



Руководство по установке  
и первичной настройке  
«РЕД Виртуализация 7.3»

# Оглавление

<b>1</b>	<b>Описание дистрибутива .....</b>	<b>4</b>
1.1	Описание программного продукта .....	4
1.2	Компоненты программного продукта .....	4
1.3	Архитектура службы .....	5
<b>2</b>	<b>Системные требования .....</b>	<b>6</b>
2.1	Аппаратная часть .....	6
2.2	Аппаратное и программное оснащение клиентов .....	7
2.3	Гипервизор .....	7
2.3.1	Центральный процессор .....	7
2.3.2	Оперативная память .....	8
2.3.3	Жёсткие диски .....	8
2.3.4	PCI устройства .....	9
2.3.5	Требования к назначению устройств .....	9
2.3.6	Требования к vGPU .....	10
2.3.7	Требования к сети .....	10
2.4	Хранилище .....	15
2.5	Ограничения РЕД Виртуализации .....	15
<b>3</b>	<b>Подготовка сетевого хранилища .....</b>	<b>17</b>
3.1	Подготовка хранилища NFS .....	17
3.2	Подготовка хранилища iSCSI .....	18
3.3	Подготовка хранилища FCP .....	19

---

3.4	Подготовка хранилища Gluster Storage.....	20
<b>4</b>	<b>Установка .....</b>	<b>21</b>
4.1	Установка РЕД Виртуализации.....	21
4.1.1	Подготовка к установке .....	21
4.1.2	Последовательность установки .....	21
4.1.3	Язык системы .....	22
4.1.4	Обзор установки .....	22
4.1.5	Клавиатура .....	23
4.1.6	Расположение установки .....	23
4.1.7	Задание пароля администратора системы .....	25
4.1.8	Дата и время .....	26
4.1.9	Сеть и имя узла .....	26
4.1.10	Установка системы виртуализации .....	27
4.2	Установка в режиме standalone.....	34
4.3	Развертывание Gluster Hyperconverged.....	42
4.3.1	Развертывание на узле РЕД Виртуализации .....	42
4.3.2	Установка и настройка томов Gluster .....	42
<b>5</b>	<b>Веб-интерфейс .....</b>	<b>51</b>

# 1. Описание дистрибутива

## 1.1 Описание программного продукта

«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.

## 1.2 Компоненты программного продукта

РЕД Виртуализация представляет собой программный продукт, основанный на базе системы управления виртуализацией с открытым исходным кодом (oVirt) и состоящий из следующих компонентов:

- программные средства, предназначенные для установки на аппаратный сервер: гипервизор, базовую операционную систему, вспомогательные ком-

- поненты 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.

### 1.3 Архитектура службы

Система управления виртуализацией РЕД Виртуализация разворачивается в варианте Hosted Engine - это виртуализированная среда, в которой Engine работает на виртуальной машине на хостах, управляемых данной службой. Виртуальная машина создается как часть конфигурации хоста, а Engine устанавливается и настраивается параллельно с процессом конфигурации хоста.

Основное преимущество варианта Hosted Engine состоит в том, что ему требуется меньше оборудования для развертывания системы виртуализации, поскольку Engine работает как виртуальная машина, а не на физическом оборудовании. Кроме того, Engine настроен на высокую доступность. Если хост, на котором запущена виртуальная машина Engine, переходит в режим обслуживания или неожиданно выходит из строя, виртуальная машина будет автоматически перенесена на другой хост в среде. Для поддержки функции высокой доступности требуется минимум два хоста.

Минимальная настройка включает в себя:

- Одну виртуальную машину Engine, которая размещается на физических хостах.
- Минимум два хоста для высокой доступности виртуальной машины.
- Одна служба хранения, которая может быть размещена локально или на удаленном сервере, в зависимости от используемого типа хранилища. Служба хранения должна быть доступна всем хостам.

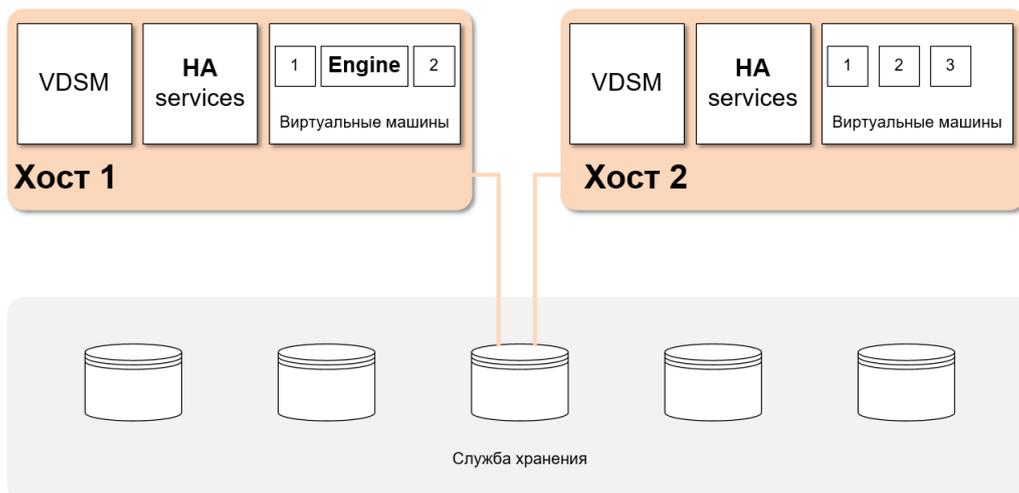


Рисунок 1 – Архитектура системы виртуализации РЕД Виртуализация

## 2. Системные требования

### 2.1 Аппаратная часть

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	Двухъядерный процессор	Четырёхъядерный 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 стабильной работы РЕД Виртуализации требуется:

- физический сервер (установка РЕД Виртуализации в виртуальной машине также возможна, но **не гарантируется** ее корректная работа, поэтому использовать данный способ следует **исключительно** в ознакомительных целях);
- готовое хранилище (программное или аппаратное);
- во время установки должен быть подключен только один сетевой интерфейс, управление которым будет передано гипервизору РЕД Виртуализации.

## 2.2 Аппаратное и программное оснащение клиентов

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.

## 2.3 Гипервизор

### 2.3.1 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.

### 2.3.2 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).

### 2.3.3 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 Вир-

туализация». 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.

### 2.3.4 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.

### 2.3.5 Требования к назначению устройств

Если вы планируете реализовать назначение устройств и передачу данных PCI, чтобы виртуальная машина могла использовать определенное устройство PCIe 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 PCIe и мосты между устройством PCIe 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.

### 2.3.6 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, установлены на каждом узле кластера;
6. vGPU-поддерживается операционной системой виртуальной машины с установленными графическими драйверами.

### 2.3.7 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.

#### Требования к брандмауэру Engine РЕД Виртуализации

Для работы модуля РЕД Виртуализации требуется открыть несколько портов, чтобы разрешить сетевой трафик через системный брандмауэр. Описанная здесь конфигурация брандмауэра предполагает конфигурацию по умолчанию.

Таблица 2. Требования к брандмауэру Engine РЕД Виртуализации

ID	Порт	Протокол	Источник	Назначение	Функциональные возможности	Шифрование
M1	-	ICMP	Хосты виртуализации	Менеджер виртуализации	Помощь в диагностике. Опционально.	Нет
M2	22	TCP	Системы, используемые для обслуживания Менеджера, включая конфигурацию бекэнда и обновления ПО	Менеджер виртуализации	Secure Shell (SSH) - доступ. Опционально.	Да

ID	Порт	Протокол	Источник	Назначение	Функциональные возможности	Шифрование
M3	2222	TCP	Клиенты, получающие доступ к последовательным консолям ВМ	Менеджер виртуализации	Secure Shell (SSH) - доступ активирован к соединению к последовательной консоли ВМ.	Да
M4	80, 443	TCP	Хосты виртуализации, клиенты портала администрирования, клиенты пользовательского портала, клиенты REST API	Менеджер виртуализации	Позволяет HTTP (порт 80, не шифруется) и HTTPS (порт 443, шифруется) доступ к менеджеру виртуализации. HTTP перенаправляет соединения к HTTPS.	Да
M5	6100	TCP	Клиенты портала администрирования, клиенты пользовательского портала	Менеджер виртуализации	Предоставляет доступ к прокси-серверу веб-сокета для клиента веб-консоли noVNC, когда прокси-сервер веб-сокета работает на Менеджере виртуализации. Если прокси-сервер веб-сокета работает на другом хосте, этот порт не используется.	Нет
M7	54323	TCP	Клиенты портала администрирования	Менеджер виртуализации (сервер ImageIO Proxy)	Требуется для соединений с ImageIO Proxy (ovirt-imageio-proxy).	Да

ID	Порт	Протокол	Источник	Назначение	Функциональные возможности	Шифрование
M11	53	TCP, UDP	Менеджер виртуализации	Сервер DNS	DNS-запросы с портов выше 1023 на порт 53 и ответы. Открыт по умолчанию.	Да
M12	123	UDP	Менеджер виртуализации	Сервер NTP	NTP-запросы с портов выше 1023 на порт 123 и ответы. Открыт по умолчанию.	Нет

### Требования к брандмауэру хоста

Для хостов РЕД Виртуализации требуется открыть несколько портов, чтобы разрешить сетевой трафик через системный брандмауэр. Правила брандмауэра автоматически настраиваются по умолчанию при добавлении нового хоста в Engine, перезаписывая любую ранее существующую конфигурацию брандмауэра.

Таблица 3. Требования к брандмауэру хоста виртуализации

ID	Порт	Протокол	Источник	Назначение	Функциональные возможности	Шифрование
H1	22	TCP	Менеджер виртуализации	Хосты виртуализации	Secure Shell (SSH) - доступ. Опционально.	Да
H2	2223	TCP	Менеджер виртуализации	Хосты виртуализации	Secure Shell (SSH) - доступ активирует соединение к последовательным консолям VM.	Да

ID	Порт	Протокол	Источник	Назначение	Функциональные возможности	Шифрование
Н3	161	UDP	Хосты виртуализации	Менеджер виртуализации	Simple network management protocol (SNMP). Необходим только в том случае, если вы хотите, чтобы ловушки Simple Network Management Protocol отправлялись с хоста на один или несколько внешних менеджеров SNMP. Опционально.	Нет
Н4	111	TCP	Сервер хранилища NFS	Хосты виртуализации	NFS соединения. Опционально.	Нет
Н5	5900 – 6923	TCP	Клиенты портала администрирования, клиенты пользовательского портала	Хосты виртуализации	Гостевой доступ к консоли через VNC и SPICE. Эти порты должны быть открыты, чтобы обеспечить клиентский доступ к виртуальным машинам.	Да (опционально)
Н6	5989	TCP, UDP	Common Information Model Object Manager (CIMOM)	Хосты виртуализации	Common Information Model Object Managers (CIMOM) для мониторинга виртуальных машин, работающих на хосте. Требуется только в том случае, если используется CIMOM для мониторинга виртуальных машин в среде виртуализации. Опционально.	Нет

ID	Порт	Протокол	Источник	Назначение	Функциональные возможности	Шифрование
N7	9090	TCP	Менеджер виртуализации, Клиентские машины	Хосты виртуализации	Необходим для доступа к web-интерфейсу сервиса Coscript, если используется.	Да
N8	16514	TCP	Хосты виртуализации	Хосты виртуализации	Миграция виртуальных машин с использованием libvirt.	Да
N9	49152 – 49215	TCP	Хосты виртуализации	Хосты виртуализации	Миграция виртуальных машин и изоляция неисправных хостов с помощью VDSM. Эти порты должны быть открыты, чтобы облегчить как автоматическую, так и ручную миграцию виртуальных машин.	Да. В зависимости от агента для изоляции неисправных хостов миграция выполняется через libvirt
N10	54321	TCP	Менеджер виртуализации, Хосты виртуализации	Хосты виртуализации	Связь VDSM с Менеджером виртуализации и другими Хостами виртуализации.	Да
N11	54322	TCP	Менеджер виртуализации (ImageIO Проху-сервер)	Хосты виртуализации	Требуется для связи с сервисом ImageIO (ovirt-imageio-daemon).	Да
N13	53	TCP, UDP	Хосты виртуализации	Сервер DNS	Запросы поиска DNS с портов выше 1023 на порт 53 и ответы. Этот порт является обязательным и открыт по умолчанию.	Нет

## 2.4 Хранилище

«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.

## 2.5 Ограничения РЕД Виртуализации

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.

## 3. Подготовка сетевого хранилища

Необходимо осуществить подготовку хранилища для использования в новой среде виртуализации. В среде РЕД Виртуализации должен быть хотя бы один домен хранения данных, но рекомендуется добавлять больше.

В области данных хранятся виртуальные жесткие диски и файлы всех виртуальных машин и шаблонов, и они не могут совместно использоваться центрами обработки данных, когда они активны (но могут быть перенесены между центрами обработки данных). Домены данных нескольких типов хранения могут быть добавлены в один и тот же центр обработки данных при условии, что они являются общими, а не локальными доменами.

