

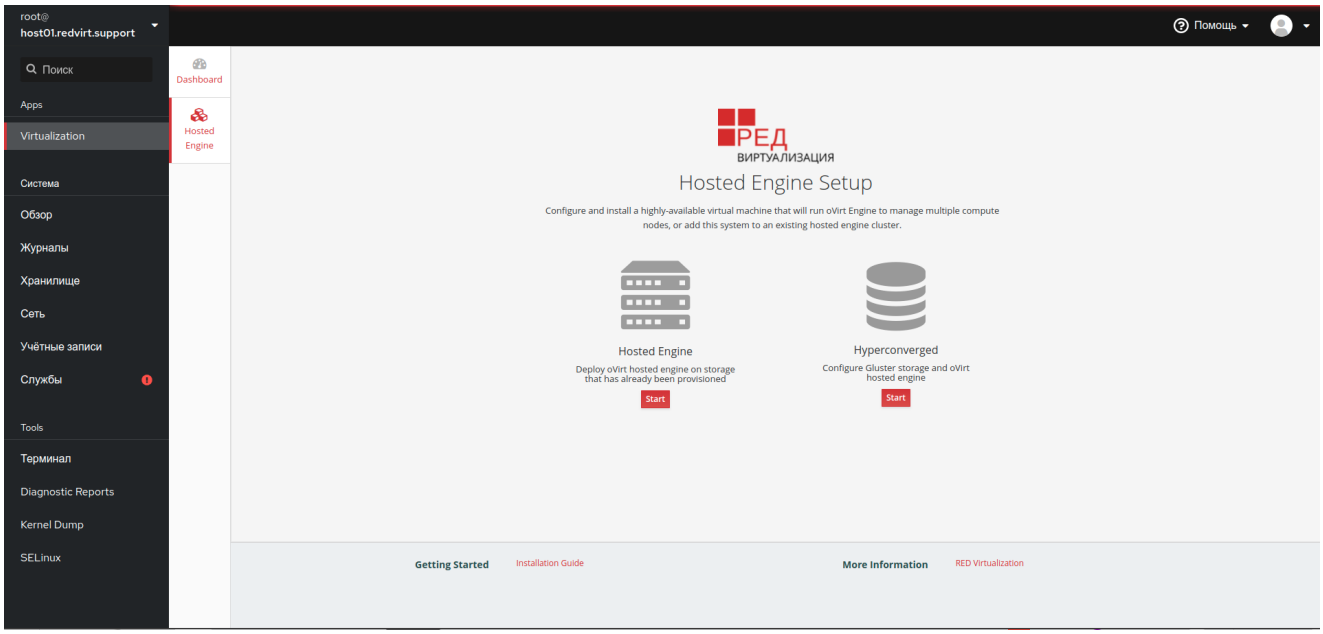
Узел РЕД Виртуализации содержит все необходимые пакеты для настройки гиперконвергентной среды. Вы можете начать настройку гиперконвергентной среды, если у вас есть хост на базе узла РЕД Виртуализации.

Установка и настройка томов Gluster

Тома **Gluster** должны быть созданы перед установкой **Hosted Engine**. Один из созданных томов используется для размещения виртуальной машины **Hosted Engine**. Используйте пользовательский интерфейс **Cockpit** для настройки развертывания с одним узлом.

1. Войдите в веб-консоль. Перейдите к интерфейсу управления веб-консоли первого гиперконвергентного хоста, например, https://<имя_хоста>:9090/ или https://<IP-адрес_хоста>:9090/, и войдите в систему, используя учетные данные суперпользователя **root**.

2. Перейдите во вкладку **Virtualization** – **Hosted Engine**.



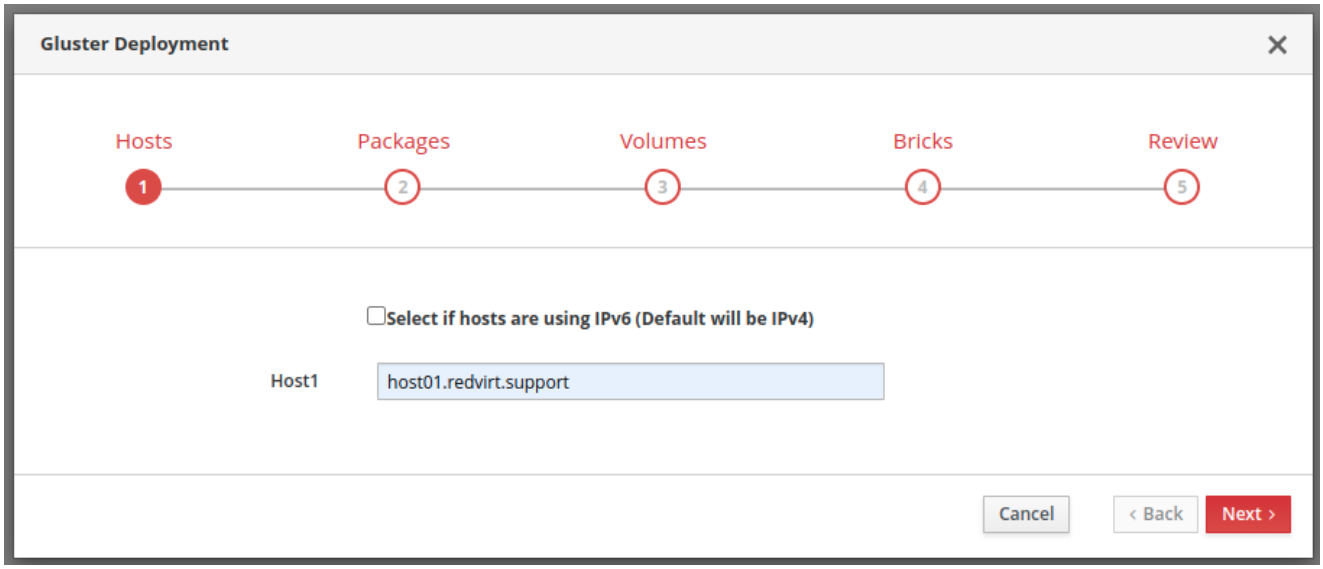
3. Запустите мастер развертывания.

После запуска мастер развертывания предложит выбрать одно из дальнейших действий:

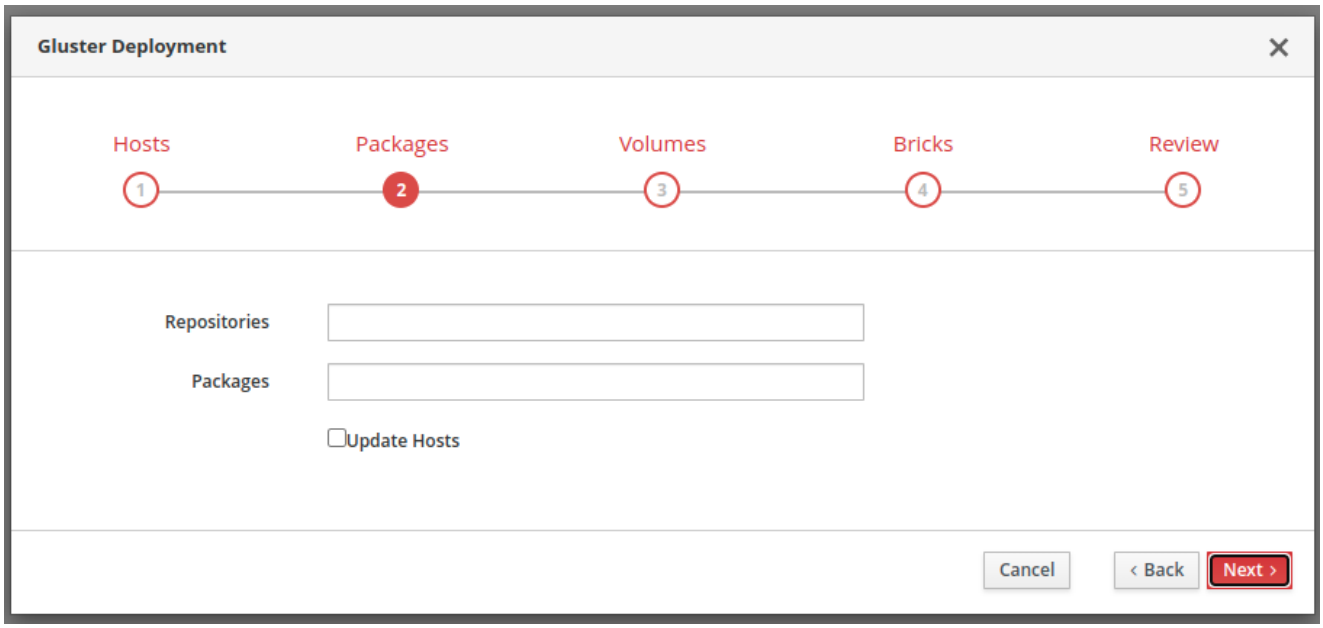
- Запустить мастер развертывания Gluster;
- Запустить мастер развертывания Gluster для единого узла.

Выберите второй вариант.

4. Укажите имя хоста.

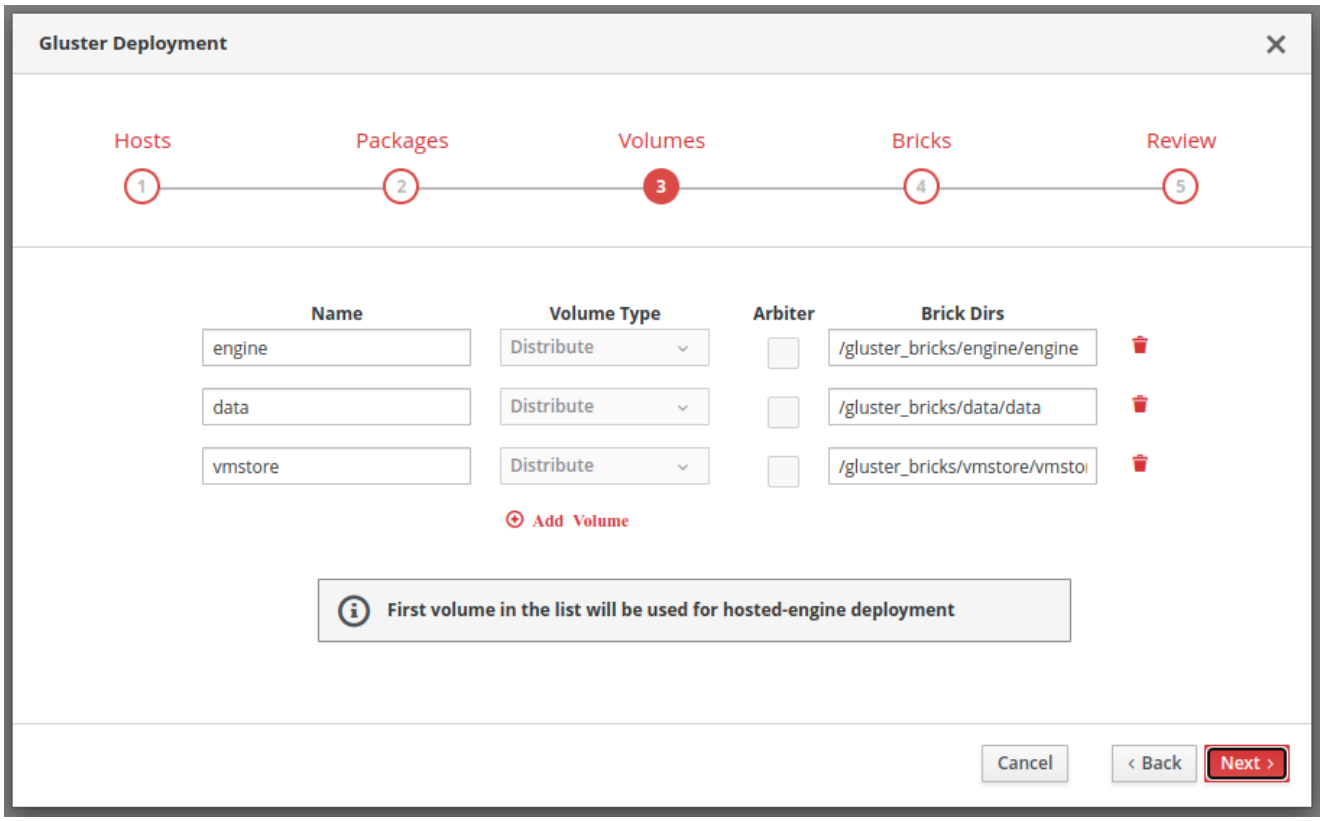


5. При необходимости загрузите репозитории и дополнительные пакеты.

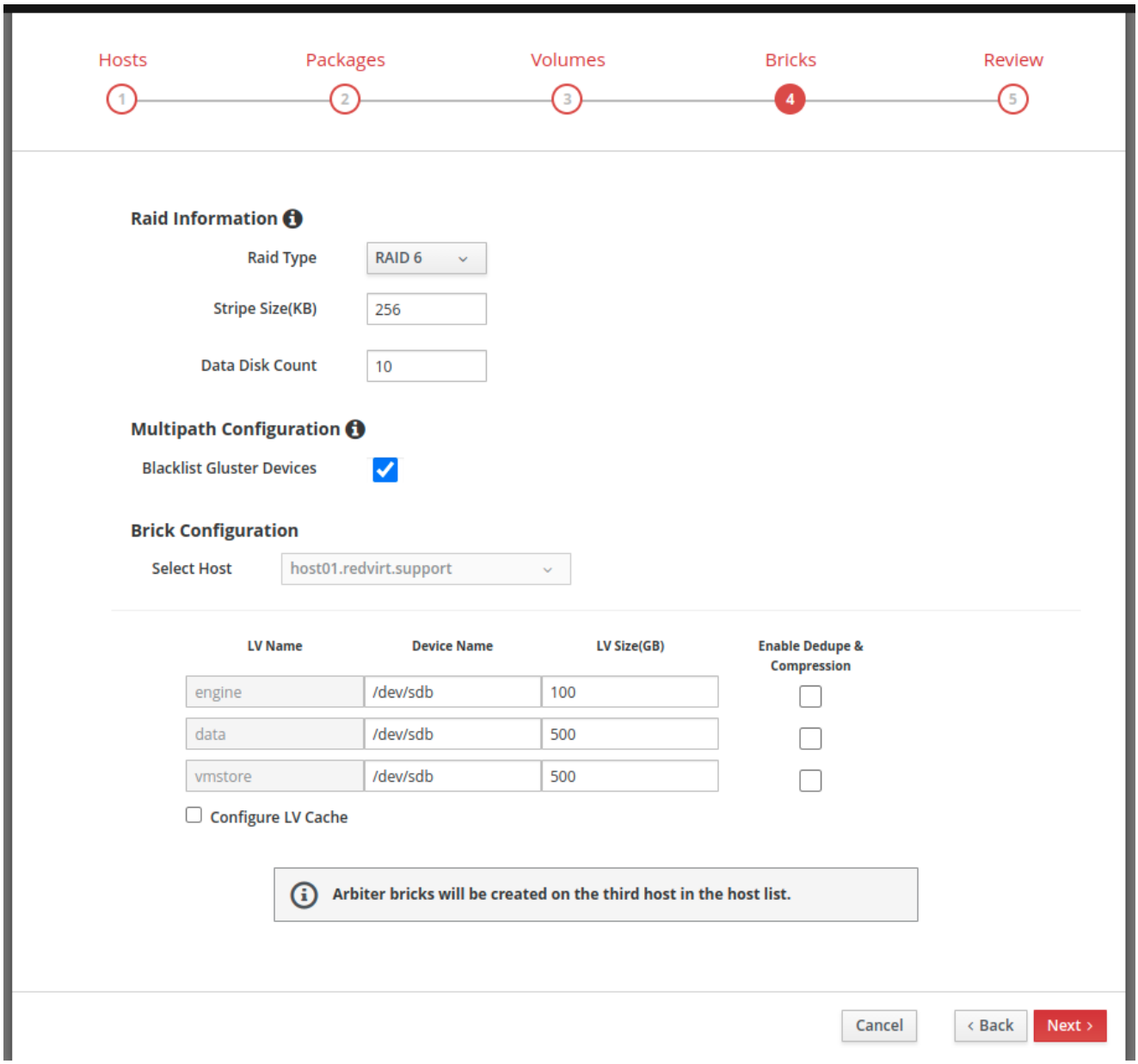


6. Определите необходимые тома.

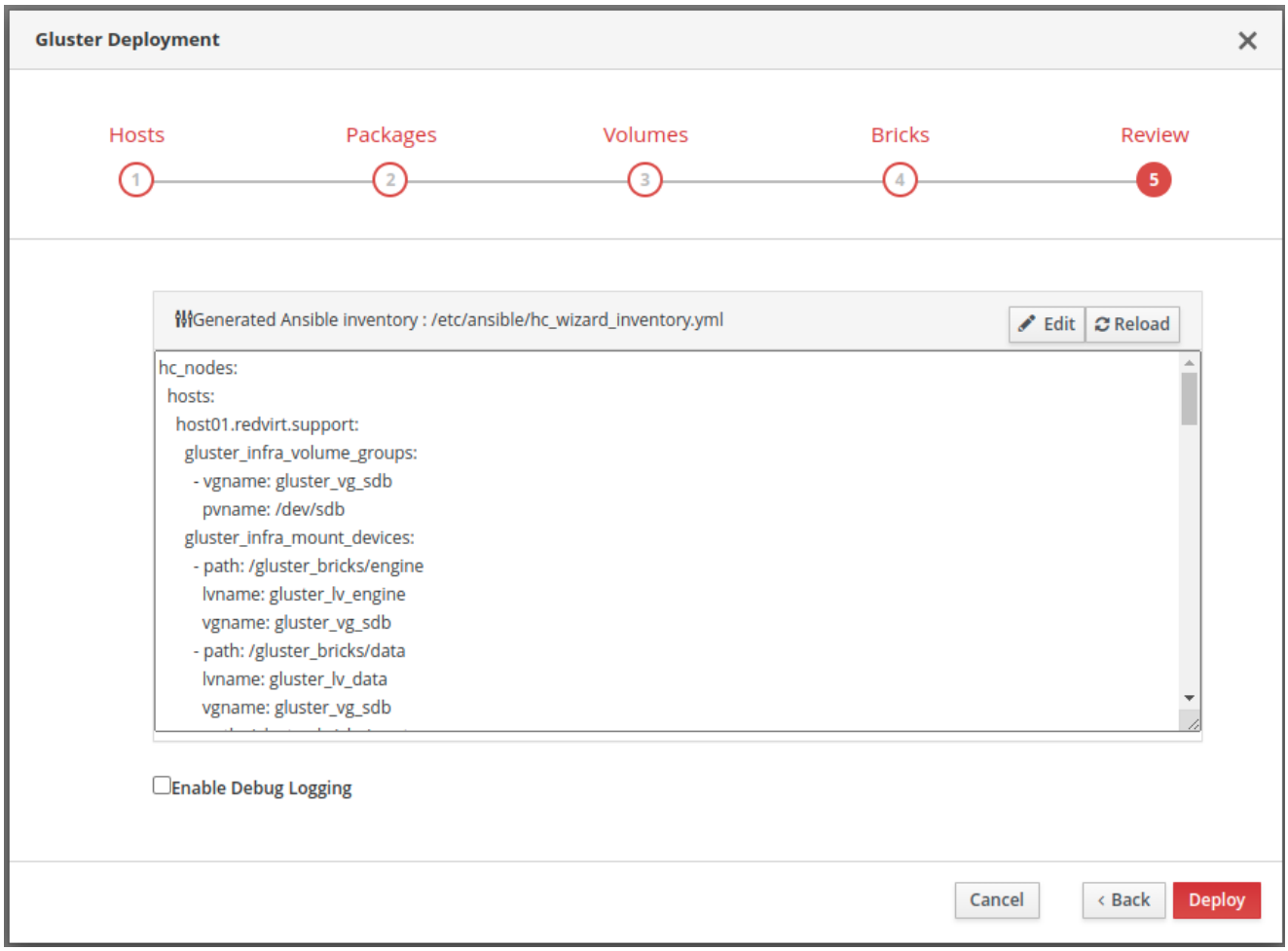
Обратите внимание, что первый указанный том будет использоваться для развертывания **Hosted Engine**.



7. Настройте жесткие диски — тип, наименование устройств и их размер.

