РУКОВОДСТВО ПО УСТАНОВКЕ

СИСТЕМА БЕЗОПАСНОГО УПРАВЛЕНИЯ СРЕДОЙ ВИРТУАЛИЗАЦИИ **ZVIRT**

Содержание

1. Архитектура ... 4
   1.1 Ключевые компоненты СУВ zVirt ... 4
   1.2 Архитектура СУВ zVirt ... 4
      1.2.1 Режим Hosted Engine ... 4
      1.2.2 Режим Standalone ... 5
2. Системные требования ... 7
   2.1 Требования к оборудованию ... 7
      2.1.1 Требования к процессору ... 7
      2.1.2 Требования к оперативной памяти ... 8
      2.1.3 Требования к хранилищу ... 8
      2.1.4 Требования к сети ... 8
      2.1.5 Требования к межсетевому экрану менеджера управления ... 9
      2.1.6 Требования к межсетевому экрану хоста виртуализации ... 10
3. Подготовка к установке ... 12
   3.1 Подготовка хранилища ... 12
      3.1.1 Подготовка хранилища NFS ... 12
      3.1.2 Подготовка хранилища iSCSI ... 13
      3.1.3 Подготовка FCP-хранилища ... 14
      3.1.4 Подготовка Gluster Storage ... 14
4. Установка ... 16
   4.1 Описание процесса установки ... 16
   4.2 Подготовка хранилища ... 16
   4.3 Установка хоста виртуализации ... 16
   4.4 Установка среды виртуализации ... 17
      4.4.1 Установка в режиме Hosted Engine с помощью командной строки ... 17
      4.4.2 Установка в режиме Hosted Engine с помощью веб-интерфейса Cockpit ... 21
      4.4.3 Установка гиперконвергентной среды виртуализации в режиме Hosted Engine с помощью веб-интерфейса Cockpit ... 28
      4.4.4 Установка в режиме Standalone ... 41
      4.4.5 Исправление хоста после неуспешной инсталляции среды виртуализации ... 43
5. После установки ... 44
   5.1 Проверка работоспособности ... 44
   5.2 Добавление хостов ... 44
   5.3 Добавление хранилища ... 45
6. Рекомендации ... 46
   6.1 Гипервизор ... 46

6.2 Центр данных ... 46
6.2.1 NFS ... 47
6.2.2 iSCSI ... 47
6.2.3 Fibre Channel ... 47
6.2.4 GlusterFS ... 47
6.2.5 Гиперконвергентная инфраструктура ... 48
6.2.6 POSIX-совместимые файловые системы ... 48
6.2.7 Локальное хранилище ... 48
6.3 Сети ... 48
6.3.1 Ограничения на количество логических сетей в СУВ zVirt: ... 50
6.4 Сервера каталогов ... 50
6.5 Общие рекомендации ... 51
6.5.1 Рекомендации по безопасности ... 51
6.5.2 Рекомендации по хостам ... 51
6.5.3 Рекомендации по работе с сетью ... 52
6.5.4 Рекомендации по настройке сетей хоста ... 52
6.5.5 Рекомендации по развертывания в режиме HostedEngine ... 53
7. Сбор и предоставление логов ... 54
Перечень используемых сокращений ... 55

1. АРХИТЕКТУРА

! Внимательно прочтите данное руководство перед установкой системы безопасного управления виртуализацией zVirt, это позволит сократить время развертывания и избежать ошибок.

1.1 Ключевые компоненты СУВ zVirt

Ключевые компоненты СУВ zVirt описаны в Таблице 1.

Таблица 1. Ключевые компоненты zVirt

Имя компонента	Описание
Хост виртуализации	Физический сервер с установленной ОС zVirt Node, использующий технологию виртуализации KVM. Предоставляет вычислительные ресурсы для запуска виртуальных машин
Виртуальная машина (ВМ)	Программная среда, эмулирующая аппаратное обеспечение платформы x86-64
Менеджер управления	Менеджер управления – операционная система, с установленной СУВ, управляющая физическими хостами виртуализации, доменами данных, кластерами, виртуальными машинами и предоставляющая администратору интерфейс управления. Менеджер управления устанавливается в режиме Standalone (как сервис на физический сервер) или HostedEngine (как сервис внутри виртуальной машины).
Домен хранения данных (хранилище)	Служба хранения используется для хранения данных, связанных с виртуальными машинами.

1.2 Архитектура СУВ zVirt

1.2.1 Режим Hosted Engine

Система безопасного управления виртуализацией zVirt разворачивается в режиме Hosted Engine, при котором менеджер управления работает внутри ВМ, запущенной на хостах, управляемых этой службой управления. ВМ и менеджер управления создаются и настраиваются при первоначальной установке кластера.

Основное преимущество режима Hosted Engine состоит в том, что отсутствует необходимость в отдельном хосте с ролью менеджера управления. Кроме того, Hosted Engine может работать в режиме высокой доступности.

Если хост, на котором запущена ВМ HostedEngine, переходит в режим обслуживания или неожиданно выходит из строя, виртуальная машина будет автоматически перенесена на другой хост в среде. Для режима высокой доступности Hosted Engine требуется минимум два хоста.

Минимальная настройка включает в себя:

- ВМ HostedEngine;
- Один (или два для режима высокой доступности ВМ HostedEngine) хоста;
- Внешняя система хранения данных (СХД) или локальное хранилище для размещения домена хранения данных (хранилища). Хранилище должно быть доступно всем хостам виртуализации.

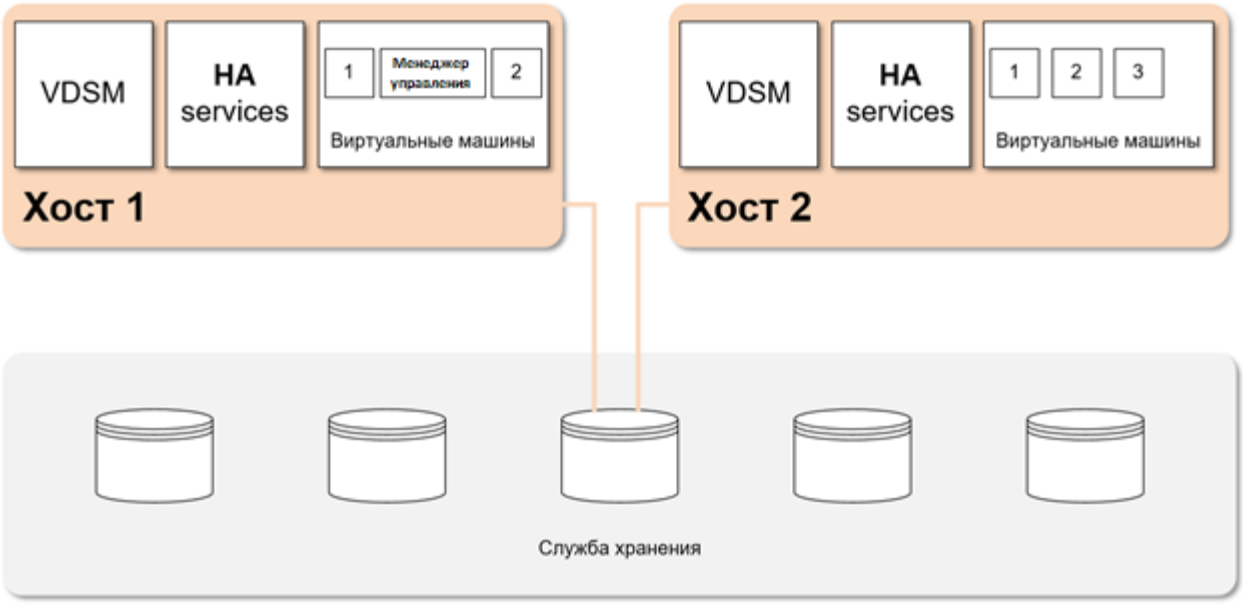

Рисунок 1. Архитектура zVirt в режиме Hosted Engine

1.2.2 Режим Standalone

Система безопасного управления виртуализацией zVirt может разворачиваться в режиме Standalone. Режим Standalone проще в развертывании и управлении, но требует дополнительного физического хоста. В исключительных случаях возможно использование хоста с менеджером управления в качестве гипервизора.

Минимальная настройка включает в себя:

- Один хост для менеджера управления. Обычно менеджер управления развертывается на физическом хосте. Менеджер управления возможно развернуть и на виртуальной машине, если эта виртуальная машина размещена в отдельной среде виртуализации. Менеджер управления должен работать под управлением zVirt Node.
- Минимум два хоста для обеспечения высокой доступности виртуальных машин.
- Внешняя система хранения данных (СХД) или локальное хранилище для размещения домена хранения данных (хранилища). Хранилище должно быть доступно всем хостам виртуализации.

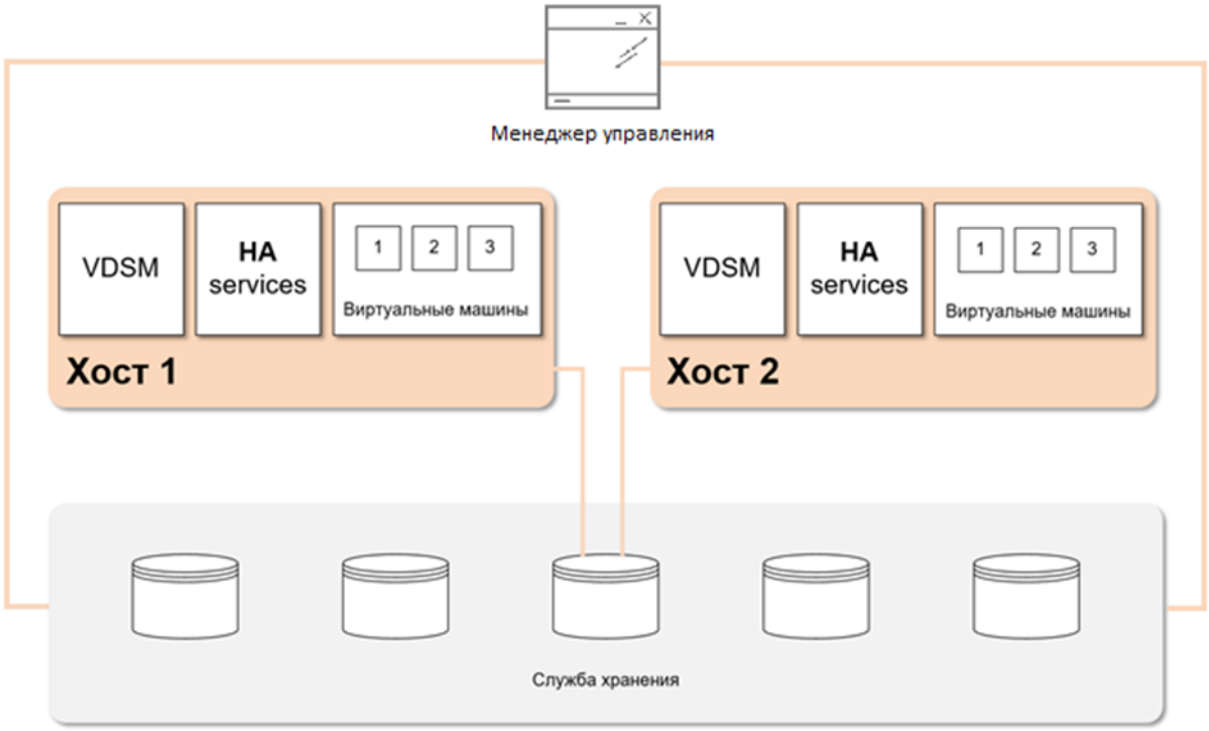

Рисунок 2. Архитектура zVirt в режиме Standalone

2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

2.1 Требования к оборудованию

Минимальные и рекомендуемые требования к оборудованию, изложенные здесь, основаны на типичной установке малого и среднего размера. Точные требования варьируются в зависимости от размеров и нагрузки.

Таблица 2. Требования к оборудованию

Ресурс	Минимальная конфигурация	Рекомендуемая конфигурация
Процессор	Двухъядерный процессор x86-64 с поддержкой VT-x/AMD-V	Четырехъядерный процессор или несколько двухъядерных процессоров
Память	4 ГБ	32 ГБ
Жесткий диск	94 ГБ	1 ТБ
Сетевой интерфейс	1 сетевой интерфейс (NIC) 1 Гбит / с.	2 сетевых интерфейса (NIC) 10 Гбит/с

2.1.1 Требования к процессору

Все процессоры должны поддерживать расширения процессоров Intel® 64 или AMD64, а также в BIOS/UEFI должны быть включены аппаратные расширения виртуализации AMD-V ™ или Intel VT®. Также требуется поддержка флага No eXecute (NX).

Проверить, какие расширения процессора доступны на системе, можно следующей командой:

```
# grep flags /proc/cpuinfo|head -n1|grep -Eo '(vmx|svm|nx)'
```

Таблица 3. Поддерживаемый процессоры

Intel	**AMD**
Nehalem	G1
Westmere	G2
SandyBridge	G3
IvyBridge	G4
Haswell	G5
Broadwell	EPYC
Skylake Client	
Skylake Server	
Cascadelake Server	

2.1.2 Требования к оперативной памяти

Минимальный необходимый объем оперативной памяти составляет 4 ГБ. Максимальный поддерживаемый объем ОЗУ на узле zVirt составляет 12 ТБ.

Объем оперативной памяти зависит от требований гостевой операционной системы (далее - виртуальная машина, ВМ), требований гостевого приложения, а также активности и использования гостевой памяти. KVM также может перезаписывать физическую оперативную память для ВМ, что позволяет вам предоставлять гостям требования к оперативной памяти, превышающие физические, при условии, что не все ВМ работают одновременно при пиковой нагрузке. KVM делает это, выделяя оперативную память только для ВМ по мере необходимости и переводя недостаточно загруженные ВМ в раздел подкачки.

2.1.3 Требования к хранилищу

Хостам требуется хранилище для хранения конфигурации, журналов, дампов ядра и для использования в качестве пространства подкачки. Хранилище может быть локальным или сетевым. zVirt Node (Хост) может загружаться с одним, несколькими или со всеми выделенными сетевыми хранилищами. Загрузка из сетевого хранилища может привести к зависанию в случае отключения сети. Если хост загружается из хранилища SAN и теряет соединение, файлы становятся доступными только для чтения, пока не восстановится сетевое соединение. Использование сетевого хранилища может привести к снижению производительности.

Минимальные требования к хранению описаны в этом разделе:

Минимальные требования и рекомендуемая схема разбиения хранилища

- / (root) - 55 GB
- /home - 1 GB
- /tmp - 1 GB
- /boot - 1 GB
- /var - 15 GB
- /var/crash - 10 GB
- /var/log - 8 GB
- /var/log/audit - 2 GB
- swap - 1 GB

Минимальный общий объём - 94 Гб.

2.1.4 Требования к сети

Хосты должны иметь хотя бы один сетевой интерфейс с минимальной пропускной способностью 1 Гбит/с. Рекомендуется, чтобы у каждого хоста было два сетевых интерфейса, один из которых предназначен для поддержки интенсивных сетевых действий, таких как миграция виртуальных машин. Производительность таких операций ограничена доступной пропускной способностью.

! Не отключайте IPv6 на хостах виртуализации и/или ВМ HostedEngine, даже если он не используется в вашей сети.

2.1.5 Требования к межсетевому экрану менеджера управления

Менеджеру управления требуется, чтобы следующие номера портов были открыты, чтобы пропускать сетевой трафик через межсетевой экран системы.

Сценарий установки автоматически настроит firewalld во время развертывания, но перезапишет старую конфигурацию, если вы используете iptables. Если вы хотите использовать iptables и оставить существующую конфигурацию, вы должны настроить его самостоятельно. Описанная здесь конфигурация межсетевого экрана предполагает конфигурацию по умолчанию.

Таблица 4. Требования к межсетевому экрану менеджера управления

Порт	Протокол	Источник	Место назначения	Предназначение	Шифрование
-	ICMP	Хосты виртуализации	Менеджер управления	Необязательный. Может помочь в диагностике.	Нет
22	TCP	Система (ы), используемая для обслуживания двигателя, включая конфигурацию бэкенда и обновление программного обеспечения.	Менеджер управления	Безопасный доступ к Shell (SSH).	Да
				Необязательный.	
2222	TCP	Клиенты, получающие доступ к консолям виртуальных машин.	Менеджер управления	Доступ через Secure Shell (SSH) для подключения к консолям виртуальной машины.	Да
80, 443	TCP	Клиенты портала администрирования	Менеджер управления	Предоставляет HTTP (порт 80, не зашифрованный) и HTTPS (порт 443, зашифрованный) доступ к Engine. HTTP перенаправляет соединения на HTTPS.	Да
		Клиенты пользовательского портала			
		Хосты виртуализации			
		REST API клиенты			
6100	TCP	Клиенты портала администрирования	Менеджер управления	Предоставляет доступ через прокси-сервер websocket для веб-консольного клиента noVNC, когда прокси-сервер websocket работает на Engine. Однако, если прокси-сервер websocket работает на другом хосте, этот порт не используется.	Нет
		Клиенты пользовательского портала			
7410	UDP	Хосты виртуализации	Менеджер управления	Если Kdump включен на хостах, откройте этот порт для приемника fence_kdump на Engine. Fence_kdump не предоставляет способ шифрования соединения. Тем не менее, вы можете вручную настроить этот порт для блокировки доступа от хостов, которые не имеют права.	Нет
54323	TCP	Клиенты портала администрирования	Менеджер управления (прокси-сервер ImageIO)	Требуется для связи с ImageIO Proxy	Да
6442	TCP	Хосты виртуализации	Открытая виртуальная сеть (OVN)	Требуется для подключения к базе данных Open Virtual Network (OVN)	Да

9696	TCP	Клиенты провайдера внешней сети для OVN	Внешний сетевой провайдер для OVN	OpenStack Networking API	Да, с конфигурацией, генерируемой настройкой менеджера управления.
35357	TCP	Клиенты провайдера внешней сети для OVN	Внешний сетевой провайдер для OVN	OpenStack Identity API	Да, с конфигурацией, генерируемой настройкой менеджера управления.
53	TCP, UDP	Менеджер управления	DNS	DNS-запросы поиска от портов выше 1023 к порту 53 и ответы. Открыты по умолчанию.	Нет
123	UDP	Менеджер управления	NTP-сервер	NTP-запросы от портов выше 1023 к порту 123 и ответы. Открыты по умолчанию.	Нет

2.1.6 Требования к межсетевому экрану хоста виртуализации

Хостам виртуализации необходимо, чтобы номера портов, перечисленные в таблице № 5 были открыты, чтобы пропускать сетевой трафик через межсетевой экран системы.