Дополнительно необходимо настроить домен данных, выделенный для виртуальной машины Engine. Этот домен создается во время развертывания системы и должен быть не менее 74 ГБ. Перед началом развертывания необходимо подготовить хранилище для этого домена.

Вы можете использовать один из следующих типов хранения:

- NFS;
- iSCSI;
- Fibre Channel (FCP);
- Gluster Storage.

Если вы используете хранилище iSCSI, домен хранения Engine должен использовать собственную цель iSCSI. Любые дополнительные домены хранения должны использовать другую цель iSCSI.

### 3.1 Подготовка хранилища NFS

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.

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

1. Создайте группу **kvm**:

```
groupadd kvm -g 36
```

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

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

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

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

4. 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
```

5. В файле настройки сервера, расположенного в **/etc/exports**, изменить следующие параметры:

```
anongid = 36, anonuid = 36
```

## 3.2 Подготовка хранилища iSCSI

РЕД Виртуализация поддерживает хранилище iSCSI, которое представляет собой домен хранилища, созданный из группы томов, состоящей из LUN. Группы томов и LUN нельзя подключать более чем к одному домену хранения одновременно.

Если вы используете блочное хранилище и собираетесь развернуть виртуальные машины на необработанных устройствах или прямых LUN и управлять ими с помощью диспетчера логических томов, вы должны создать фильтр, чтобы скрыть гостевые логические тома. Это предотвратит активацию гостевых логических томов при загрузке хоста, что может привести к устареванию логических томов и повреждению данных.

РЕД Виртуализация в настоящее время не поддерживает хранилище с размером блока 4К. Вы должны настроить блочное хранилище в устаревшем режиме (блок 512 байт). Если ваш хост загружается из хранилища SAN и теряет возможность подключения к хранилищу, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления подключения.

Чтобы предотвратить эту ситуацию, добавьте в корневую файловую систему SAN файл конфигурации с несколькими путями для загрузочного LUN, чтобы гарантировать, что он будет поставлен в очередь при наличии соединения:

```
cat /etc/multipath/conf.d/host.conf
```

```
multipaths {
  multipath {
    wwid boot_LUN_wwid
    no_path_retry queue
  }
}
```

### 3.3 Подготовка хранилища FCP

РЕД Виртуализация поддерживает хранилище SAN, создавая домен хранилища из группы томов, состоящей из уже существующих LUN. Ни группы томов, ни LUN нельзя подключать более чем к одному домену хранения одновременно.

Если вы используете блочное хранилище и собираетесь развернуть виртуальные машины на необработанных устройствах или прямых LUN и управлять ими с помощью диспетчера логических томов, вы должны создать фильтр, чтобы скрыть гостевые логические тома. Это предотвратит активацию гостевых логических томов при загрузке хоста, что может привести к устареванию логических томов и повреждению данных.

РЕД Виртуализация в настоящее время не поддерживает хранилище с размером блока 4К. Вы должны настроить блочное хранилище в устаревшем режиме (блок 512 байт). Если ваш хост загружается из хранилища SAN и теряет возможность подключения к хранилищу, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления подключения.

Чтобы предотвратить эту ситуацию, добавьте в корневую файловую систему SAN файл конфигурации с несколькими путями для загрузочного LUN, чтобы гарантировать, что он будет поставлен в очередь при наличии соединения:

```
cat /etc/multipath/conf.d/host.conf
```

```
multipaths {
  multipath {
    wwid boot_LUN_wwid
    no_path_retry queue
  }
}
```

### 3.4 Подготовка хранилища Gluster Storage

Информацию по настройке Gluster Storage см. в Руководстве по администрированию РЕД Виртуализации.

## 4. Установка

### 4.1 Установка РЕД Виртуализации

#### 4.1.1 Подготовка к установке

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

Оборудование должно соответствовать требованиям, описанным в главе 2 настоящего руководства.

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

#### 4.1.2 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:

1. Установка предпочитаемой раскладки клавиатуры;
2. Выбор типа накопителя хоста и подготовка разделов диска;
3. Задание пароля администратора системы;
4. Выбор часового пояса и установка даты и времени;
5. Присвоение имени компьютера в сети и настройка сетевых интерфейсов;
6. Сохранение настроек;
7. Установка системы;
8. Установка загрузчика;
9. Перезагрузка системы;
10. Завершение установки.

### 4.1.3 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.

### 4.1.4 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.

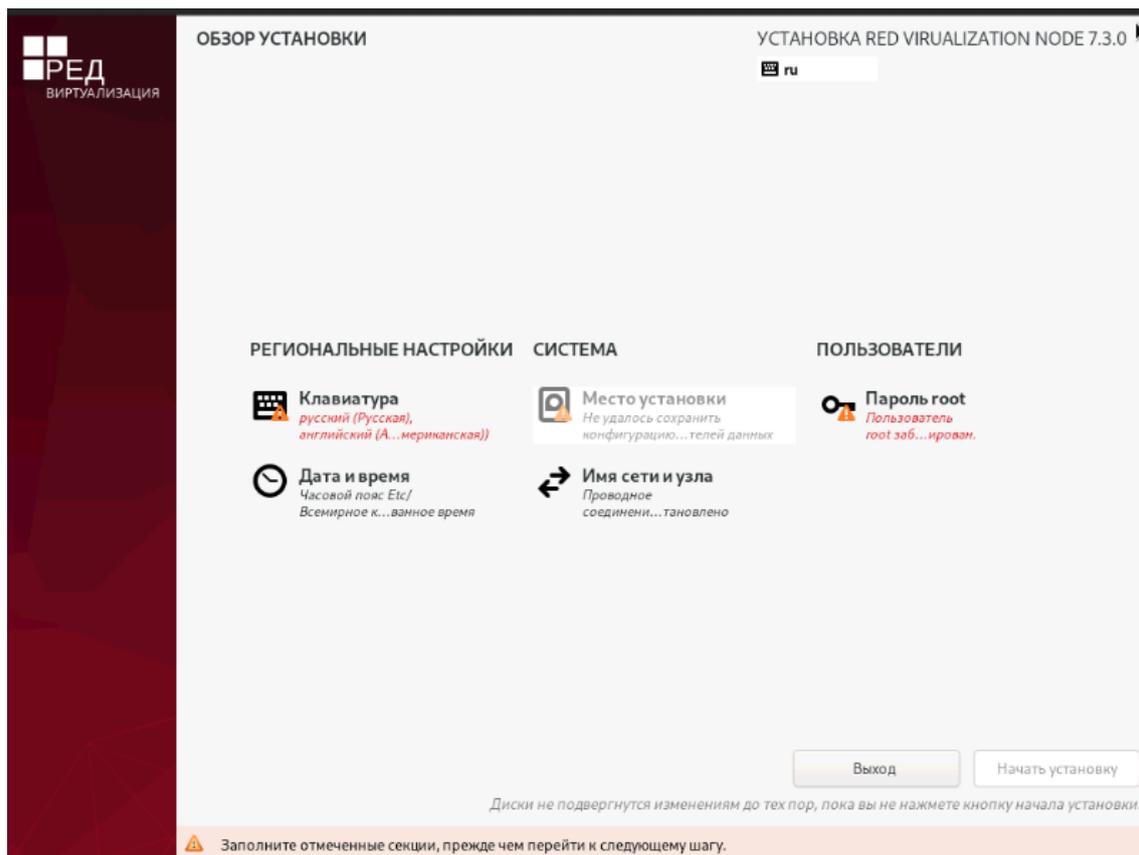


Рисунок 2 – Обзор установки

#### 4.1.5 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».

#### 4.1.6 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;
- настроить 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 формируются 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 зашифрованные 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.

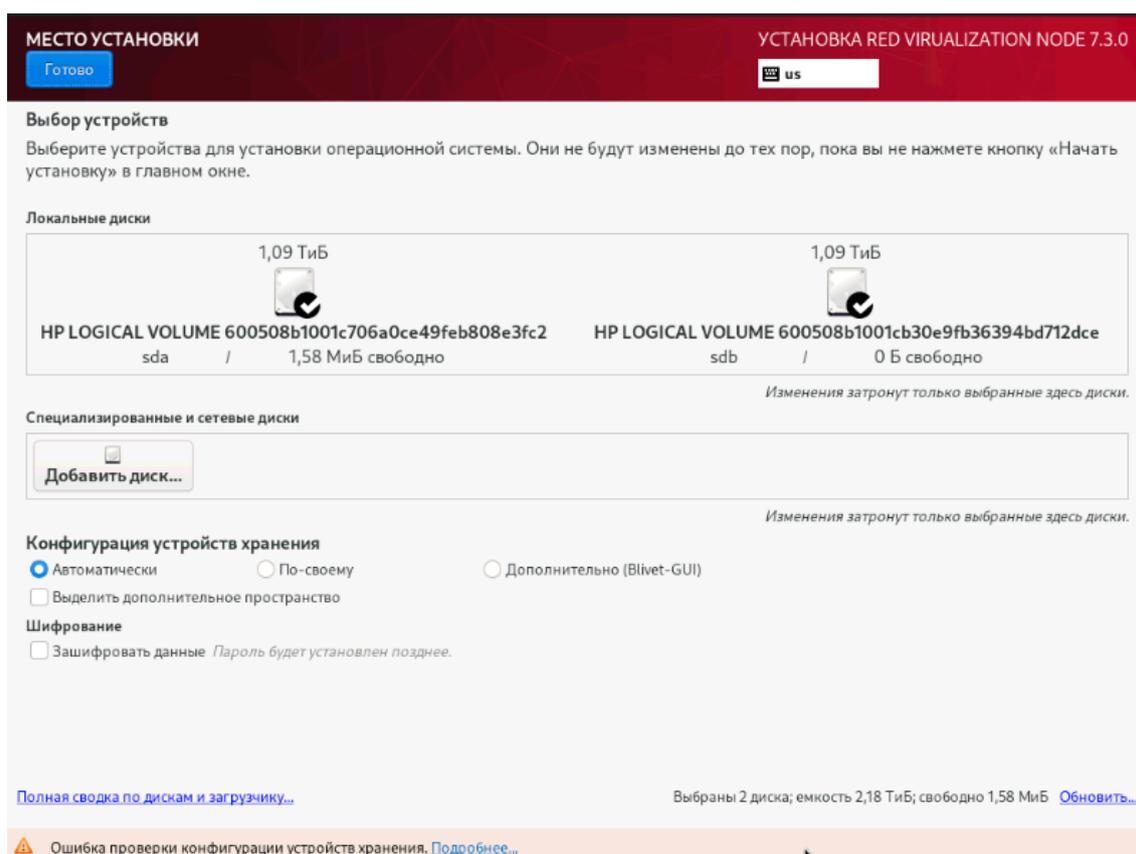


Рисунок 3 – Расположение установки

#### 4.1.7 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.

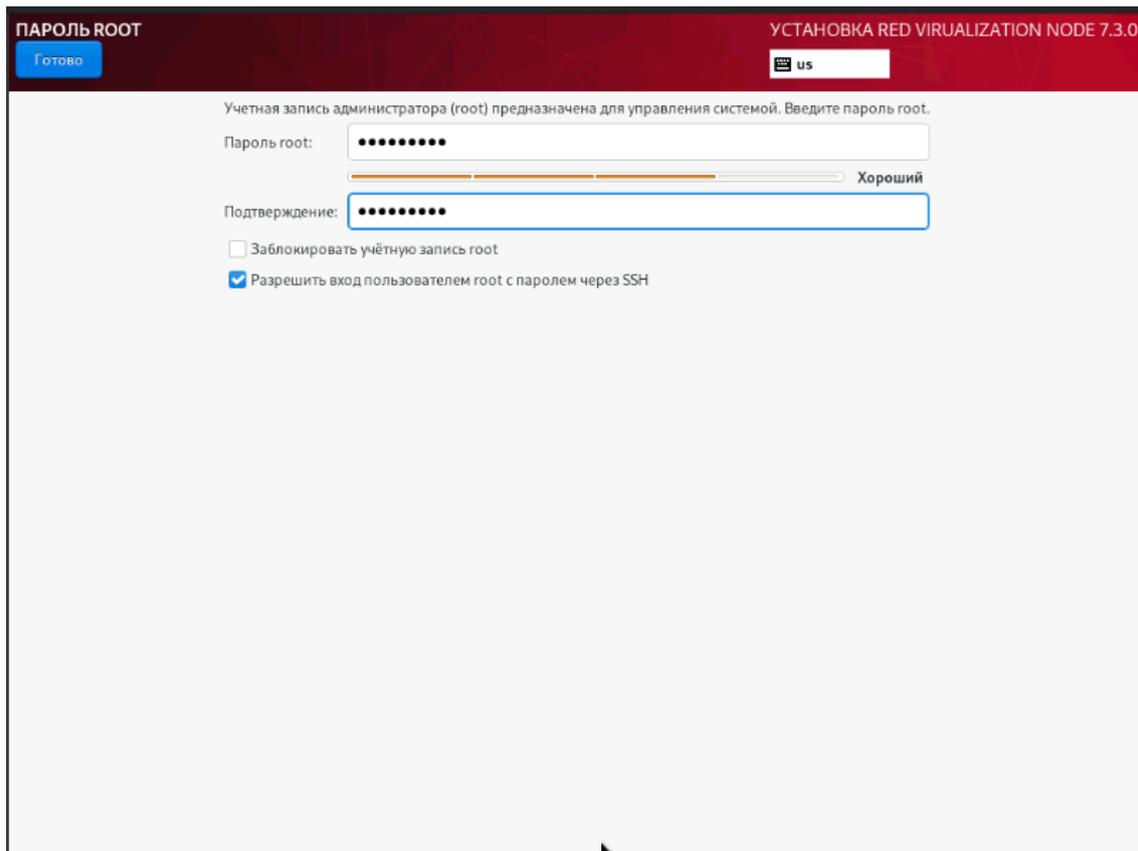


Рисунок 4 – Установка пароля администратора системы