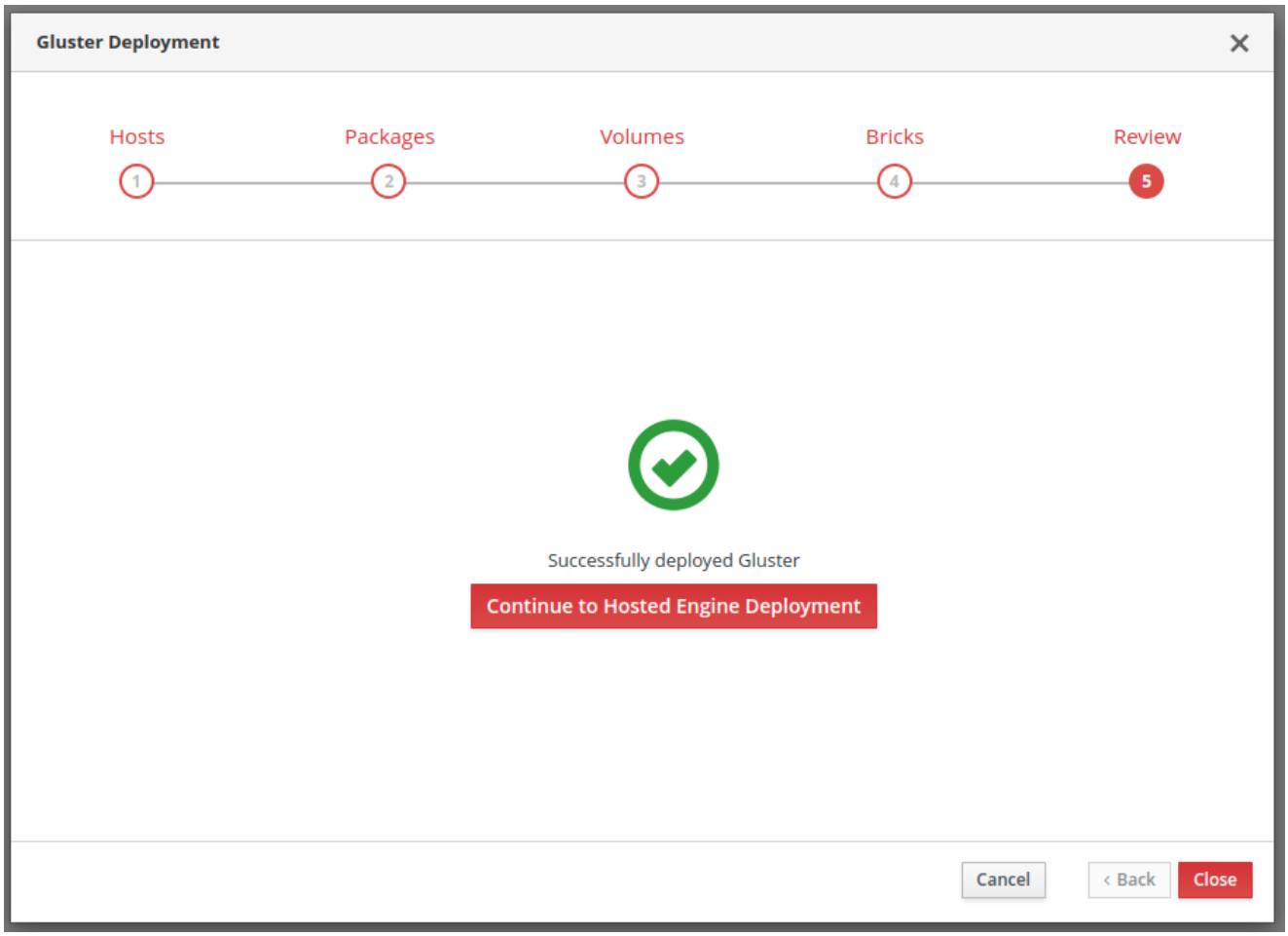


8. Проверьте установленные значения и характеристики, если все настроено верно, нажмите «**Deploy**».



Затем начнется процедура развертывания единого узла **Gluster**.

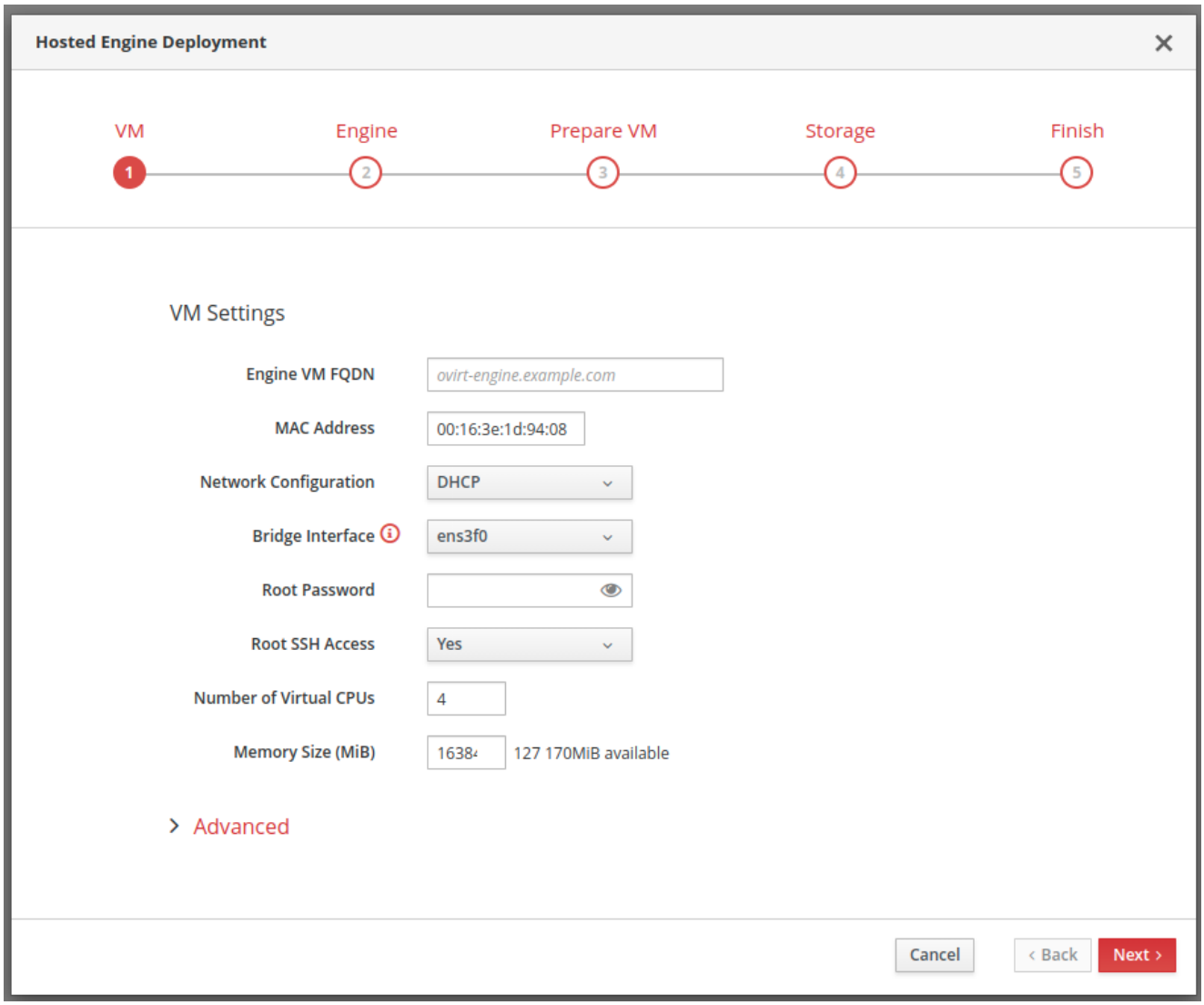
После успешной установки будет выведено соответствующее сообщение и предложено перейти к развёртыванию **Hosted Engine**.



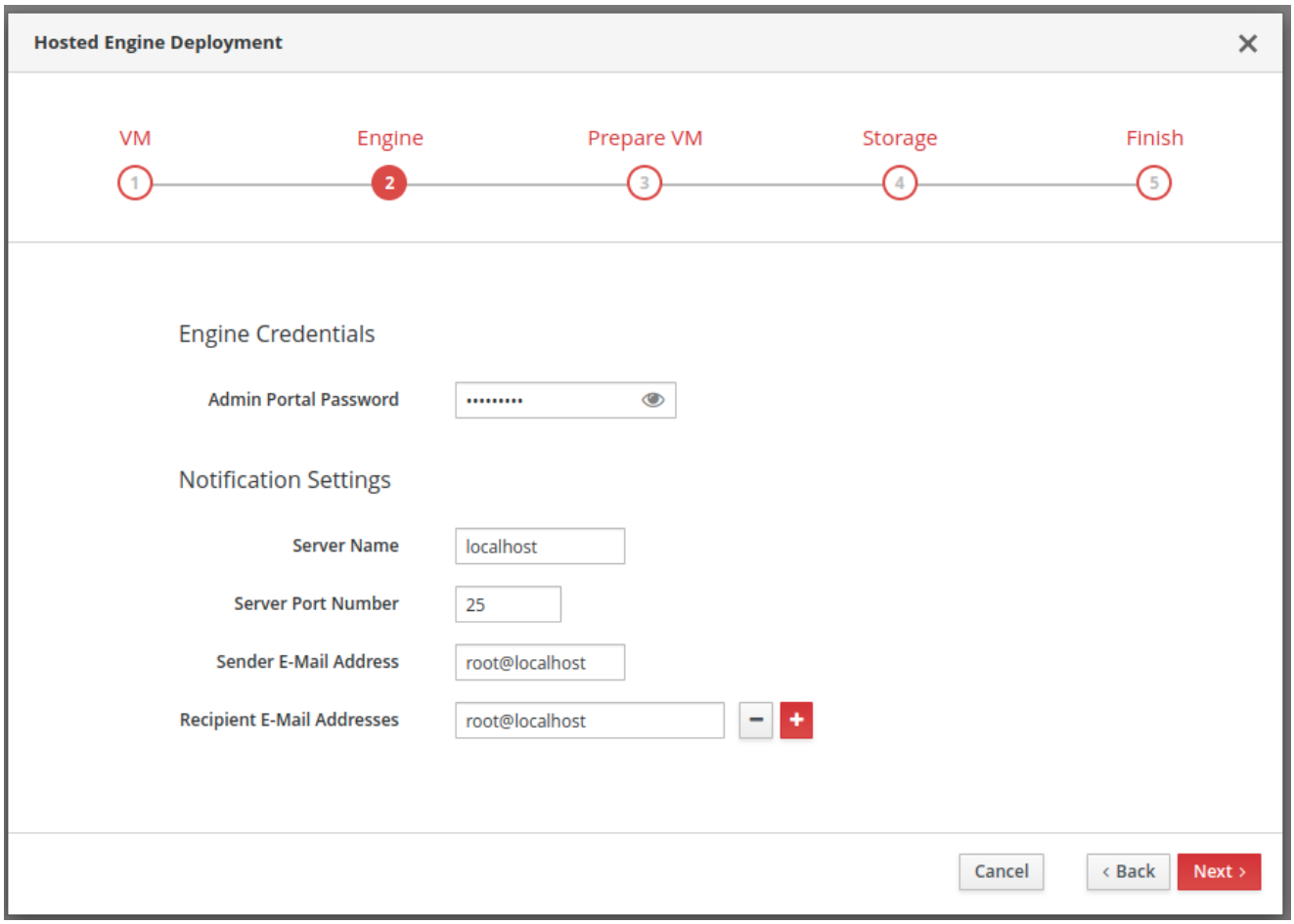
Развертывание Hosted Engine

Процедура настройки **Hosted Engine** стандартная.

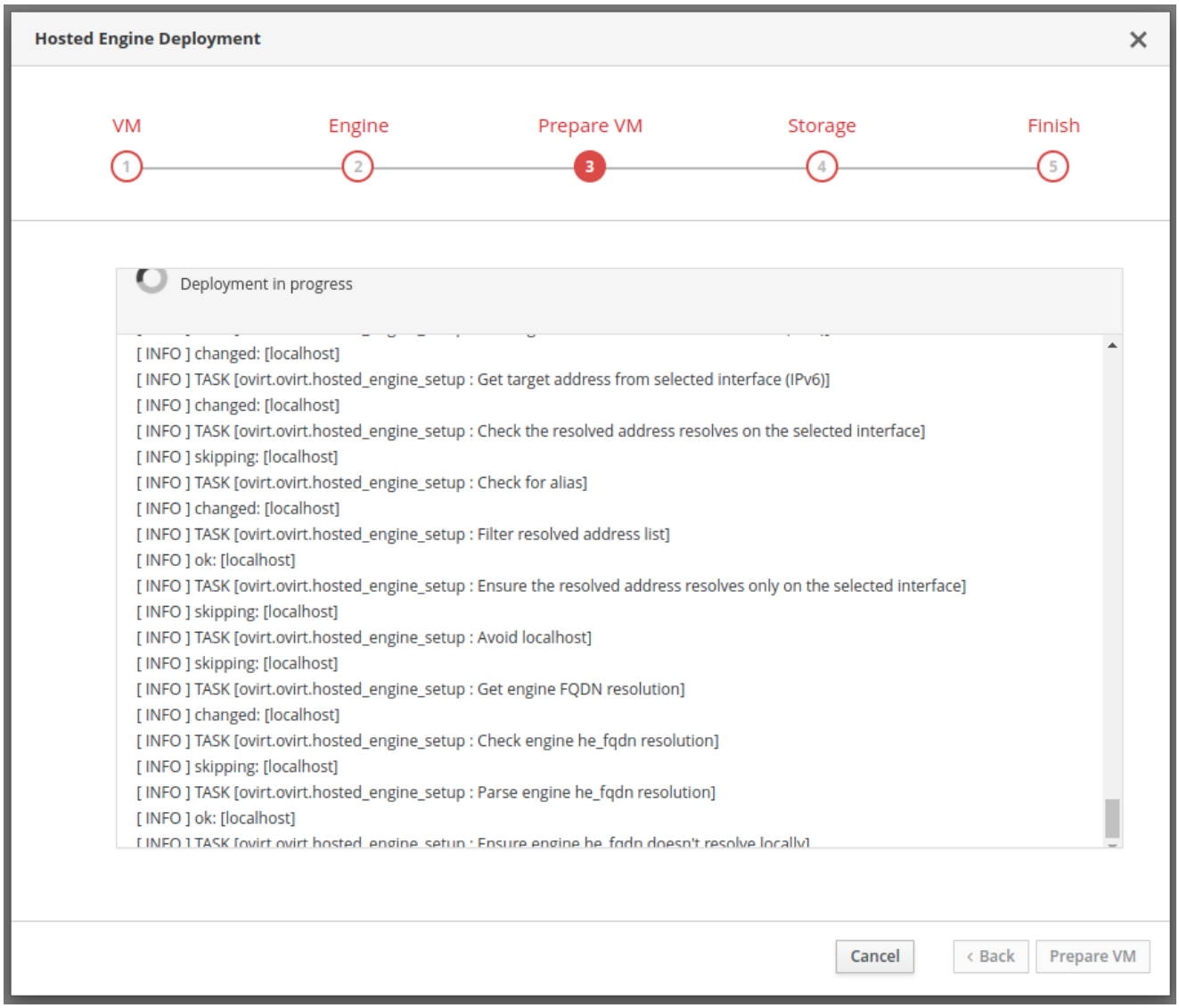
На вкладке **VM** заполните поля в соответствии с вашими параметрами сети. Нажмите **Next**.



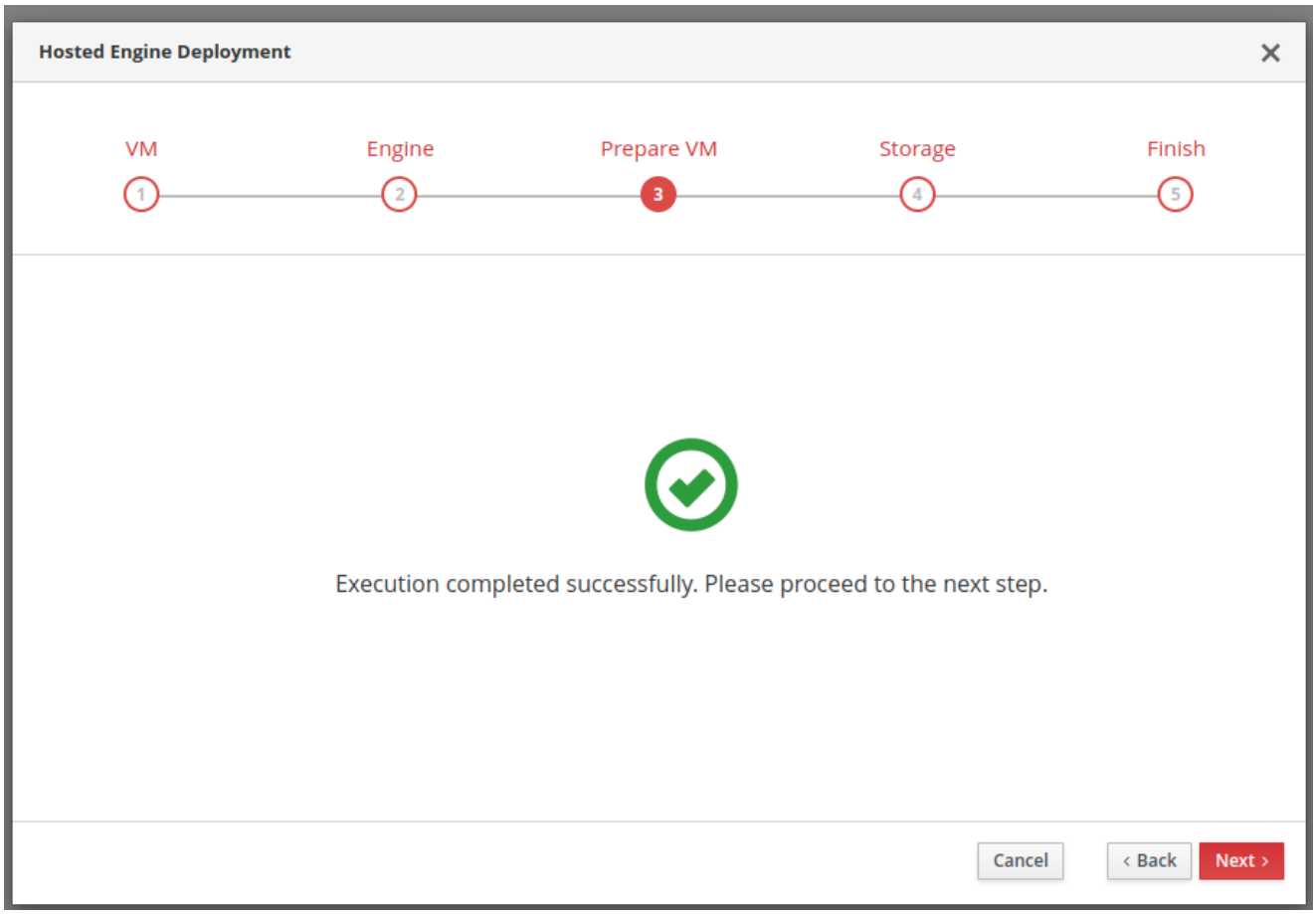
На вкладке **Engine** назначьте пароль администратору портала, а также настройте службу уведомлений.