Таблица 5. Требования к межсетевому экрану хоста виртуализации

Порт	Протокол	Источник	Место назначения	Назначение	Шифрование
22	TCP	Менеджер управления	Хосты виртуализации	Безопасный доступ к Shell (SSH). Необязательный.	Да
2223	TCP	Менеджер управления	Хосты виртуализации	Доступ через Secure Shell (SSH) для подключения к последовательным консолям виртуальной машины.	Да
161	UDP	Хосты виртуализации	Менеджер управления	Простой протокол управления сетью (SNMP). Требуется только в том случае, если вы хотите, чтобы прерывания Simple Network Management Protocol отправлялись с хоста одному или нескольким внешним SNMP-менеджерам. Необязательный.	Нет
111	TCP	Сервер хранения NFS	Хосты виртуализации	NFS соединения. Необязательный.	Нет
5900 - 6923	TCP	Клиенты портала администрирования Клиенты пользовательского портала	Хосты виртуализации	Удаленный доступ к гостевой консоли через VNC и SPICE. Эти порты должны быть открыты для облегчения доступа клиентов к виртуальным машинам.	Да (необязательно)
5989	TCP, UDP	Менеджер объектов общей информационной модели (CIMOM)	Хосты виртуализации	Используется менеджерами объектов общей информационной модели (CIMOM) для мониторинга виртуальных машин, работающих на хосте. Требуется только в том случае, если вы хотите использовать CIMOM для мониторинга виртуальных машин в вашей среде виртуализации. Необязательный.	Нет

9090	TCP	Менеджер управления Клиентские машины	Хосты виртуализации	Требуется для доступа к веб-интерфейсу Cockpit, если он установлен.	Да
16514	TCP	Хосты виртуализации	Хосты виртуализации	Миграция виртуальной машины с использованием libvirt.	Да
49152 - 49215	TCP	Хосты виртуализации	Хосты виртуализации	Миграция и ограждение виртуальной машины с использованием VDSM. Эти порты должны быть открыты для облегчения как автоматической, так и ручной миграции виртуальных машин.	Да
54321	TCP	Менеджер управления Хосты виртуализации	Хосты виртуализации	Связь VDSM с Engine и другими узлами виртуализации.	Да
54322	TCP	Менеджер управления (прокси-сервер ImageIO)	Хосты виртуализации	Требуется для связи с демоном ImageIO.	Да
6081	UDP	Хосты виртуализации	Хосты виртуализации	Требуется, когда в качестве сетевого поставщика используется открытая виртуальная сеть (OVN), чтобы OVN мог создавать туннели между хостами.	Нет
53	TCP, UDP	Хосты виртуализации	DNS	DNS-запросы поиска от портов выше 1023 к порту 53 и ответы. Этот порт обязателен и открыт по умолчанию.	Нет

Правила межсетевого экрана автоматически настраиваются по умолчанию при добавлении нового хоста в среду виртуализации, перезаписывая любую существующую конфигурацию межсетевого экрана.

Чтобы отключить автоматическую настройку межсетевого экрана при добавлении нового хоста, снимите флажок «**Автоматически настраивать межсетевой экран хоста»** в разделе «**Дополнительные параметры»**.

3. ПОДГОТОВКА К УСТАНОВКЕ

3.1 Подготовка хранилища

! Требуется хотя бы один домен хранения данных, используемый для развертывания ВМ HostedEngine, объёмом не менее 94 ГиБ. Это хранилище необходимо подготовить перед установкой.

После установки рекомендуется добавить отдельный (отдельные) домены хранения данных для хранения дисков ВМ.

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

Поддерживаются следующие протоколы:

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

! При использовании протокола iSCSI, домен хранения HostedEngine должен использовать выделенный iSCSI target. Любые дополнительные домены хранения должны использовать отдельные iSCSI target.

! В случае появления следующей ошибки во время установки:

```
[ ERROR ] Error: Fault reason is "Operation Failed". Fault detail is "[Physical device initialization failed. Please check that the device is empty and accessible by the host.]". HTTP response code is 400.
```

Выполнить инициализацию системы хранения при помощи команды:

```
# dd if=/dev/zero of=/dev/mapper/LUN_ID bs=1M count=200 oflag=direct
```

где */dev/mapper/LUN_ID* - путь до LUN

! Будьте аккуратны при выполнении этой операции: не выполняйте её на LUN, содержащим важные данные. Подробнее об этом поведении можно ознакомиться в пункте 2.5.5.4 руководства администратора.

3.1.1 Подготовка хранилища NFS

Следующие шаги универсальны для всех операционных систем. Для уточнения конкретных шагов обратитесь к официальному руководству ОС или порталу техподдержки.

! Если в качестве ОС используется не zVirt Node, то необходимо выполнить следующие шаги:

1. Создать служебных пользователей и группы:

```
# groupadd sanlock -g 179
# groupadd kvm -g 36
# useradd sanlock -u 179 -g 179 -G kvm
# useradd vdsm -u 36 -g 36 -G sanlock
```

2. Создать каталог (должно быть доступно более 55 Гб свободного места):

```
# mkdir –p /storage/he
```

3. Установить права доступа:

```
# chown 36:36 /storage/he
# chmod 0775 /storage/he
```

4. Опубликовать папку, прописав ее в конфигурационном файле NFS-сервера:

```
# echo "/storage/he *(rw,anonuid=36,anongid=36)" > /etc/exports
```

5. Убедиться в правильности задания параметров доступа:

```
# cat /etc/exports
```

6. Запустить необходимые сервисы:

```
# systemctl enable nfs-server
# systemctl enable rpcbind
# systemctl enable nfs-blkmap
# systemctl restart nfs-server
# systemctl restart rpcbind
# systemctl restart nfs-blkmap
```

7. Создать правила межсетевого экрана для обеспечения доступности хранилища для других хостов:

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

3.1.2 Подготовка хранилища iSCSI

zVirt поддерживает хранилище iSCSI, которое представляет собой домен хранения, созданный из группы томов, состоящей из LUN. Группы томов и LUN не могут быть одновременно подключены к нескольким доменам хранения.

Если вы используете блочное хранилище и намереваетесь развернуть виртуальные машины на необработанных устройствах или прямых логических устройствах и управлять ими с помощью диспетчера логических томов, необходимо 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. Справочная информация по созданию фильтра LVM доступна в файле */etc/lvm/lvm.conf*.

В настоящее время zVirt не поддерживает хранилище с размером блока 4K. Вы должны сконфигурировать хранилище блоков в устаревшем режиме (512b block).

Если ваш хост загружается из хранилища SAN и теряет связь с хранилищем, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления соединения.

Чтобы предотвратить эту ситуацию, zVirt рекомендует добавить в корневую файловую систему SAN файл конфигурации с multipath для загрузочного LUN, чтобы обеспечить его постановку в очередь при наличии соединения:

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
    multipath {
        wwid LUN_ID
        no_path_retry queue
    }
```

3.1.3 Подготовка FCP-хранилища

zVirt поддерживает хранилище SAN, создавая домен хранилища из группы томов, состоящей из существующих LUN. Ни группы томов, ни LUN не могут быть подключены более чем к одному домену хранения одновременно.

Если вы используете блочное хранилище и намереваетесь развернуть виртуальные машины на необработанных устройствах или прямых логических устройствах и управлять ими с помощью диспетчера логических томов, необходимо 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. Справочная информация по созданию фильтра LVM доступна в файле */etc/lvm/lvm.conf*.

В настоящее время zVirt не поддерживает хранилище с размером блока 4K. Вы должны сконфигурировать хранилище блоков в устаревшем режиме (512b block).

Если ваш хост загружается из хранилища SAN и теряет связь с хранилищем, файловые системы хранилища становятся доступными только для чтения и остаются в этом состоянии после восстановления соединения.

Чтобы предотвратить эту ситуацию, zVirt рекомендует добавить в корневую файловую систему SAN файл конфигурации с multipath для загрузочного LUN, чтобы обеспечить его постановку в очередь при наличии соединения:

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
    multipath {
        wwid LUN_ID
        no_path_retry queue
    }
```

3.1.4 Подготовка Gluster Storage

Информацию по настройке Gluster Storage см. в официальной документации, учитывая следующие особенности:

! Тома Gluster Storage должны использовать либо трехстороннюю репликацию, либо арбитражную репликацию. Это снижает риск возникновения split-brain в кластере. Поддерживаются следующие типы томов:

- трехсторонне реплицированные и распределенные реплицированные тома (replica count 1)
- арбитражные реплицированные или распределенные арбитражные реплицированные тома (replica 3 arbiter 1)

Дополнительно необходимо назначить следующие настройки для тома:

```
# gluster volume set VOLUME_NAME group virt
# gluster volume set VOLUME_NAME performance.strict-o-direct on
# gluster volume set VOLUME_NAME network.remote-dio off
# gluster volume set VOLUME_NAME storage.owner-uid 36
# gluster volume set VOLUME_NAME storage.owner-gid 36
# gluster volume set VOLUME_NAME network.ping-timeout 30
```

4. УСТАНОВКА

4.1 Описание процесса установки

Установка службы включает в себя следующие шаги:

1. Подготовка хранилища для домена хранения HostedEngine и для стандартных доменов хранения. Вы можете использовать один из следующих типов хранения:
   a) NFS
   b) ISCSI
   c) Fibre Channel (FCP)
   d) Gluster Storage
2. Установка ОС хоста. Этот хост станет первым хостом с размещенным на нем менеджером управления.
3. Установка и настройка менеджера управления.

4.2 Подготовка хранилища

Подготовка хранилища описана в разделе *3.1* Подготовка хранилища

4.3 Установка хоста виртуализации

zVirt Node - это минимальная операционная система, основанная на Enterprise Linux, предназначенная для обеспечения простого метода настройки физической машины для работы в качестве гипервизора в среде zVirt. Минимальная операционная система содержит только пакеты, необходимые для работы компьютера в качестве гипервизора, и имеет веб-интерфейс *Cockpit* для мониторинга хоста и выполнения административных задач.

Хост должен соответствовать минимальным требованиям к оборудованию. Требования к оборудованию описаны в разделе *2.1*

Процедура:

1. Загрузите zVirt Node.
   a. Обратитесь к репозиторию и загрузите последнюю доступную версию zVirt (для доступа к странице загрузки и репозиторию zVirt необходимо получить учетные данные для входа).
   b. Запишите ISO-образ zVirt Node на USB, CD или DVD.
2. Запустите компьютер, на котором вы устанавливаете ОС, загрузившись с подготовленного установочного носителя.
3. В меню загрузки выберите Install Node и нажмите Enter.
4. Выберите язык и нажмите «Продолжить».
5. Выберите часовой пояс на экране «Дата и время» и нажмите «Готово».
6. Выберите раскладку клавиатуры на экране клавиатуры и нажмите «Готово».
7. Выберите устройство, на которое нужно установить узел, в окне «Место назначения установки». При желании включите шифрование. Выберите «Автоматическое разбиение» и нажмите «Готово».
8. Выберите сеть из сети и хост - имя экрана и нажмите кнопку «Настроить» ..., чтобы настроить параметры соединения. Установите флажок «Автоматически подключаться к этой сети, если он доступен». Введите имя хоста в поле «Имя хоста» и нажмите «Готово».
9. При необходимости настройте поддержку языков, политику безопасности и Kdump.
10. Нажмите «Начать установку».

11. Установите пароль пользователя root.

    ! Настоятельно не рекомендуется создавать обычных пользователей, так как это может привести к использованию локальных уязвимостей безопасности.

4.4 Установка среды виртуализации

4.4.1 Установка в режиме Hosted Engine с помощью командной строки

1. Подготовьте полные доменные имена менеджера управления виртуализации и хостов перед развертыванием. Записи прямого и обратного просмотра должны быть установлены в DNS.

   Заполните для себя по аналогии следующую таблицу:

Таблица 6. Выбор имен для развертывания

Объект	FQDN	IP адрес
Менеджер управления	zvirtvm.infoland.local	172.25.1.186
Хост 1	host1.infoland.local	172.25.1.181
Хост 2	host2.infoland.local	172.25.1.182
Хост 3	host3.infoland.local	172.25.1.183

После установки имя HostedEngine будет являться именем виртуальной машины с менеджером управления и адресом веб-интерфейса управления. Задаваемый адрес должен быть свободен.

В случае невозможности использования внешнего DNS добавьте в файл */etc/hosts* IP-адреса и FQDN хоста виртуализации и разворачиваемого менеджера управления.

2. Включите репозиторий:

```
# dnf config-manager --enable zvirt-3.0
```

3. Настройте репозиторий:

```
# zvirt-credentials -u USERNAME -p PASSWORD
или
# zvirt-credentials --username=USERNAME --password=PASSWORD
```

   При этом доступ к репозиторию будет настроен на использование учетных данных, значения которых сохранятся в файлах */etc/yum/vars/zuser* и */etc/yum/vars/zpasswd*. В противном случае потребуется ручное указание параметров username и password в файле */etc/yum.repos.d/zvirt.repo*.

4. Проверьте правильность подключения репозитория. Следующие команды должны отработать без ошибок, напротив репозитория должно стоять ненулевое число:

```
# dnf clean all
# dnf repolist all
```

5. Выполните обновление:

```
# dnf update
```

6. Установите пакет *ovirt-engine-appliance*:

```
# dnf install -y ovirt-engine-appliance
```

! В случае отсутствия доступа к сети Интернет на хосте, необходимо скачать пакет ovirt-engine-appliance по ссылке http://repo-zvirt.infoland.ru/repository/updates/zvirt/ovirt-engine-appliance-latest.rpm, после чего перенести его на хост любым удобным способом в папку /root и затем установить:

```
# dnf localinstall -y /root/ovirt-engine-appliance-latest.rpm
```

7. Запустите процесс установки:

```
# hosted-engine --deploy
```

8. Следуйте сообщениям в консоли:

```
[root@host1 ~]# hosted-engine --deploy
[ INFO ] Stage: Initializing
[ INFO ] Stage: Environment setup
          During customization use CTRL-D to abort.
          Continuing will configure this host for serving as hypervisor and will
create a local VM with a running engine.
          The locally running engine will be used to configure a new storage
domain and create a VM there.
          At the end the disk of the local VM will be moved to the shared storage.
          Are you sure you want to continue? (Yes, No) [Yes]: Enter
# Подтвердите готовность установить Engine на данный хост.
          It has been detected that this program is executed through an SSH
connection without using screen.
          Continuing with the installation may lead to broken installation if the
network connection fails.
          It is highly recommended to abort the installation and run it inside a
screen session using command "screen".
          Do you want to continue anyway? (Yes, No) [No]: Yes
# Предупреждение об использовании ssh. При сбое сетевого подключения произойдет
сбой установки.
          Configuration files: []
          Log file: /var/log/zvirt-hosted-engine-setup/zvirt-hosted-engine-setup-
20200319163815-bm0sa2.log
# По данному пути находится лог текущей установки.

          --== STORAGE CONFIGURATION ==--
          --== HOST NETWORK CONFIGURATION ==--

          Please indicate the gateway IP address [172.25.1.254]: Enter
# Введите или подтвердите адрес шлюза
          Please indicate a nic to set ovirt mgmt bridge on: (eth0) [eth0]: Enter
# Укажите мсетевой интерфейс, который будет использоваться для создания bridge для
ВМ.
          Please specify which way the network connectivity should be checked
(ping, dns, tcp, none) [dns]: Enter
# Укажите, каким образом будет выполняться проверка сети.
# !!!Используйте только dns.
          --== VM CONFIGURATION ==--
          Please enter the name of the datacenter where you want to deploy this
hosted-engine host. [Default]: ]: Enter
```

```
# Укажите название создаваемого центра данных.
          Please enter the name of the cluster where you want to deploy this
hosted-engine host. [Default]: Enter
# Укажите название создаваемого центра данных.
          If you want to deploy with a custom engine appliance image,
          please specify the path to the OVA archive you would like to use
          (leave it empty to skip, the setup will use ovirt-engine-appliance rpm
installing it if missing):  Enter
# Здесь указывается путь к ova файлу, в стандартном сценарии строку нужно оставить
пустой.
          Please specify the number of virtual CPUs for the VM (Defaults to
appliance OVF value): [4]: Enter
# Укажите количество vCPU, выделенных для ВМ с сервером управления.
          Please specify the memory size of the VM in MB (Defaults to maximum
available): [4759]: Enter
# Укажите количество оперативной памяти, выделенной для ВМ с сервером управления.
[ INFO ] Detecting host timezone.
          Please provide the FQDN you would like to use for the engine.
          Note: This will be the FQDN of the engine VM you are now going to
launch,
          it should not point to the base host or to any other existing machine.
          Engine VM FQDN: []: zvirtvm.infoland.local
# Введите имя для ВМ Engine.
          Please provide the domain name you would like to use for the engine
appliance.
          Engine VM domain: [infoland.local] Enter
# Введите домен, в котором будет находиться сервер управления.
          Enter root password that will be used for the engine appliance: Password
# Введите пароль для пользователя root ВМ Engine.
          Confirm appliance root password: Password
# Подтвердите пароль.
          You may provide an SSH public key, that will be added by the deployment
script to the authorized_keys file of the root user in the engine appliance.
          This should allow you password less login to the engine machine
after deployment.
          If you provide no key, authorized_keys will not be touched.
          SSH public key []: Enter
# Введите открытый ключ ssh для пользователя root, который будет использоваться
для ВМ с сервером управления.
[WARNING] Skipping appliance root ssh public key
          Do you want to enable ssh access for the root user (yes, no, without-
password) [yes]: Enter
# Хотите ли вы включить доступ по ssh для пользователя root.
          Do you want to apply a default OpenSCAP security profile (Yes, No) [No]:
Enter
# Хотите ли вы применить профиль безопасности OpenSCAP.
          You may specify a unicast MAC address for the VM or accept a randomly
generated default [00:16:3e:24:4d:60]: Enter
# Подтвердите сгенерированный mac адрес для ВМ или введите свой.
          How should the engine VM network be configured (DHCP, Static)[DHCP]?
Static
# Используйте статическую конфигурацию сети ВМ Engine.
          Please enter the IP address to be used for the engine VM []:
172.25.1.186
# Введите IP адрес ВМ Engine.
[ INFO ] The engine VM will be configured to use 172.25.1.186/24
```

```
          Please provide a comma-separated list (max 3) of IP addresses of domain
name servers for the engine VM
          Engine VM DNS (leave it empty to skip) [172.25.1.1]: Enter
# Подтвердите или введите адрес DNS сервера.
          Add lines for the appliance itself and for this host to /etc/hosts on
the engine VM?
          Note: ensuring that this host could resolve the engine VM hostname is
still up to you
          (Yes, No)[No] Yes
# Добавить ли запись о хосте в файл hosts на ВМ Engine?

          --== HOSTED ENGINE CONFIGURATION ==--

          Please provide the name of the SMTP server through which we will send
notifications [localhost]: Enter
# Введите имя SMTP сервера, через который будут отсылаться уведомления.
          Please provide the TCP port number of the SMTP server [25]: Enter
# Введите порт для SMTP сервера.
          Please provide the email address from which notifications will be sent
[root@localhost]: Enter
# Введите e-mail адрес, откуда будут отсылаться уведомления.
          Please provide a comma-separated list of email addresses which will get
notifications [root@localhost]: Enter
# Введите список адресов e-mail через запятую, которые будут получать уведомления.
          Enter engine admin password: Password
# Введите пароль для пользователя admin на сервере управления.
          Confirm engine admin password: Password
# Подтвердите пароль
[ INFO ] Stage: Setup validation
          Please provide the hostname of this host on the management network
[host1.infoland.local]: Enter
# Укажите имя хоста в сети управления.
--------------------------------------------------------------------------------
                                Процесс установки
--------------------------------------------------------------------------------
          Please specify the storage you would like to use (glusterfs, iscsi, fc,
nfs)[nfs]: Enter
# Введите тип хранилища, которое вы хотите использовать для размещения ВМ с
сервером управления.
          Please specify the nfs version you would like to use (auto, v3, v4,
v4_1)[auto]: Enter
#Укажите версию протокола nfs, если это необходимо.
          Please specify the full shared storage connection path to use (example:
host:/path): storage.infoland.local:/storage/he
# Укажите правильный путь к сетевому ресурсу.
          If needed, specify additional mount options for the connection to the
hosted-engine storage domain (example: rsize=32768,wsize=32768) []:Enter
# При необходимости укажите дополнительные параметры монтирования.
         Please specify the size of the VM disk in GiB: [51]: Enter
# Укажите другой размер диска для ВМ HostedEngine, если это необходимо.
[ INFO ] Creating Storage Domain
# После успешного разворачивания сервера виртуализации будет выведено сообщение:
[ INFO ] Hosted Engine successfully deployed
```