#### 4.1.8 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).

#### 4.1.9 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.

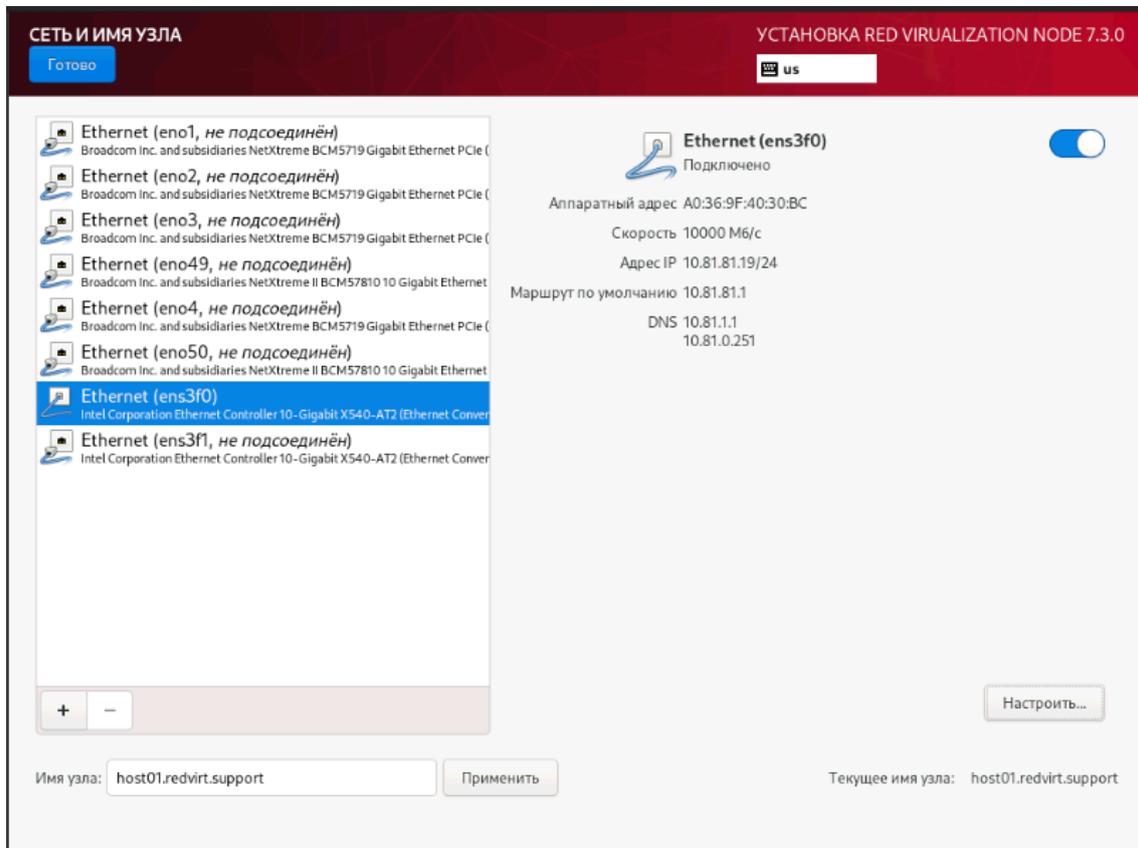


Рисунок 5 – Настройка сети

#### 4.1.10 Установка системы виртуализации

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

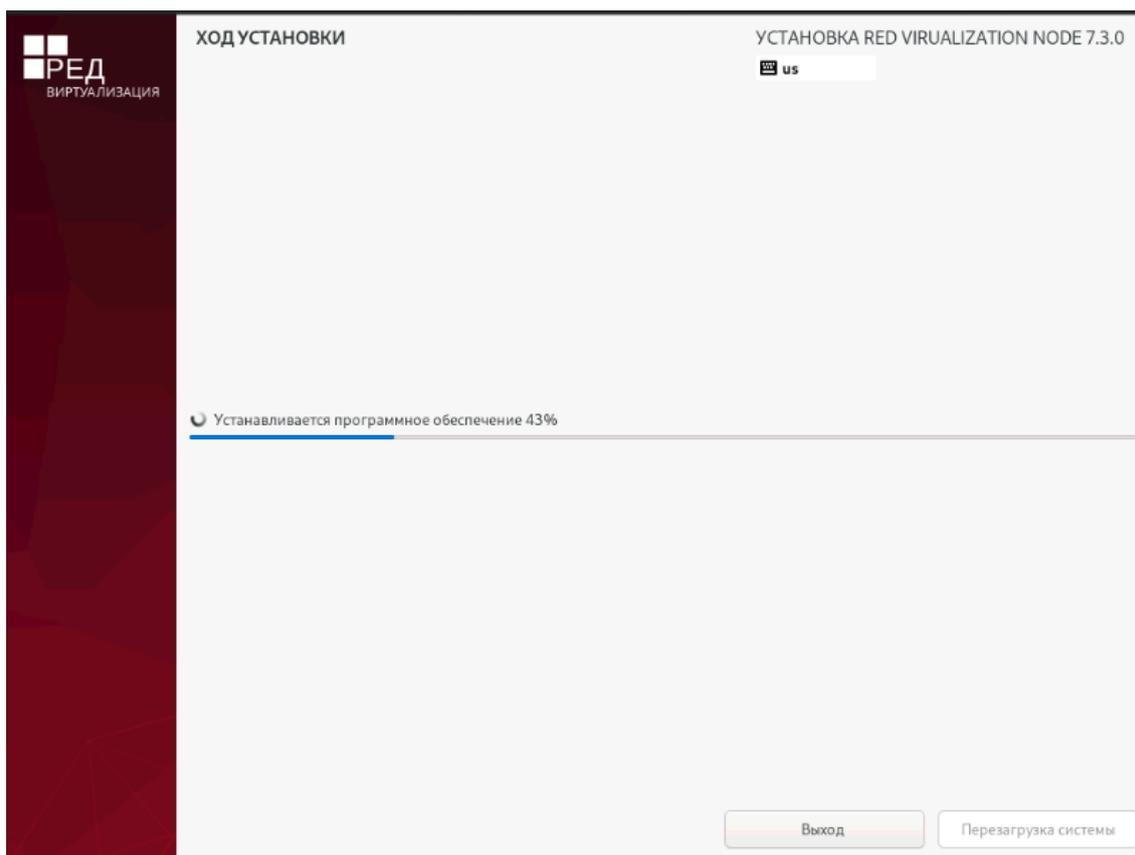


Рисунок 6 – Ход установки

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» (Рисунок 7).

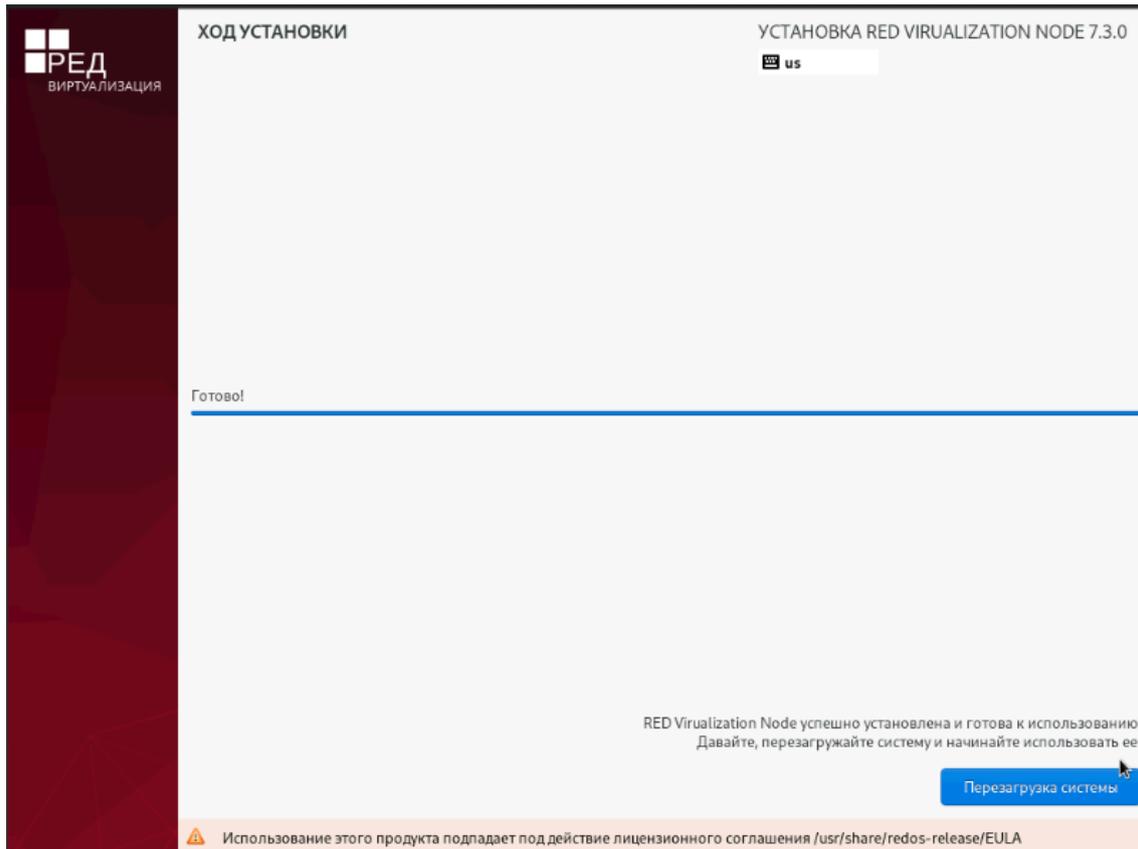


Рисунок 7 – Завершение установки

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

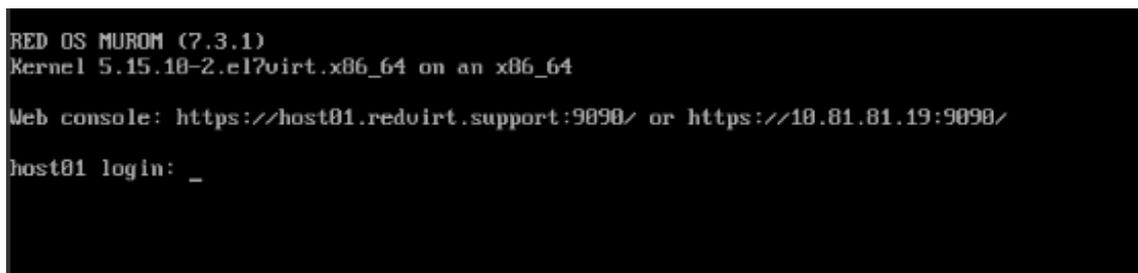


Рисунок 8 – Терминал установленной системы

**Примечание.** В случае, если во время установки системы вы по каким-то причинам не указали или указали неверно имя 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-гипервизор*
192.168.0.44 nfs.redvirt.test *NFS-хранилище*
192.168.0.221 redvirt-engine1.test *Менеджер 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.



### Подключение не защищено

Злоумышленники могут попытаться похитить ваши данные с сайта **host1.redvirt.test** (например, пароли, сообщения или номера банковских карт). [Подробнее...](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

💡 Чтобы браузер Chrome стал максимально безопасным, [включите режим "Улучшенная защита"](#).

Скрыть подробности

Вернуться к безопасной странице

Не удалось подтвердить, что это сервер **host1.redvirt.test**. Операционная система компьютера не доверяет его сертификату безопасности. Возможно, сервер настроен неправильно или кто-то пытается перехватить ваши данные.

[Перейти на сайт host1.redvirt.test \(небезопасно\)](#)

Рисунок 9 – Уведомление о незащищенном соединении

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

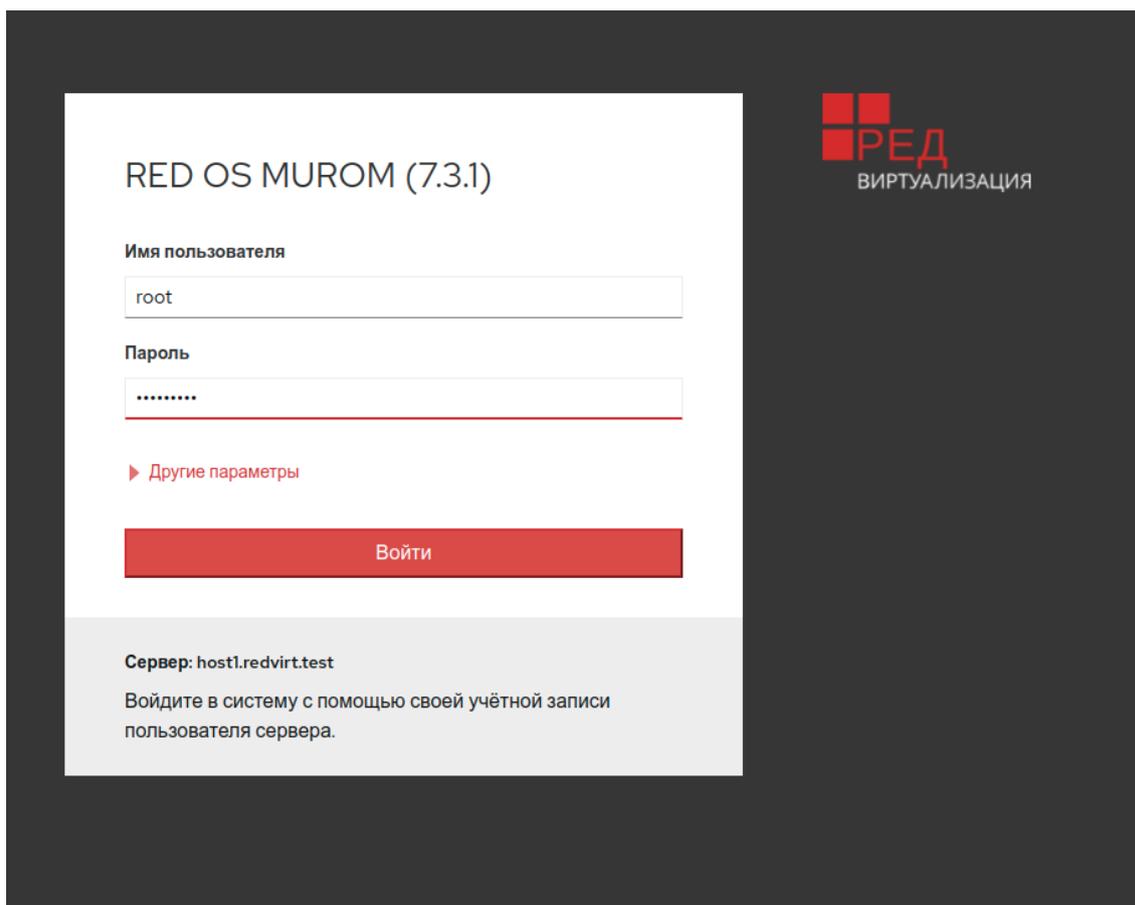


Рисунок 10 – Окно авторизации хоста

Перейдите во вкладку Virtualization – Hosted Engine (Рисунок 11).