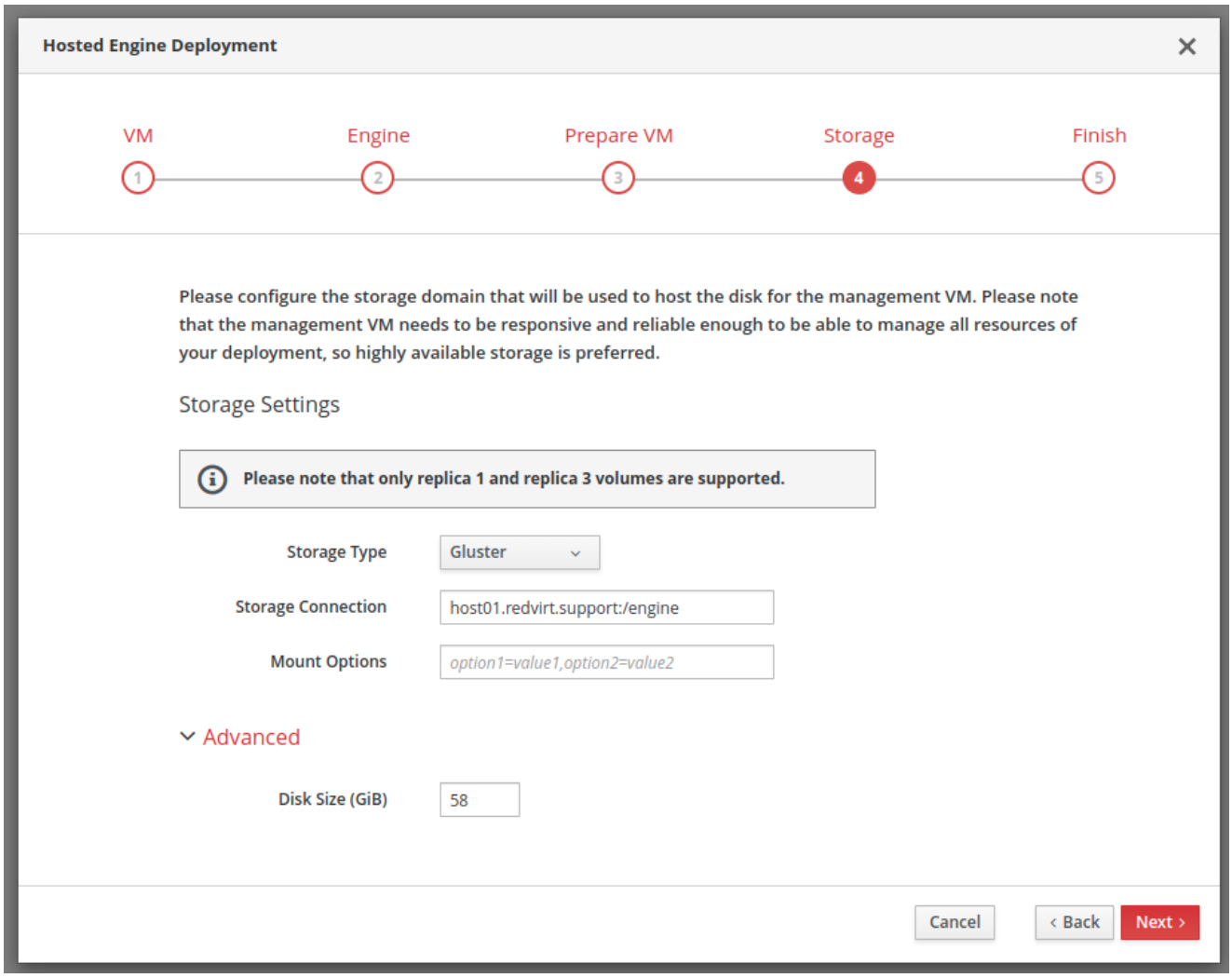
Во вкладке **Prepare VM** проверьте данные для ВМ и, если все настроено верно, нажмите кнопку «**Prepare VM**». Будет запущен процесс подготовки виртуальной машины и развертывание **Hosted Engine**.



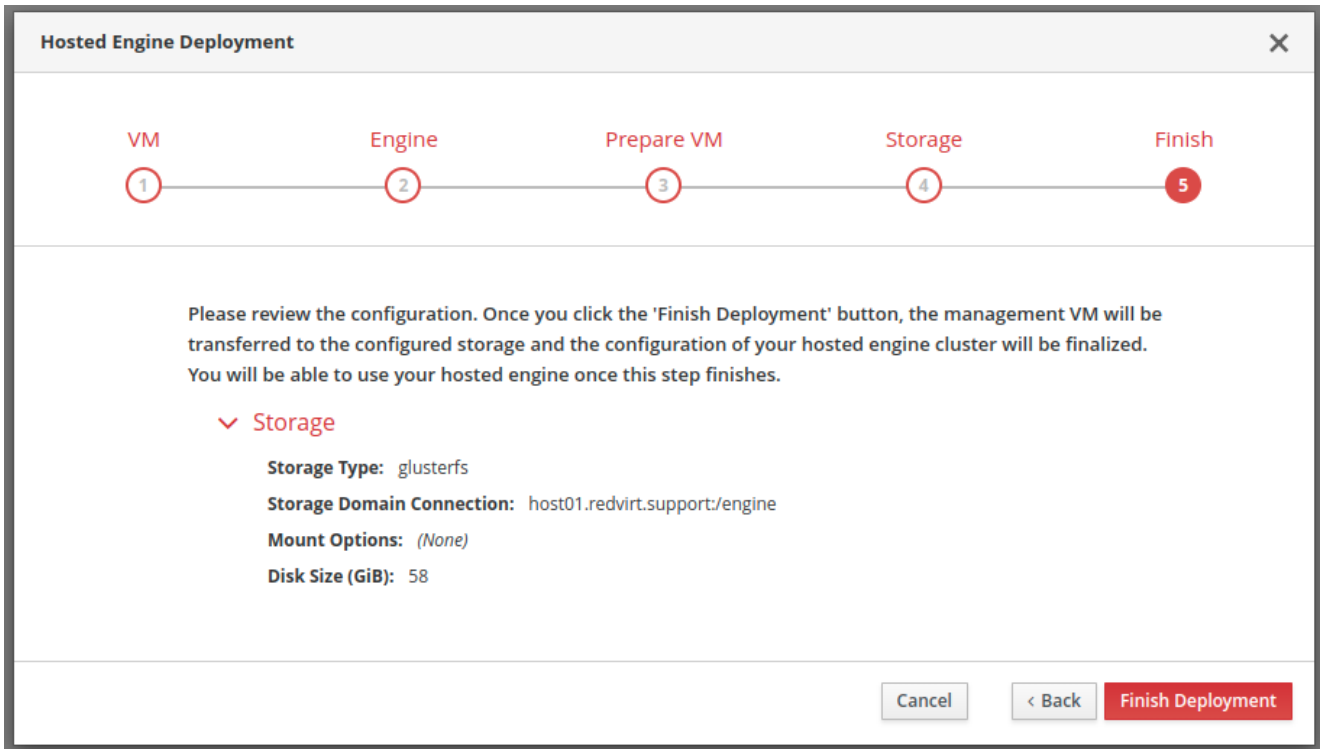
После успешного завершения процесса будет выведено соответствующее сообщение. Нажмите **Next**.



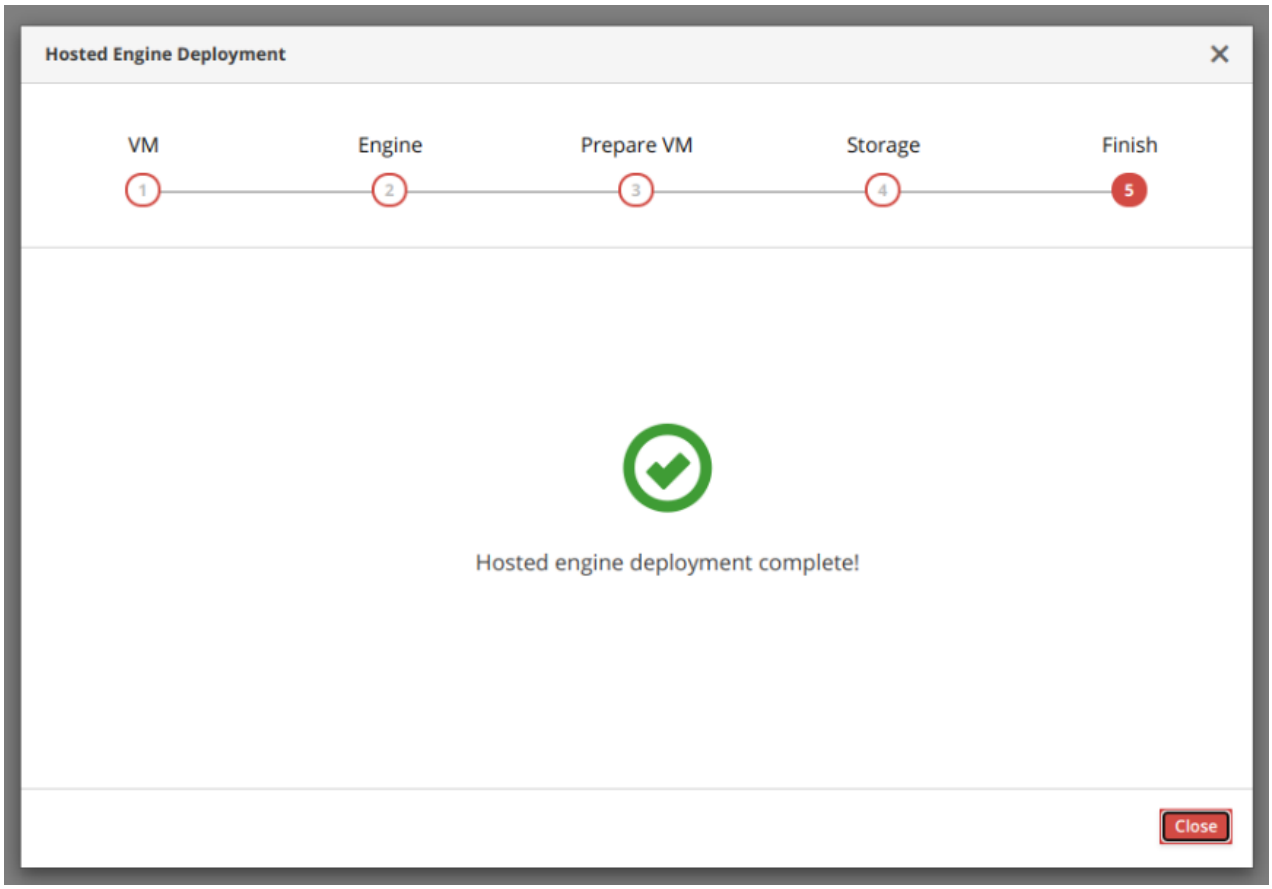
Во вкладке **Storage** будет автоматически определен ранее развернутый **Gluster** и предложение его подключить в качестве сетевого хранилища данных. Нажмите **Next**.



Для завершения развертывания проверьте данные хранилища, если все настроено верно, нажмите **Finish Deployment**.



После успешной установки нажмите **Close**.


Hosted Engine Deployment
VM
Engine
Prepare VM
Storage
Finish
1
2
3
4
5
Hosted engine deployment complete!
Close

Установка в режиме Gluster Hyperconverged для нескольких узлов

В разделе Базы знаний «**РЕД Виртуализация**» описаны **начальные этапы** работы с системой.
Скачать полную документацию

Предварительные требования

Предварительные требования:

1. Хост РЕД Виртуализации, содержащий три неразмеченных жестких диска, на которых в процессе развёртывания будут созданы необходимые разделы **Gluster**.

2. На хосте должно быть как минимум 2 интерфейса, чтобы можно было разделить трафик на внешний (**frontend**) и внутренний (**backend**).

Наличие только одной сети приведет к тому, что мониторинг **Engine**, клиентский трафик, трафик ввода-вывода **Gluster** будут работать вместе и мешать друг другу. Чтобы разделить сеть **backend**, кластер **Gluster** формируется с использованием адресов сети **backend**, а узлы добавляются к **Engine** с использованием адресов сети **frontend**.

3. Подготовленное полное доменное имя для вашего **Engine** и хостов. В DNS должны быть установлены записи прямого и обратного поиска. **Engine** должен использовать ту же подсеть, что и сеть управления.

4. Беспарольный **SSH** от первого хоста к другим, так как роль **ansible** должна удаленно выполнять команды — обязательное условие. Для настройки выполните следующие команды:

```
# ssh-keygen
# ssh-copy-id root@gluster.host1
# ssh-copy-id root@gluster.host2
# ssh-copy-id root@gluster.host3
```

Развертывание на узле РЕД Виртуализации

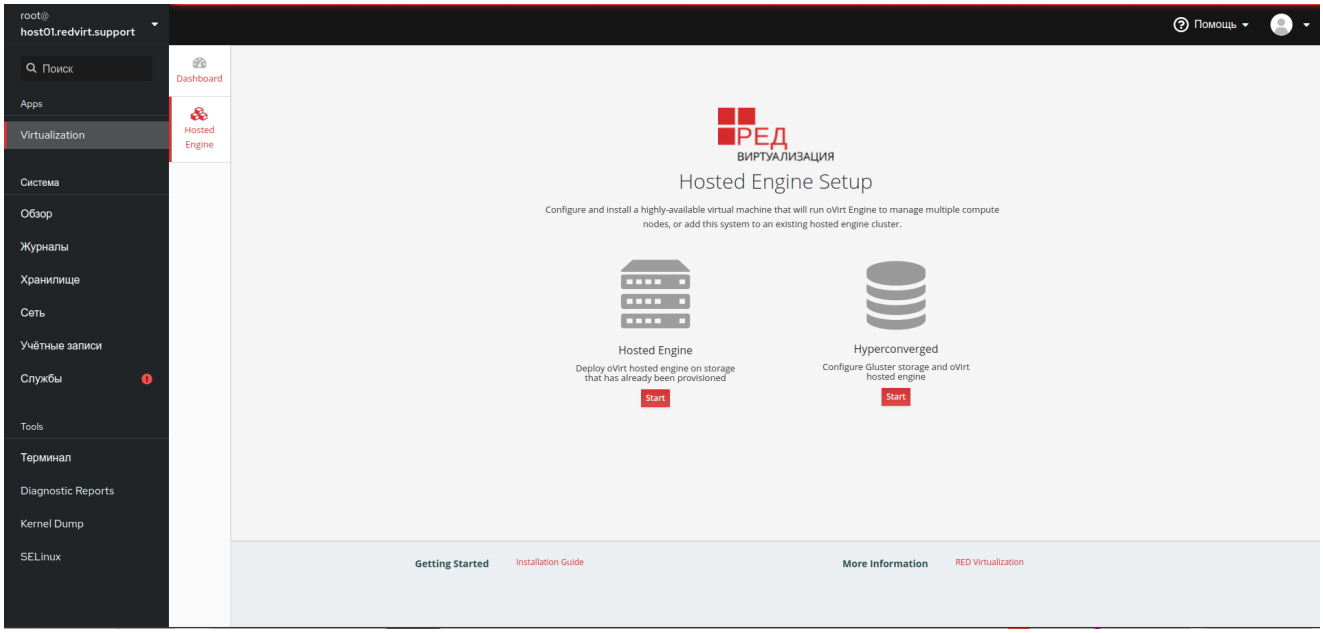
Хост РЕД Виртуализации содержит все необходимые пакеты для настройки гиперконвергентной среды. Начать настройку гиперконвергентной среды можно, если существует хотя бы один хост на базе РЕД Виртуализации.

Установка и настройка томов Gluster

Тома **Gluster** должны быть созданы перед установкой **Hosted Engine**. Один из созданных томов будет использован для размещения виртуальной машины **Hosted Engine**. Используйте пользовательский интерфейс **Cockpit** для настройки развертывания **Gluster** для нескольких узлов.

1. Войдите в веб-консоль. Перейдите к интерфейсу управления веб-консоли основного узла виртуализации, например, https://<имя_хоста>:9090/, и войдите в систему, используя учетные данные суперпользователя **root**.

2. Перейдите во вкладку **Virtualization** – **Hosted Engine** и нажмите **Start** в разделе **Hyperconverged**.



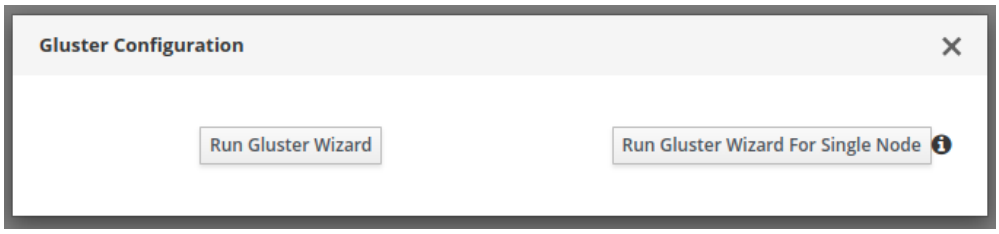
Откроется окно настройки **Gluster**.

3. Запустите мастер развертывания.

После запуска мастер развертывания предложит выбрать одно из дальнейших действий:

- Запустить мастер развертывания Gluster;
- Запустить мастер развертывания Gluster для одиночного узла.

Выберите первый вариант.



Откроется окно развертывания **Gluster** в режиме трех узлов.

4. Укажите имена хостов хранилища.

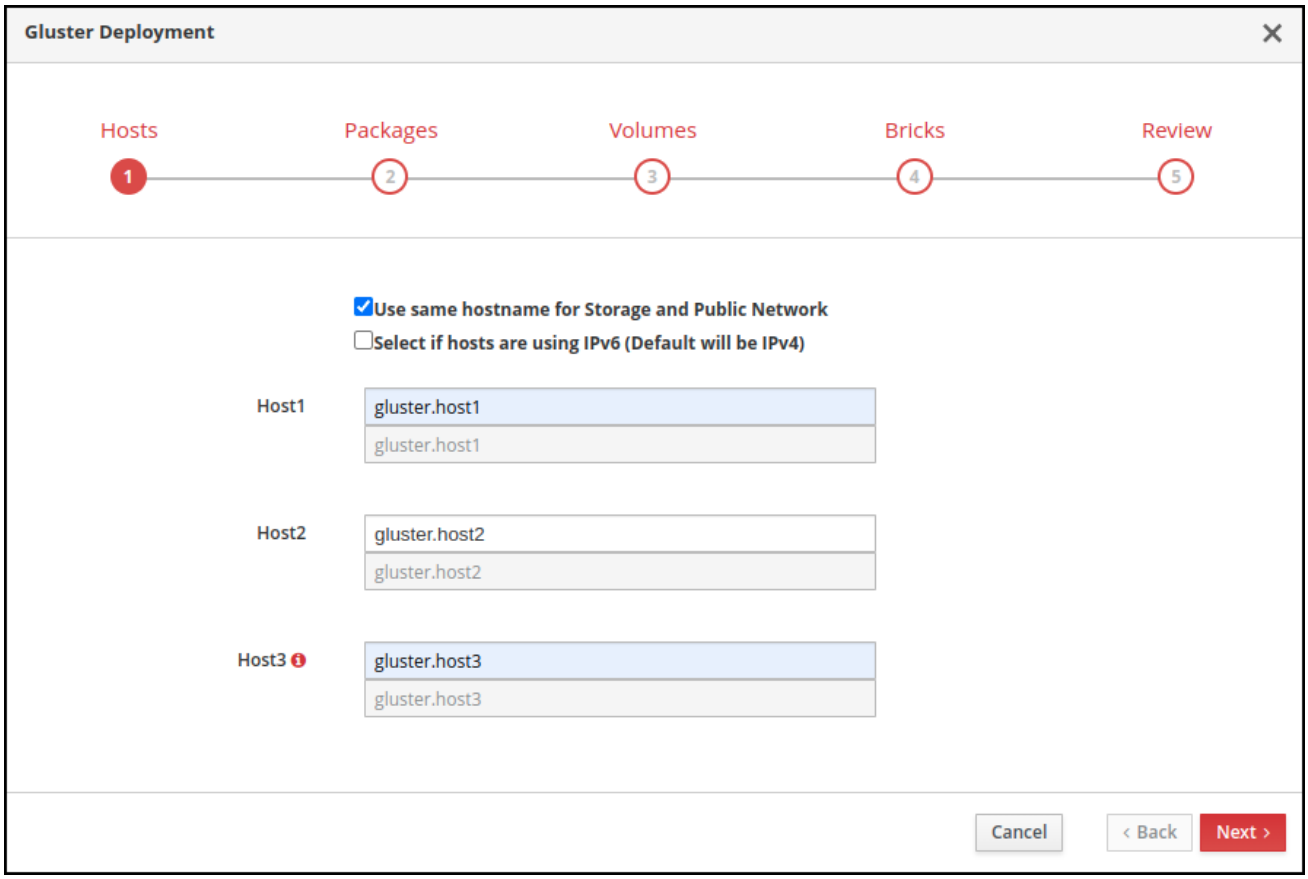
Укажите полные доменные имена сетевых хранилищ (не сети управления) для трех узлов виртуализации. Хост виртуализации, использующий авторизацию по **SSH** с помощью пар ключей, должен быть указан первым, так как именно на нем будет разворачиваться **Hosted Engine** и запускаться команда развертывания **Gluster**.

Примечание.

Для обеспечения высокой доступности требуется минимум два узла, но в случаях, когда два узла **не синхронизированы**, такой системе необходим третий компонент, называемый арбитром.