4.4.2 Установка в режиме Hosted Engine с помощью веб-интерфейса Cockpit

! Если планируется установка в iSCSI-хранилище, рекомендуем произвести установку при помощи командной строки, см. «4.4.1 Установка в режиме Hosted Engine с помощью командной строки».

1. Подготовьте полные доменные имена менеджера управления виртуализации и хостов перед развертыванием. Записи прямого и обратного просмотра должны быть установлены в DNS.
   Заполните для себя по аналогии следующую таблицу:

Таблица 7. Выбор имен для развертывания

Объект	FQDN	IP адрес
Менеджер управления	zvirtvm.infoland.local	172.25.1.186
Хост 1	host1.infoland.local	172.25.1.181
Хост 2	host2.infoland.local	172.25.1.182
Хост 3	host3.infoland.local	172.25.1.183

После установки имя HostedEngine будет являться именем виртуальной машины с менеджером управления и адресом веб-интерфейса управления. Задаваемый адрес должен быть свободен.

В случае невозможности использования внешнего DNS добавьте в файл */etc/hosts* IP-адреса и FQDN хоста виртуализации и разворачиваемого менеджера управления.

2. Перейдите в веб-интерфейс управления хостом виртуализации *Cockpit*. Сервис доступен по доменному имени сервера и порту 9090. Например, https://host1.infoland.local:9090/.

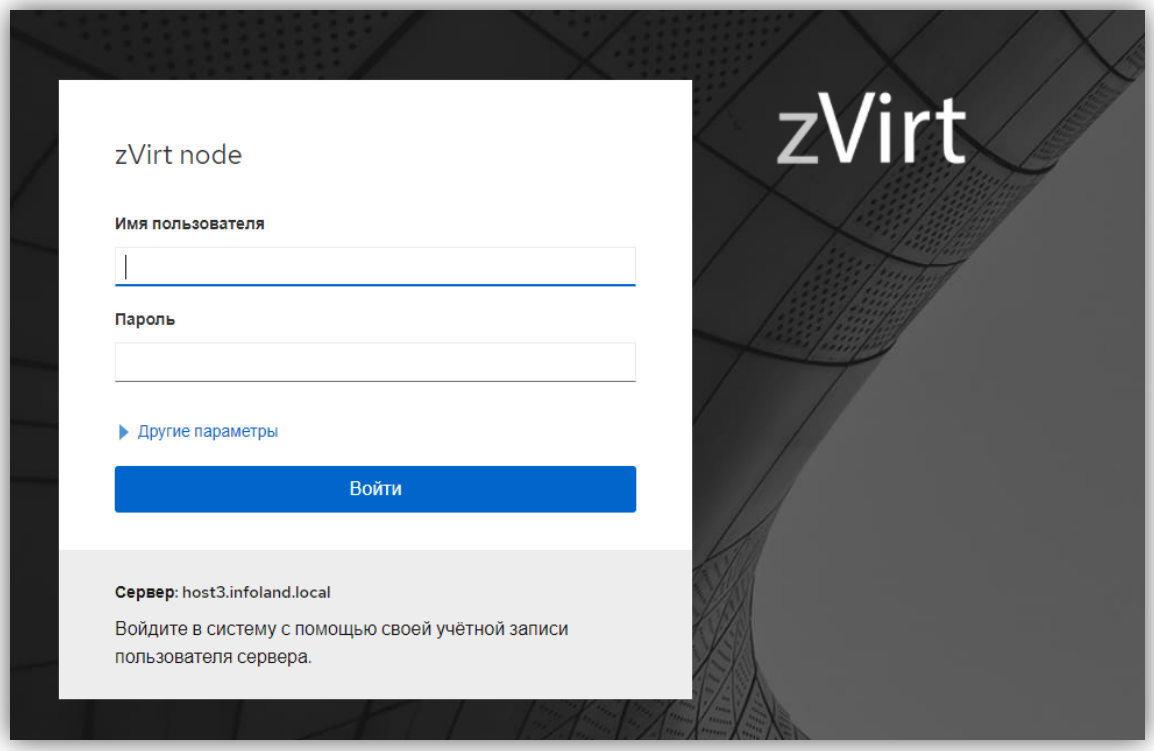

Рисунок 3. Окно аутентификации.

3. Выберите из основного списка вкладку «Терминал» для выполнения нижеуказанных команд.

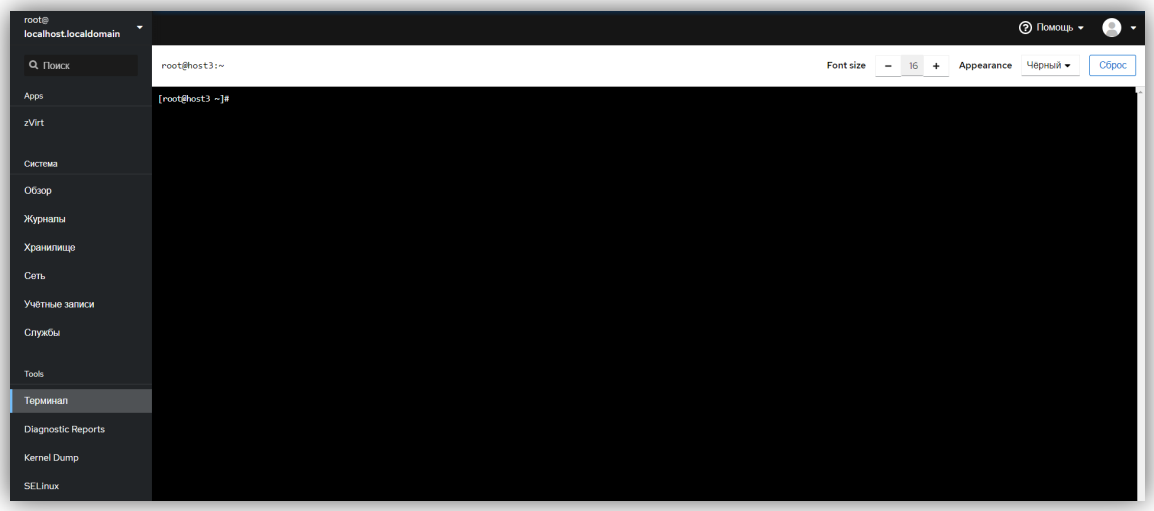

Рисунок 4. Терминал в веб-интерфейсе Cockpit.

4. Включите репозиторий:

```
# dnf config-manager --enable zvirt-3.0
```

5. Настройте репозиторий:

```
# zvirt-credentials -u USERNAME -p PASSWORD
или
# zvirt-credentials --username=USERNAME --password=PASSWORD
```

   При этом доступ к репозиторию будет настроен на использование учетных данных, значения которых сохранятся в файлах */etc/yum/vars/zuser* и */etc/yum/vars/zpasswd*. В противном случае потребуется ручное указание параметров username и password в файле */etc/yum.repos.d/zvirt.repo*.

6. Проверьте правильность подключения репозитория. Следующие команды должны отработать без ошибок, напротив репозитория должно стоять ненулевое число:

```
# dnf clean all
# dnf repolist all
```

7. Выполните обновление:

```
# dnf update
```

8. Выберите из основного списка вкладку «zVirt», далее Hosted Engine и нажмите «Запустить» для запуска процесса развертывания среды виртуализации в режиме Hosted Engine.

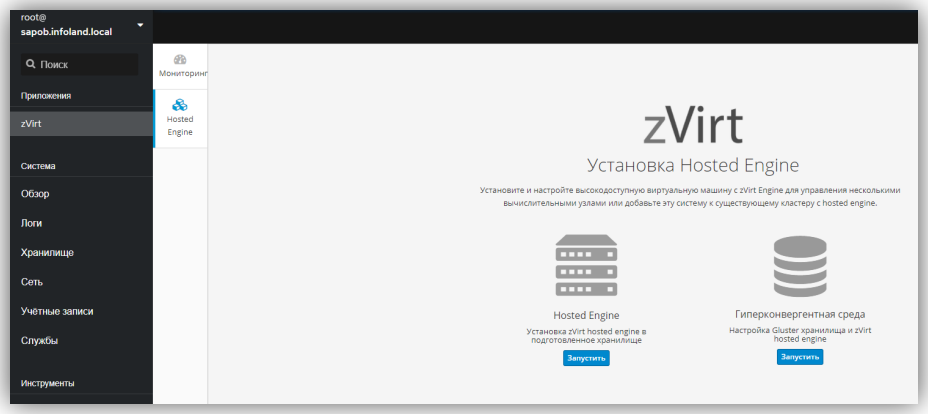

Рисунок 5. Меню развертывания среды виртуализации.

9. Заполните поля для настройки ВМ HostedEngine.

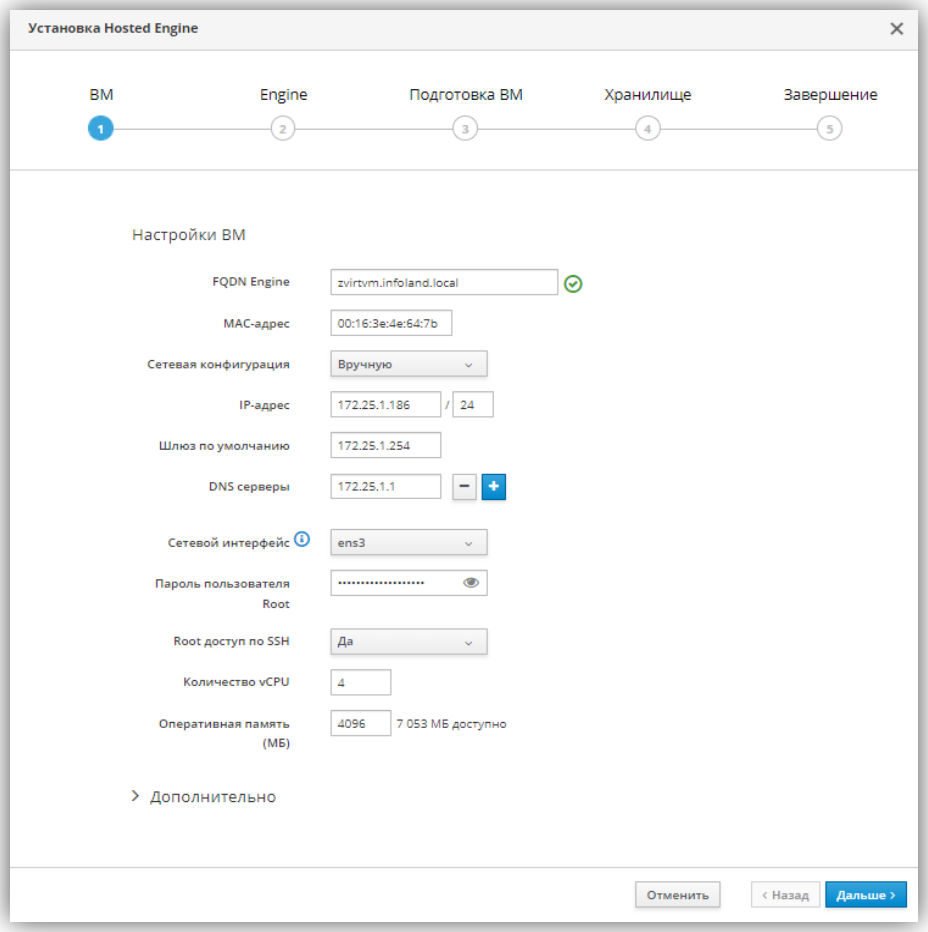

Рисунок 6. Основные настройки для ВМ Engine.

10. Укажите пароль для учётной записи администратора (root) для ВМ HostedEngine и определите параметры оповещения.

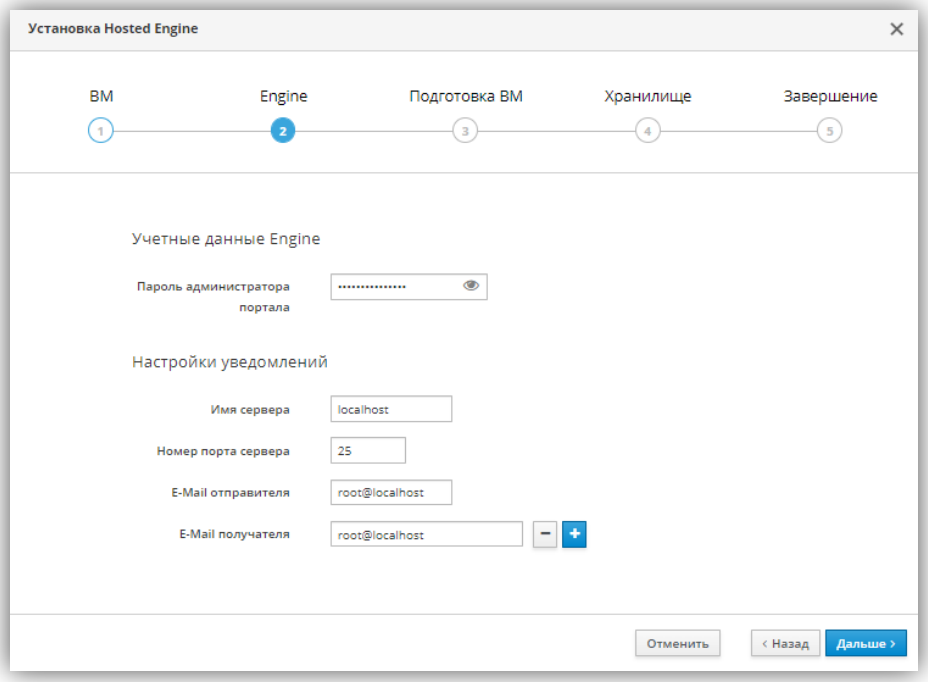

Рисунок 7. Настройка учётной записи администратора и оповещений.

11. Проверьте конфигурацию, если она корректна, нажмите на кнопку «Подготовить ВМ».