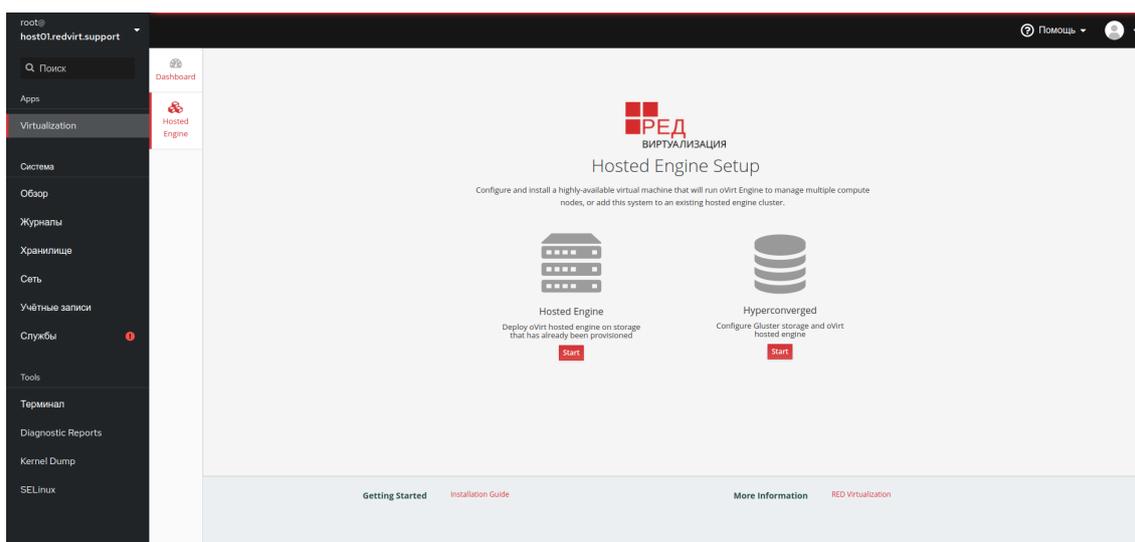


Рисунок 11 – Страница Hosted Engine

Нажмите Hosted Engine – Start и заполните поля на вкладке VM в соответствии с вашими параметрами сети (Рисунок 12-13).

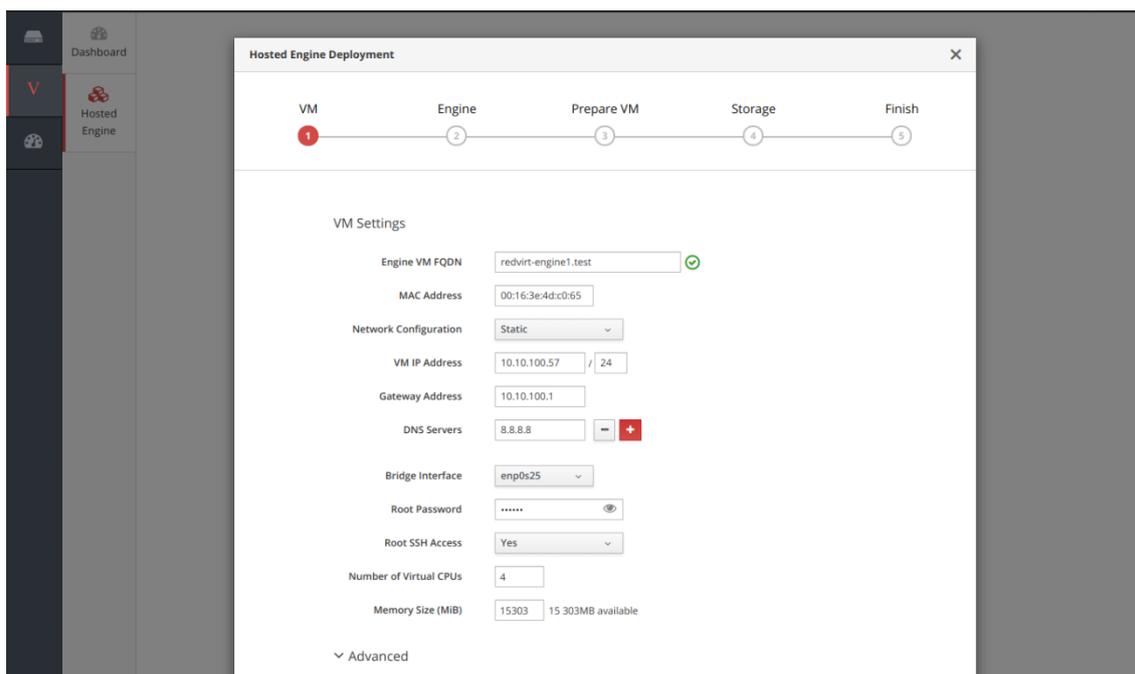


Рисунок 12 – Вкладка VM

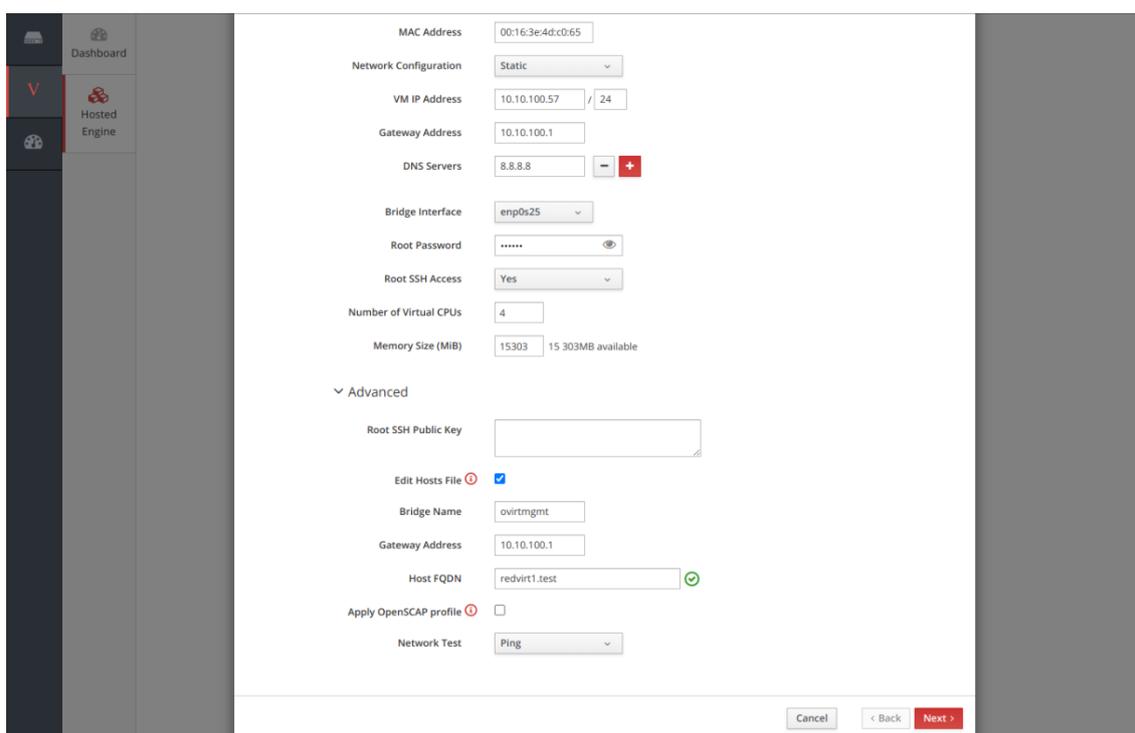


Рисунок 13 – Вкладка VM

Нажмите Next.

Во вкладке Engine назначьте пароль администратору портала, а также настройте службу уведомлений (Рисунок 14).

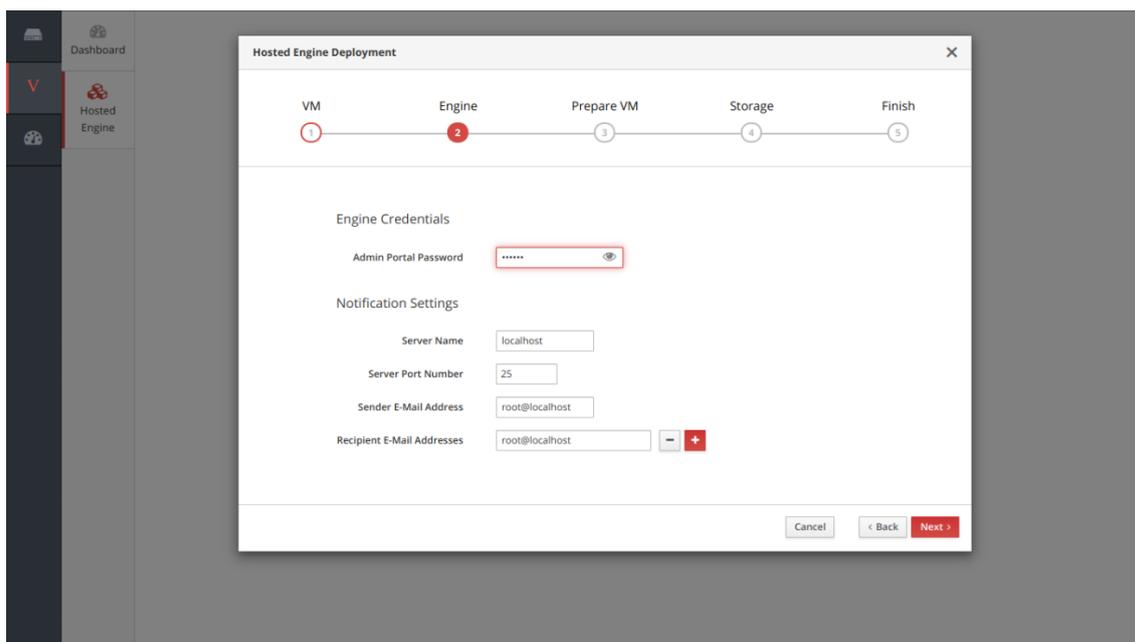


Рисунок 14 – Вкладка Engine

Во вкладке Storage добавьте хранилище (Рисунок 15).

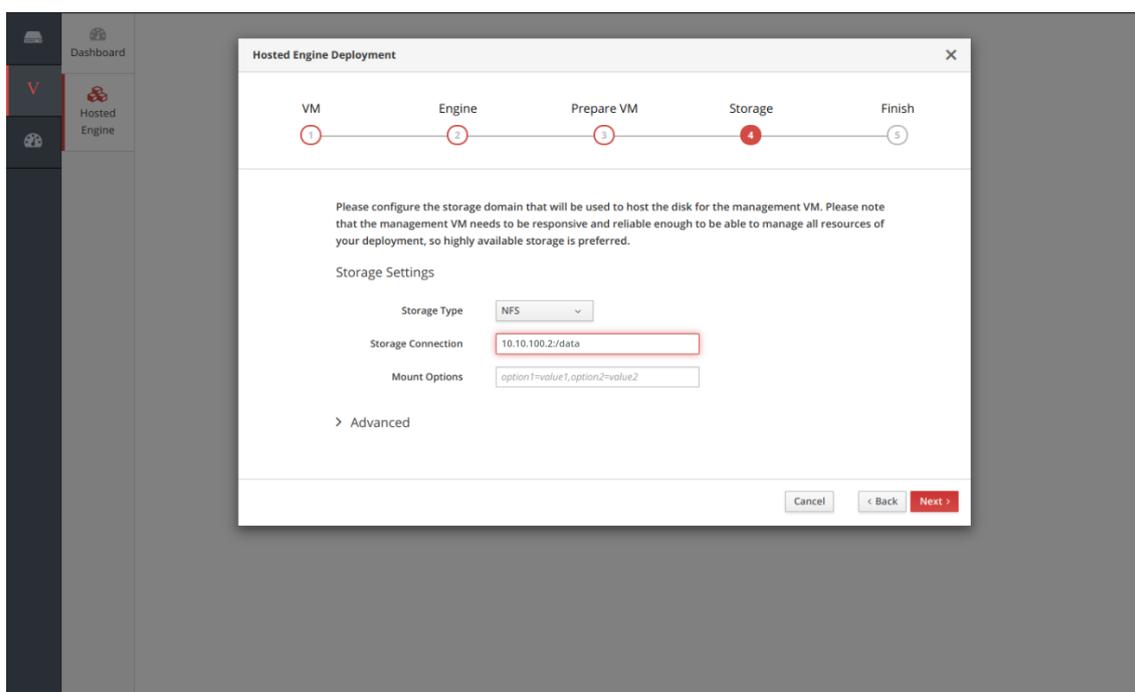


Рисунок 15 – Вкладка Storage

Нажмите Next.

После успешной установки нажмите Close (Рисунок 16).

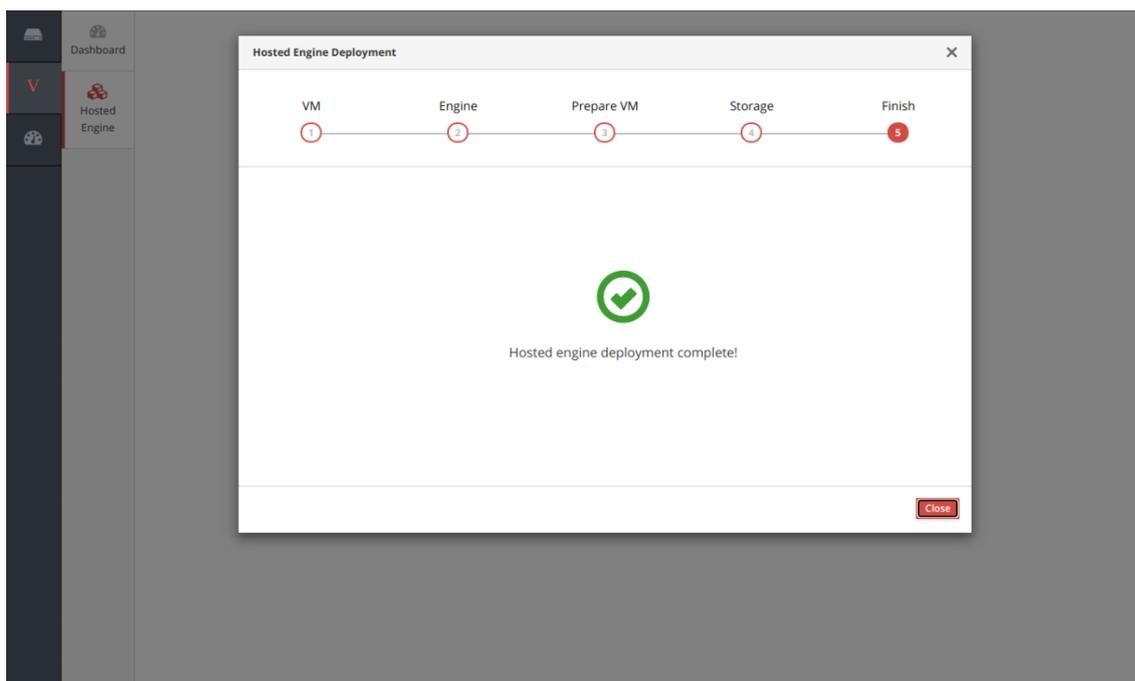


Рисунок 16 – Окончание установки

## 4.2 Установка в режиме standalone

**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**» (Рисунок 17).



Рисунок 17 – Меню установщика

Откроется стандартное окно установки РЕД Виртуализации (Рисунок 18), 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. п. 4.1.2 – 4.1.9 настоящего руководства.

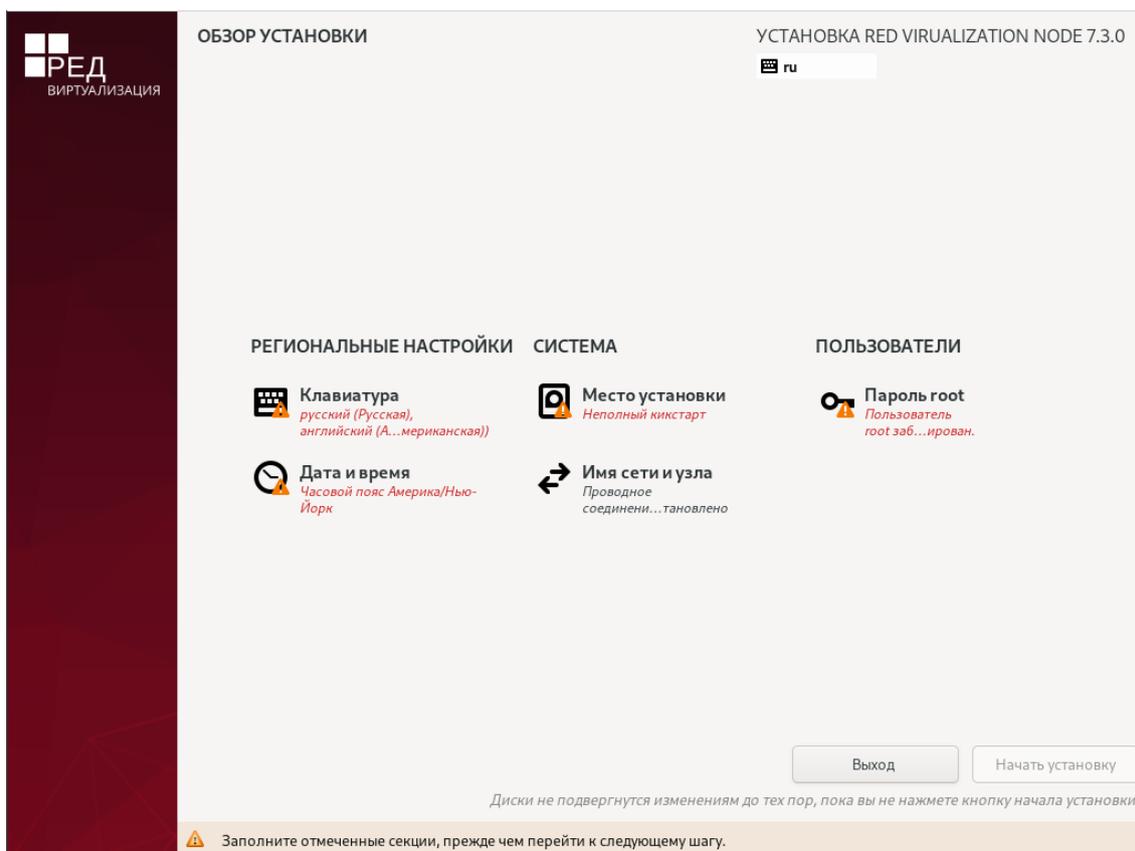


Рисунок 18 – Обзор установки в режиме standalone

После определения всех необходимых настроек начинается этап установки РЕД Виртуализации (Рисунок 19). После данного шага программа установки будет работать с файлами только что установленной базовой системы.

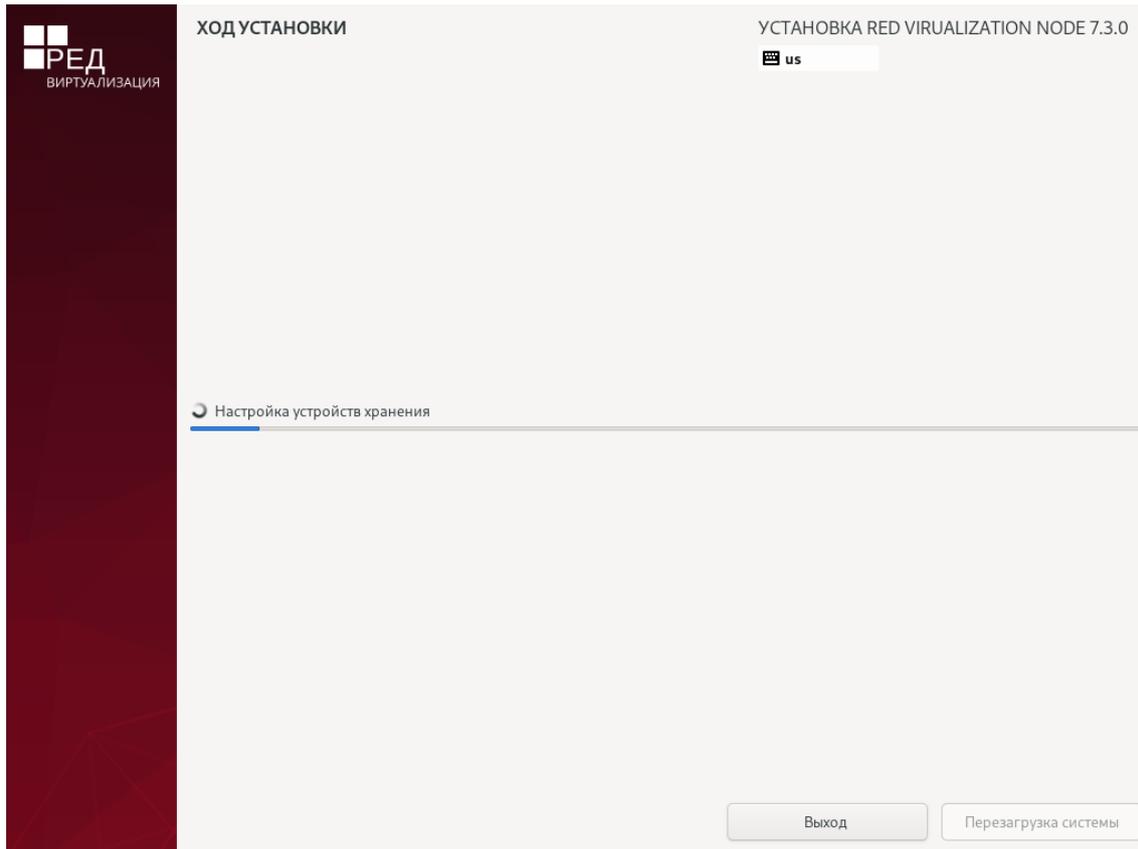


Рисунок 19 – Ход установки

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

Затем откроется терминал установленной системы (Рисунок 20).

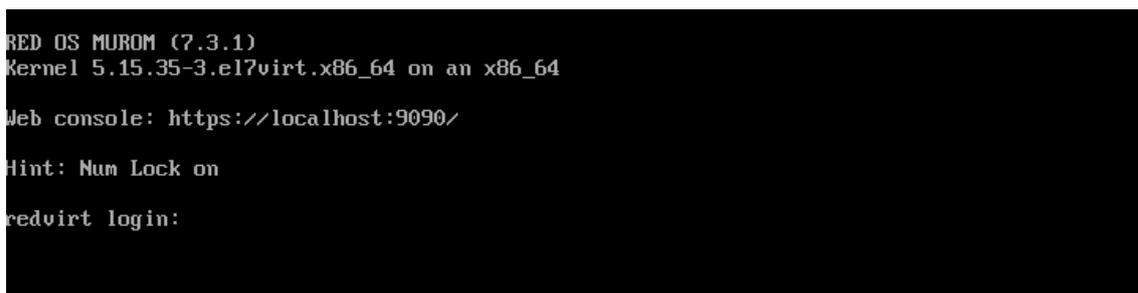


Рисунок 20 – Терминал установленной системы

**Примечание.** В случае если во время установки системы вы по каким-то причинам не указали или указали неверно имя 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 хоста.