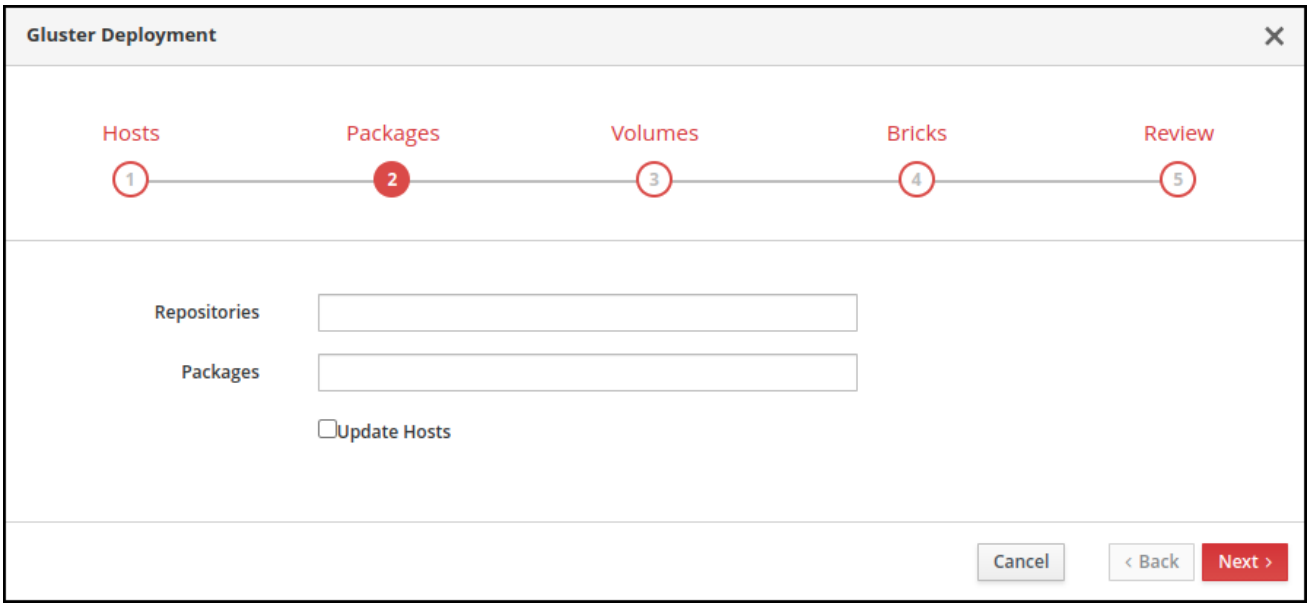
В случае потери прямой связи между узлами арбитр предотвращает состояние, когда на обоих узлах работают копии одних и тех же виртуальных машин и выполняется независимая модификация хранимых данных (**split brain**).

В роли арбитра на вкладке **Hosts** выступает указанный в поле **Host3** узел.



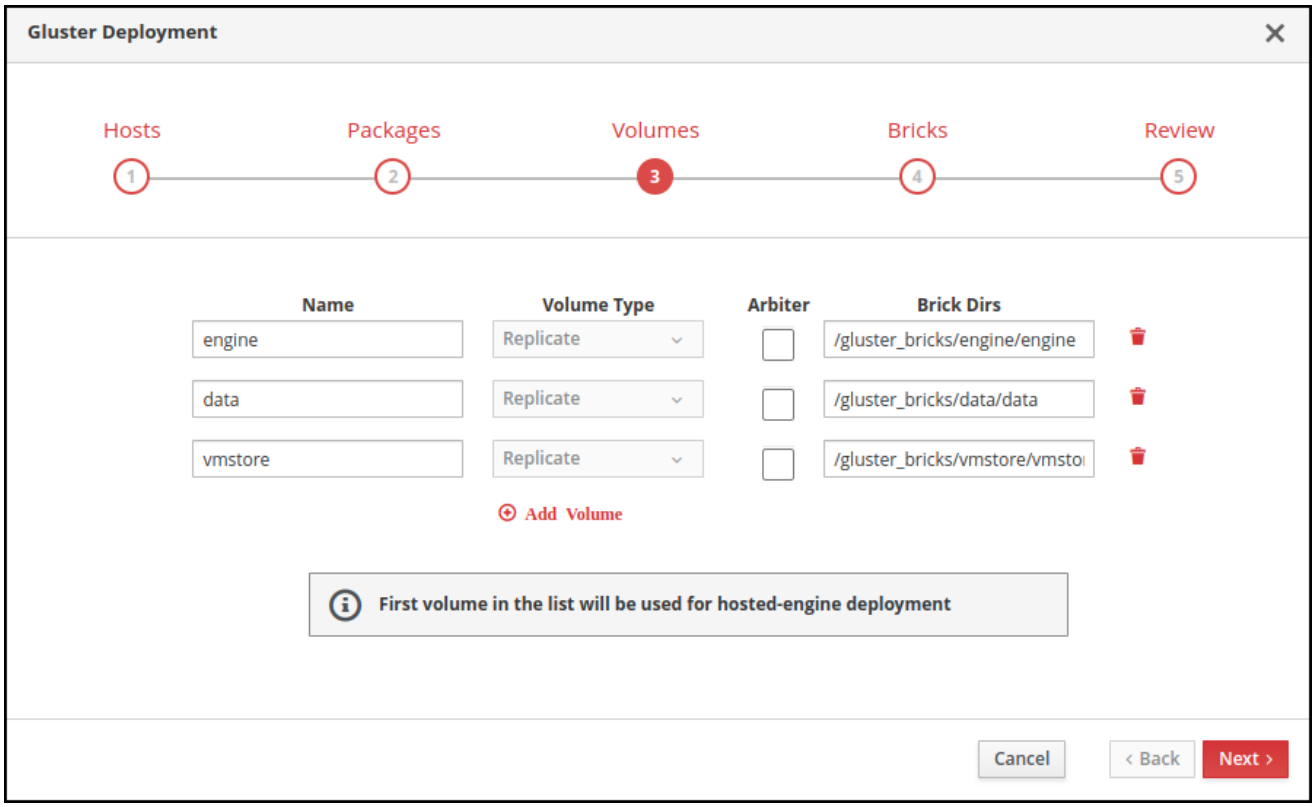
Нажмите **Next**.

5. При необходимости загрузите репозитории и дополнительные пакеты.



6. Определите необходимые тома.

Обратите внимание, что первый указанный том будет использоваться для развертывания **Hosted Engine**.

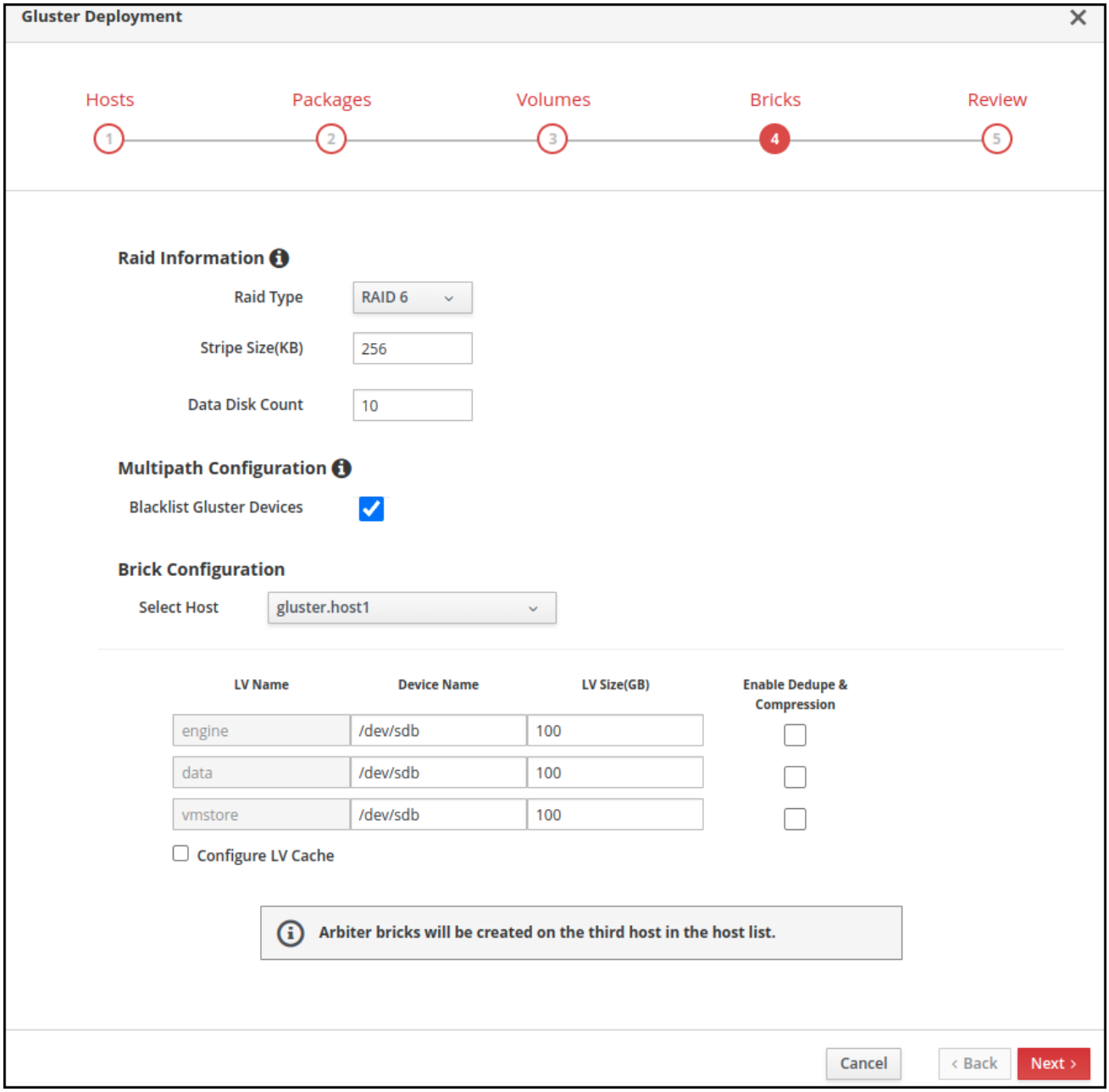


- **Name**: Имя создаваемого тома.
- **Volume Type**: Тип тома – **Replicate**. В данной версии поддерживаются только реплицированные тома.
- **Arbiter**: Необходимость создания тома с блоком арбитра. Если флаг установлен, на третьем диске будут храниться только метаданные.
- **Brick Dirs**: Каталог, содержащий блоки указанного тома.

В указанных полях можно оставить значения по умолчанию.

7. Настройте жесткие диски — укажите тип, наименование устройств и их размер.

Для редактирования информации о настраиваемом хосте можно использовать раскрывающееся меню **Select Host**.



В блоке **Raid Information** укажите:

- тип используемого массива **RAID** (он должен совпадать с используемым типом **RAID** на хосте);
- объем данных, записываемых **RAID**-контроллером на один диск в рамках одной полосы;
- количество дисков данных в массиве **RAID**.

В блоке **Brick Configuration** укажите:

- имя создаваемого тома (определяется автоматически из предыдущего шага);
- имя устройства, которое будет использовано (рекомендуется использовать неразмеченное устройство);
- размер создаваемого логического тома в ГБ (значение должно быть одинаковым для всех блоков в наборе, размер блока арбитра может быть меньше других блоков);
- необходимость использования на дисках дедупликации с технологией **VDO**.

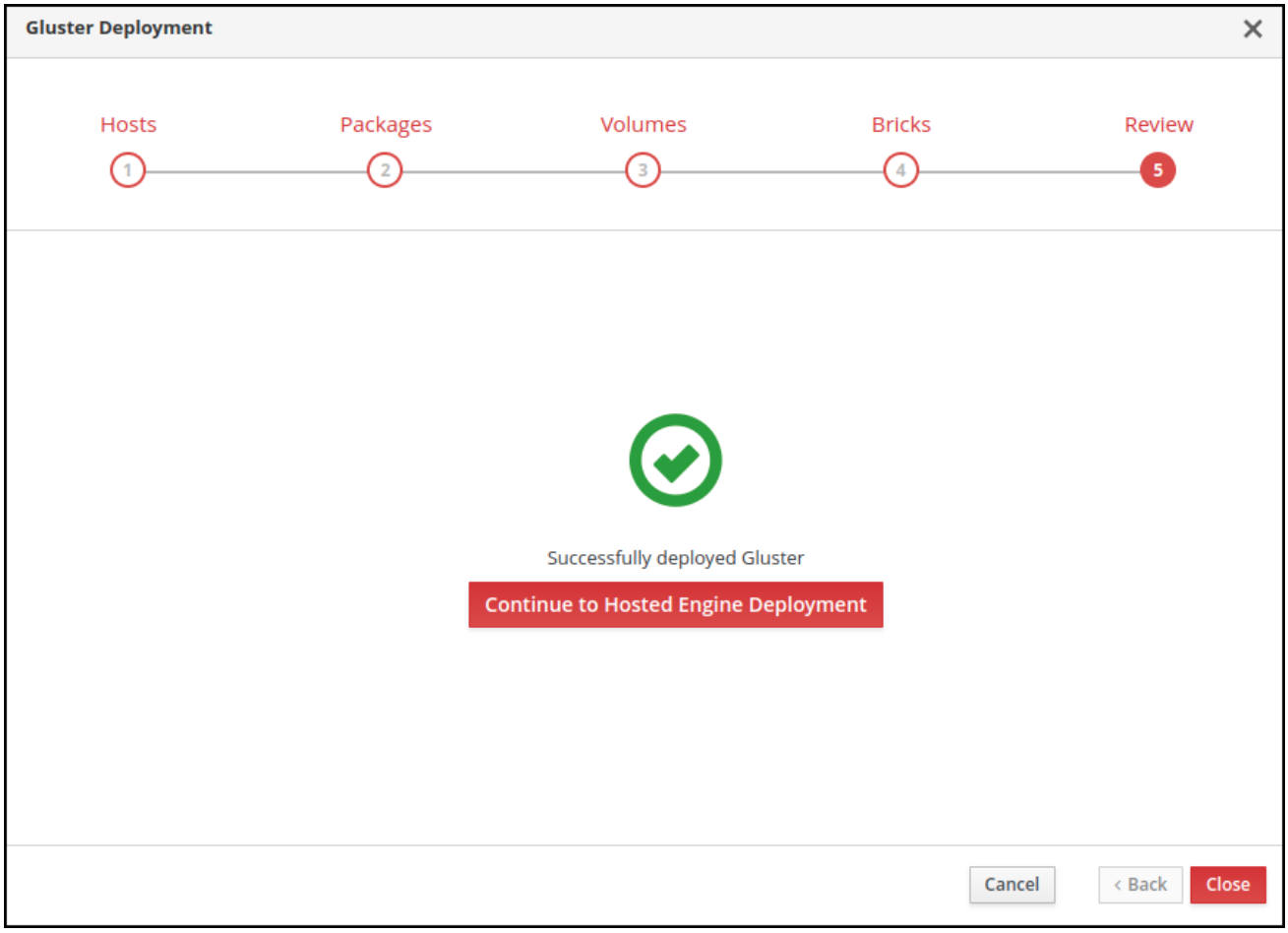
При активации параметра **Configure LV Cache** появляется возможность настройки **SSD**-кеширования.

SSD-кеширование — технология, когда твердотельные **SSD**-накопители используются в качестве буфера для часто запрашиваемых данных. Система определяет данные по степени востребованности и перемещает их на быстрый накопитель, используемый в качестве кеширующего диска. Кеш позволяет получать доступ к данным в несколько раз быстрее, чем если бы они были получены с более медленного жесткого диска.

8. Проверьте установленные значения и характеристики, если все настроено верно, нажмите **Deploy**.

Начнется процедура развертывания **Gluster**.

После успешной установки будет выведено соответствующее сообщение и предложено перейти к развёртыванию **Hosted Engine.**



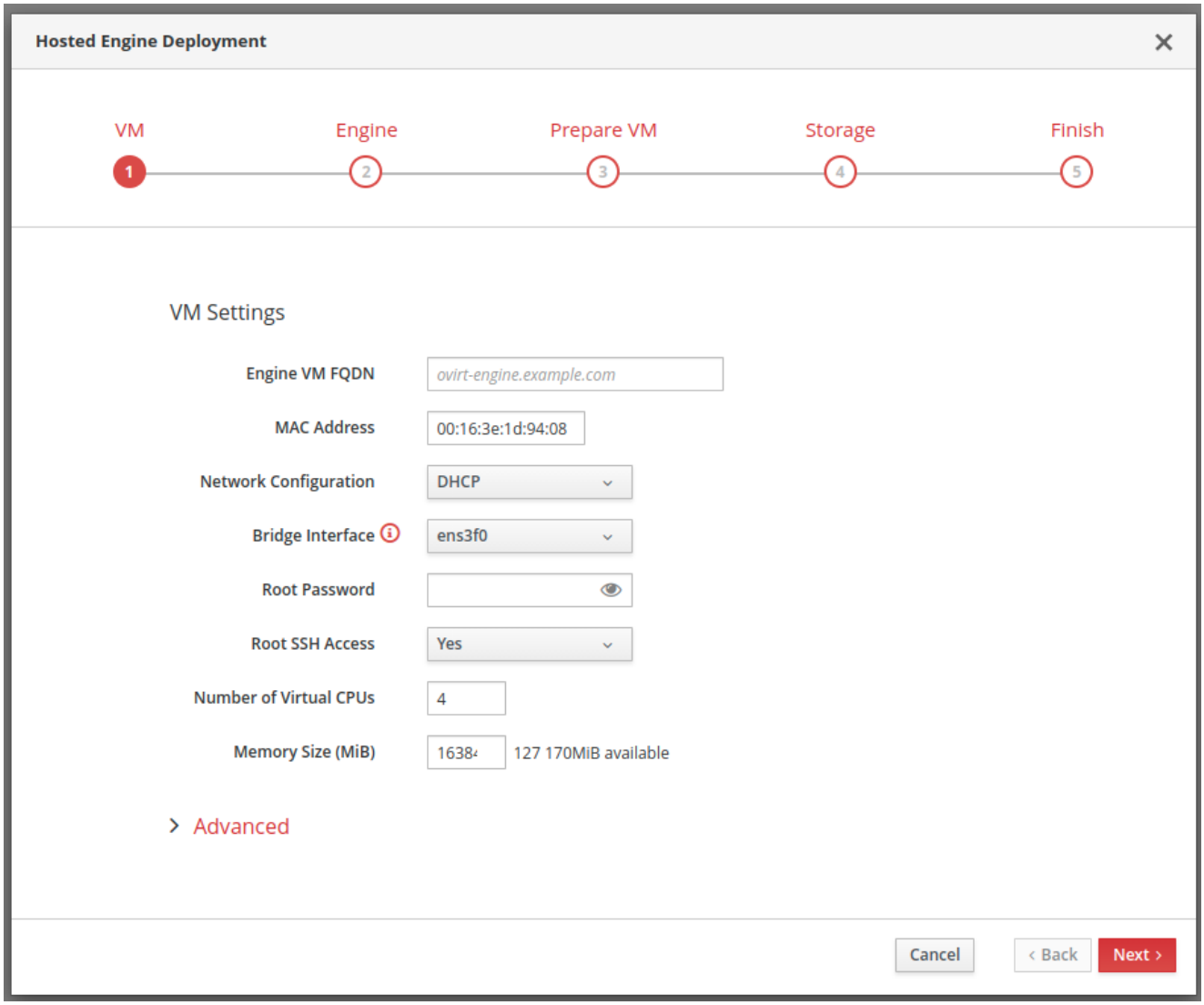
Примечание.

Если развертывание **Gluster** завершилось неудачей, нажмите кнопку **Redeploy**. Будет открыта вкладка **Review**, где с помощью кнопки **Edit** можно внести необходимые изменения в сгенерированный файл конфигурации **Gluster** и повторить попытку развертывания.

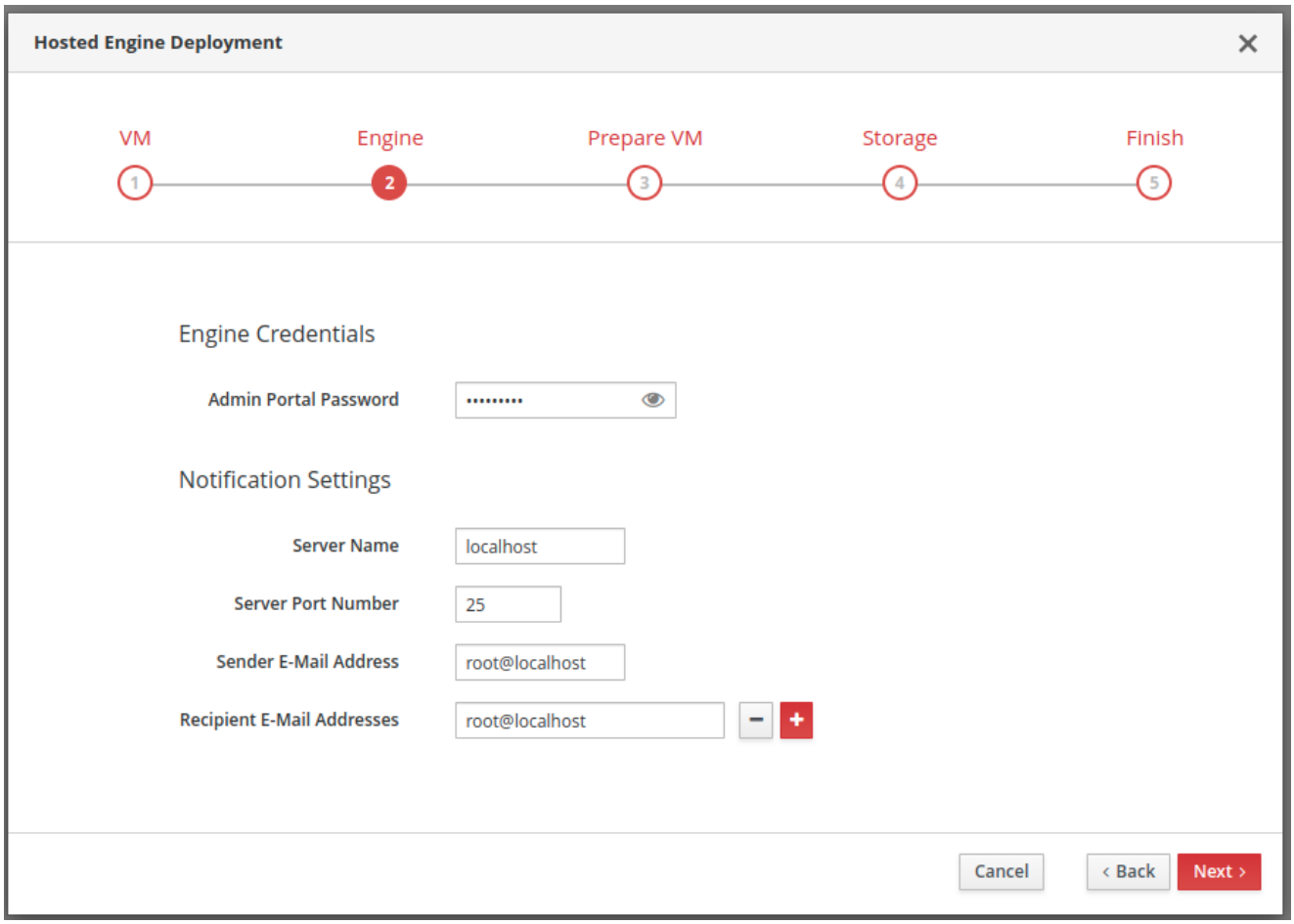
Развертывание Hosted Engine

Процедура настройки **Hosted Engine** стандартная.