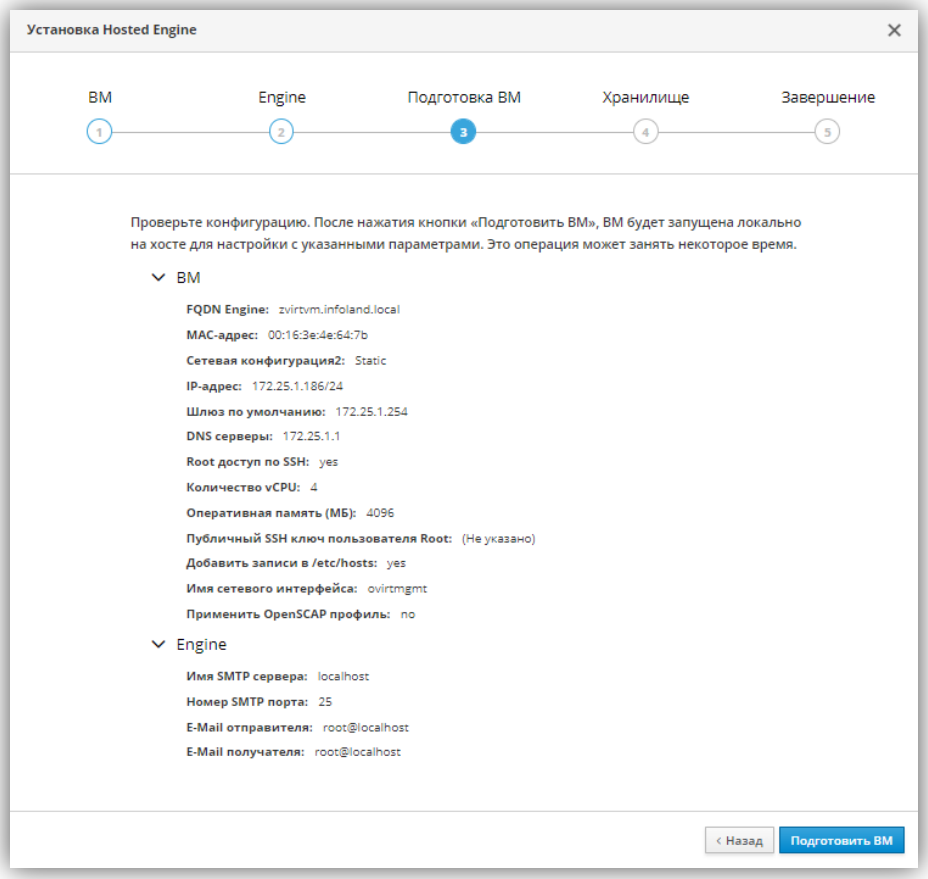

Рисунок 8. Предварительная конфигурация ВМ.

12. Процесс подготовки и создания ВМ HostedEngine.

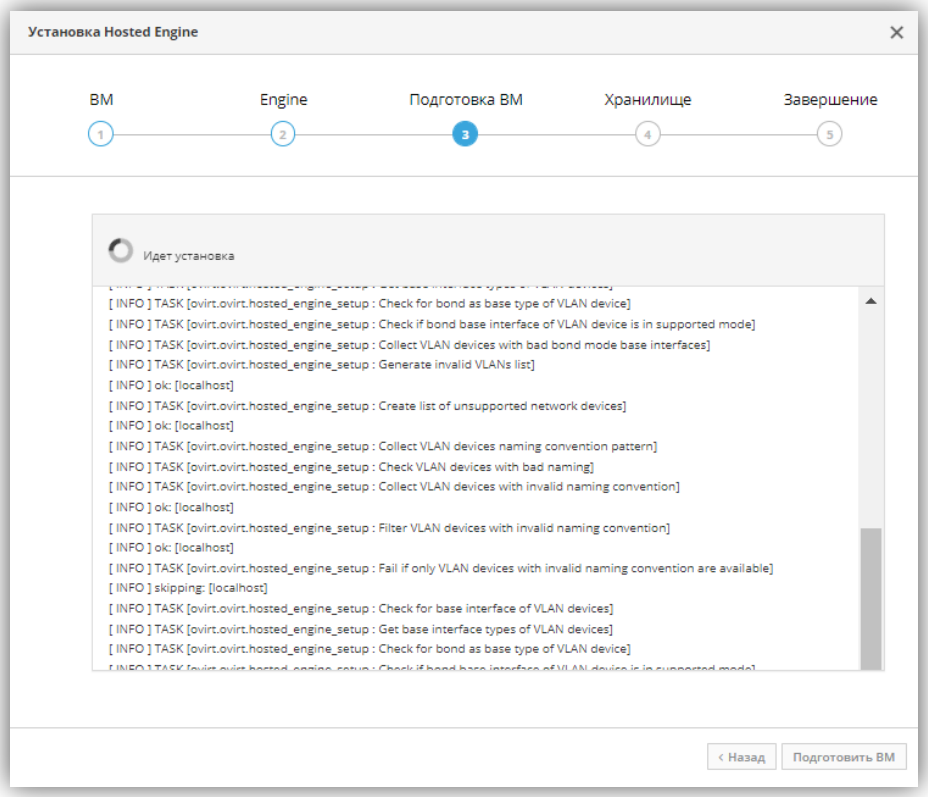

Рисунок 9. Процесс подготовки и создания ВМ HostedEngine.

13. Завершение процесса подготовки и создания ВМ HostedEngine.

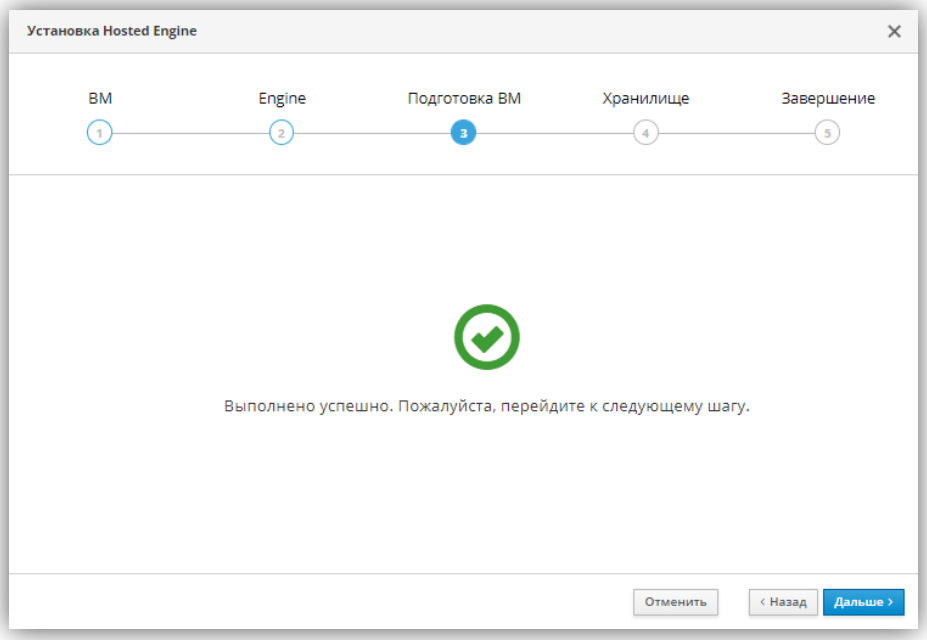

Рисунок 10. Завершение процесса подготовки и создания ВМ HostedEngine.

14. Выполните настройку домена хранения для ВМ HostedEngine.

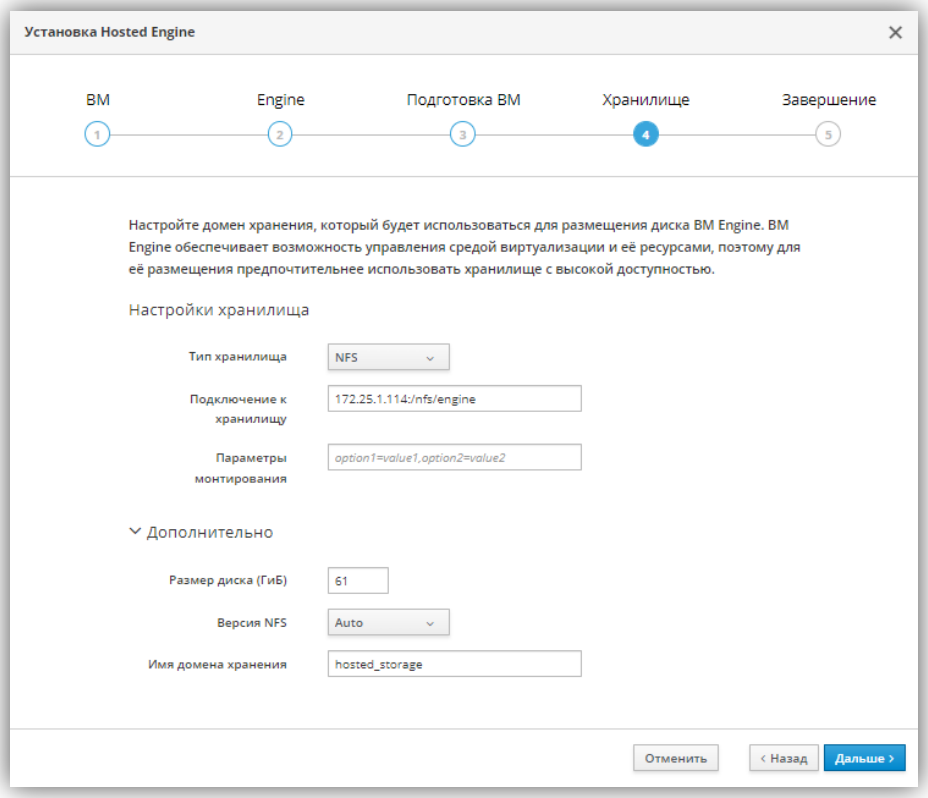

Рисунок 11. Настройка домена хранения.

15. Проверьте итоговую конфигурацию, если она корректна, нажмите на кнопку «Завершить установку».

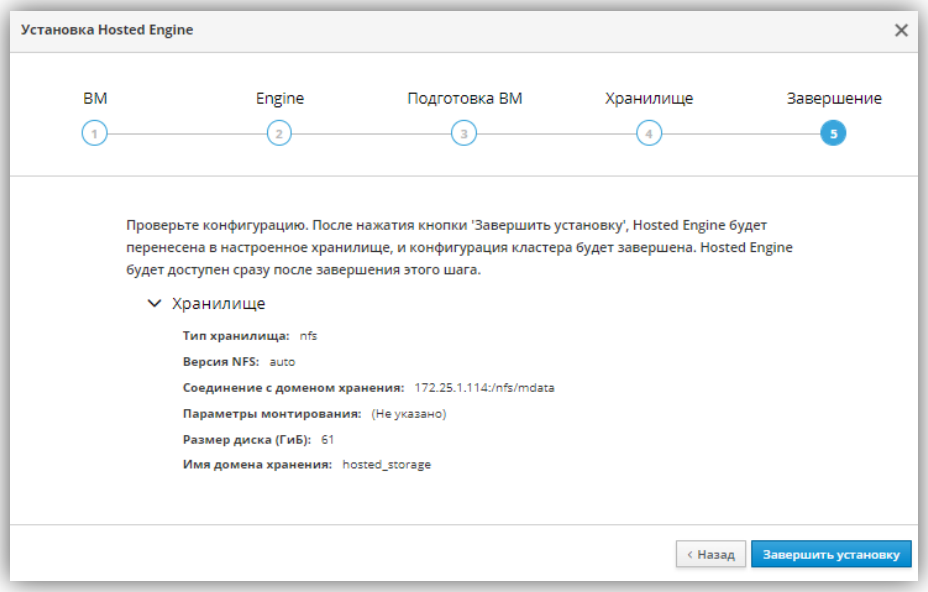

Рисунок 12. Предварительная конфигурация хранилища.

16. Процесс развертывания среды виртуализации в режиме Hosted Engine.

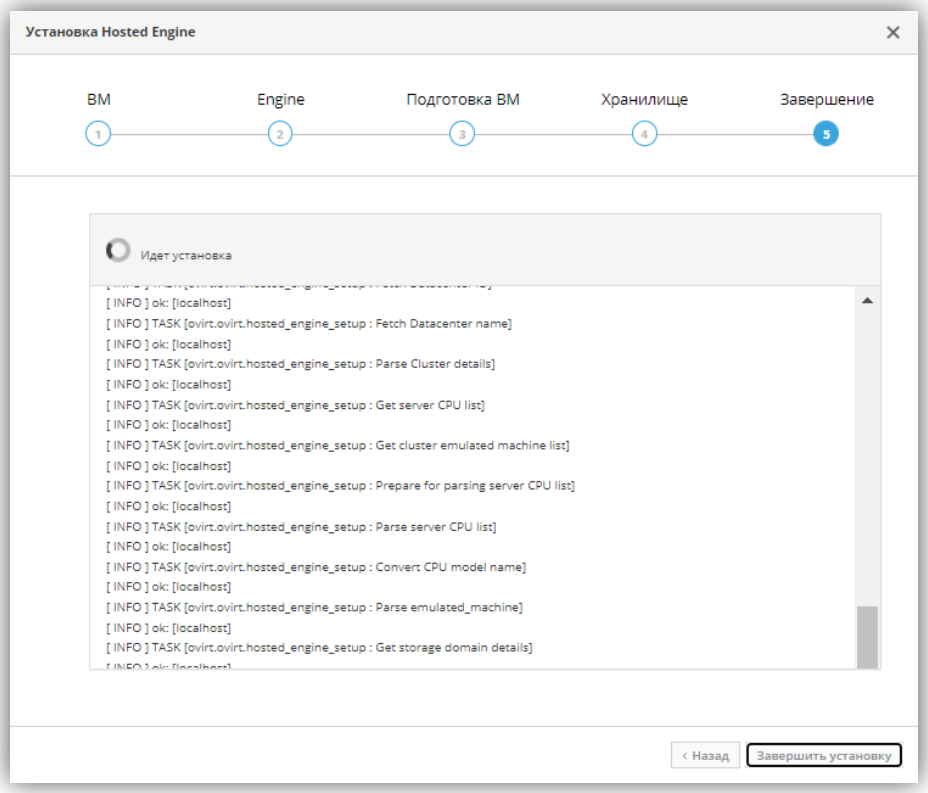

Рисунок 13. Процесс развертывания среды виртуализации.

17. После успешного развертывания Вы увидите сообщение.

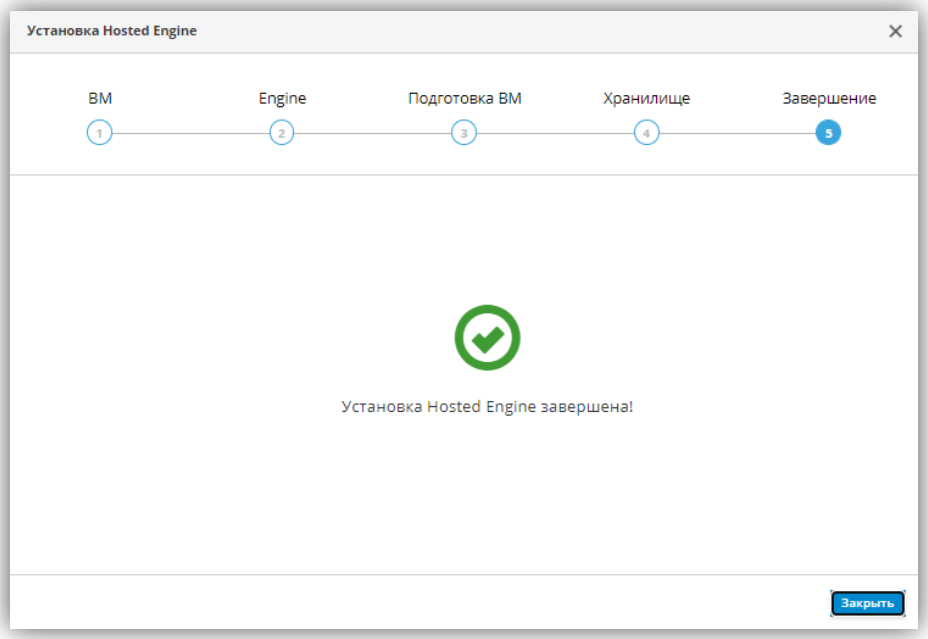

Рисунок 14. Оповещение при успешном развертывании.

4.4.3 Установка гиперконвергентной среды виртуализации в режиме Hosted Engine с помощью веб-интерфейса Cockpit

Гиперконвергентный вариант развертывания среды виртуализации объединяет вычислительные возможности, хранилища, сети хостов и предоставляет управление инфраструктурой в веб-интерфейсе.

Хосты должны иметь минимум два сетевых интерфейса для разделения трафика на общедоступную сеть и сеть хранения.

Поддерживаются только RAID5 и RAID6.

1. Подготовьте полные доменные имена менеджера управления виртуализации и хостов перед развертыванием. Записи прямого и обратного просмотра должны быть установлены в DNS.
2. Необходимо использовать внешние и внутренние FQDN для разделения трафика, например, первый хост, имеющий *hostname* mhost1.infoland.local, с ip – адресом 172.25.1.181 на первом сетевом интерфейсе, должен быть доступен по доменному имени ghost1.infoland.local через второй сетевой интерфейс с ip – адресом 172.25.4.181.

Заполните для себя по аналогии следующую таблицу:

Таблица 8. Выбор имен для развертывания

Объект	FQDN	IP адрес
Менеджер управления	zvirtvm.infoland.local	172.25.1.186
Хост 1	mhost1.infoland.local	172.25.1.181
	ghost1.infoland.local	172.25.4.181
Хост 2	mhost2.infoland.local	172.25.1.182
	ghost2.infoland.local	172.25.4.182
Хост 3	mhost3.infoland.local	172.25.1.183
	ghost3.infoland.local	172.25.4.183

После установки имя HostedEngine будет являться именем виртуальной машины с менеджером управления и адресом веб-интерфейса управления. Задаваемый адрес должен быть свободен.

В случае невозможности использования внешнего DNS добавьте в файл */etc/hosts* IP-адреса и FQDN хоста виртуализации и разворачиваемого менеджера управления.

В процессе развертывания необходимо настроить SSH - аутентификацию используя беспарольный публичный ключ пользователя *root* для всех хостов. Это необходимо сделать для всех интерфейсов (общедоступной сети и сети хранения), а также для IP-адресов и полных доменных имен.

3. Перейдите в веб-интерфейс управления хостом виртуализации Cockpit.

Используйте учетную запись *root*. Сервис доступен по доменному имени сервера и порту 9090. Например, *https://mhost1.infoland.local:9090/*.