```
192.168.0.43 host1.redvirt.test *Хост-гипервизор*
```

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 (Рисунок 21).

```
[ INFO ] Configuring PostgreSQL
[ INFO ] Creating CA: /etc/pki/ovirt-engine/ca.pem
[ INFO ] Creating CA: /etc/pki/ovirt-engine/qemu-ca.pem
[ INFO ] Updating OVM SSL configuration
[ INFO ] Updating OVM timeout configuration
[ INFO ] Creating/refreshing DWH database schema
[ INFO ] Setting up ovirt-vmconsole proxy helper PKI artifacts
[ INFO ] Setting up ovirt-vmconsole SSH PKI artifacts
[ INFO ] Configuring WebSocket Proxy
[ INFO ] Creating/refreshing Engine database schema
[ INFO ] Creating a user for Grafana
[ INFO ] Creating/refreshing Engine 'internal' domain database schema
[ INFO ] Creating default mac pool range
[ INFO ] Adding default OVM provider to database
[ INFO ] Adding OVM provider secret to database
[ INFO ] Setting a password for internal user admin
[ INFO ] Install selinux module /usr/share/ovirt-engine/selinux/ansible-runner-service.cil
[ INFO ] Generating post install configuration file '/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf'
[ INFO ] Stage: Transaction commit
[ INFO ] Stage: Closing up
[ INFO ] Starting engine service
[ INFO ] Starting dwh service
[ INFO ] Starting Grafana service
[ INFO ] Restarting ovirt-vmconsole proxy service

---- SUMMARY ----

[ INFO ] Restarting httpd
Please use the user 'admin@internal' and password specified in order to login
Web access is enabled at:
  http://redvirt.test.standalone:80/ovirt-engine
  https://redvirt.test.standalone:443/ovirt-engine
Internal CA F2:0A:E8:32:07:52:66:C0:41:D7:FD:EF:32:B5:39:9C:56:EA:4D:A5
SSH fingerprint: SHA256:JGsJ8ab3sh90unuUknjxA0ZRNfdUGhhuuAsFkDSGtdc
Web access for grafana is enabled at:
  https://redvirt.test.standalone/ovirt-engine-grafana/
Please run the following command on the engine machine redvirt.test.standalone, for SSO to work:
systemctl restart ovirt-engine

---- END OF SUMMARY ----

[ INFO ] Stage: Clean up
Log file is located at /var/log/ovirt-engine/setup/ovirt-engine-setup-20220804105519-h7iq1t.log
[ INFO ] Generating answer file '/var/lib/ovirt-engine/setup/answers/20220804105915-setup.conf'
[ INFO ] Stage: Pre-termination
[ INFO ] Stage: Termination
[ INFO ] Execution of setup completed successfully
[root@redvirt ~]#
```

Рисунок 21 – Настройка среды управления виртуализацией

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

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

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

Подробную информацию об авторизации в веб-интерфейсе см. в гл. 5 «Веб-интерфейс».

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

Откройте «Виртуализация» - «Дата-центр», нажмите «Редактировать» и в поле «Тип хранилища» выберите «Локальный» (Рисунок 22). Нажмите «ОК».

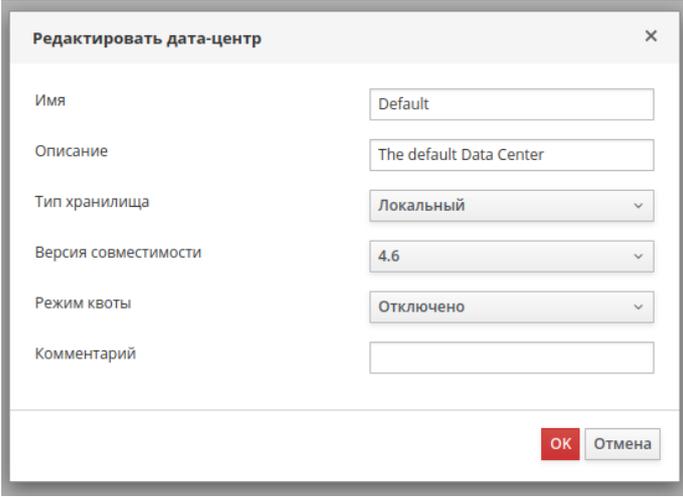


Рисунок 22 – Редактирование дата-центра

Далее необходимо создать вычислительный хост.

Для этого откройте «Виртуализация» – «Узлы» и нажмите кнопку «Новый». В открывшемся окне в полях «Имя» и «Имя узла/IP» впишите имя машины, на которую производится установка. В примере – `host1.redvirt.test`.

**Важно!** При добавлении узла используйте его FQDN имя, как в примере `host1.redvirt.test`, а не его IP-адрес. Иначе, в случае подключения узла по IP-адресу, могут возникнуть проблемы с загрузкой ISO-образов на внутреннее хранилище через веб-интерфейс портала управления. ■

В поле «Пароль» впишите действующий пароль `root`-пользователя (рисунок 23). Нажмите «OK».

Новый хост

Общее >

Узел кластера: Default  
Дата-центр: Default

Имя: host1.redvirt.test

Комментарий:

Имя узла/IP: host1.redvirt.test

Порт SSH: 22

Включить хост-сервер после установки

Reboot host after Install

Аутентификация

Имя пользователя: root

Пароль

Публичный ключ SSH

OK Отмена

Рисунок 23 – Основные настройки хоста

На вопрос «Вы не настроили управление питанием для этого хоста. Вы уверены, что хотите продолжить?» нажмите «ОК». Вы можете настроить политику питания позже.

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

После успешного запуска хоста создайте локальный домен хранения.

Откройте «Хранилище» – «Домен» и нажмите кнопку «Новый домен». В открывшемся окне в поле «Имя» впишите имя создаваемого домена, например, LocalData. В поле «Тип хранилища» выберите «Локально на хосте». В поле «Путь» впишите путь к каталогу, который вы указывали ранее в командах консоли (рисунок 24). Нажмите «ОК».

Новый домен

Дата-центр: Default (Локальный)

Имя: LocalData

Функция домена: Данные

Описание:

Тип хранилища: Локально на хосте

Комментарий:

Хост: host1.redvirt.test

Путь: /srv/data

OK Отмена

Рисунок 24 – Создание домена хранения

## 4.3 Развертывание Gluster Hyperconverged

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 команды:

```
# ssh-keygen
# ssh-copy-id root@<host_address>
```

### 4.3.1 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.

### 4.3.2 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/](https://<имя_хоста>:9090/) или [https://<IP-адрес\\_хоста>:9090/](https://<IP-адрес_хоста>:9090/), и войдите в систему, используя учетные данные суперпользователя root.

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

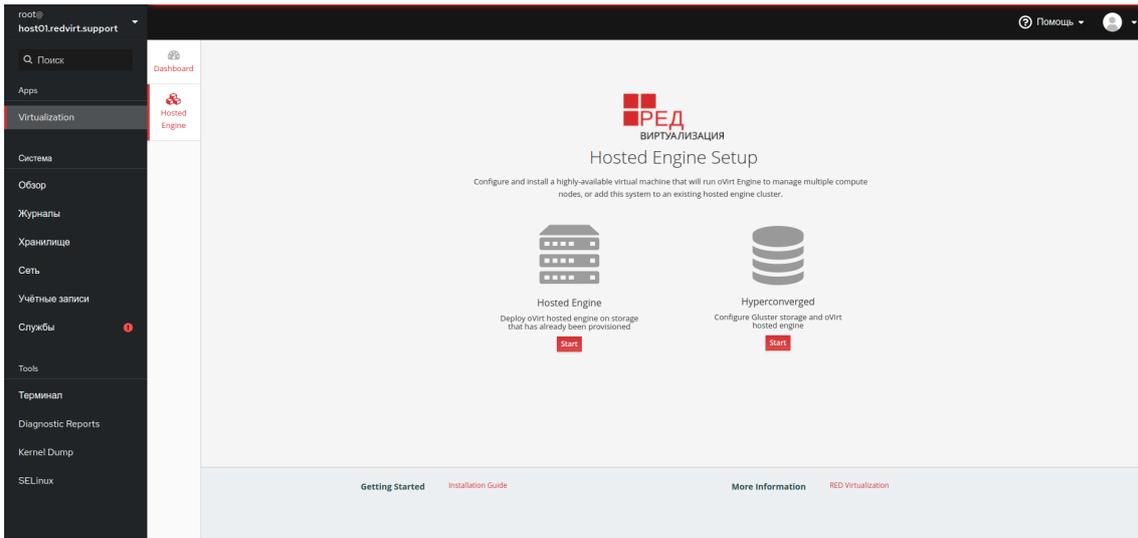


Рисунок 25 – Страница Hosted Engine

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.



Рисунок 26 – Выбор мастера установки

4. Укажите имя хоста.

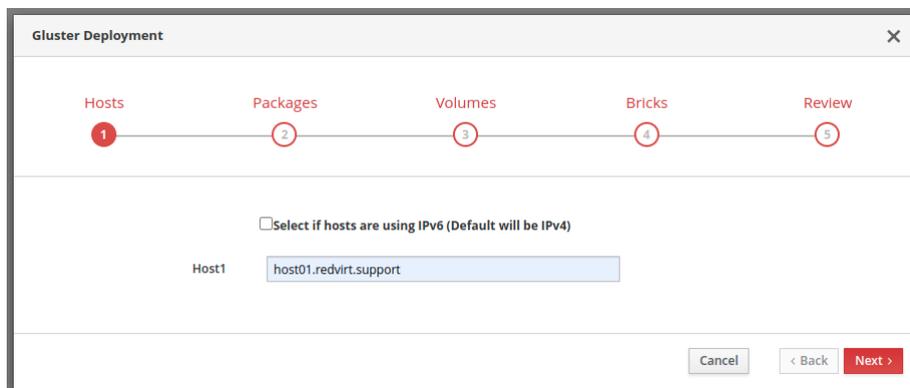


Рисунок 27 – Вкладка Hosts

5. При необходимости загрузите репозитории и дополнительные пакеты.

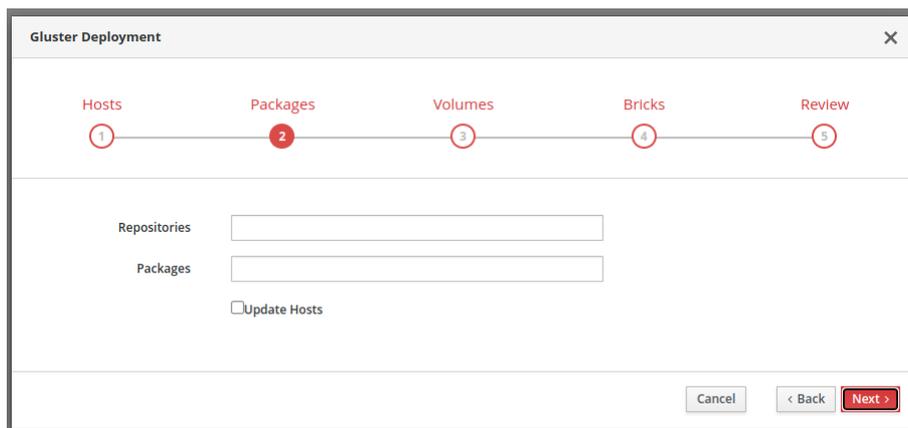


Рисунок 28 – Вкладка Packages

6. Определите необходимые тома.

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

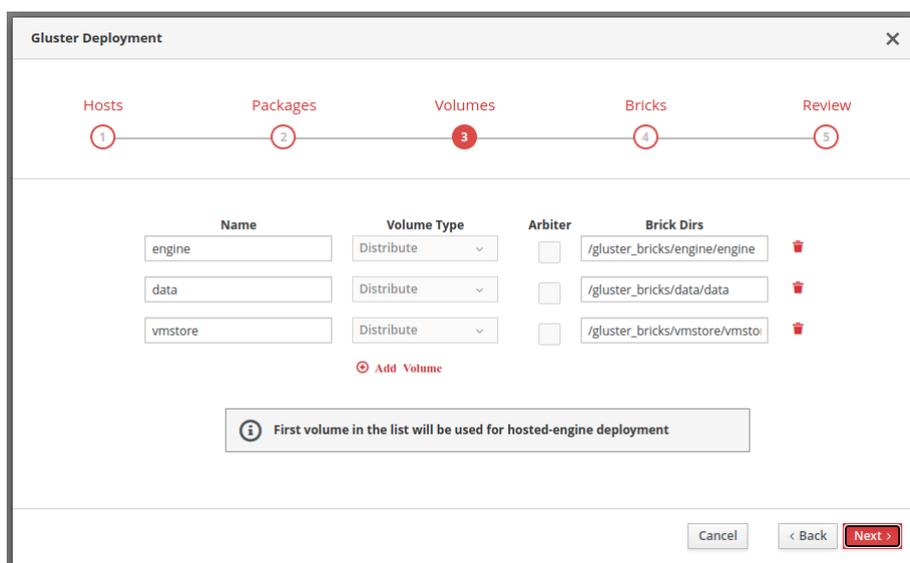


Рисунок 29 – Вкладка Volumes

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

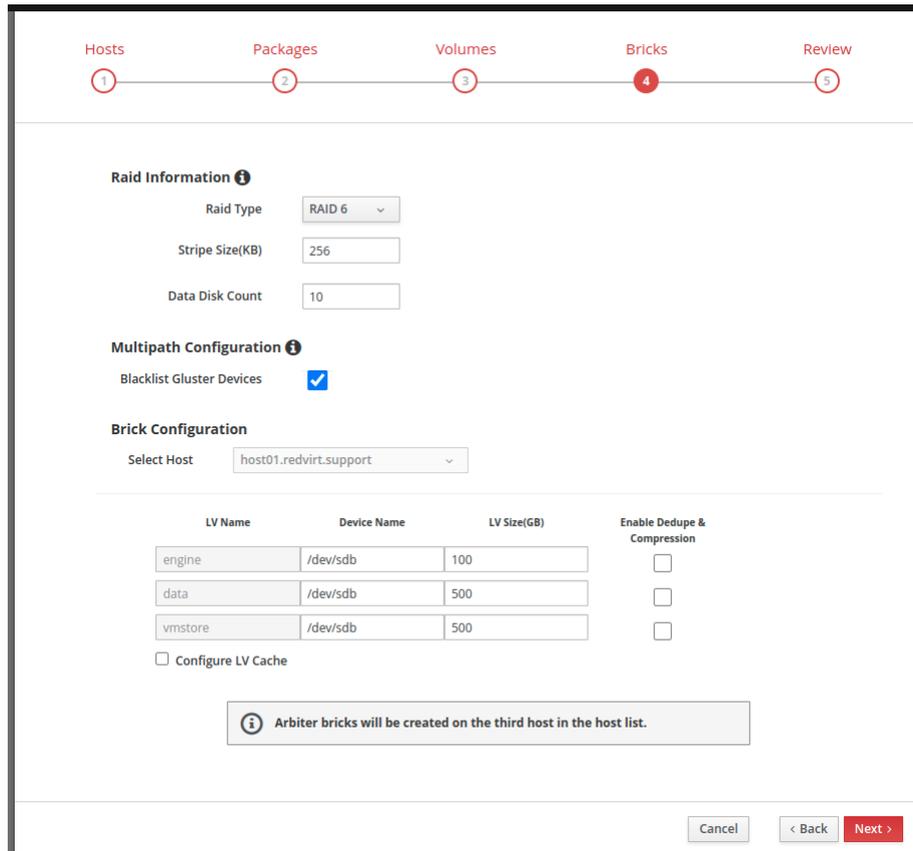


Рисунок 30 – Вкладка Bricks

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

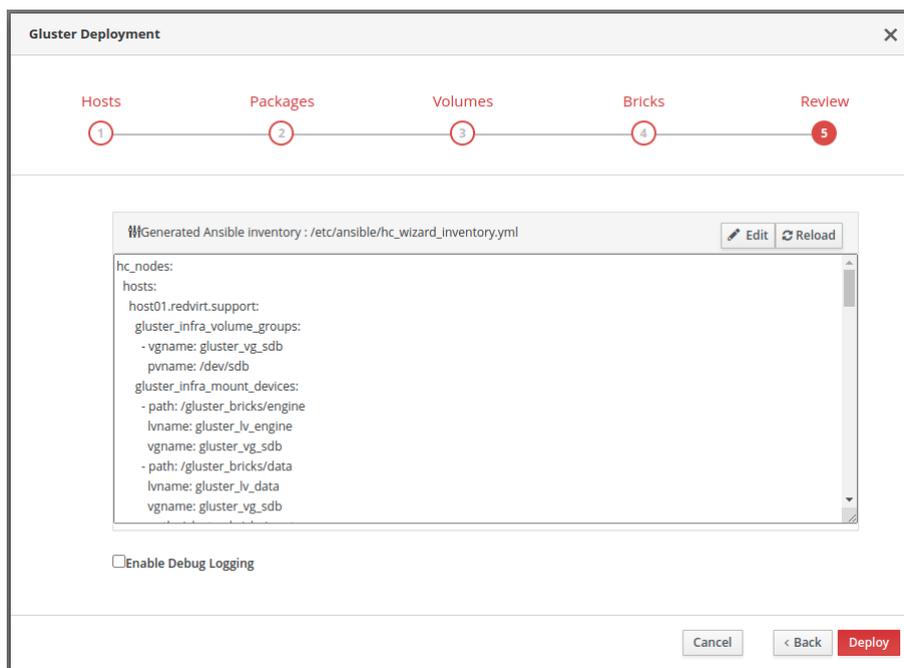


Рисунок 31 – Вкладка Review

Затем начнется процедура развертывания единого узла Gluster.

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

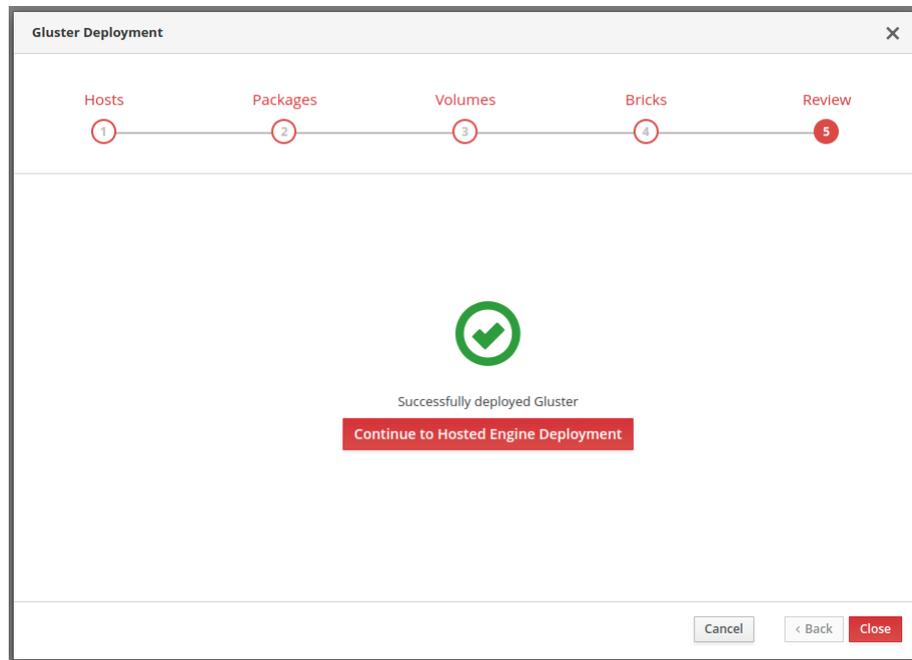


Рисунок 32 – Завершение настройки

Процедура настройки Hosted Engine стандартная.

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

The screenshot shows the 'Hosted Engine Deployment' window with the 'VM' tab selected. A progress bar at the top indicates five steps: VM (1), Engine (2), Prepare VM (3), Storage (4), and Finish (5). The 'VM Settings' section includes the following fields:

- Engine VM FQDN:
- MAC Address:
- Network Configuration:
- Bridge Interface:
- Root Password:
- Root SSH Access:
- Number of Virtual CPUs:
- Memory Size (MiB):  (127 170MiB available)

At the bottom right, there are 'Cancel', '< Back', and 'Next >' buttons. A '> Advanced' link is also present.

Рисунок 33 – Вкладка VM

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

The screenshot shows the 'Hosted Engine Deployment' window with the 'Engine' tab selected. The progress bar at the top shows step 2 ('Engine') as the current step. The 'Engine Credentials' and 'Notification Settings' sections include the following fields:

- Engine Credentials: Admin Portal Password (password field)
- Notification Settings: Server Name ()
- Server Port Number ()
- Sender E-Mail Address ()
- Recipient E-Mail Addresses () with add (+) and remove (-) buttons

At the bottom right, there are 'Cancel', '< Back', and 'Next >' buttons.

Рисунок 34 – Вкладка Engine

Во вкладке **Prepare VM** проверьте данные для VM и, если все настроено верно, нажмите кнопку «**Prepare VM**». Будет запущен процесс подготовки

виртуальной машины и развертывание Hosted Engine.

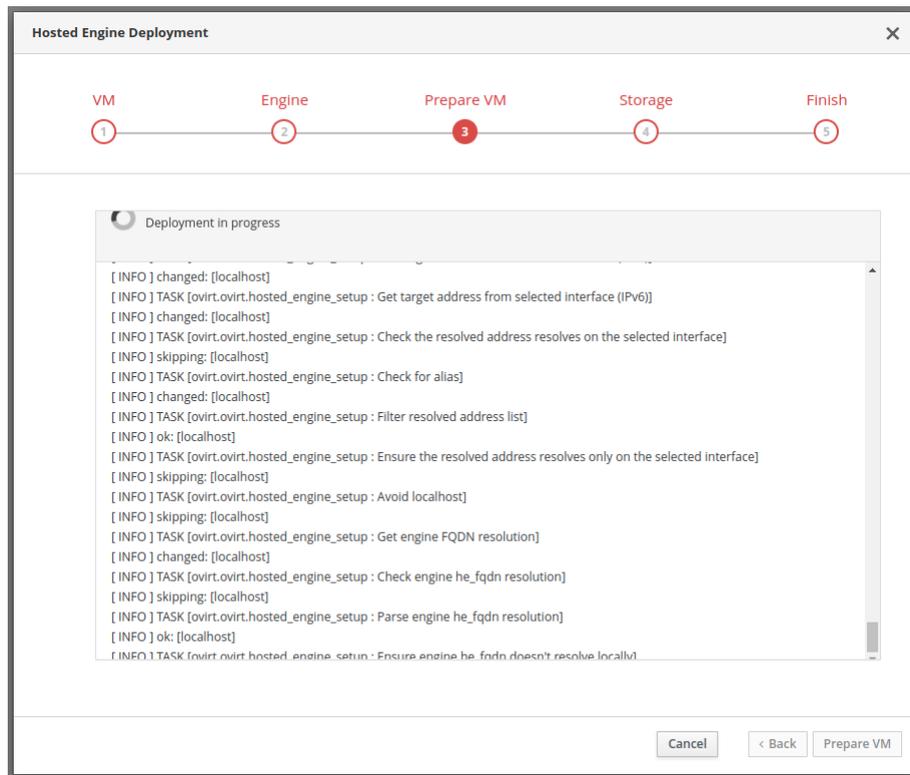


Рисунок 35 – Вкладка Prepare VM

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

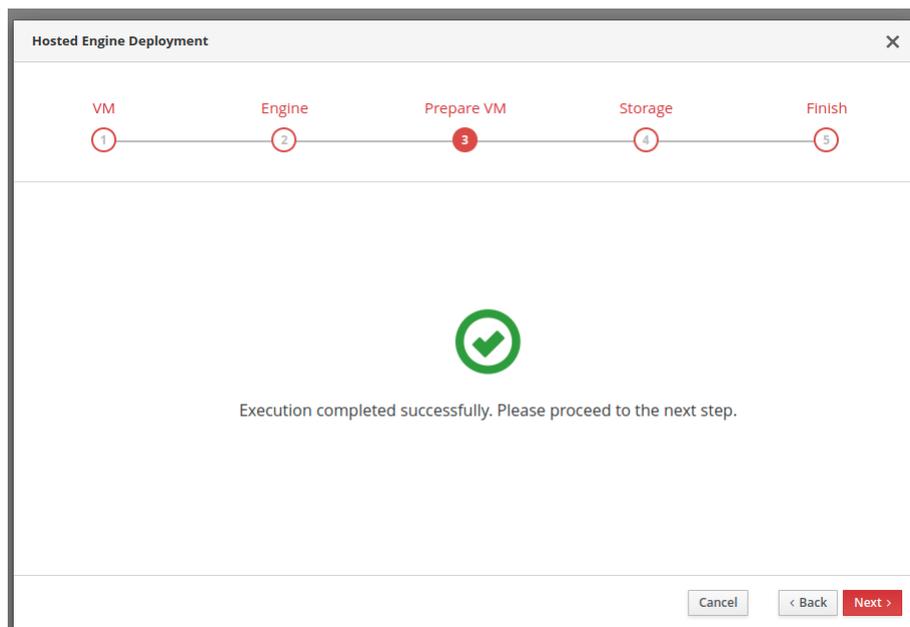


Рисунок 36 – успешное завершение развертывания

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

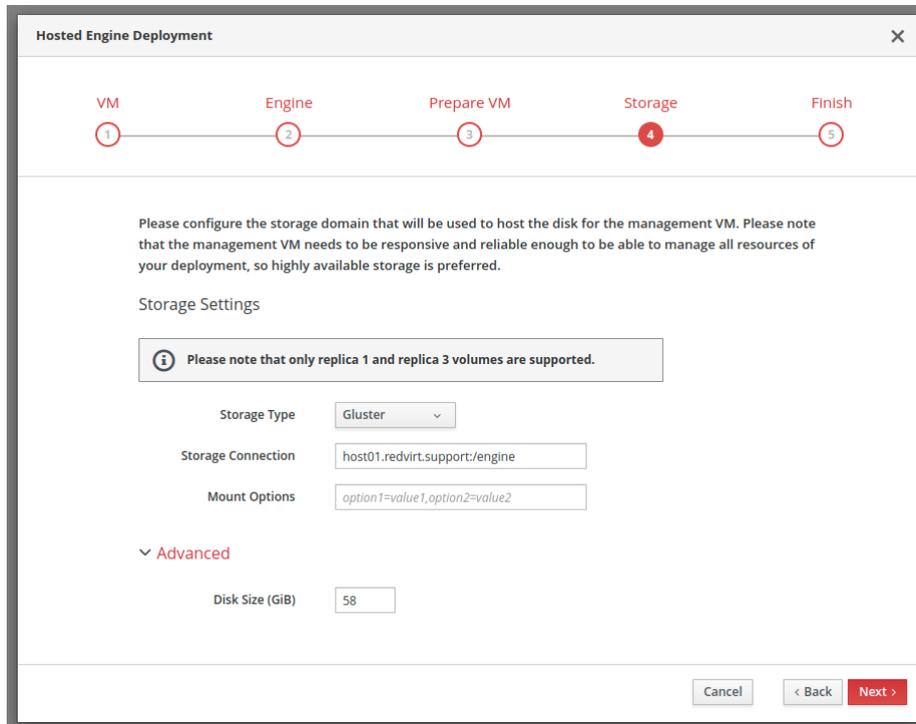


Рисунок 37 – Вкладка Storage

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

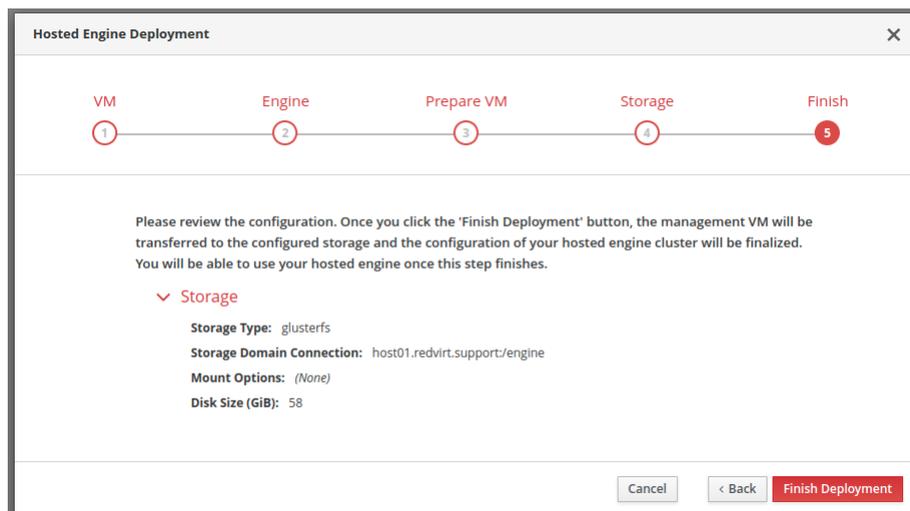


Рисунок 38 – Вкладка Finish

После успешной установки нажмите **Close**.

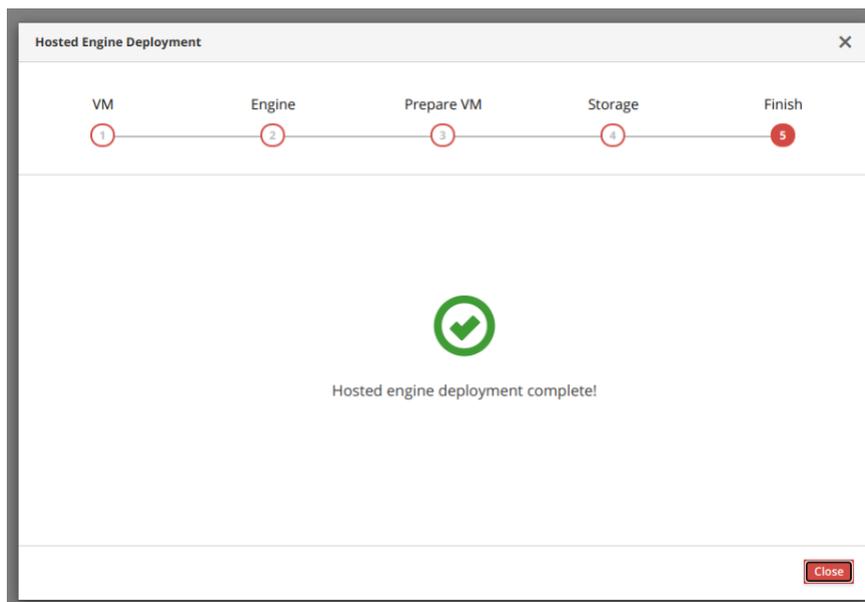


Рисунок 39 – Успешное завершение установки

## 5. Веб-интерфейс

Для работы с РЕД Виртуализацией перейдите по адресу `https://<hosted-engine>`.

Для дальнейшей корректной работы в системе необходимо загрузить сертификат.

Загрузка сертификата доступна на приветственной странице РЕД Виртуализации в поле «Загрузки» - «Корневой сертификат».

После загрузки сертификата перейдите в настройки браузера, выберите пункт «Безопасность» - «Настройка сертификатов», в открывшемся окне перейдите на вкладку «Доверенные корневые центры сертификации», нажмите «Импорт», выберите загруженный ранее сертификат и добавьте его.

Затем откроется главная страница РЕД Виртуализации, где нужно выбрать необходимый портал (Рисунок 40).

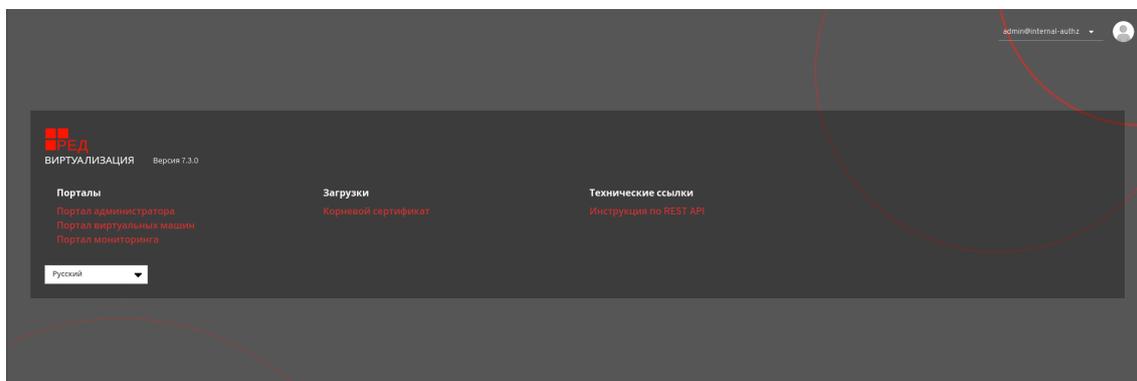


Рисунок 40 – Страница выбора порталов

После выбора портала откроется окно авторизации, где необходимо ввести

имя пользователя и пароль. В выпадающем меню «Профиль» есть возможность выбора необходимого домена аутентификации (Рисунок 41).

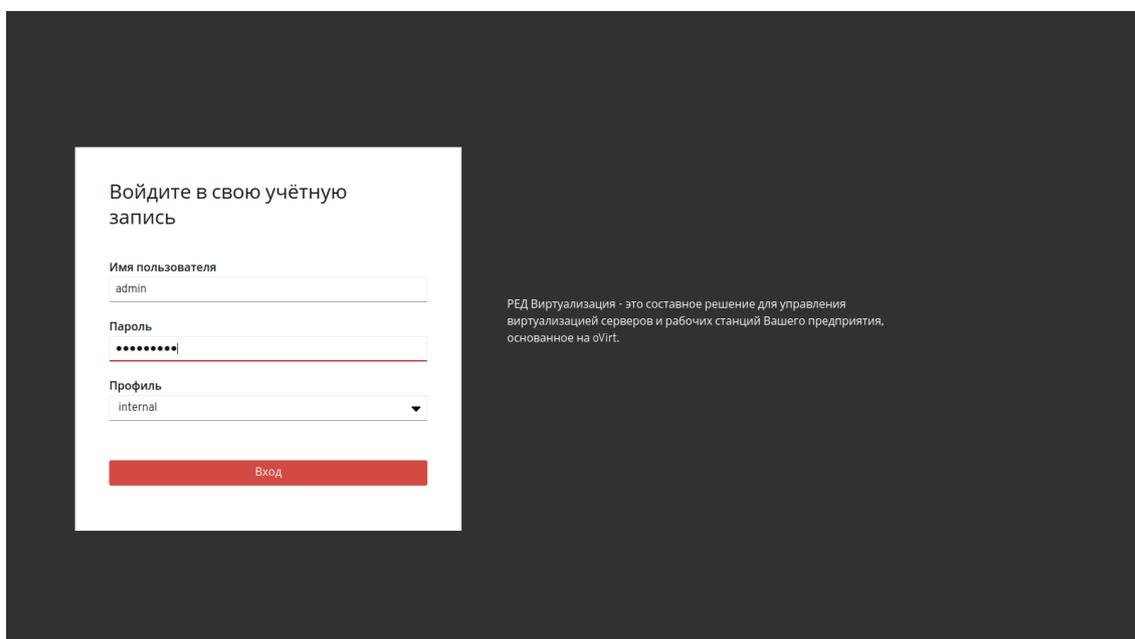


Рисунок 41 – Авторизация на портале

После успешной авторизации на портале откроется веб-интерфейс управления системой виртуализации РЕД Виртуализация.

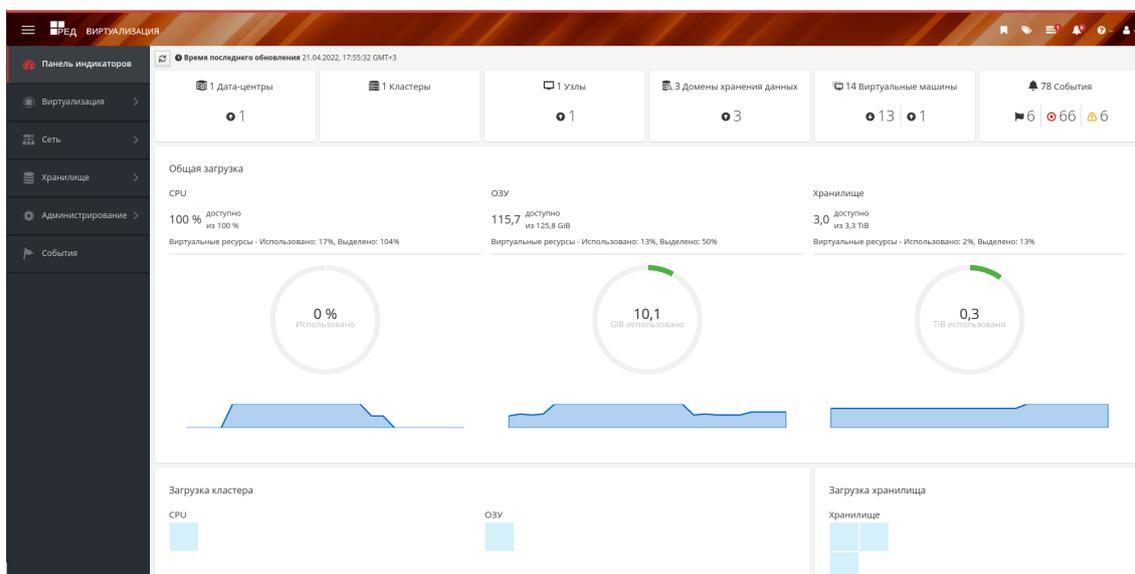


Рисунок 42 – Панель мониторинга ресурсов