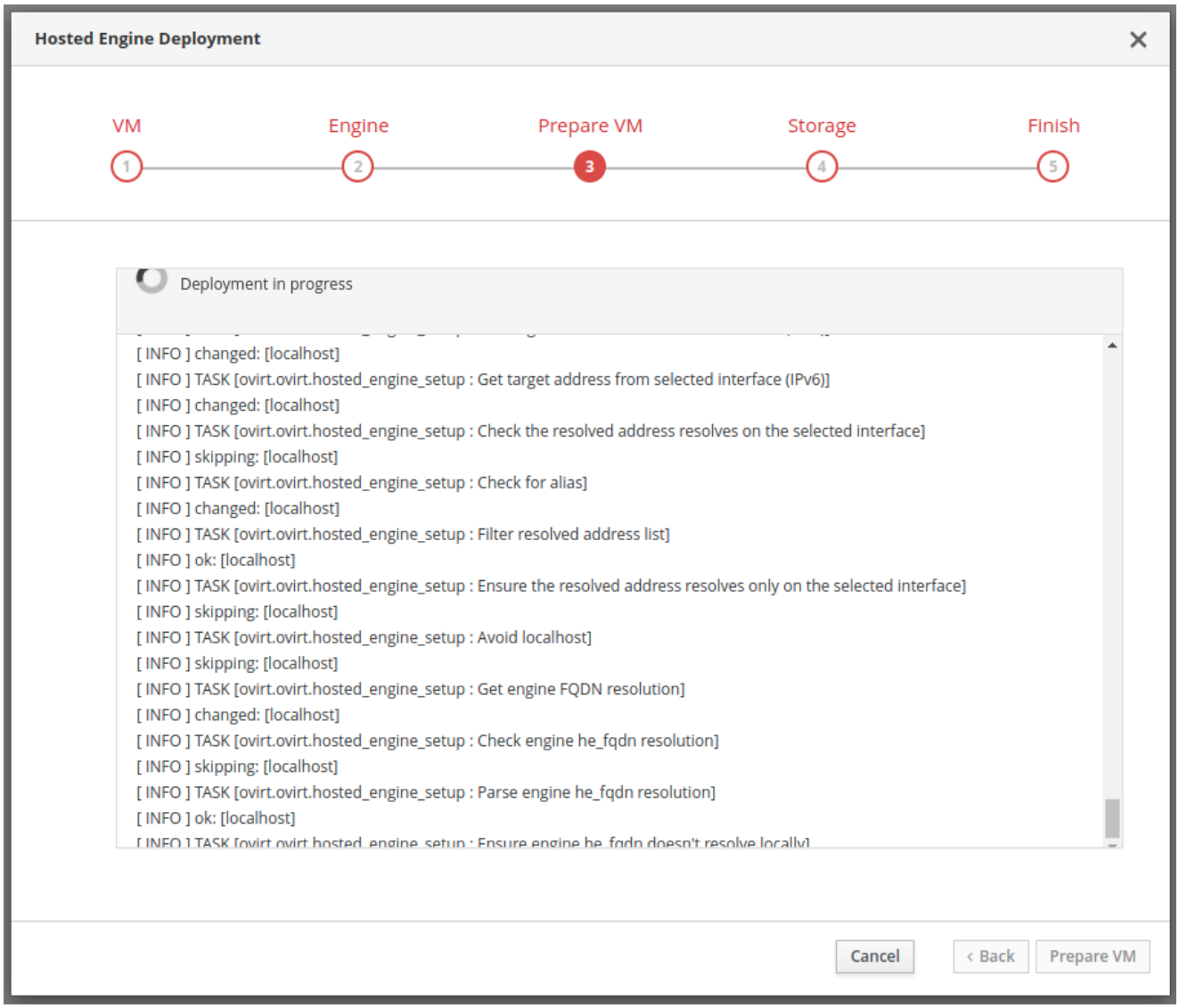
На вкладке **VM** заполните поля в соответствии с вашими параметрами сети. Нажмите **Next**.



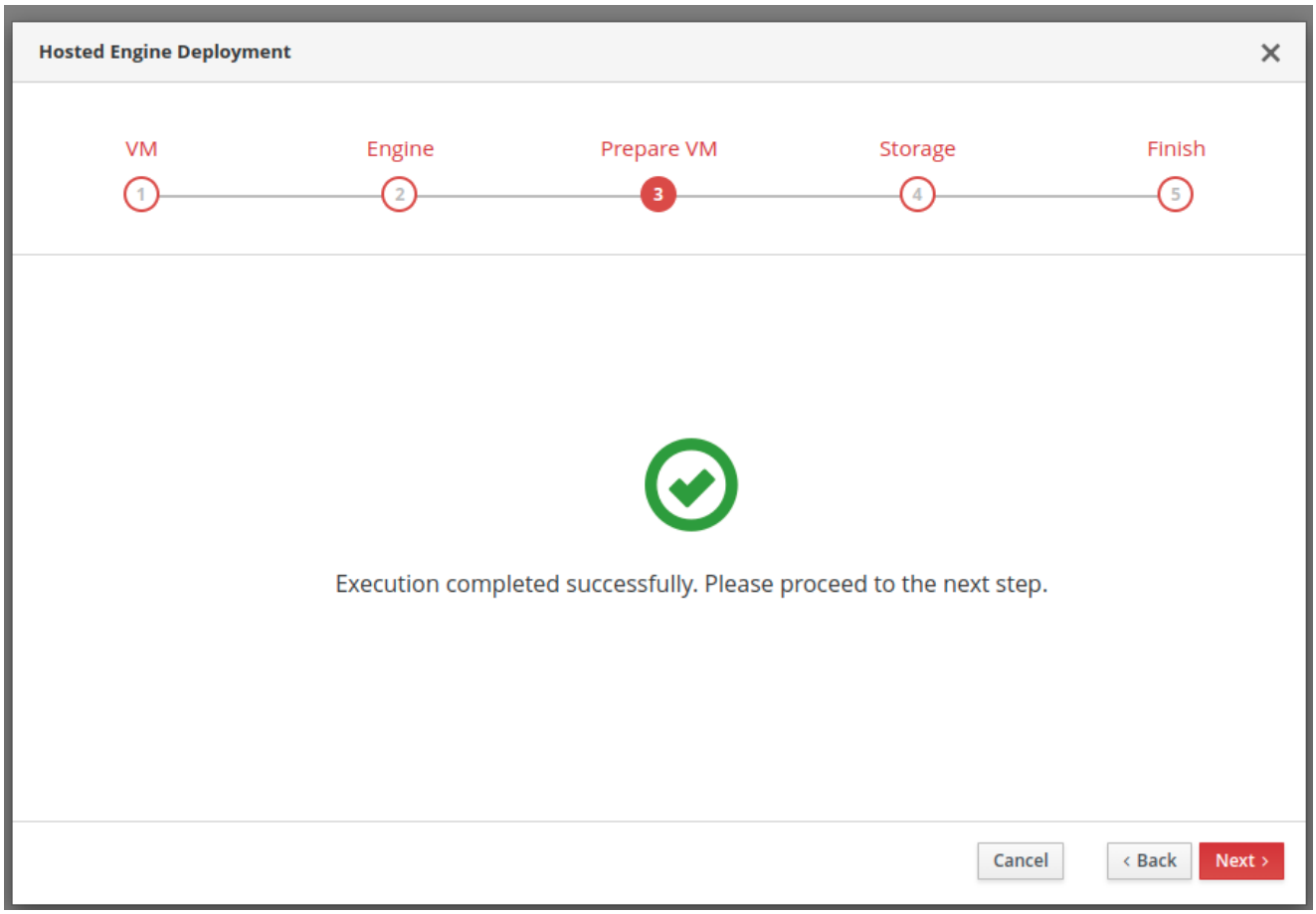
На вкладке **Engine** назначьте пароль администратору портала, а также настройте службу уведомлений.



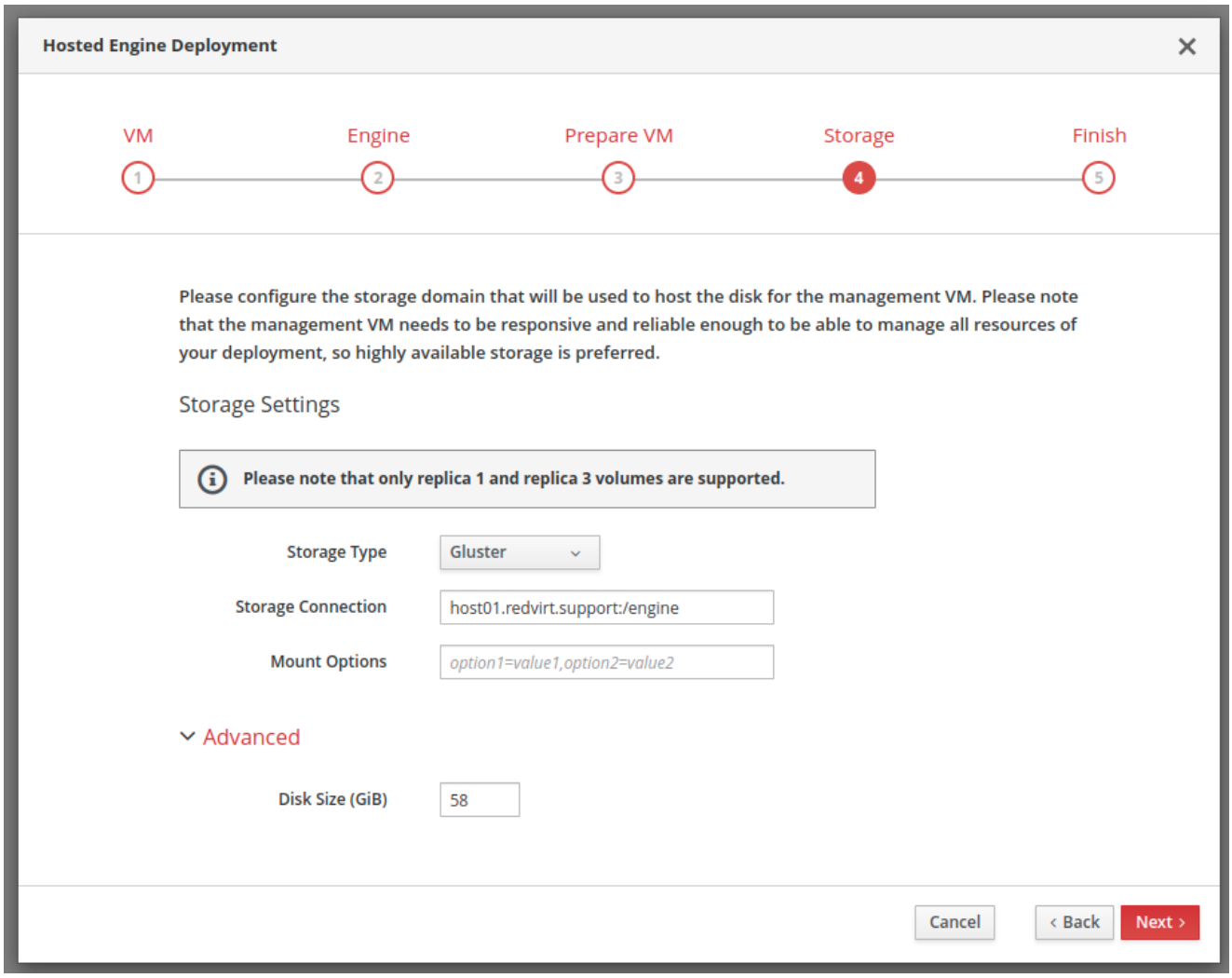
Во вкладке **Prepare VM** проверьте данные для ВМ и, если все настроено верно, нажмите кнопку «**Prepare VM**». Будет запущен процесс подготовки виртуальной машины и развертывание **Hosted Engine**.



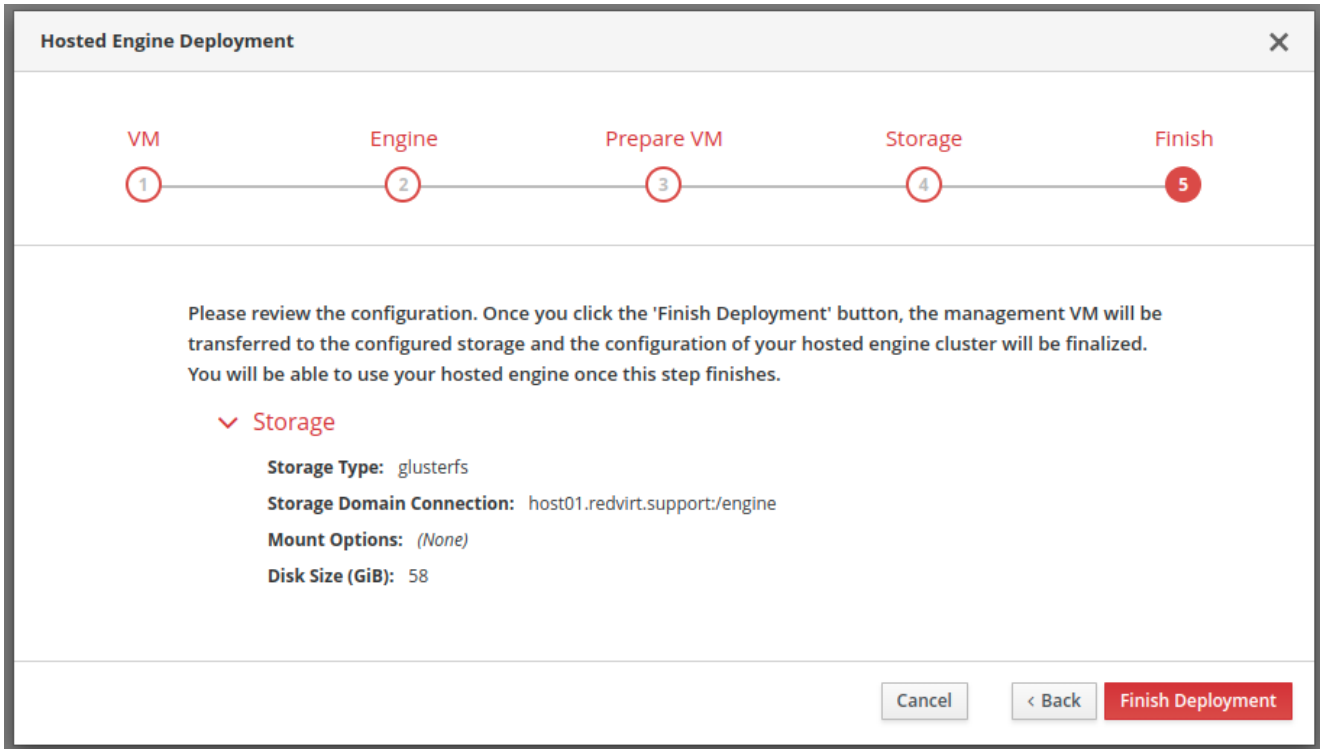
После успешного завершения процесса будет выведено соответствующее сообщение. Нажмите **Next**.



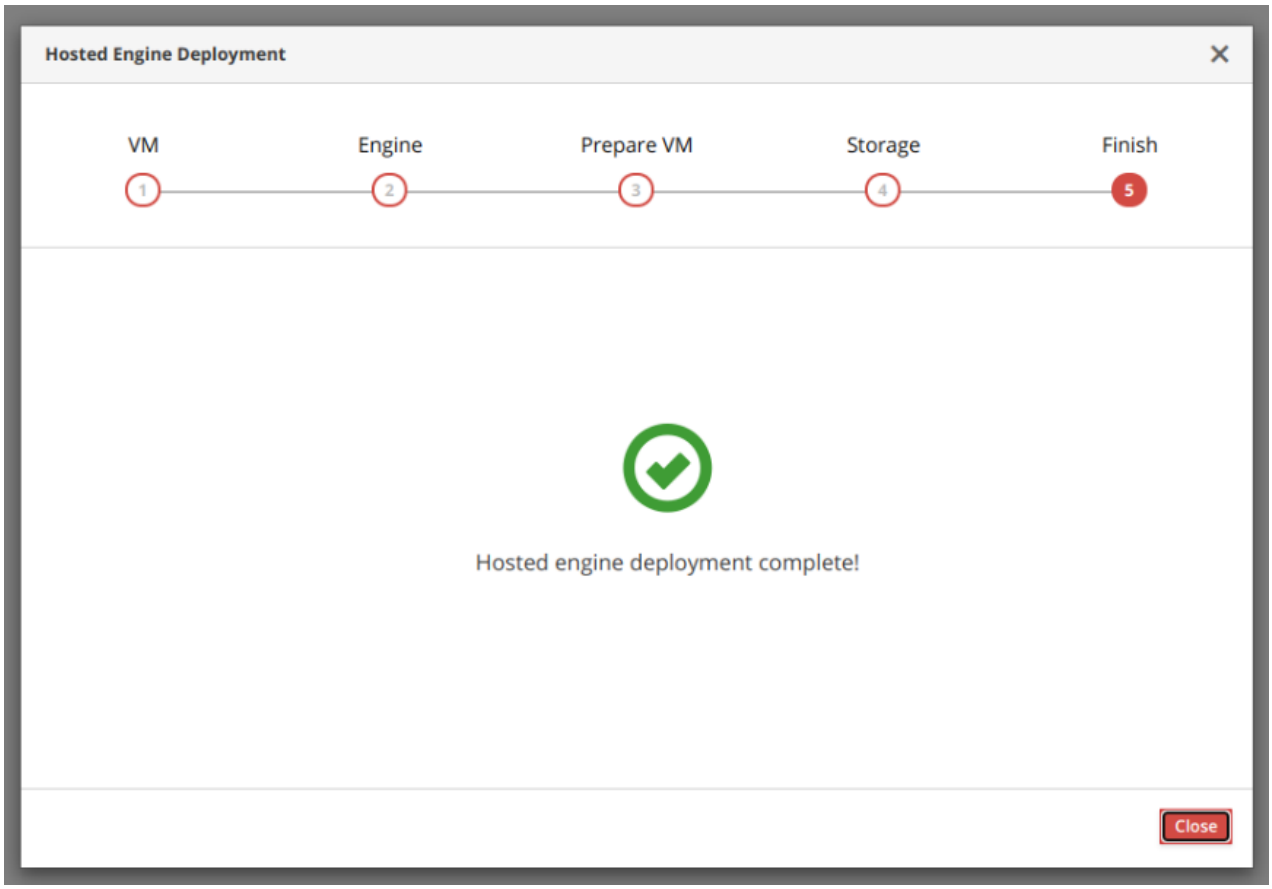
Во вкладке **Storage** будет автоматически определен ранее развернутый **Gluster** и предложение его подключить в качестве сетевого хранилища данных. Нажмите **Next**.



Для завершения развертывания проверьте данные хранилища, если все настроено верно, нажмите **Finish Deployment**.



После успешной установки нажмите **Close**.