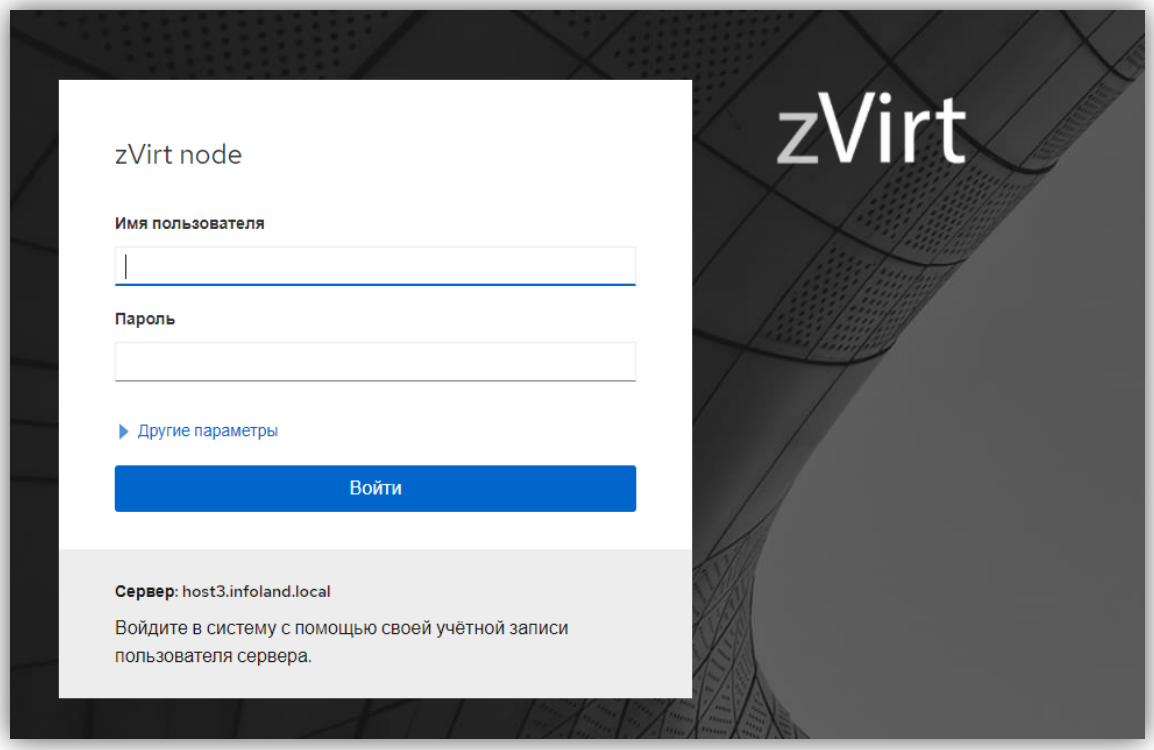

Рисунок 15. Окно аутентификации.

4. Выберите из основного списка вкладку «Терминал» для выполнения нижеуказанных команд.

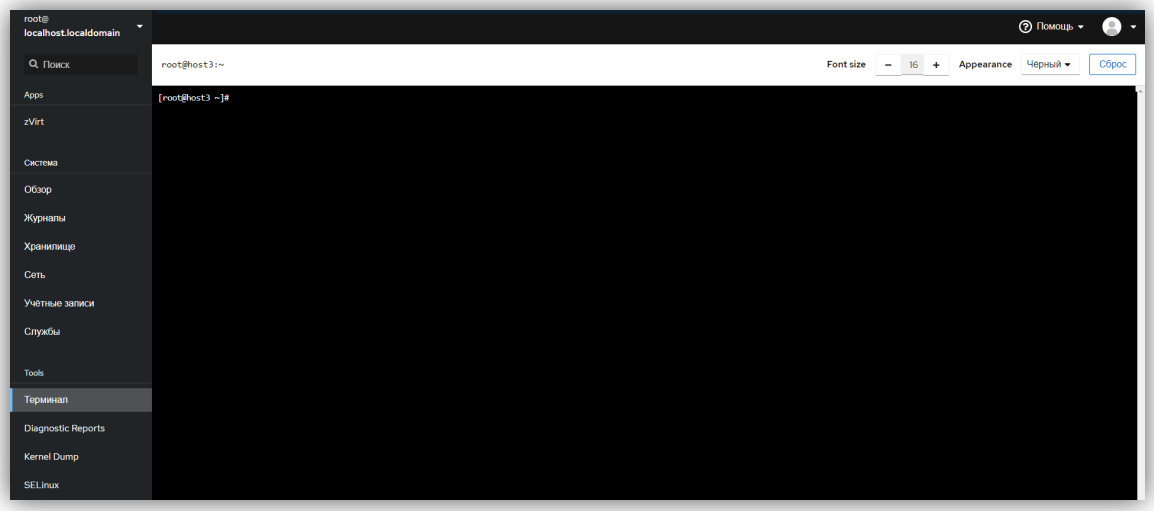

Рисунок 16. Терминал в веб-интерфейсе Cockpit.

5. Включите репозиторий:

```
# dnf config-manager --enable zvirt-3.0
```

6. Настройте репозиторий:

```
# zvirt-credentials -u USERNAME -p PASSWORD
или
# zvirt-credentials --username=USERNAME --password=PASSWORD
```

При этом доступ к репозиторию будет настроен на использование учетных данных, значения которых сохранятся в файлах */etc/yum/vars/zuser* и */etc/yum/vars/zpasswd*. В противном случае потребуется ручное указание параметров *username* и *password* в файле */etc/yum.repos.d/zvirt.repo*.

7. Проверьте правильность подключения репозитория. Следующие команды должны отработать без ошибок, напротив репозитория должно стоять ненулевое число:

```
# dnf clean all
# dnf repolist all
```

8. Выполните обновление:

```
# dnf update
```

9. Сгенерируйте беспарольный ключ:

```
# ssh-keygen -t rsa
```

В процессе генерации будет предложено указать каталог для хранения ключа или выбрать каталог по умолчанию.

Не используйте парольную фразу.

10. Скопируйте полученный открытый ключ на каждый хост, к которому вы хотите получить доступ, включая хост, на котором вы выполняете команду, используя как внешние, так и внутренние полные доменные имена.

Синтаксис команды:

```
# ssh-copy-id -i <расположение ключа>/<имя ключа>.pub <пользователь>@<имя хоста>
```

Пример выполнения копирования ключа:

```
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@mhost1.infoland.local
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@mhost2.infoland.local
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@mhost3.infoland.local
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@ghost1.infoland.local
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@ghost2.infoland.local
# ssh-copy-id -i /root/.ssh/id_rsa.pub root@ghost3.infoland.local
```

Перед развертыванием убедитесь, что сервис *multipath* не использует локальные диски, которые подготовлены для Gluster Storage. Информацию см. в *Отключение multipath для работы дополнительных дисков.*

11. Выберите из основного списка вкладку «zVirt», далее «Гиперконвергентная среда» и нажмите «Запустить» для запуска процесса подготовки хранилища.

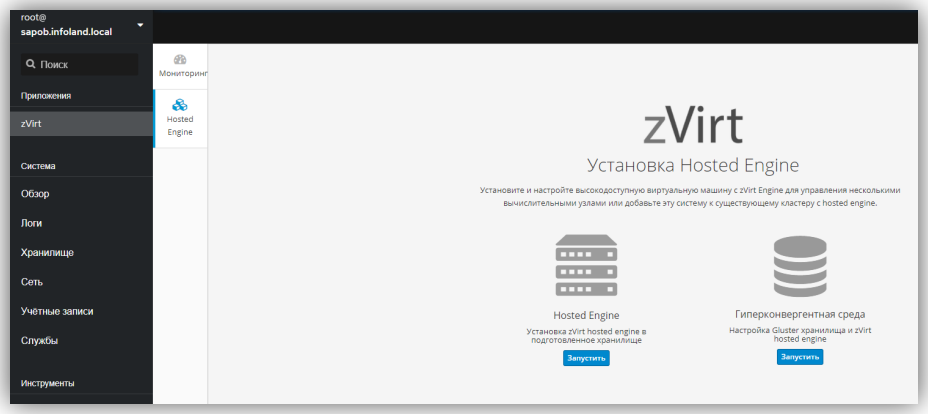

Рисунок 17. Меню развертывания среды виртуализации.

12. Укажите полные доменные имена хостов, которые будут использоваться для общедоступной сети и сети хранения.

    Если хосты используют только одну сеть, включите опцию «Используется одно и тоже имя хоста для общедоступной сети и сети хранения».

    Если хосты используют сеть IPv6, включите опцию «Хосты используют IPv6 (по умолчанию IPv4). Перед включением опции убедитесь, что хосты используют полные доменные имена. Указание IPv6 адресов не поддерживается.

    В поле «Хост 1» укажите полное доменное имя гиперконвергентного хоста, который используя беспарольную SSH - аутентификацию может подключаться к другим хостам.

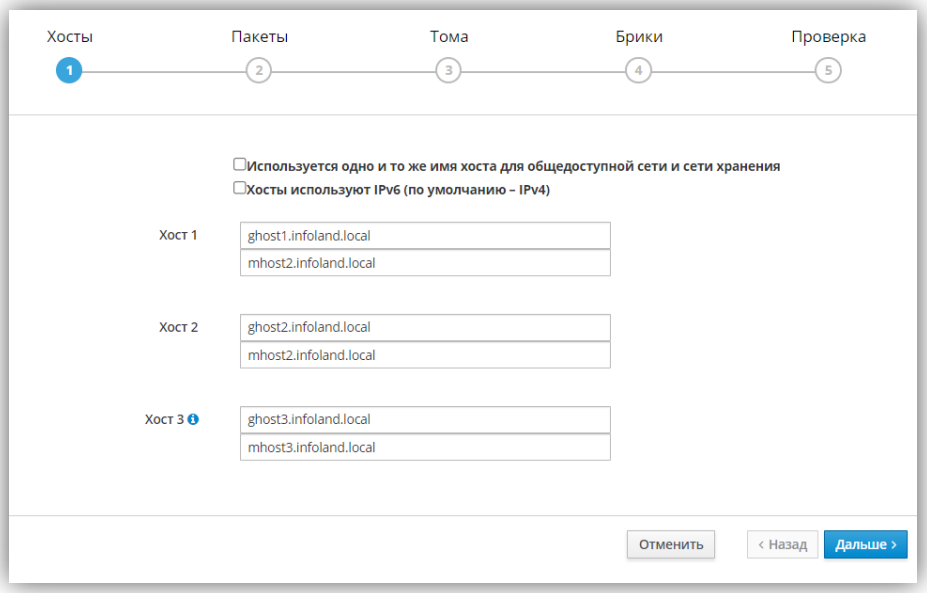

Рисунок 18. Вкладка «Хосты».

13. На вкладке «Выбор пакетов» возможно установить дополнительные пакеты на всех хостах.

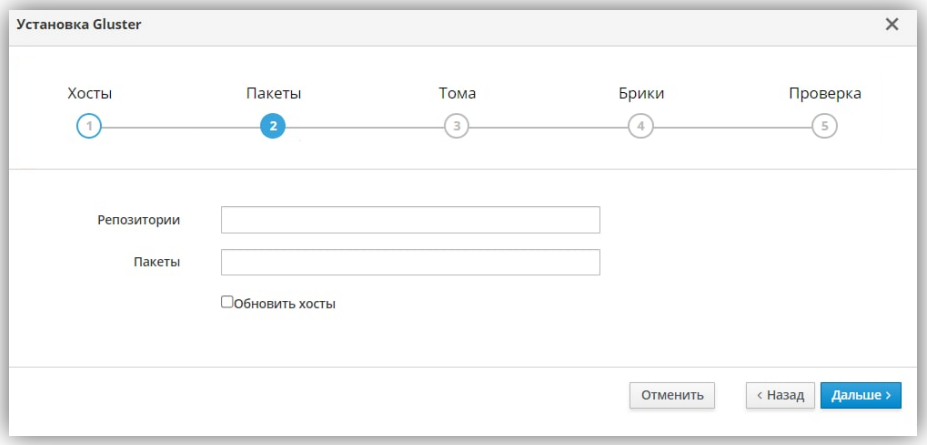

Рисунок 19. Вкладка «Пакеты».

14. На вкладке «Тома» определяются тома, которые будут созданы. Указанные тома будут использоваться для создания доменов хранения в zVirt.

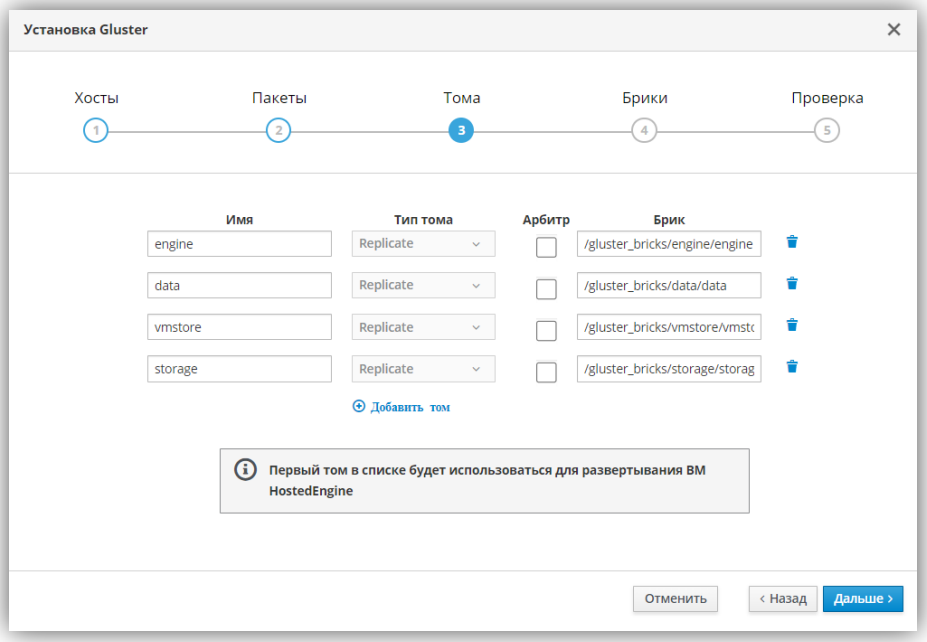

Рисунок 20. Вкладка «Тома».

15. Укажите для каждого хоста устройства, на которых будут созданы брики.

    Если устройства, используемые для бриков, настроены как устройства RAID, укажите это в параметре «Тип RAID».

    Опция «Черный список устройств Gluster» запрещает использовать для диска имя в формате multipath. Если вы хотите использовать имя устройства в формате multipath, не используйте эту опцию и укажите имя устройства в формате */dev/mapper/<WWID>.*
    Если на хостах различаются имена или размеры устройств, используйте выпадающее меню «Хост» для определения устройств для каждого хоста.

    В поле «Имя устройства» укажите необработанное устройство в формате - */dev/sdc*, которое будет использоваться для создания томов.
    Используйте формат - */dev/mapper/<WWID>* для multipath - устройств.

    При необходимости настройте LV Cache. Этот параметр позволяет использовать для *lvmcache* SSD диски, если для бриков используются HDD диски.

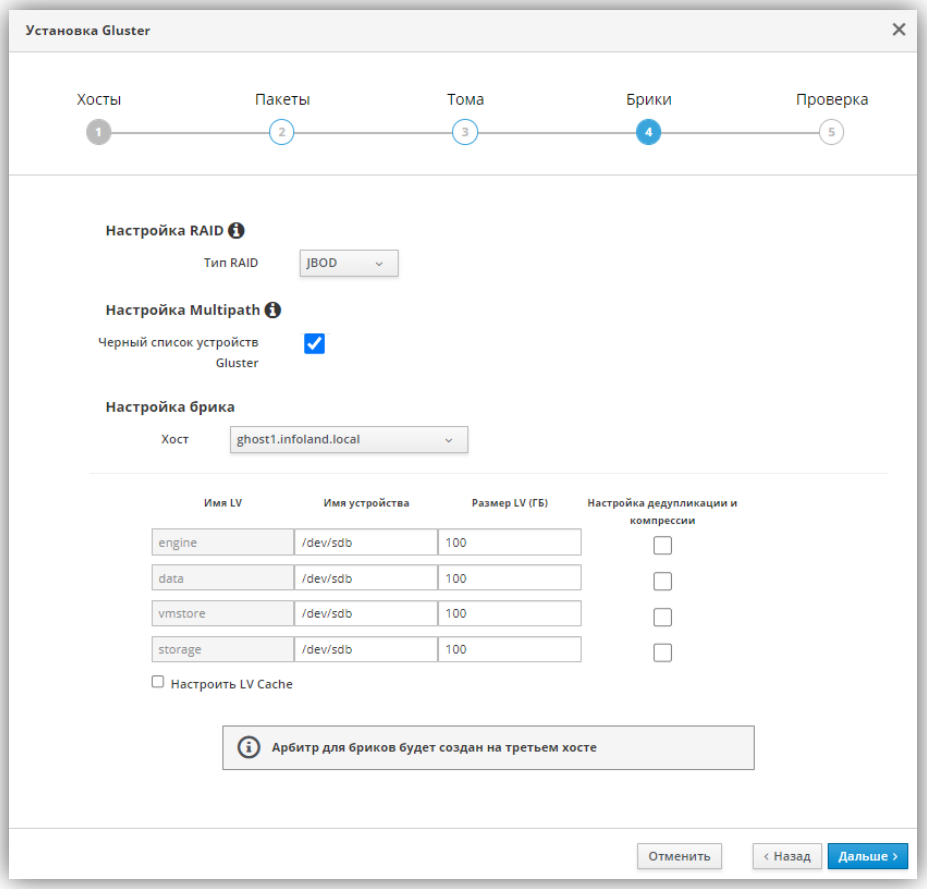

Рисунок 20. Вкладка «Брики».

16. На вкладке «Проверка» доступен для просмотра и редактирования сгенерированный сценарий Ansible.