Hosted Engine Deployment
VM
Engine
Prepare VM
Storage
Finish
1
2
3
4
5
Hosted engine deployment complete!
Close

Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Standalone с помощью стороннего центра сертификации

Создание центра сертификации

Для создания локального центра сертификации в РЕД ОС 7.3 необходимо выполнить следующие действия:

1. Создать закрытый ключ **Root**:

```
openssl genrsa -des3 -out root.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
..............+++++
e is 65537 (0x010001)
Enter pass phrase for root.key: ********
Verifying - Enter pass phrase for root.key: ********
```

ВАЖНО!

Рекомендуется указать парольную фразу и защитить закрытый ключ.

2. Сгенерировать корневой сертификат. В процессе выполнения команды будет предложено ввести указанную на предыдущем шаге парольную фразу. После этого потребуется ввести некоторые данные для запроса сертификата - страну, область, город или другой населенный пункт, наименование организации, наименование подразделения организации и имя сертификата.

```
openssl req -x509 -new -nodes -key root.key -sha256 -days 7200 -out root.pem
```

где:

- **-x509**– экземпляр сертификата;
- **-new**– новый запрос сертификата;
- **-nodes**– отключить шифрование выходного ключа;
- **-key root.key**– файл ключа;
- **-sha256**– алгоритм подписи;
- **-days 7200**– период действия сертификата (в днях);
- **-out root.pem**– имя сгенерированного сертификата.

```
Enter pass phrase for root.key: ********
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:moscow
Locality Name (eg, city) [Default City]:moscow
Organization Name (eg, company) [Default Company Ltd]:redsoft
Organizational Unit Name (eg, section) []:drsp
Common Name (eg, your name or your server's hostname) []:Private RED Virt Authority
Email Address []:
```

3. Проверить содержание сгенерированного сертификата, выполнив команду:

```
openssl x509 -text -noout -in root.pem | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
60:05:f3:81:4d:b9:33:bd:a6:d7:34:9b:bb:31:40:d3:c3:8a:1d:86
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 6 13:29:10 2023 GMT
Not After : May 24 13:29:10 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

4. Убедиться в том, что был создан именно центр сертификации, выполнив команду:

```
openssl x509 -text -noout -in root.pem | grep CA:

CA:TRUE
```

5. Для использования созданного сертификата в качестве локального центра сертификации необходимо импортировать его на все доступные устройства. Корневой сертификат можно добавить в хранилище ключей/сертификатов ОС либо загрузить напрямую в браузер.

Существуют различные типы сертификатов (OV, EV, Wildcard и т. д.) и иерархии полномочий

(Root, Intermediate, Sub CA и т. д.). В рамках приведенной инструкции будет рассмотрен вариант иерархии **Root Authority** с выпуском сертификата типа **Wildcard**, что позволит иметь один **SSL**-сертификат для всех внутренних доменов **redvirt.home**. Сертификат типа **Wildcard** может быть применен к домену и всем его поддоменам. Для генерации самоподписанного группового сертификата, необходимо создать файл с расширением **csr** и закрытый ключ.

Для создания закрытого ключа необходимо выполнить:

```
openssl genrsa -out wildcard.redvirt.home.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
.....................+++++
e is 65537 (0x010001)
```

6. Для создания запроса самоподписанного сертификата следует использовать файл конфигурации, содержимое которого приведено ниже.

В разделе **[alt_names]** необходимо определить расширение **Subject Alternative Name** (**SAN**).

```
nano opensslsan.cnf
```

```
[req]
distinguished_name=req_distinguished_name
req_extensions=v3_req
prompt=no

[req_distinguished_name]
C=ru
ST=moscow
L=moscow
O=redsoft
OU=drsp
CN=*.redvirt.home

[v3_req]
keyUsage=keyEncipherment, dataEncipherment, digitalSignature
extendedKeyUsage=serverAuth
subjectAltName=@alt_names

[alt_names]
DNS.1 = *.redvirt.home
```

7. Сгенерировать корневой сертификат **wildcard.redvirt.home.csr** с помощью созданного файла конфигурации:

```
openssl req -new -out wildcard.redvirt.home.csr -key wildcard.redvirt.home.key -config opensslsan.cnf
```

8. Далее необходимо подписать файл с расширением csr собственным закрытым ключом.

```
openssl x509 -req -in wildcard.redvirt.home.csr -CA root.pem -CAkey root.key -CAcreateserial -out wildcard.redvirt.home.crt -days 7200 -sha256 -extensions v3_req -extfile opensslsan.cnf

Signature ok
subject=C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN =*.redvirt.home
Getting CA Private Key
Enter pass phrase for root.key:
```

9. Ввести пароль корневого закрытого ключа.

10. Проверить, что сертификат действителен и цепочка доверена.

```
openssl verify -CAfile root.pem wildcard.redvirt.home.crt

wildcard.redvirt.home.crt: OK
```

11. Проверить содержимое сертификата **Wildcard**, выполнив команду:

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
64:27:99:f3:81:3e:b3:ae:df:4c:35:78:b1:e6:0f:87:6e:01:eb:a6
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 7 08:14:35 2023 GMT
Not After : May 25 08:14:35 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = *.redvirt.home
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | grep DNS
```

```
DNS:*.redvirt.home
```

Сертификат выдан и будет действителен в течение следующих 20 лет. Все файлы, включая **wildcard.redvirt.home.crt** (сертификат), **wildcard.redvirt.home.key** (закрытый ключ) и **root.pem** (сертификат ЦС), будут использоваться для настройки **SSL** на любом из веб-серверов.

```
ll

-rw-r--r--. 1 root root 325 сен 6 16:39 opensslsan.cnf
-rw-------. 1 root root 1743 сен 6 16:27 root.key
-rw-r--r--. 1 root root 1375 сен 6 16:29 root.pem
-rw-r--r--. 1 root root 41 сен 7 11:14 root.srl
-rw-r--r--. 1 root root 1334 сен 7 11:14 wildcard.redvirt.home.crt
-rw-r--r--. 1 root root 1110 сен 7 11:14 wildcard.redvirt.home.csr
-rw-------. 1 root root 1679 сен 6 16:39 wildcard.redvirt.home.key
```

Добавление сертификата

Все последующие действия должны производиться на хосте, где развернута система РЕД Виртуализации, в каталоге **/tmp**.

Для добавления сертификата в систему РЕД Виртуализации необходимо:

1. Скопировать с созданного ранее центра сертификации файлы **wildcard.redvirt.home.crt**, **wildcard.redvirt.home.key**, **root.pem** на хост РЕД Виртуализации в папку **/tmp**.

2. Создать файл с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -export -out apache.p12 -inkey wildcard.redvirt.home.key -in wildcard.redvirt.home.crt
```

Пароль указывать не нужно.

3. Экспортировать ключ из созданного на предыдущем шаге файла с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -in apache.p12 -nocerts -nodes > apache.key
```

Пароль указывать не нужно.

4. Экспортировать файл с расширением cer из файла **apache.p12**:

```
openssl pkcs12 -in apache.p12 -nokeys > apache.cer
```

Теперь с точки зрения самоподписанного SSL-сертификата в системе РЕД Виртуализации существуют все необходимые файлы:

- **/tmp/root.pem;**
- **/tmp/apache.p12;**
- **/tmp/apache.key;**
- **/tmp/apache.cer.**

5. Затем создать резервную копию текущего файла **apache.p12**:

```
cp -p /etc/pki/ovirt-engine/keys/apache.p12 /tmp/apache.p12.bck
```

6. Заменить текущий файл **apache.p12** на созданный в п. 2 файл:

```
cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

7. Заменить имеющийся ЦС на созданный в п. 2 раздела 1 «Создание центра сертификации» корневой сертификат и обновить хранилище доверенных сертификатов:

```
cp /tmp/root.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

8. Удалить символическую ссылку и сохранить сертификат как apache-ca.pem в соответствующий каталог:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
cp /tmp/root.pem /etc/pki/ovirt-engine/apache-ca.pem
```

9. Создать резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-
engine/keys/apache.key.nopass.bck
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

10. Скопировать выданный закрытый ключ и сертификат в соответствующие каталоги:

```
cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

11. Перезапустить сервер **apache**:

```
systemctl restart httpd.service
```

12. Создать новый файл конфигурации доверенного хранилища со следующим содержимым:

```
nano /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
```

```
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

13. Сохранить файл.

14. Отредактировать файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf**:

```
nano /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf
```

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

15. Перезапустить необходимые службы:

```
systemctl restart ovirt-provider-ovn.service
systemctl restart ovirt-websocket-proxy
systemctl restart ovirt-engine.service
```

Если все настроено верно, подключение к порталу администратора и порталу виртуальных машин будет производиться без вывода предупреждений о подлинности сертификата, используемого для шифрования **HTTPS**-трафика.

Инструкция по созданию и замене внутренних сертификатов РЕД Виртуализации в режиме Hosted Engine с помощью стороннего центра сертификации

Создание центра сертификации

Для создания локального центра сертификации в РЕД ОС 7.3 необходимо выполнить следующие действия:

1. Создать закрытый ключ **Root**:

```
openssl genrsa -des3 -out root.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
..............+++++
e is 65537 (0x010001)
Enter pass phrase for root.key: ********
Verifying - Enter pass phrase for root.key: ********
```

ВАЖНО!

Рекомендуется указать парольную фразу и защитить закрытый ключ.

2. Сгенерировать корневой сертификат. В процессе выполнения команды будет предложено ввести указанную на предыдущем шаге парольную фразу. После этого потребуется ввести некоторые данные для запроса сертификата - страну, область, город или другой населенный пункт, наименование организации, наименование подразделения организации и имя сертификата.

```
openssl req -x509 -new -nodes -key root.key -sha256 -days 7200 -out root.pem
```

где:

- **-x509**– экземпляр сертификата;
- **-new**– новый запрос сертификата;
- **-nodes**– отключить шифрование выходного ключа;
- **-key root.key**– файл ключа;
- **-sha256**– алгоритм подписи;
- **-days 7200**– период действия сертификата (в днях);
- **-out root.pem**– имя сгенерированного сертификата.

```
Enter pass phrase for root.key: ********
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:moscow
Locality Name (eg, city) [Default City]:moscow
Organization Name (eg, company) [Default Company Ltd]:redsoft
Organizational Unit Name (eg, section) []:drsp
Common Name (eg, your name or your server's hostname) []:Private RED Virt Authority
Email Address []:
```

3. Проверить содержание сгенерированного сертификата, выполнив команду:

```
openssl x509 -text -noout -in root.pem | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
60:05:f3:81:4d:b9:33:bd:a6:d7:34:9b:bb:31:40:d3:c3:8a:1d:86
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 6 13:29:10 2023 GMT
Not After : May 24 13:29:10 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

4. Убедиться в том, что был создан именно центр сертификации, выполнив команду:

```
openssl x509 -text -noout -in root.pem | grep CA:

CA:TRUE
```

5. Для использования созданного сертификата в качестве локального центра сертификации необходимо импортировать его на все доступные устройства. Корневой сертификат можно добавить в хранилище ключей/сертификатов ОС либо загрузить напрямую в браузер.

Существуют различные типы сертификатов (OV, EV, Wildcard и т. д.) и иерархии полномочий

(Root, Intermediate, Sub CA и т. д.). В рамках приведенной инструкции будет рассмотрен вариант иерархии **Root Authority** с выпуском сертификата типа **Wildcard**, что позволит иметь один **SSL**-сертификат для всех внутренних доменов **redvirt.home**. Сертификат типа **Wildcard** может быть применен к домену и всем его поддоменам. Для генерации самоподписанного группового сертификата, необходимо создать файл с расширением **csr** и закрытый ключ.

Для создания закрытого ключа необходимо выполнить:

```
openssl genrsa -out wildcard.redvirt.home.key 2048

Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
.....................+++++
e is 65537 (0x010001)
```

6. Для создания запроса самоподписанного сертификата следует использовать файл конфигурации, содержимое которого приведено ниже.

В разделе **[alt_names]** необходимо определить расширение **Subject Alternative Name** (**SAN**).

```
nano opensslsan.cnf
```

```
[req]
distinguished_name=req_distinguished_name
req_extensions=v3_req
prompt=no

[req_distinguished_name]
C=ru
ST=moscow
L=moscow
O=redsoft
OU=drsp
CN=*.redvirt.home

[v3_req]
keyUsage=keyEncipherment, dataEncipherment, digitalSignature
extendedKeyUsage=serverAuth
subjectAltName=@alt_names

[alt_names]
DNS.1 = *.redvirt.home
```

7. Сгенерировать корневой сертификат **wildcard.redvirt.home.csr** с помощью созданного файла конфигурации:

```
openssl req -new -out wildcard.redvirt.home.csr -key wildcard.redvirt.home.key -config opensslsan.cnf
```

8. Далее необходимо подписать файл с расширением csr собственным закрытым ключом.

```
openssl x509 -req -in wildcard.redvirt.home.csr -CA root.pem -CAkey root.key -CAcreateserial -out wildcard.redvirt.home.crt -days 7200 -sha256 -extensions v3_req -extfile opensslsan.cnf

Signature ok
subject=C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN =*.redvirt.home
Getting CA Private Key
Enter pass phrase for root.key:
```

9. Ввести пароль корневого закрытого ключа.

10. Проверить, что сертификат действителен и цепочка доверена.

```
openssl verify -CAfile root.pem wildcard.redvirt.home.crt

wildcard.redvirt.home.crt: OK
```

11. Проверить содержимое сертификата **Wildcard**, выполнив команду:

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | head -15

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
64:27:99:f3:81:3e:b3:ae:df:4c:35:78:b1:e6:0f:87:6e:01:eb:a6
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = Private RED Virt Authority
Validity
Not Before: Sep 7 08:14:35 2023 GMT
Not After : May 25 08:14:35 2043 GMT
Subject: C = ru, ST = moscow, L = moscow, O = redsoft, OU = drsp, CN = *.redvirt.home
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
```

```
openssl x509 -text -noout -in wildcard.redvirt.home.crt | grep DNS
```

```
DNS:*.redvirt.home
```

Сертификат выдан и будет действителен в течение следующих 20 лет. Все файлы, включая **wildcard.redvirt.home.crt** (сертификат), **wildcard.redvirt.home.key** (закрытый ключ) и **root.pem** (сертификат ЦС), будут использоваться для настройки **SSL** на любом из веб-серверов.

```
ll

-rw-r--r--. 1 root root 325 сен 6 16:39 opensslsan.cnf
-rw-------. 1 root root 1743 сен 6 16:27 root.key
-rw-r--r--. 1 root root 1375 сен 6 16:29 root.pem
-rw-r--r--. 1 root root 41 сен 7 11:14 root.srl
-rw-r--r--. 1 root root 1334 сен 7 11:14 wildcard.redvirt.home.crt
-rw-r--r--. 1 root root 1110 сен 7 11:14 wildcard.redvirt.home.csr
-rw-------. 1 root root 1679 сен 6 16:39 wildcard.redvirt.home.key
```

Добавление сертификата

Все последующие действия должны производиться на развернутом Engine РЕД Виртуализации, в каталоге **/tmp**.

Для добавления сертификата в систему РЕД Виртуализации необходимо:

1. Скопировать с созданного ранее центра сертификации файлы **wildcard.redvirt.home.crt**, **wildcard.redvirt.home.key**, **root.pem** на хост РЕД Виртуализации в папку **/tmp**.

2. Создать файл с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -export -out apache.p12 -inkey wildcard.redvirt.home.key -in wildcard.redvirt.home.crt
```

Пароль указывать не нужно.

3. Экспортировать ключ из созданного на предыдущем шаге файла с расширением **.p12** (в примере **apache.p12**):

```
openssl pkcs12 -in apache.p12 -nocerts -nodes > apache.key
```

Пароль указывать не нужно.

4. Экспортировать файл с расширением cer из файла **apache.p12**:

```
openssl pkcs12 -in apache.p12 -nokeys > apache.cer
```

Теперь с точки зрения самоподписанного **SSL**-сертификата в системе РЕД Виртуализации существуют все необходимые файлы:

- **/tmp/root.pem;**
- **/tmp/apache.p12;**
- **/tmp/apache.key;**
- **/tmp/apache.cer.**

5. Затем создать резервную копию текущего файла **apache.p12**:

```
cp -p /etc/pki/ovirt-engine/keys/apache.p12 /tmp/apache.p12.bck
```

6. Заменить текущий файл **apache.p12** на созданный в п. 2 файл:

```
cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

7. Заменить имеющийся ЦС на созданный в п. 2 раздела 1 «Создание центра сертификации» корневой сертификат и обновить хранилище доверенных сертификатов:

```
cp /tmp/root.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

8. Удалить символическую ссылку и сохранить сертификат как apache-ca.pem в соответствующий каталог:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
cp /tmp/root.pem /etc/pki/ovirt-engine/apache-ca.pem
```

9. Создать резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-
engine/keys/apache.key.nopass.bck
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

10. Скопировать выданный закрытый ключ и сертификат в соответствующие каталоги:

```
cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

11. Перезапустить сервер **apache**:

```
systemctl restart httpd.service
```

12. Создать новый файл конфигурации доверенного хранилища со следующим содержимым:

```
nano /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

13. Сохранить файл.

14. Отредактировать файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf**:

```
nano /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf
```

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

15. Переопределить конфигурацию **ovirt-engine /etc/ovirt-imageio/conf.d/50-engine.conf**:

```
cp /etc/ovirt-imageio/conf.d/50-engine.conf /etc/ovirt-imageio/conf.d/99-local.conf
```

16. Перезапустить необходимые службы:

```
systemctl restart ovirt-provider-ovn.service
systemctl restart ovirt-imageio
systemctl restart ovirt-websocket-proxy
systemctl restart ovirt-engine.service
```

17. Скопировать и установить сертификат **root.pem** в качестве корневого на машине, где будет производиться администрирование системы РЕД Виртуализация. Если все настроено верно, подключение к порталу администратора и порталу виртуальных машин будет производиться без вывода предупреждений о подлинности сертификата, используемого для шифрования **HTTPS**-трафика.

Инструмент для смены доменного имени Engine

Когда команда `engine-setup` запускается в чистой среде, она создает ряд сертификатов и ключей, в которых используется полное доменное имя Engine, указанное в процессе установки. Если полное доменное имя Engine позднее необходимо изменить (например, из-за переноса машины, на которой размещен Engine, в другой домен), записи полного доменного имени должны быть обновлены, чтобы отразить новое имя. Команда **`ovirt-engine-rename`** автоматизирует эту задачу.

Команда `ovirt-engine-rename` обновляет записи полного доменного имени Engine в следующих файлах:

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf;
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf;
- /etc/pki/ovirt-engine/cert.conf;
- /etc/pki/ovirt-engine/cert.template;
- /etc/pki/ovirt-engine/certs/apache.cer;
- /etc/pki/ovirt-engine/keys/apache.key.nopass;
- /etc/pki/ovirt-engine/keys/apache.p12.

Примечание.

Хотя команда `ovirt-engine-rename` создает новый сертификат для веб-сервера, на котором работает Engine, она не влияет на сертификат для Engine или центр сертификации. В связи с этим использование команды `ovirt-engine-rename` связано с определенным риском. Поэтому по возможности рекомендуется изменить полное доменное имя Engine, выполнив `engine-cleanup` и `engine-setup`.

Примечание.

В процессе обновления старое имя хоста должно быть разрешено. Если **Engine Rename Tool** выводит сообщение:

```
[ ERROR ] Host name is not valid: <OLD FQDN> did not resolve into an IP address
```

добавьте старое имя хоста в файл **/etc/hosts**, используйте **Engine Rename Tool**, а затем удалите старое имя хоста из файла **/etc/hosts**.

Синтаксис команды

Основной синтаксис команды `ovirt-engine-rename`:

```
/usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

Команда также принимает следующие параметры:

- **--newname=<новое_имя>** - позволяет указать новое полное доменное имя для Engine без взаимодействия с пользователем;
- **--log=<путь_к_файлу>** - позволяет указать путь и имя файла, в который должны быть записаны журналы операции переименования;
- **--config=<путь_к_файлу>** - позволяет указать путь и имя файла конфигурации для загрузки в операцию переименования;
- **--config-append=<путь_к_файлу>** - позволяет указать путь и имя файла конфигурации для добавления к операции переименования. Этот параметр можно использовать для указания пути и имени существующего файла ответов для автоматизации операции переименования.
- **--generate-answer=<путь_к_файлу>** - позволяет указать путь и имя файла, в который `ovirt-engine-rename` записываются ваши ответы и значения, измененные командой.

Процедура смены доменного имени Engine

Вы можете использовать команду `ovirt-engine-rename` для обновления записей полного доменного имени (**FQDN**) Engine.

Инструмент проверяет, предоставляет ли Engine локальный домен ISO или хранилище данных. Если предоставляет, инструмент предлагает пользователю извлечь, завершить работу или перевести в режим обслуживания любую виртуальную машину или домен хранения, подключенный к хранилищу, прежде чем продолжить операцию. Это гарантирует, что виртуальные машины не потеряют связь со своими виртуальными дисками, а домены хранения ISO не потеряют связь во время процесса переименования.

Для смены доменного имени Engine необходимо выполнить следующие действия:

1. Переведите всю систему РЕД Виртуализации в режим глобального обслуживания. Для этого на одном из хостов выполните команду:

```
hosted-engine --set-maintenance --mode=global
```

2. Подготовьте все DNS и другие соответствующие записи для создания нового полного доменного имени.

Если DNS не используется, внесите изменения в файлы с именем /etc/hosts как на хостах, так и на Engine.

3. Обновите конфигурацию DHCP-сервера, если используется DHCP.

4. Обновите имя в Engine:

```
hostnamectl set-hostname <новое_доменное_имя>
```

5. Запустите утилиту следующей командой:

```
/usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

6. При появлении запроса введите новое полное доменное имя для Engine:

```
New fully qualified server name:<новое_доменное_имя>
```

7. При появлении запроса нажмите «**Enter**», чтобы остановить обслуживание Engine:

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

После этого команда `ovirt-engine-rename` обновит записи полного доменного имени Engine.

8. Перезапустите службу загрузки образов, чтобы она обновила свои данные по сертификатам:

```
systemctl restart ovirt-imageio
```

9. Для **self-hosted Engine** выполните следующие дополнительные действия:

9.1. Выполните нижеприведенную команду на каждом существующем хосте **self-hosted Engine**:

```
hosted-engine --set-shared-config fqdn <новое_доменное_имя> --type=he_local
```

Данная команда изменяет полное доменное имя в локальной копии **/etc/ovirt-hosted-engine/hosted-engine.conf** каждого узла **self-hosted Engine**.

9.2. Выполните следующую команду на одном из хостов **self-hosted Engine**:

```
hosted-engine --set-shared-config fqdn <новое_доменное_имя> --type=he_shared
```

Данная команда изменяет полное доменное имя в основной копии **/etc/ovirt-hosted-engine/hosted-engine.conf** в общем домене хранения.

Теперь все новые и существующие узлы **self-hosted engine** будут использовать новое полное доменное имя.

10. Отключите режим глобального обслуживания. Для этого выполните на одном из улов команду:

```
hosted-engine --set-maintenance --mode=none
```

Хосты со статусом «Non Responsive»

Статус «**Non Responsive**» означает, что *HostedEngine* не получил своевременного ответа от службы **vdsmd**, запущенной на хосте.

> **ВАЖНО!**
>
> ВМ *HostedEngine* **запрещено** выключать и перезагружать!

1. Сначала необходимо убедиться, что все остальные ВМ работают. Например, проверить доступность через **ping**, подключение по **ssh** и т. д.

2. Выяснить причину, по которой *HostedEngine* не получил своевременного ответа (неполадки сети, блокировка или аварийное завершение службы **vdsmd**).

Для этого на хосте необходимо выполнить:

```
grep "Worker blocked" /var/log/vdsm/vdsm.log
grep -A20 "Traceback" /var/log/vdsm/vdsm.log
```

3. Журналы на момент инцидента передать в **Техническую поддержку РЕД Виртуализации**.

Файлы журналов находятся в папке **/var/log**.

4. Проверить доступность хоста и работоспособность его служб следующими командами:

- проверка работоспособности путей до СХД:

```
multipath -ll
```

- проверка доступных ресурсов:

```
top
```

- проверка блокировки областей памяти на хранилищах:

```
sanlock status
```

5. Проверить лог-файл **/var/log/messages** на наличие критических ошибок системы.

Для этого можно воспользоваться командой:

```
journalctl -b -p err
```

6. Выполнить проверку и перезапуск службы **vdsm**:

```
systemctl status vdsmd
systemctl restart vdsmd
```

Настройка параметров расширения "тонких" дисков ВМ

Для настройки параметров расширения "тонких" дисков необходимо выполнить следующий алгоритм действий:

1. Переведите хост в режим обслуживания, выбрав в веб-интерфейсе «**Управление** — **Обслуживание**».

2. Перейдите в терминал хоста.

3. Откройте файл:

```
nano /etc/vdsm/vdsm.conf.d/99-local.conf
```

4. Измените следующие параметры:

```
volume_utilization_percent=25
volume_utilization_chunk_mb=2048
```

здесь:

- `volume_utilization_percent=25` — процент заполнения блока, при достижении которого начнётся расширение виртуального диска;
- `volume_utilization_chunk_mb=2048` — размер блока, на который производится увеличение объема виртуального диска при достижении процента заполнения.

Т.е. при заполнении блока на 25% от его размера (2048 МБ) будет произведено увеличение виртуального диска на 2048 МБ.

5. Выполните команду применения настроек:

```
vdsm-tool configure --force
```

6. Выполните перезапуск сервиса **vdsm**:

```
systemctl restart vdsm
```

7. Выведите хост из режима обслуживания, выбрав в веб-интерфейсе «**Управление** — **Включить**».

Часто задаваемые вопросы (FAQ)

Как пользоваться РЕД Виртуализацией?

Через веб-интерфейс необходимо подключиться к «**Порталу виртуальных машин**» или «**Порталу администрирования**». При выборе нужной ВМ следует нажать кнопку «**Консоль**», работа с гостевой ОС будет осуществляться через программу **virt-viewer** (существует для Linux и Windows).

Какие гостевые системы поддерживает «РЕД Виртуализация»?

РЕД Виртуализация поддерживает гостевые операционные системы *GNU / Linux*, *Microsoft Windows* и *FreeBSD*.

Какими протоколами обеспечивается доступ к виртуальным машинам?

Доступ к ВМ обеспечивается протоколами **SPICE**, **VNC** или **RDP** (только для Windows). Рекомендуется использовать протокол **SPICE**, т.к. он поддерживает максимальное разрешение 2560x1600 пикселей, а также проброс USB с рабочего ПК пользователя в гостевую ОС.

Каким браузером пользоваться для доступа к веб-интерфейсу РЕД Виртуализации?

Мы рекомендуем использовать последние версии браузеров **Mozilla Firefox** или **Chromium**.

Как проверить, поддерживает ли процессор виртуализацию?

Необходимо включить виртуализацию в BIOS и перезагрузить хост. После этого:

- Загрузить ОС и зарегистрироваться под пользователем, имеющим права администратора;
- В командной строке выполнить следующую команду:

```
grep -E 'svm|vmx' /proc/cpuinfo
```

Если в ответе команды отображается какой-либо вывод, значит процессор поддерживает аппаратную виртуализацию.

Какие хранилища могут использоваться РЕД Виртуализацией?

Хранение данных может быть реализовано с использованием:

- сетевой файловой системы *NFS*;
- *GlusterFS*;
- других *POSIX*-совместимые файловые системы;
- *iSCSI*;
- *локального* хранилища, подключенного непосредственно к хостам виртуализации;
- протокола *Fibre Channel* (FCP);
- параллельной *NFS* (pNFS).

Настройка хранилища является **обязательным** условием для нового центра обработки данных, поскольку центр обработки данных не может быть инициализирован, если домены хранения не подключены и не активированы.

+ Чем подключиться к консоли ВМ?

На компьютере, с которого планируется подключение, должен быть установлен клиент удаленного просмотра «**Virt-viewer**». В операционной системе РЕД ОС его можно установить командой:

```
dnf install virt-viewer
```

Для Windows также существует версия данного приложения.

+ Какие типы процессоров поддерживаются системой РЕД Виртуализации?

Поддерживаются следующие модели процессоров **AMD**:

- Opteron G1-G5 (при развёртывании РЕД Виртуализации 7.3 по умолчанию поддерживаются только G4-G5);
- EPYC.

Поддерживаются следующие модели процессоров **Intel**:

- Nehalem;
- Westmere;
- SandyBridge;
- IvyBridge;
- Haswell;
- Broadwell;
- Cascadelake (поддерживается, но будет определяться как Skylake);
- Skylake.

Поддерживаются следующие модели процессоров **AArch64**:

- Huawei Kunpeng 920.

Как определить, может ли на хост мигрировать ВМ управления?

В списке хостов на панели администрирования РЕД Виртуализации рядом с именами тех хостов, которые могут принять на себя *Engine*, отображается значок короны. *Серебряный* означает, что хост может принять на себя ВМ управления, *золотой* — на хосте уже находится ВМ управления. Если значка *короны нет,* значит хост не может принимать ВМ *Engine*.

Что нужно для успешной миграции виртуальных машин в реальном времени?

Для успешной миграции виртуальных машин в реальном времени должны быть выполнены следующие условия:

- исходный и целевой хосты должны находиться в пределах одного кластера;

Примечание.

Живая миграция виртуальных машин между разными кластерами обычно не рекомендуется.

- хосты источника и назначения имеют статус **Up**;
- хосты источника и назначения имеют доступ к одним и тем же виртуальным сетям и VLAN;
- хосты источника и назначения имеют доступ к домену хранения данных, в котором находится виртуальная машина;
- у хоста назначения достаточно ЦП для поддержки требований виртуальной машины;
- у хоста назначения достаточно неиспользуемой ОЗУ для поддержки требований виртуальной машины;
- у переносимой виртуальной машины нет **cache!=none** настраиваемых свойств.

Что нужно для миграции высокодоступных виртуальных машин?

Для миграции высокодоступных виртуальных машин должны быть соблюдены следующие условия:

- для хостов, на которых запущены высокодоступные виртуальные машины, необходимо настроить управление питанием;
- хост, на котором запущена виртуальная машина с высокой доступностью, должен быть частью кластера, в котором есть другие доступные хосты;
- хост назначения должен быть запущен;
- хосты источника и назначения должны иметь доступ к домену данных, в

котором находится виртуальная машина;
- хосты источника и назначения должны иметь доступ к одним и тем же виртуальным сетям и VLAN;
- на хосте назначения должно быть достаточно ЦП, которые не используются для поддержки требований виртуальной машины;
- на целевом хосте должно быть достаточно оперативной памяти, которая не используется для поддержки требований виртуальной машины.

+ Не получается загрузить ISO-образ в РЕД Виртуализации. После начала загрузки выводится сообщение вида «Приостановлено системой». Почему?

Для загрузки образов и дисков в систему необходимо загрузить в используемый браузер **сертификат** установленной РЕД Виртуализации. Загрузка сертификата доступна на приветственной странице РЕД Виртуализации в поле «**Загрузки**» - «**Корневой сертификат**».

+ После скачивания сертификата РЕД Виртуализации и попытке его установить браузер не видит сертификат. Как исправить?

При загрузке сертификата через **Mozilla Firefox** сертификат сохраняется как файл без расширения. Чтобы браузер увидел сертификат в папке, достаточно выбрать отображение «**Все файлы**».

+ Как добавить пользователя в систему РЕД Виртуализации?

Пользователи в системе РЕД Виртуализация могут быть подключены извне, например, из домена, или созданы локально на виртуальной машине *HostedEngine*.

Для создания локального пользователя можно зайти в консоль *Engine* через веб-интерфейс «**Портал администратора**» или подключиться по *ssh*, после этого выполнить команду:

```
ovirt-aaa-jdbc-tool user add <username> --attribute=firstName=<First-Name> \ --attribute=lastName=<Last-Name>
```

Задать пароль новому пользователю можно командой:

```
ovirt-aaa-jdbc-tool user password-reset <username>
```

+ Почему после перезапуска системы РЕД Виртуализации не получается зайти под доменной учётной записью в веб-портал?

Такое случается, если отсутствует A-запись о домене на сервере *DNS*. Если нет возможности сделать такую запись, нужно прописать *IP* домена в **/etc/resolv.conf** на ВМ *Engine* первой записью.

+ В чём различие между предварительно распределённым виртуальным диском и тонким предоставлением виртуального диска?

Виртуальный диск с предварительно выделенным форматом (*RAW*) имеет значительно более высокую скорость записи, чем виртуальный диск с форматом тонкой подготовки (*QCOW2*).

Тонкая подготовка занимает значительно меньше времени для создания виртуального диска. Формат *thin provision* подходит для виртуальных машин, не требующих интенсивного ввода-вывода.

Предварительно выделенный формат рекомендуется для виртуальных машин с высокой скоростью записи ввода-вывода. Если виртуальная машина способна записывать более 1 ГБ каждые четыре секунды, по возможности используйте предварительно выделенные диски.

+ Как отключить и обратно подключить домен хранения к системе РЕД Виртуализации?

Для отсоединения домена хранения от центра обработки данных выполните следующий алгоритм действий:

1. Перейдите в **Storage** — **Domains**.
2. Нажмите на имя домена, будут открыты подробные сведения.
3. Выберите вкладку **Data Center**.
4. Нажмите «**Maintenance**».
5. Щелкните **OK**, чтобы перейти в режим обслуживания.
6. Выберите «**Detach**».
7. Нажмите **OK**, чтобы отсоединить домен.

Домен хранения будет отключен от дата-центра.

Для присоединения домена хранения к центру обработки данных выполните следующий алгоритм действий:

1. Перейдите в **Storage** — **Domains**.
2. Нажмите на имя домена, будут открыты подробные сведения.
3. Выберите вкладку **Data Center**.
4. Щелкните «**Attach**».
5. Выберите нужный дата-центр.
6. Щелкните **OK**.

Домен хранения присоединяется к центру обработки данных и активируется

автоматически.

+ Образ РЕД Виртуализации 7.2 записан на флешку, но установить не получается. Почему?

ISO-образ РЕД Виртуализации 7.2 необходимо разместить на жёстком диске установленной системы РЕД ОС 7.2 конфигурации Сервер минимальный (без графики) и смонтировать в заранее подготовленную папку. После этого запустить установку можно файлом **install.run**.

+ Как увеличить время тикета для загрузки виртуальных дисков? По умолчанию он составляет 10 часов.

На ВМ HostedEngine необходимо выполнить команду с установкой жизни тикета в секундах:

```
engine-config -s ImageTransferClientTicketValidityInSeconds=180000
```

После этого следует перезапустить сервис командой:

```
systemctl restart ovirt-engine
```

+ Как настроить автоматический запуск виртуальных машин в случае перезапуска системы РЕД Виртуализации?

Необходимо сделать эти машины «высокодоступными» (*HA — high available*).

Высокая доступность должна быть настроена индивидуально для каждой виртуальной машины.

Для настройки высокодоступной виртуальной машины выполните следующие действия:

1. Нажмите **Виртуализация** — **Виртуальные машины** и выберите виртуальную машину.
2. Нажмите **Изменить**.
3. Перейдите на вкладку **Высокая доступность**.
4. Установите флажок **Высокая доступность**, чтобы включить высокую доступность виртуальной машины.
5. В раскрывающемся списке **No VM Lease** виртуальной машины выберите домен хранения, в котором будет храниться аренда виртуальной машины, или выберите **No VM Lease**, чтобы отключить эту функцию.
6. Выберите **AUTO_RESUME**, **LEAVE_PAUSED** или **KILL** из раскрывающегося списка **Resume Behavior**. Если вы определили аренду виртуальной машины,

Уничтожить - единственный доступный вариант.

7. В раскрывающемся списке **Приоритет** выберите **Низкий**, **Средний** или **Высокий**. Когда запускается миграция, создается очередь, в которой сначала переносятся виртуальные машины с высоким приоритетом. Если в кластере не хватает ресурсов, переносятся только виртуальные машины с высоким приоритетом.
8. Нажмите **OK**.

+ Заканчивается место на виртуальной машине управления Hosted Engine. Что делать?

При активной работе с системой и виртуальными машинами в ней место могут занимать логи. Проверьте размер папки **/var/log**. При необходимости настройте ротацию логов в файле **/etc/logrotate.conf**.

+ Не пробрасывается USB с пользовательского ПК в гостевую ОС. Почему?

Необходимо проверить, по какому протоколу реализовано подключение к ВМ. **VNC** не пробрасывает USB, для этого нужно использовать протокол **SPICE**.

+ Есть ли встроенное решение по созданию бекапов ВМ в РЕД Виртуализации?

Нет, в данный момент такое решение от нашей компании разрабатывается для РЕД Виртуализации 7.3. Для резервного копирования можно воспользоваться сторонними решениями.

+ Как перенести виртуальный диск машины управления Engine в другое сетевое хранилище?

Через веб-интерфейс перенос диска ВМ управления невозможен.

Для переноса диска используется следующий алгоритм действий:

1. На *ВМ Engine* запускается резервное копирование «движка».
2. Резервная копия переносится на один из хостов и запускается развёртывание *Engine* из файла.
3. В процессе развёртывания указывается новый домен хранения.
4. После развёртывания запускается восстановленная система управления с диском в новом домене хранения.

+ Мне необходимо привязать к ВМ диск объёмом более 8 ТБ, но система не

позволяет. Как можно увеличить размер диска?

На ВМ *HostedEngine* выполните команду:

```
engine-config -s MaxBlockDiskSizeInGibiBytes=16384
```

Примечание.

Стабильная работа виртуального диска размером более 8 ТБ не гарантируется.

На вычислительных нодах есть много свободного места на жёстких дисках. Как их подключить в качестве хранилища к системе РЕД Виртуализации?

Не рекомендуется использовать диски на вычислительных хостах РЕД Виртуализации для хранения данных.

Если вы принимаете риски, есть возможность настроить на ОС хоста *NFS* или *ISCSI*-сервисы. Следует учитывать, что после настройки необходимо внести эти сервисы в **firewall**. Пример команд *для nfs*:

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

Какие логи смотреть, когда что-то не работает в системе РЕД Виртуализации?

Основные данные по работе системы находятся на *ВМ Engine* по пути **/var/log/ovirt-engine**.

Данные по работе конкретного хоста РЕД Виртуализации находятся в папке **/var/log/vdsm/** на этом хосте.

Для полноценного анализа ошибки необходимы все логи из папки **/var/log** из *ВМ Engine* и хоста.

Хост подключен к системе РЕД Виртуализации, но после установки он переходит в состояние «Non Operational» и не запускается. Почему?

Возможно тип процессора нового хоста не соответствует типу ЦП, заданному в кластере. То есть ЦП кластера новее, чем тип ЦП нового узла. Для работы нового узла нужно указать тип ЦП в кластере такой же, как на новом хосте. Следует учитывать, что после этого все хосты кластера будут работать «на уровне» самого медленного узла.

Есть ли возможность установить РЕД Виртуализацию 7.3 не через веб-интерфейс, а через терминал?

Да, такая возможность есть. После установки образа системы РЕД Виртуализации 7.3 запустите установку командой:

```
ovirt-hosted-engine-setup
```

Что делать, если после установки меню Cockpit отличается от того, что указано в инструкции (нет пунктов виртуализации, оформлено не в цветах РЕД Виртуализации)?

Для решения данной проблемы установите дополнительный модуль:

```
dnf install cockpit-ovirt-dashboard
```

При развёртывании Engine разрывается соединение с хостом. Почему?

В момент развертывания на сервере происходит создание виртуального сетевого интерфейса и переключение его «мостом» на физический интерфейс. Поскольку у нового интерфейса другой mac-адрес, он может получить другой IP, из-за этого возможна потеря связи с хостом.

Где я могу найти драйвера и гостевые агенты для гостевых ОС Windows?

Пакет драйверов можно найти в сети интернет.

Например: https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/.

Можно ли на серверах РЕД Виртуализации использовать программный продукт Secret Net?

SecretNet накладывает ограничения на использование конкретной версии ядра. С

другой версией ядра **SecretNet** работать не будет (ОС, соответственно, тоже).

Поэтому использование **SecretNet** — это отключение обновлений ядра и связанных пакетов (то есть будет невозможно устранять уязвимости ИБ).

Работа с **SecretNet** обычно ведется на рабочих станциях. Применения **SecretNet** на серверах РЕД Виртуализации не предусмотрено.

+ В чём отличие между установкой РЕД Виртуализации в режиме Standalone и Host?

Установка **Standalone** подразумевает использование только одного вычислительного хоста. Вся структура управления разворачивается на хостовой ОС. ВМ управления РЕД Виртуализацией не создаётся. В качестве базового СХД может быть использовано локальное хранилище сервера. Дальнейшее расширение вычислительных мощностей до кластера невозможно. Только добавление дополнительных СХД.

Установка типа **Host** подразумевает развёртывание ВМ управления *HostedEngine*. Так же установка должна проходить на заранее подготовленное СХД. Локальные хранилища напрямую использовать не получится. Возможно дальнейшее расширение до кластера.

+ Что делать, когда при попытке доступа к своей ВМ пользователь получает всплывающее сообщение вида «Консоль используется другим пользователем, продолжить?».

При этом ни принятие положительного решения, ни перезагрузка ВМ не даёт результата.

Такое бывает, когда администратор РЕД Виртуализации подключается через консоль к рабочей ВМ пользователя для настройки гостевой ОС.

Чтобы после этого права на доступ к консоли вернулись к пользователю, необходимо в настройках ВМ установить флажок «**Выключить строгую проверку пользователей**». Для этого на вкладке «**Консоль**» разверните область «**Дополнительные параметры**».

+ Как переименовать существующий хост в системе РЕД Виртуализация?

Для смены имени существующего хоста в системе РЕД Виртуализация необходимо:

1. Удалить хост из системы РЕД Виртуализация:

- перейдите во вкладку «Виртуализация - Узлы»;
- переведите хост в режим обслуживания, выбрав пункт меню «Управление - Обслуживание»;

- нажмите кнопку «Удалить».

2. Сменить имя в хостовой ОС командой:

```
hostnamectl set-hostname <новое_имя_хоста>
```

3. Внести изменения имени в DNS или, если DNS не используется, во все файлы **/etc/hosts** (на хостах и на ВМ Engine).

4. Подключить хост к системе РЕД Виртуализации, используя новое имя.

+ Как можно мигрировать ВМ из Proxmox в РЕД Виртуализацию?

Прямое подключение Proxmox к РЕД Виртуализации не предусмотрено в силу отсутствия у PVE libvirt. Для переноса ВМ необходимо выгрузить её в формате **.ova** из Proxmox. После чего перенести образ на хост РЕД Виртуализации и произвести импорт из ova-файла.

+ Какой образ необходим, чтобы установить гостевые агенты, инструменты и драйверы на ВМ с операционными системами Windows XP и Windows Server 2003?

Для операционных систем Windows XP и Windows Server 2003 рекомендуем использовать ISO-образ oVirt-toolsSetup: https://share.red-soft.ru/index.php/s/qodTijx5DXtkNYn.

+ Как можно выяснить какая конфигурация гипервизора установлена на сервере?

Конфигурацию гипервизора можно проверить следующими способами:

1. По списку репозиториев.
   - При установке в режиме Standalone в директории /etc/yum.repos.d/ будут находиться следующие файлы репозиториев: **RedVirtualization-7.3-engine-updates.repo** и **RedVirtualization-7.3-host-updates.repo;**
   - При установке в режиме Host по пути /etc/yum.repos.d/ будет доступен только репозиторий **RedVirtualization-7.3-host-updates.repo**.

2. По содержанию логов.
   - По пути /var/log при установке в режиме Standalone будут находится папки vdsm и ovirt-engine, тогда как при установке в режиме Host только vdsm, ovirt-engine отсутствует.

+ Как можно получить список всех ВМ, у которых есть снимки диска?

Чтобы получить список всех ВМ, у которых есть снимки диска, выполните следующие действия:

1. На портале администрирования нажмите **«Хранилище»** – **«Домены»** .
2. Нажмите имя домена. Откроется окно сведений.
3. Выберите вкладку **«Снимки диска»** . Отобразится список всех ВМ, у которых есть снимки диска.

+ Не удалось осуществить подключение к графическому интерфейсу ВМ через SPICE консоль.

Для того, чтобы подключиться к графическому интерфейсу ВМ через SPICE консоль необходимо выполнить следующие условия:

1. В сети должны быть доступны следующие порты:
   - для SSH подключения к хосту 22 порт;
   - к консоли виртуальной машины 2222 порт (hosted-engine), 2223 порт (Standalone);
   - диапазон портов 5900-6923 для SPICE+VNC.
2. Необходимо разрешить все входящие соединения.

+ После успешной миграции ВМ из одного хранилища данных в другое необходимо отключить пустое хранилище данных из домена хранения. Как это корректно сделать?

Можно удалить LUN, переведя область хранения в режим обслуживания. Для этого необходимо выключить все виртуальные машины, работающие в домене хранения.

Для удаления LUN выполните следующие действия:

1. На портале администрирования нажмите **«Хранилище»** – **«Домены»**.
2. Нажмите имя домена. Откроется окно сведений.
3. Выберите вкладку **«Дата-центр»**.
4. Нажмите кнопку **«Обслуживание»**, затем нажмите **«ОК»**.

Примечание.

Флажок **«Игнорировать сбой обновления OVF»** позволяет домену хранения перейти в режим обслуживания даже в случае сбоя обновления OVF.

После выполнения перечисленных выше действий домен хранения будет деактивирован и будет иметь состояние **«Неактивный»**. Теперь можно

редактировать, отсоединять, удалять или повторно активировать неактивные домены хранения из центра обработки данных.

Почему при добавлении в РЕД Виртуализацию доменного пользователя, он не отображается в поиске?

Для того, чтобы пользователь отобразился на портале администрирования, необходимо в подключенном к РЕД Виртуализации Active Directory задать атрибут **«sn»**. В случае, если этого атрибута нет, то необходимо включить атрибут **«sAMAccountName»**.

Как исправить ошибку обновления в терминале хоста через dnf update?

У хоста есть доступ в Интернет. При попытке его обновления через терминальную команду **«dnf update»** выводится ошибка **«Error: Не удалось загрузить метаданные для репозитория 'virtualization-7.3-host-updates': repomd.xml parser error: Parse error at line: 15 (SYSTEM or PUBLIC, the URI is missing)»**. Это означает, что необходимо отключить или корректно настроить межсетевой экран, который блокирует доступ до репозитория РЕД Виртуализации.

Как поменять язык интерфейса?

После осуществления входа в веб-интерфейс открывается главная страница РЕД Виртуализации, где происходит выбор портала. На данной странице в выпадающем меню в левом нижнем углу можно выбрать желаемый язык интерфейса.

Как изменить часовой пояс в гостевой ОС?

Когда часовой пояс в гостевой ОС отличается от настроек конфигурации, напротив ВМ появляется предупреждение: **«Actual timezone in the guest differs from the configuration»**.

Для изменения часового пояса в гостевой ОС выполните следующие действия:

1. На портале администрирования нажмите **«Виртуализация»** – **«Виртуальные машины»**.
2. Выберите виртуальную машину, на которой необходимо изменить часовой пояс и нажмите **«Изменить»**.
3. Выберите вкладку **«Система»**.
4. Измените параметр смещения **«Смещение аппаратных часов»** на значение **«Russian Standart Time»**, затем нажмите **«ОК»**.

Как настроить роли так, чтобы пользователь мог самостоятельно выбирать ISO-образы для своей виртуальной машины на портале виртуальных машин?

Для этого необходимо добавить пользователю роли **DiskProfileUser** и **DiskOperator** в разрешениях для домена хранения, на котором хранятся ISO-образы.

Информация об обновлениях

UPD-20250429

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление для ВМ управления:

- **cross-cluster-migration-ui-extension-1.0.0-3.el7**
  - Расширение для ручной миграции ВМ между кластерами одного датацентра

- **grafana-10.3.5-1.el7**
  - Устранены уязвимости (CVE-2024-1313, CVE-2024-1442)

- **ovirt-engine-4.4.10.8-39.el7**
- **ovirt-engine-dwh-4.4.11-11.el7**
- **ovirt-engine-extension-aaa-jdbc-1.2.0-13.el7**
- **ovirt-engine-extension-aaa-ldap-1.4.2-3.el7**
- **ovirt-engine-extensions-api-1.0.1-5.el7**
- **ovirt-engine-ui-extensions-1.2.7-4.el7**
- **ovirt-web-ui-1.7.2-4.el7**
- **redvirt-backend-1.0.0-13.el7**
- **redvirt-backup-broker-0.0.5-17.el7**
- **redvirt-engine-backup-ui-extension-0.1.3-3.el7**
- **redvirt-infrastructure-map-ui-extension-1.0.0-10.el7**
- **redvirt-reports-ui-extension-1.0.0-9.el7**
- **red-virtualization-engine-branding-4.4.9.2-8.el7**
- **red-virtualization-web-ui-branding-4.4.9.2-8.el7**
- **redvirt-ui-extensions-1.0-2.el7**
  - Реализован механизм резервного копирования ВМ на NFS
  - Реализован механизм резервного копирования виртуальной инфраструктуры в интерфейсе администратора (функционал engine-backup),
    с возможностью выгрузки резервной копии на NFS
  - Реализованы возможности использования функционала утилиты ovirt-aaa-jdbc-tool средствами Web-портала администрирования
  - Реализована возможность создания и настройки дополнительных профилей парольных политик для разных групп пользователей
    Реализована возможность проверки паролей по "черным спискам"
  - Реализована возможность объединения ВМ в логические группы
    Реализована возможность назначения прав доступа на логическую группу ВМ
  - Релализована выгрузка журналов и формирование отчетов через Web-портал администрирования
    Добавлена категория "События безопасности" в ленте событий в Web-портале администрирования
  - Реализовано отображения типовых метрик объектов виртуальной инфраструктуры (ВМ, виртуальных дисков, узлов)
    Реализован логический граф состояния инфраструктуры в Web-портале администрирования (карта виртуальной инфраструктуры)

Добавлена возможность включения вывода сообщений о попытках входа в систему для привилегированных учетных записей
- Добавлен переключатель тем в Web-портале администрирования
- Реализовано отображение сроков действия TLS-сертификатов вирт инфраструктуры в Web-портале администрирования
  Добавлена возможность добавления сертификата узла в статусе non responsive,
  что позволяет перевыпускать сертификаты узлов после истечения сроков их действия из Web-портала администрирования
- Реализована возможность выбора типа ввода/вывода и типа кеширования для виртуальных дисков.
  Реализована возможность выбора приоритета master-домена
- Реализована возможность просматривать и разрывать пользовательские сессии к ВМ (SPICE, VNC) из Web-портала администрирования.

Обновление для гипервизора:

- **redvirt-backup-agent-0.0.3-9.el7**
- **ovirt-ansible-collection-1.6.6-14.el7**
  - Исполняющий сервис расширения резервного копирования ВМ

- **vdsm-4.40.100.2-14.el7**
  - Обновлены зависимости пакета

+ UPD-20250418

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление для гипервизора:

- **libvirt-7.6.0-11.el7**
  - Исправлена ошибка импорта ВМ, с интерфейсом без имени сети (например, подключенным к Distributed Switch) из VMWare.

- **nbdkit-1.36.3-3.el7**
- **virt-v2v-1.45.90-6.el7**
  - Добавлена опция игнорирования ошибки server does not support 'range' (byte range) request,
    которая приводит к невозможности импорта ВМ напрямую из ESXi.
    Пример использования:

```
virt-v2v -v -x -ic 'esx://root@esxi01.test/?
no_verify=1&suppress_range_error=1' "TestForExport" -o local -of qcow2 -
os /import -ip /tmp/pass
```

UPD-20250404

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **curl-7.85.0-24.el7.3**
  - Устранены множественные уязвимости (CVE-2023-46219, CVE-2024-2398, CVE-2024-2004, CVE-2024-6197, CVE-2024-7264, CVE-2024-8096, CVE-2024-9681)

Обновление для гипервизора:

- **vdsm-4.40.100.2-13.el7**
  - Исправлено подключение Master-домена, в случаях когда автоматическое исправление файловой системы завершается с ошибкой
  - Исправлена ошибка импорта виртуальных машин из OVA-контейнера
- **curl-7.85.0-24.el7.3**
  - Устранены множественные уязвимости (CVE-2023-46219, CVE-2024-2398, CVE-2024-2004, CVE-2024-6197, CVE-2024-7264, CVE-2024-8096, CVE-2024-9681)

UPD-20250312

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **vdsm-jsonrpc-java-1.6.0-2.el7**
  - Исправлена логика работы обработчика входящих сообщений от службы управления гипервизором

UPD-20241120

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **openssl-1.1.1q-10.el7**
  - Устранены множественные уязвимости (CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466)

Обновление ВМ управления:

- **ansible-2.9.27-5.el7**
  - Устранены множественные уязвимости (CVE-2021-3620, CVE-2023-5115, CVE-2024-0690)
- **gdk-pixbuf2-2.40.0-10.el7**
  - Устранена уязвимость CVE-2022-48622
- **libgsf-1.14.47-4.el7**
  - Устранены множественные уязвимости (CVE-2024-36474, CVE-2024-42415)
- **openssl-1.1.1q-10.el7**
  - Устранены множественные уязвимости (CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466)
- **python-werkzeug-3.0.3-1.el7**
  - Устранены множественные уязвимости (CVE-2023-23934, CVE-2023-25577, CVE-2023-46136, CVE-2024-34069)

+ UPD-20241118

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **openvswitch-2.11.3-91.el7**
  - Устранены множественные уязвимости (CVE-2024-22563, CVE-2023-1668, CVE-2023-5366, CVE-2022-4337, CVE-2022-4338)

Обновление ВМ управления:

- **openvswitch-2.11.3-91.el7**
  - Устранены множественные уязвимости (CVE-2024-22563, CVE-2023-1668, CVE-2023-5366, CVE-2022-4337, CVE-2022-4338)
- **postgresql-jdbc-42.2.8-3.el7**
  - Устранена уязвимость CVE-2022-21724
  - Для установки необходимо внести изменения в файл /etc/dnf/plugins/versionlock.list (заменить postgresql-jdbc-42.2.8-2.el7.noarch на postgresql-jdbc-42.2.8-3.el7.noarch)

+ UPD-20240913

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **vdsm-4.40.100.2-7.el7**
  - Устранена утечка файловых дескрипторов.
- **sudo-1.9.15p5-1.el7**
  - Устранена уязвимость BDU-2023-07551.

Обновление ВМ управления:

- **sudo-1.9.15p5-1.el7**
  - Устранена уязвимость BDU-2023-07551.
- **python-PyMySQL-0.10.1-13.el7**
  - Устранена уязвимость CVE-2024-36039.

UPD-20240715

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **libtiff-4.5.1-8.el7**
  - Устранены уязвимости CVE-2023-6228, CVE-2023-52356.
- **openssh-8.9p1-12.el7**
  - Устранена уязвимость CVE-2024-6387.

Обновление ВМ управления:

- **libtiff-4.5.1-8.el7**
  - Устранены уязвимости CVE-2023-6228, CVE-2023-52356.
- **openssh-8.9p1-12.el7**
  - Устранена уязвимость CVE-2024-6387.

UPD-20240521

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **virt-v2v-1.45.90-5**
  - Исправлена ошибка миграции дисков из ESXi через SSH-соединение.
- **libvirt-7.6.0-10**
  - Устранено дублирование сообщения "Domain id= is tainted: custom-ga-

command".

UPD-20240517

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **grub2-redos-theme-0.1-990.el7**
- **grub2-redvirt-theme-0.1-4.el7**
  - Заменена тема загрузки grub2.

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-27.el7**
  - Исправлены ошибки интерфейса.
  - Исправлена ошибка зависания загрузки диска в фазе "Завершение очистки".
  - Добавлена возможность использовать общие папки SPICE.

UPD-20240425

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-25.el7**
  - Исправлена ошибка с аутентификацией через внешний провайдер.
  - Устранена уязвимость CVE-2024-0822.

UPD-20240416

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-23.el7**
  - Исправлены ошибки работы сторонних продуктов через RESTful API, возникшей после обновления UPD-20240411.

UPD-20240411

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **selinux-policy-3.14.5-62.el7**
  - Исправлен контекст SELinux системных сервисов vdsmd и supervdsmd.
  - Устранена ошибка импорта ВМ из внешних источников.

- **python-aiohttp-3.9.3-1.el7**
  - Устранена уязвимость CVE-2024-23334.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **postgresql-*-12.18-2.el7**
  - Устранены множественные уязвимости CVE-2022-1552, CVE-2022-2625, CVE-2022-41862, CVE-2023-2454, CVE-2023-2455, CVE-2023-39417, CVE-2023-5868, CVE-2023-5869, CVE-2023-5870, CVE-2024-0985.

- **ovirt-engine-ui-extensions-1.2.7-3.el7**
  - Исправлены ошибки перевода.

- **ovirt-engine-4.4.10.8-21.el7**
- **ovirt-engine-extension-aaa-jdbc-tool-1.2.0-8.el7**
  - Исправлены множественные ошибки перевода.
  - Добавлено отключаемое информационное окно о последних входах пользователя в систему.
  - В окне настроек ВМ (а также шаблонов, экземпляров, пулов) добавлен переключатель совместимости с Termidesk.
  - Добавлен запрет на удаление дата-центра, если есть хоть один ассоциированный с ним кластер.

- **ovirt-web-ui-1.7.2-3.el7**
  - Исправлены ошибки перевода.

UPD-20240226

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.131-2.el7virt**
  - Исправлена ошибка при обновлении.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **kernel-lt-5.15.131-2.el7virt**
  - Исправлена ошибка при обновлении.

Обновление включает зависимые пакеты.

UPD-20240206

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **openssh-8.9p1-11.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **openssh-8.9p1-11.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.

Обновление включает зависимые пакеты.

UPD-20240202

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **libssh-0.9.8-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.
- **libssh2-1.11.0-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.
- **traceroute-3:2.1.3-1.el7.x86_64**
  - Устранена уязвимость ROS-20231102-01, CVE-2023-46316.
- **kernel-lt-0:5.15.131-1.el7.3.x86_64**
  - Устранена уязвимость ROS-20231024-01, CVE-2023-4273.
- **glibc-0:2.28-9.el7.x86_64**
  - Устранена уязвимость ROS-20231020-10, CVE-2016-10228.
- **subscription-manager-0:1.29.0-3.el7.x86_64**

- Устранена уязвимость ROS-20231018-03, CVE-2023-3899.

- **procps-ng-0:3.3.17-1.el7.x86_64**
  - Устранена уязвимость ROS-20231020-03, CVE-2023-4016.

- **curl-0:7.85.0-15.el7.3.x86_64**
  - Устранены множественные уязвимости CVE-2023-38546, CVE-2023-38545, ROS-20231016-05.

Обновление ВМ управления:

- **libssh-0.9.8-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.

- **libssh2-1.11.0-1.el7**
  - Устранена уязвимость BDU:2023-08853, CVE-2023-48795.

- **traceroute-3:2.1.3-1.el7.x86_64**
  - Устранена уязвимость ROS-20231102-01, CVE-2023-46316.

- **kernel-lt-0:5.15.131-1.el7.3.x86_64**
  - Устранена уязвимость ROS-20231024-01, CVE-2023-4273.

- **glibc-0:2.28-9.el7.x86_64**
  - Устранена уязвимость ROS-20231020-10, CVE-2016-10228.

- **subscription-manager-0:1.29.0-3.el7.x86_64**
  - Устранена уязвимость ROS-20231018-03, CVE-2023-3899.

- **procps-ng-0:3.3.17-1.el7.x86_64**
  - Устранена уязвимость ROS-20231020-03, CVE-2023-4016.

- **curl-0:7.85.0-15.el7.3.x86_64**
  - Устранены множественные уязвимости CVE-2023-38546, CVE-2023-38545, ROS-20231016-05.

+ UPD-20231208

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-9-el7**
  - Исправлено отображение ассоциированных ВМ с дисками типа iso.
  - Добавлена панель с кнопками для отключения iso от ВМ.

UPD-20231127

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **vdsm-4.40.100.2-3.el7**
  - Исправлены ошибки, возникающие при попытке расширения тонких дисков.
  - Улучшена работа с сетью и подсистемой хранения.

- **ovirt-image-2.5.0-1.el7**
  - Улучшена работа с дисковой подсистемой.
  - Добавлена утилита для загрузки/выгрузки дисков из доменов хранения (ovirt-img).

Обновление включает зависимые пакеты.

UPD-20231009

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.117-4.el7**
- **kexec-tools-2.0.27-1.el7**
- **dracut-056-9.el7**
  - Исправлены ошибки в работе kdump.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **kernel-lt-5.15.117-4.el7**
- **kexec-tools-2.0.27-1.el7**
- **dracut-056-9.el7**
  - Исправлены ошибки в работе kdump.

Обновление включает зависимые пакеты.

UPD-20230925

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **expat-2.5.0-1.el7**

- Устранена уязвимость с идентификаторами BDU:2023-02688 и CVE-2022-43680.

Обновление ВМ управления:

- **expat-2.5.0-1.el7**
  - Устранена уязвимость с идентификаторами BDU:2023-02688 и CVE-2022-43680.

UPD-20230915

В репозитории РЕД Виртуализации 7.3 доступны следующие обновления:

Обновления для гипервизора:

- **kernel-lt-5.15.117-3.el7virt**
  - Решена проблема аварийного завершения виртуальных машин с гостевой ОС Windows. Ранее для решения проблемы предоставлялось ядро kernel-lt-5.4.227-2.el7virt.

- **libguestfs-1.45.5-9.el7**
- **virt-v2v-1.45.90-4.el7**
  - Исправлена проблема импорта виртуальной машины с гостевой ОС Astra Linux.

- **rpm-4.17.0-9.el7.3**
  - Обновлен пакетный менеджер RPM.

Обновление включает зависимые пакеты.

Обновление ВМ управления:

- **ovirt-engine-4.4.10.8-7.el7**
  - Исправлена логика сохранения переменных nvram.

- **rpm-4.17.0-9.el7.3**
  - Обновлен пакетный менеджер RPM.

Обновление включает зависимые пакеты.