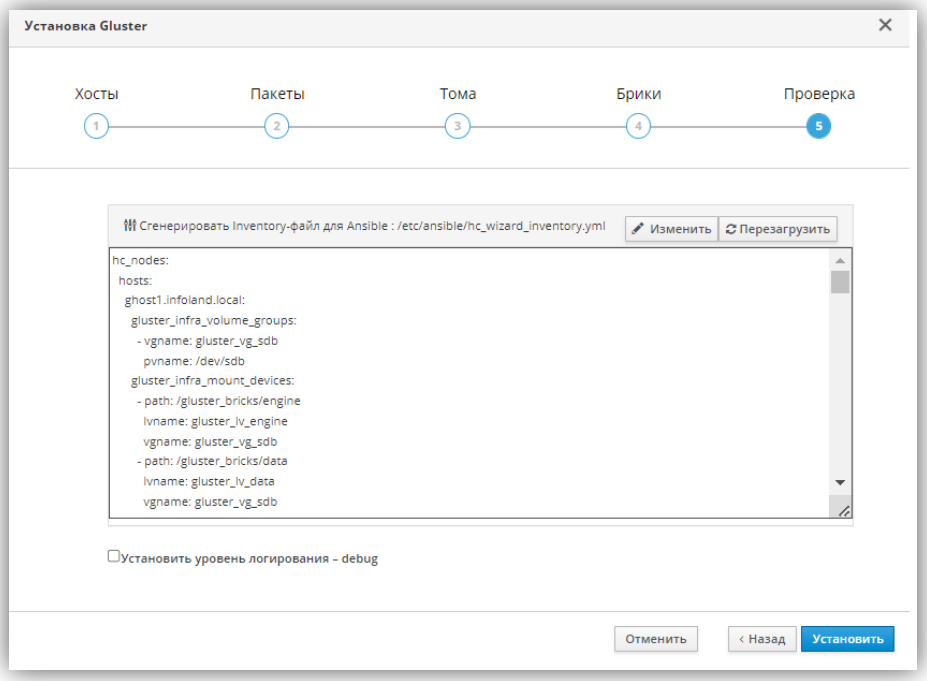

Рисунок 21. Вкладка «Проверка».

17. По нажатию на кнопку «Установить» будет запущен процесс подготовки томов.

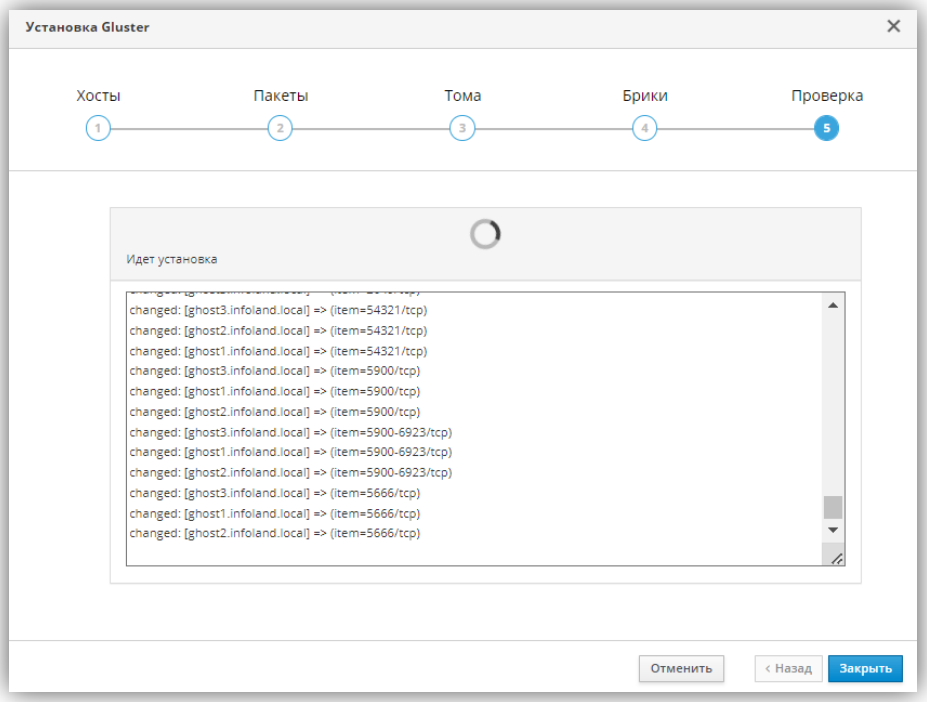

Рисунок 22. Процесс установки.

18. После успешной подготовки томов будет предложено продолжить развертывание среды виртуализации в режиме Hosted Engine. Нажмите на кнопку «Продолжить установку Hosted Engine».

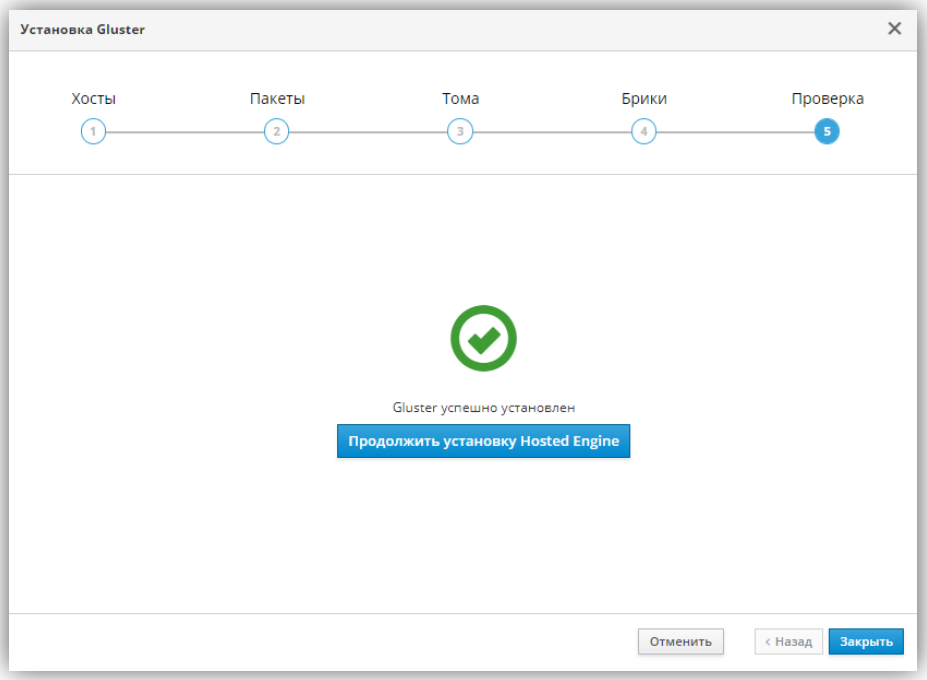

Рисунок 23. Успешное выполнение процесса установки.

19. Заполните поля для настройки ВМ HostedEngine.

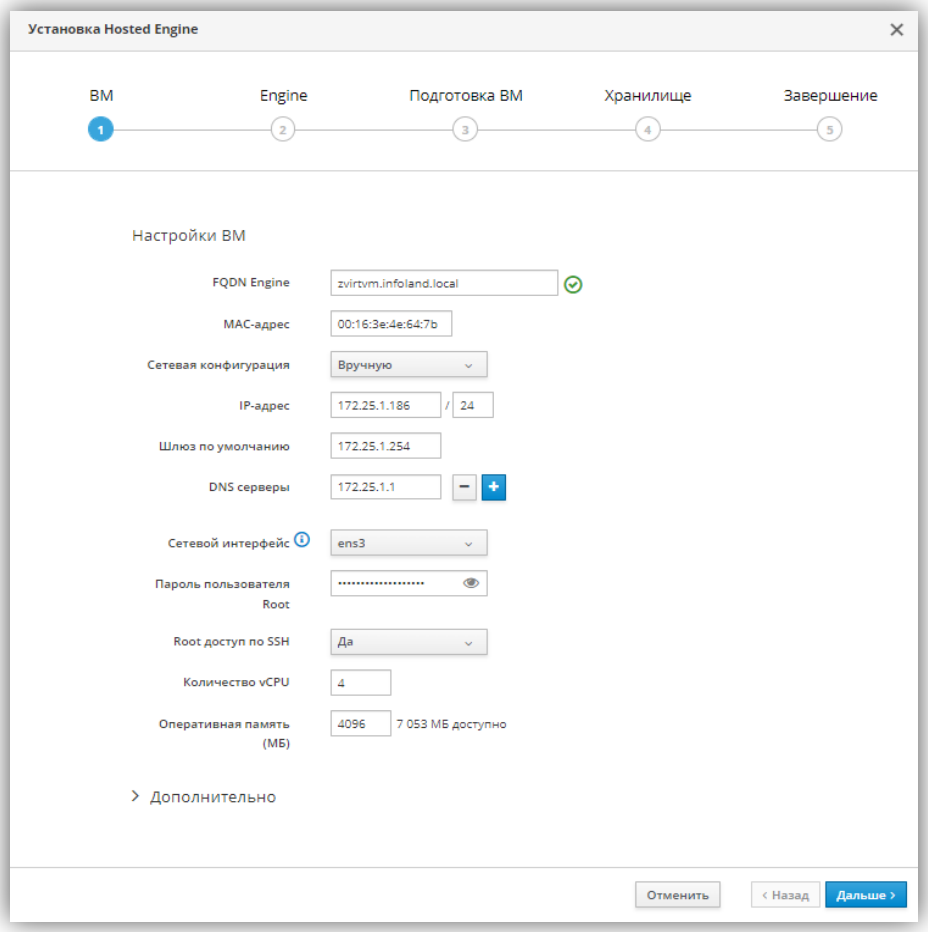

Рисунок 24. Основные настройки для ВМ Engine.

20. Укажите пароль учётной записи администратора (root) для ВМ HostedEngine и определите параметры оповещения.

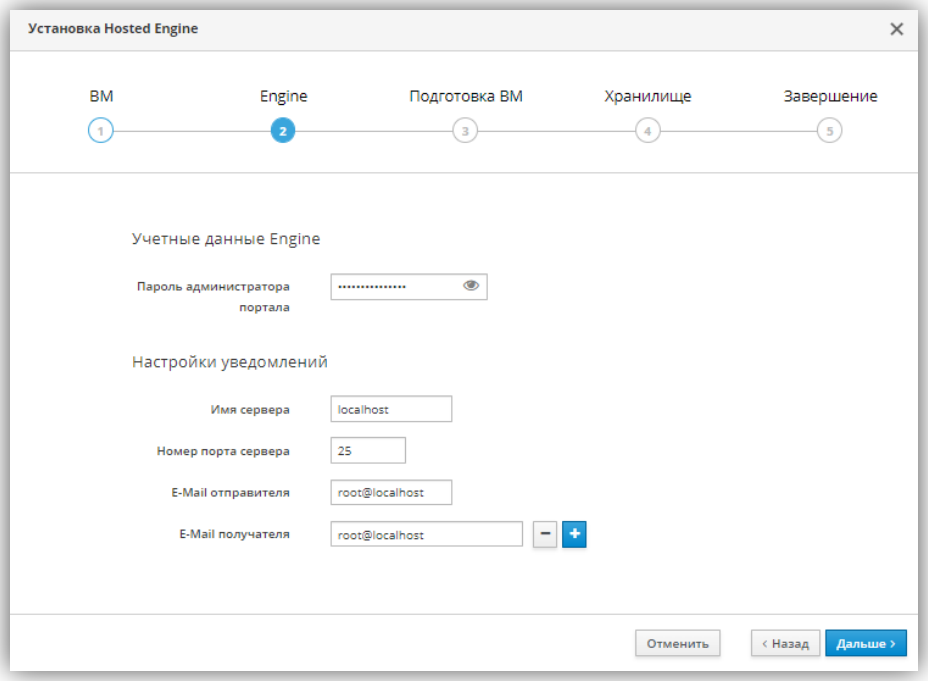

Рисунок 25. Настройка учётной записи администратора и оповещений.

21. Проверьте конфигурацию, если она корректна, нажмите на кнопку «Подготовить ВМ».

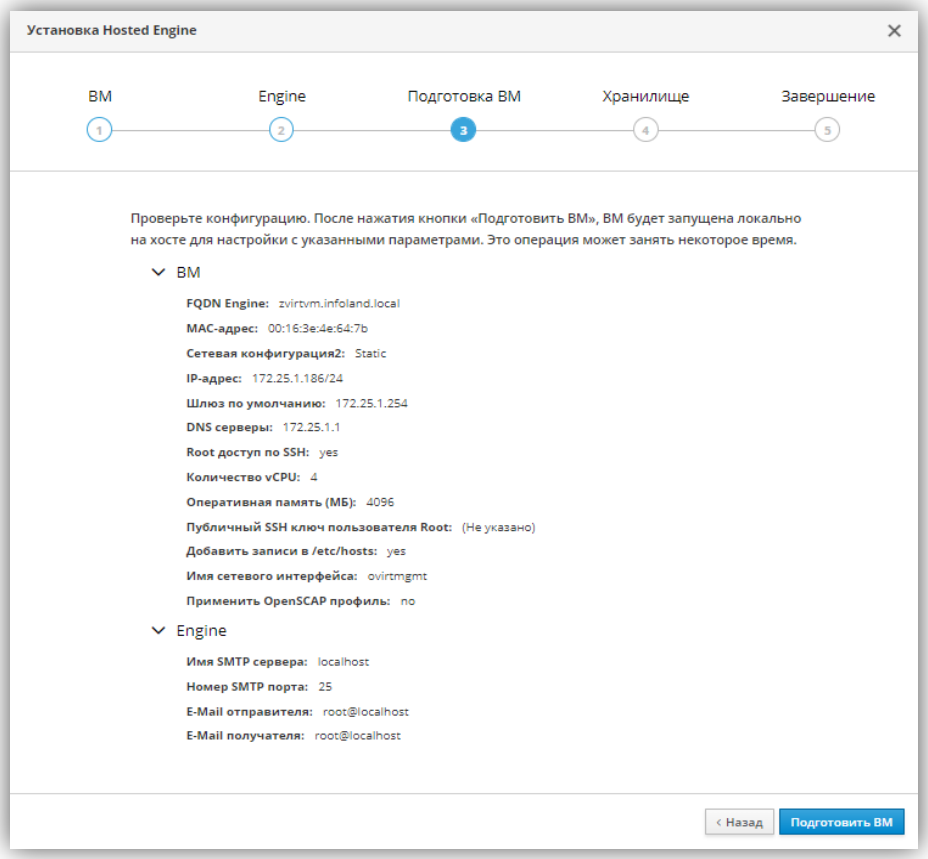

Рисунок 26. Предварительная конфигурация ВМ.

22. Процесс подготовки и создания ВМ HostedEngine.

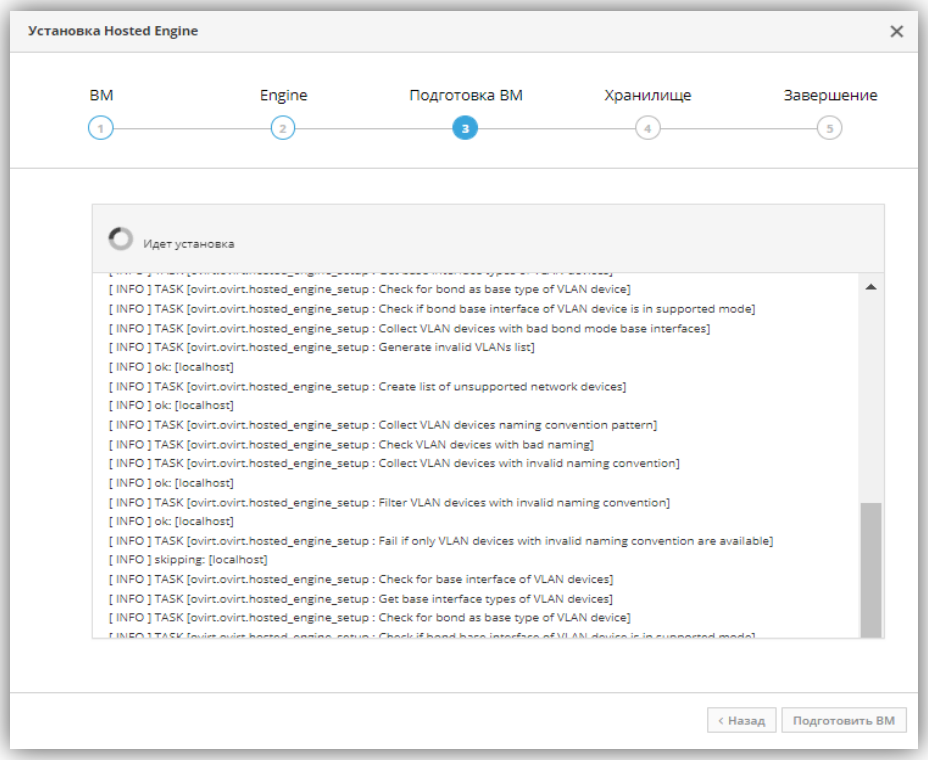

Рисунок 27. Процесс подготовки и создания ВМ HostedEngine.

23. Завершение процесса подготовки и создания ВМ HostedEngine.

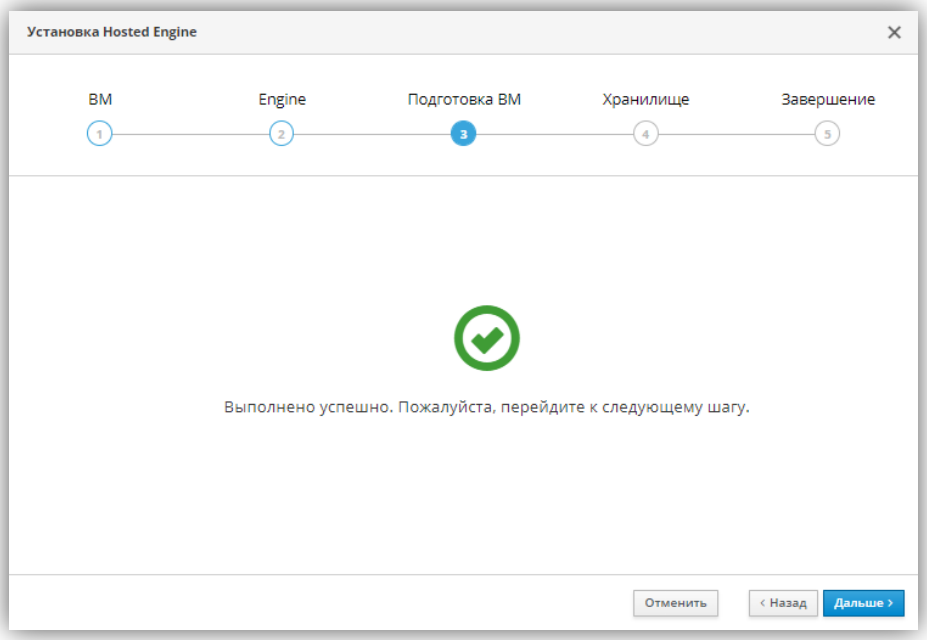

Рисунок 28. Завершение процесса подготовки и создания ВМ HostedEngine.

24. Выполните настройку домена хранения для ВМ HostedEngine. Конфигуратор автоматически предложит использовать ранее подготовленный том.

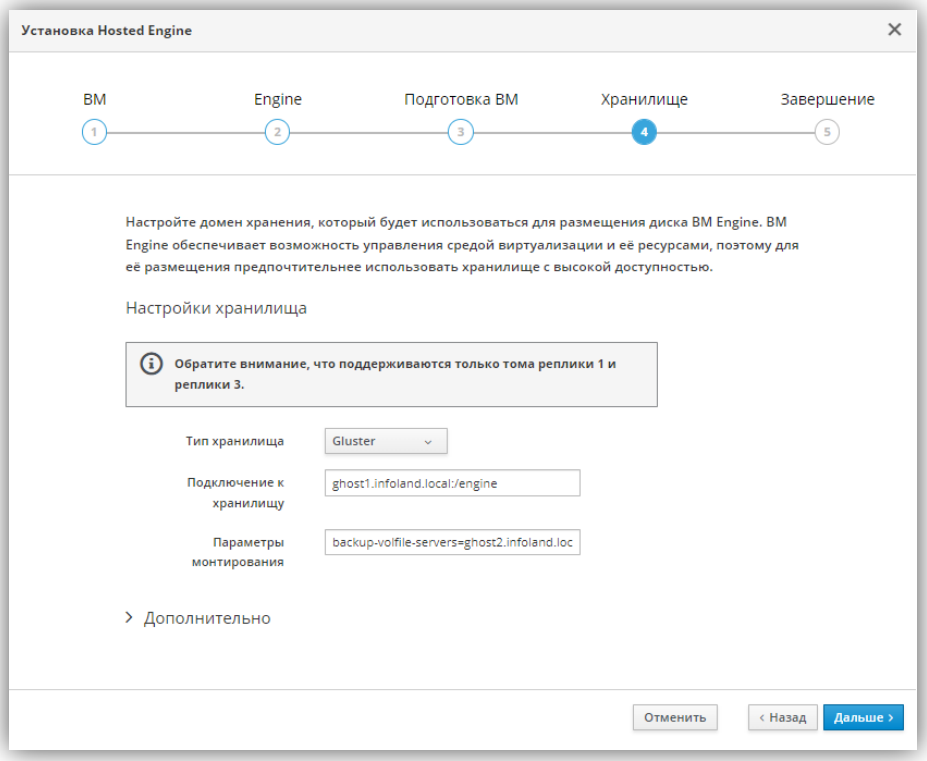

Рисунок 29. Настройка домена хранения.

25. Проверьте итоговую конфигурацию, если она корректна, нажмите на кнопку «Завершить установку».

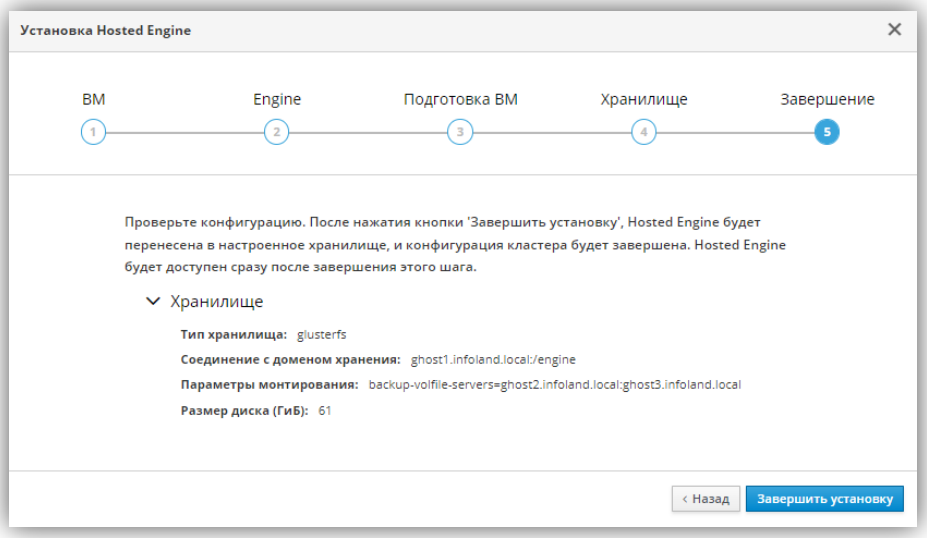

Рисунок 30. Предварительная конфигурация хранилища.

26. Процесс развертывания среды виртуализации в режиме Hosted Engine.

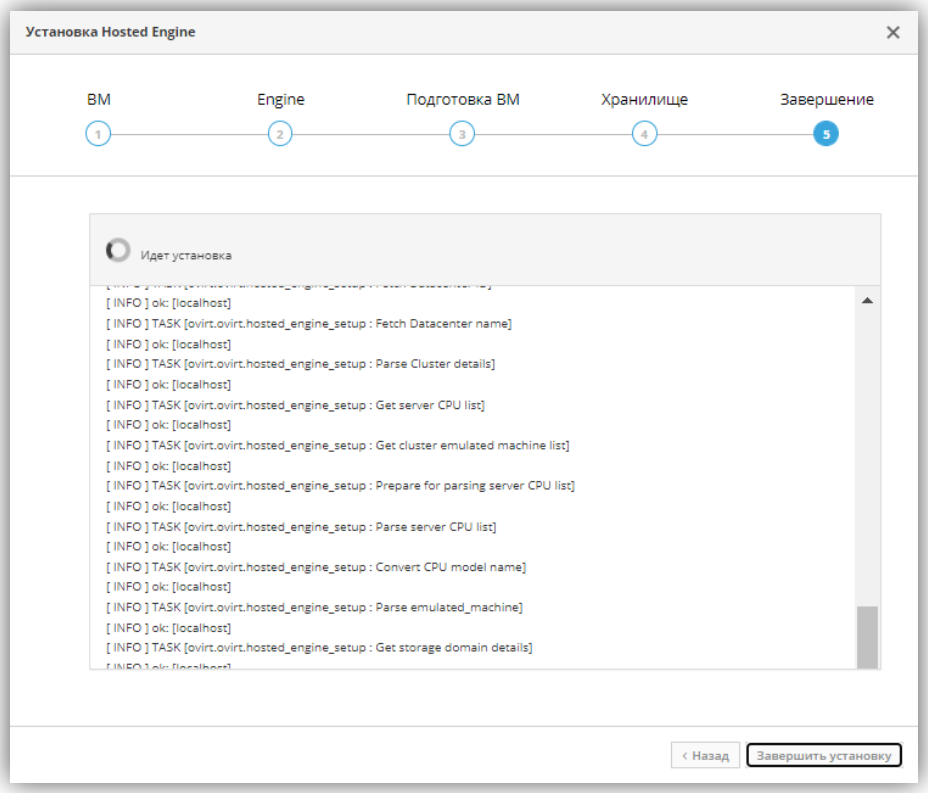

Рисунок 31. Процесс развертывания среды виртуализации.

27. После успешного развертывания Вы увидите сообщение.

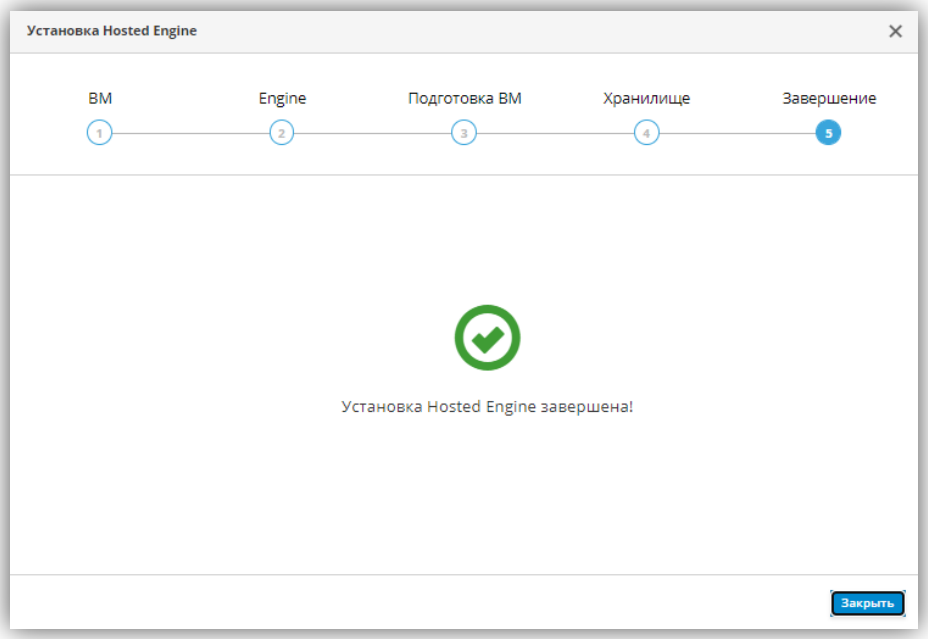

Рисунок 32. Оповещение при успешном развертывании.

4.4.4 Установка в режиме Standalone

В режиме Standalone менеджер управления виртуализации устанавливается на отдельно стоящем сервере, но при необходимости сервер с менеджером управления виртуализацией может быть использован как гипервизор.

1. Подготовьте полное доменное имя для хоста развертывания. Записи прямого и обратного просмотра должны быть установлены в DNS.

Заполните по аналогии для себя следующую таблицу:

Таблица 9. Выбор имен для развертывания

Объект	FQDN	IP адрес
Хост с менеджером управления	zvirtvm.infoland.local	172.25.1.186
Хост 1	host1.infoland.local	172.25.1.181
Хост 2	host2.infoland.local	172.25.1.182
Хост 3	host3.infoland.local	172.25.1.183

В случае невозможности использования внешнего DNS добавьте в файл */etc/hosts* IP-адреса и FQDN хоста виртуализации и разворачиваемого менеджера управления.

2. Запустите процесс установки:

```
# engine-setup
```

3. Следуйте сообщениям в консоли:

```
                          --== PRODUCT OPTIONS ==--

Configure Cinderlib integration (Currently in tech preview) (Yes, No) [No]:
# Настройка интеграции с Cinderlib.

Configure Engine on this host (Yes, No) [Yes]:
# Подтвердите, что на данном хосте будет развернут менеджер управления.

Configuring ovirt-provider-ovn also sets the Default cluster's default network
provider to ovirt-provider-ovn.
Non-Default clusters may be configured with an OVN after installation.
Configure ovirt-provider-ovn (Yes, No) [Yes]:
# Подтвердите, что необходимо выполнить настройку сетевого провайдера ovirt-
provider-ovn.

Configure WebSocket Proxy on this host (Yes, No) [Yes]:
# Подтвердите, что необходимо выполнить на данном хосте настройку WebSocket Proxy.

Configure Data Warehouse on this host (Yes, No) [Yes]:
# Подтвердите установку Data Warehouse на данном хосте.

Configure VM Console Proxy on this host (Yes, No) [Yes]:
# Подтвердите настройку прокси-сервера для консолей ВМ.

Configure Grafana on this host (Yes, No) [Yes]: Enter
# Подтвердите настройку сервера мониторинга Grafana на данном хосте.

                                --== PACKAGES ==--
```

```
                          --== NETWORK CONFIGURATION ==--

Host fully qualified DNS name of this server [host1.infoland.local]:
# Подтвердите полное доменное имя данного хоста.

Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current settings.
Do you want Setup to configure the firewall? (Yes, No) [Yes]:
# Согласитесь с автоматической настройкой сетевого экрана.

                          --== DATABASE CONFIGURATION ==--

Where is the DWH database located? (Local, Remote) [Local]:
# Подтвердите установку базы данных Data Warehouse на данном хосте.

Setup can configure the local postgresql server automatically for the DWH to run.
This may conflict with existing applications.
Would you like Setup to automatically configure postgresql and create DWH
database, or prefer to perform that manually? (Automatic, Manual) [Automatic]:
# Согласитесь с автоматической настройкой базы данных DWH.

Where is the Engine database located? (Local, Remote) [Local]:
# Подтвердите расположение базы данных Engine на данном хосте.

Setup can configure the local postgresql server automatically for the engine to
run. This may conflict with existing applications.
Would you like Setup to automatically configure postgresql and create Engine
database, or prefer to perform that manually? (Automatic, Manual) [Automatic]:
# Согласитесь с автоматической настройкой базы данных Engine.

                        --== OVIRT ENGINE CONFIGURATION ==--
Engine admin password:
# Установите пароль администратора

Confirm engine admin password:
# Подтвердите установленный пароль

Application mode (Virt, Gluster, Both) [Both]:
# Выберите режим Both.
Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]:
# Согласитесь с использованием учётных данных по умолчанию для сетевого
провайдера.
                          --== STORAGE CONFIGURATION ==--

Default SAN wipe after delete (Yes, No) [No]:
# По умолчанию не стирать данные после удаления SAN хранилищ.

                            --== PKI CONFIGURATION ==--

Organization name for certificate [infoland.local]:
# Название организации для сертификата.

                          --== APACHE CONFIGURATION ==--

Setup can configure the default page of the web server to present the application
home page. This may conflict with existing applications.
```

```
Do you wish to set the application as the default page of the web server? (Yes,
No) [Yes]:
# Согласитесь на установку веб-страницы системы виртуализации по умолчанию на веб-
сервере.

Setup can configure apache to use SSL using a certificate issued from the internal
CA.
Do you wish Setup to configure that, or prefer to perform that manually?
(Automatic, Manual) [Automatic]:
# Согласитесь с автоматической настройкой SSL на apache.

                          --== SYSTEM CONFIGURATION ==--
                           --== MISC CONFIGURATION ==--

Please choose Data Warehouse sampling scale:
(1) Basic
(2) Full
(1, 2) [1]:
# Выберите режим Basic.
Use Engine admin password as initial Grafana admin password (Yes, No) [Yes]:
# Подтвердите, что пароль администратора менеджера управления будет использоваться
в качестве начального пароля администратора Grafana.

                         --== CONFIGURATION PREVIEW ==--
Please confirm installation settings (OK, Cancel) [OK]:
# Просмотрите предварительную конфигурацию установки и подтвердите её.

[ INFO ] Execution of setup completed successfully
# Сообщение после успешного разворачивания сервера виртуализации
```

4.4.5 Исправление хоста после неуспешной инсталляции среды виртуализации

Если по каким-либо причинам развертывание среды виртуализации закончилось ошибкой, выполните следующие команды:

1. Для режима Hosted Engine.

   Выполните очистку хоста виртуализации:

```
# ovirt-hosted-engine-cleanup
```

2. Для режима Standalone.

   Выполните команду и следуйте инструкциям:

```
# engine-cleanup
```

5. ПОСЛЕ УСТАНОВКИ

5.1 Проверка работоспособности

Зайдите в веб-интерфейс по адресу, который вы задали для ВМ HostedEngine, например, http://zvirtvm.infoland.local/ → Портал администрирования → Введите имя пользователя admin и пароль заданный при установке системы. Откроется веб интерфейс управления СУВ zVirt (Рисунок 15).

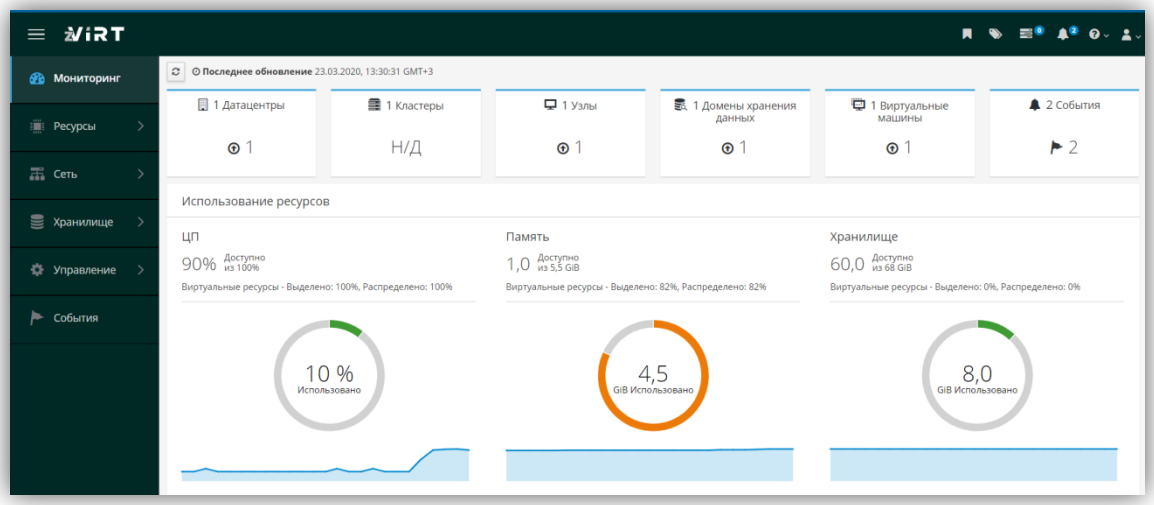

Рисунок 33. Веб - интерфейс управления СУВ ZVIRT.

5.2 Добавление хостов

Добавьте все физические серверы в кластер, через «Ресурсы» → «Хосты» → «Новый».

Для обеспечения доступности менеджера управления, в случае выхода из строя первого хоста, при добавлении дополнительных хостов выберите «Развернуть» на вкладке «Hosted Engine»:

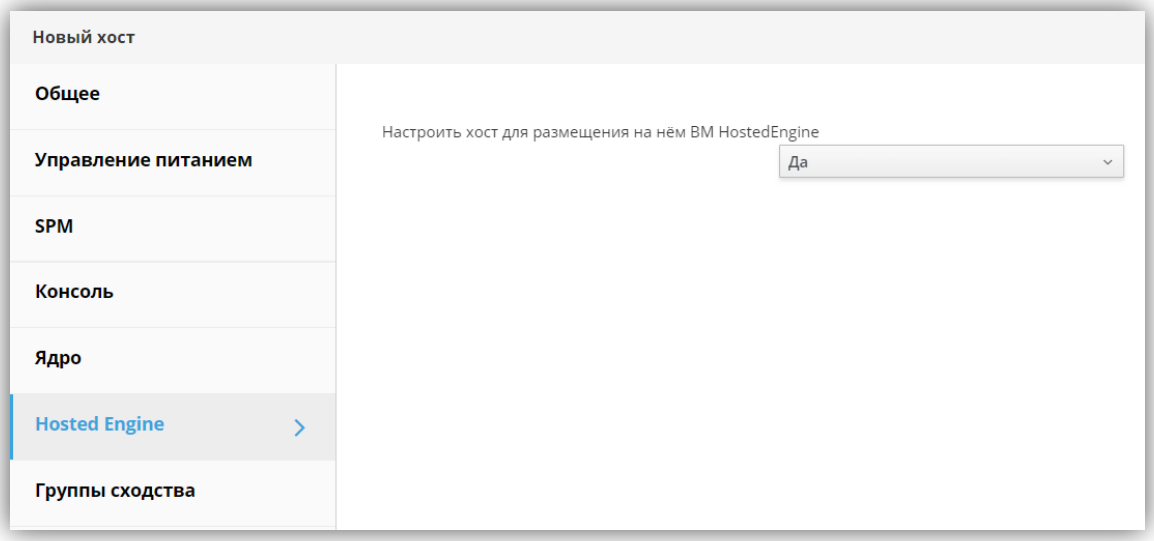

Рисунок 34. Окно «Новый хост».

Дополнительную информацию по работе с системой смотрите в «Руководстве администратора ZVIRT».

5.3 Добавление хранилища

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

- Сетевая файловая система (NFS)
- GlusterFS
- Другие POSIX-совместимые файловые системы
- Интерфейс небольшой компьютерной сети Интернет (iSCSI)
- Локальное хранилище подключено непосредственно к хостам виртуализации
- Протокол Fibre Channel (FCP)
- Параллельная NFS (pNFS)

Чтобы добавить новый домен хранения перейдите «Хранилище» → «Новый домен» и добавьте домены хранения:

- Домен данные
- ISO-домен
- Экспорт-домен

! ISO-домен и Экспорт-домен поддерживают только локальное хранилище, NFS или GlusterFS.

Дополнительную информацию по работе с системой смотрите в «Руководстве администратора ZVIRT».

6. РЕКОМЕНДАЦИИ

Не устанавливайте дополнительные пакеты после установки ОС, так как они могут вызвать проблемы с зависимостями при попытке установить пакеты, необходимые для менеджера управления.

Не включайте дополнительные репозитории, кроме тех, которые предоставляются вендором zVirt.

6.1 Гипервизор

Все процессоры должны поддерживать расширения Intel® 64 или AMD64 CPU, а также расширения аппаратной виртуализации AMD-V™ или Intel VT®. Также требуется поддержка флага No eXecute (NX). Виртуализация должна быть включена в BIOS.

Проверьте, что ваш процессор имеет необходимые расширения и что они включены, выполнив следующую команду:

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

Все хосты в кластере должны иметь одинаковый тип процессора. Процессоры Intel и AMD не могут сосуществовать в рамках одного кластере.

Хостам требуется хранилище для хранения конфигурации, журналов, дампов ядра и для использования в качестве пространства подкачки. Хранилище может быть локальным или сетевым. Хост zVirt может загружаться с одним, несколькими или всеми выделенными по умолчанию разделами в сетевом хранилище. Загрузка из сетевого хранилища может привести к зависанию при отключении сети. Добавление конфигурационного файла *multipath* может помочь решить проблему потери сетевого соединения. Если гипервизор загружается с сетевого хранилища и теряет связь, файлы становятся доступными только для чтения до восстановления сетевого подключения. Использование сетевого хранилища может привести к снижению производительности.

Если вы планируете использовать перераспределение памяти, добавьте достаточно места для подкачки, чтобы обеспечить виртуальную память для всех виртуальных машин.
Хосты должны иметь как минимум один сетевой интерфейс с минимальной пропускной способностью 1 Гбит/с. Каждый хост должен иметь два сетевых интерфейса, причем один из них должен быть выделен для поддержки интенсивной сетевой нагрузки, такой как миграция виртуальных машин.

6.2 Центр данных

Каждый центр данных должен иметь как минимум один домен хранения данных. Также рекомендуется иметь один домен хранения ISO для каждого центра данных. Если планируете хранить iso-образы в домене хранения данных – используйте отдельный домен данных с типом NFS.

Домен хранения может состоять либо из блочных устройств (iSCSI или Fibre Channel), либо из файловой системы.

Домены ISO и Экспорт поддерживают только файловые типы хранения. Домен ISO поддерживает локальное хранение при использовании в локальном центре хранения данных.

6.2.1 NFS

zVirt поддерживает NFS версий 3 и 4. Для производственных рабочих нагрузок требуется сервер NFS корпоративного уровня, если NFS не используется только в качестве домена хранения ISO. Когда корпоративная NFS развернута на 10 Гбит/с, разделена с помощью VLAN, а отдельные службы настроены на использование определенных портов, она является одновременно быстрой и безопасной.

При расширении NFS хранилища СУВ zVirt сразу же распознает изменение размера хранилища данных. Никакой дополнительной настройки на хостах или внутри СУВ zVirt не требуется. Это дает NFS небольшое преимущество перед блочным хранилищем с точки зрения масштабирования и эксплуатации.

6.2.2 iSCSI

Для производственных рабочих нагрузок требуется сервер iSCSI корпоративного уровня. Если корпоративный iSCSI развернут на 10 Гбит/с, разделен на виртуальные локальные сети и использует аутентификацию CHAP, он является одновременно быстрым и безопасным. iSCSI также может использовать многоканальность (*multipathing*) для повышения высокой доступности.

СУВ zVirt поддерживает 1500 логических томов на блочный домен хранения. Разрешается использовать не более 300 LUN.

6.2.3 Fibre Channel

Fibre Channel является одновременно быстрым и безопасным, и его следует использовать, если он уже используется в целевом центре обработки данных. Его преимущество заключается в низкой нагрузке на процессор по сравнению с iSCSI и NFS. Fibre Channel также может использовать многоканальность (*multipathing*) для повышения высокой доступности.

СУВ zVirt поддерживает 1500 логических томов на блочный домен хранения. Разрешается использовать не более 300 LUN.

Чтобы использовать Fibre Channel over Ethernet (FCoE) в СУВ zVirt, необходимо включить ключ fcoe в менеджере управления виртуализации и установить пакет *vdsm-hook-fcoe* на хосты.

6.2.4 GlusterFS

Gluster Storage (GS) - это POSIX-совместимая файловая система с открытым исходным кодом. Три или более серверов конфигурируются как кластер Gluster Storage, вместо сетевых устройств хранения данных (NAS) или массива сети хранения данных (SAN).
Gluster следует использовать по 10 Гбит/с и разделять с помощью виртуальных локальных сетей.

По умолчанию домены GlusterFS и локальные домены хранения поддерживают размер блока 4K, но в настоящее время СУВ zVirt не поддерживает блочные хранилища с размером блока 4K. Вы должны настроить блочное хранилище в режиме (512b block).

6.2.5 Гиперконвергентная инфраструктура

zVirt поддерживает гиперконвергентный вариант развертывания с помощью Gluster. Вместо того чтобы подключать zVirt к внешнему хранилищу Gluster, существует возможность объединить zVirt и Gluster в одной инфраструктуре, что позволяет снизить эксплуатационные расходы и накладные расходы.

6.2.6 POSIX-совместимые файловые системы

Другие POSIX-совместимые файловые системы могут использоваться в качестве доменов хранения в СУВ zVirt, если они являются кластерными файловыми системами и поддерживают разреженные (тонкие) файлы и прямой ввод-вывод. Файловая система Common Internet File System (CIFS), например, не поддерживает прямой ввод/вывод, что делает ее несовместимой с СУВ zVirt.

6.2.7 Локальное хранилище

Локальное хранилище создается на отдельном хосте, используя собственные ресурсы. Когда вы настраиваете хост на использование локального хранилища, он автоматически добавляется в новый центр данных и кластер, в который не могут быть использованы другими хостами. Виртуальные машины, созданные в кластере с одним хостом, не могут быть перемещены, использовать "Высокую доступность" или использовать политики планирования в кластере.

Для хостов виртуализации локальное хранилище всегда должно быть определено в файловой системе, отдельной от / (root). Используйте отдельный логический том или диск.

6.3 Сети

Для zVirt требуется, чтобы IPv6 оставался включенным на физической или виртуальной машине, на которой запущен менеджер управления. Не отключайте IPv6 на ВМ HostedEngine, даже если в вашей сети его не используют.

Менеджер управления не создает сервер DNS или NTP, поэтому сетевому экрану не нужно иметь открытые порты для входящего трафика.

По умолчанию система виртуализации zVirt разрешает исходящий трафик к DNS и NTP на любой адрес назначения. Если вы запрещаете исходящий трафик, определите исключения для запросов, отправляемых на серверы DNS и NTP.

Менеджер управления виртуализации и все хосты должны иметь определенное доменное имя (FQDN), а также прямое и обратное разрешение имен.

Запуск службы DNS в виртуальной машине в среде виртуализации не рекомендуется. Все службы DNS, используемые виртуализацией, должны быть размещены за её пределами. Рекомендуется использовать DNS вместо файла */etc/hosts* для разрешения имен.

Каждый хост в кластере должен иметь возможность подключаться к устройствам ограждения всех остальных хостов в кластере. Если хосты кластера получают ошибку (сетевая ошибка, ошибка хранилища и т.д.) и не могут функционировать как хосты, они должны иметь возможность подключения к другим хостам в центре данных.

При планировании и настройке сетей в среде виртуализации, настоятельно рекомендуется ознакомиться руководствами производителя сетевого оборудования для получения дополнительной информации об управлении сетями.

Логические сети могут использовать физические устройства, такие как сетевые карты, или логические устройства, такие как bond. Объединение портов обеспечивает повышенную отказоустойчивость, поскольку все сетевые порты в объединении должны выйти из строя, чтобы сам bond вышел из строя. Только режимы объединения 1, 2, 3 и 4 могут использоваться для сетей виртуальных машин. Режимы 0, 5 и 6 не предназначены для сети виртуальных машин. Система виртуализации по умолчанию использует режим 4.

Режимы объединения:

1. Режим 0 (round-robin) - передача пакетов через сетевые интерфейсы в последовательном порядке. Пакеты передаются в цикле, который начинается с первого доступного сетевого интерфейса на хосте и заканчивается последним доступным сетевым интерфейсом на хосте. Все последующие циклы начинаются с первой доступной карты сетевого интерфейса. Режим 0 обеспечивает отказоустойчивость и распределяет нагрузку между всеми сетевыми интерфейсными картами в связке. Однако режим 0 не может использоваться в сочетании с bridge и поэтому не совместим с логическими сетями виртуальных машин.
2. Режим 1 (active-backup) - переводит все сетевые интерфейсы в резервное состояние, в то время как один сетевой интерфейс остается активным. В случае отказа активного сетевого интерфейса один из резервных интерфейсов заменяет сбойный интерфейс в качестве единственного активного сетевого интерфейса в бонде. MAC-адрес соединения в режиме 1 виден только на одном порту, чтобы предотвратить путаницу, которая может возникнуть, если MAC-адрес соединения изменится на MAC-адрес активной сетевой интерфейсной карты. Режим 1 обеспечивает отказоустойчивость и поддерживается в zVirt.
3. Режим 2 (XOR) - выбирает сетевой интерфейс, через который будут передаваться пакеты, на основе результата операции XOR над MAC-адресами источника и назначения по модулю количества сетевых интерфейсов. Этот расчет гарантирует, что для каждого используемого MAC-адреса назначения будет выбрана одна и та же карта сетевого интерфейса. Режим 2 обеспечивает отказоустойчивость и балансировку нагрузки и поддерживается в zVirt.
4. Режим 3 (broadcast) - передает все пакеты всем сетевым интерфейсам. Режим 3 обеспечивает отказоустойчивость и поддерживается в zVirt.
5. Режим 4 (IEEE 802.3ad) - создает группы агрегации, в которых интерфейсы имеют одинаковые настройки скорости и дуплекса. Режим 4 использует все сетевые интерфейсы в активной группе агрегации в соответствии со спецификацией IEEE 802.3ad и поддерживается в zVirt.
6. Режим 5 (adaptive transmit load balancing) - обеспечивает распределение исходящего трафика с учетом нагрузки на каждый сетевой интерфейс в связке и то, что текущий сетевой интерфейс получает весь входящий трафик. Если сетевой интерфейс, назначенный для приема трафика, выходит из строя, роль приема входящего трафика возлагается на другой сетевой интерфейс. Режим 5 нельзя использовать в сочетании с bridge, поэтому он не совместим с логическими сетями виртуальных машин.
7. Режим 6 (adaptive load balancing) - объединяет режим 5 (adaptive transmit load balancing) с балансировкой нагрузки при приеме для трафика IPv4 без каких-либо специальных требований к коммутатору. Для балансировки принимаемой нагрузки используется согласование ARP. Режим 6 нельзя использовать в сочетании с bridge, поэтому он не совместим с логическими сетями виртуальных машин.

Нет необходимости для каждой логической сети использовать физическое устройство, поскольку несколько логических сетей могут совместно использовать одно устройство с помощью тегов виртуальных локальных сетей (VLAN) для изоляции сетевого трафика. Чтобы использовать эту функцию, тегирование VLAN должно поддерживаться на уровне коммутатора.

6.3.1 Ограничения на количество логических сетей в СУВ zVirt:

Количество логических сетей, подключенных к хосту, ограничено количеством доступных физических сетевых устройств в сочетании с максимальным количеством виртуальных локальных сетей (VLAN), которое составляет 4096.

Количество сетей, которые могут быть присоединены к хосту за одну операцию, в настоящее время ограничено 50.

Количество логических сетей в кластере ограничено количеством логических сетей, которые могут быть присоединены к хосту, поскольку сетевое взаимодействие должно быть одинаковым для всех хостов в кластере.

Количество логических сетей в центре данных ограничено только количеством содержащихся в нем кластеров в сочетании с количеством логических сетей, разрешенных для каждого кластера.

Будьте особенно внимательны при изменении свойств сети управления (*ovirtmgmt*). Неправильные изменения свойств сети *ovirtmgmt* могут привести к тому, что хосты станут недоступны.

6.4 Сервера каталогов

Во время установки менеджер управления по умолчанию создает пользователя *admin* в домене *internal*. Эта учетная запись предназначена для использования при первоначальной настройке среды и для устранения неполадок. Вы можете создать дополнительных пользователей во внутреннем домене с помощью *ovirt-aaa-jdbc-tool* или на портале администрирования.

Вы также можете подключить внешний сервер каталогов к среде виртуализации и использовать его в качестве внешнего домена.

Поддерживается подключение более одного сервера каталогов.

Для взаимодействия со средой виртуализации поддерживаются следующие серверы каталогов:
1 - 389ds;
2 - 389ds RFC-2307 Schema;
3 - Active Directory;
4 - IBM Security Directory Server;
5 - IBM Security Directory Server RFC-2307 Schema;
6 – IPA;
7 - Novell eDirectory RFC-2307 Schema;
8 - OpenLDAP RFC-2307 Schema;
9 - OpenLDAP Standard Schema;
10 - Oracle Unified Directory RFC-2307 Schema;
11 - RFC-2307 Schema (Generic);
12 – RHDS;
13 - RHDS RFC-2307 Schema;
14 – iPlanet.

Пользователь с правами на чтение всех пользователей и групп должен быть создан на сервере каталогов специально для использования в качестве пользователя с правами администратора в системе виртуализации. Не используйте пользователя с правами

администратора сервера каталогов в качестве пользователя с правами администратора в системе виртуализации.

6.5 Общие рекомендации

Сразу после завершения развертывания создайте полную резервную копию менеджера управления и сохраните ее в отдельном месте. После этого регулярно создавайте резервные копии.

Не рекомендуется запускать службы или сервисы (например, NTP, DNS, DHCP и др.), от которых зависит менеджер управления, внутри виртуальных машин в той же среде виртуализации. Если это делается, необходимо тщательно спланировать это, чтобы минимизировать время простоя, если виртуальная машина, содержащая службу или сервис, выйдет из строя.

Убедитесь, что пустой хост или виртуальная машина, на которой будет установлен менеджер управления, имеет достаточную энтропию. Значения ниже 200 могут привести к сбою установки менеджера. Чтобы проверить значение энтропии, выполните команду **`cat /proc/sys/kernel/random/entropy_avail.`** Чтобы увеличить энтропию, установите пакет *rng-tools*.

Вы можете автоматизировать развертывание хостов и виртуальных машин с помощью PXE, Kickstart, Satellite, CloudForms, Ansible или их комбинации. Развертывание в режиме HostedEngine с помощью PXE не поддерживается.

Используйте протокол сетевого времени (NTP) на всех хостах и виртуальных машинах в системе виртуализации для синхронизации времени. Аутентификация и сертификаты особенно чувствительны к разнице во времени.

6.5.1 Рекомендации по безопасности

Не отключайте функции безопасности (такие как HTTPS, SELinux и межсетевой экран) на хостах или виртуальных машинах.

Создайте индивидуальные учетные записи администраторов, вместо того чтобы допускать использование одной учетной записи администратора несколькими сотрудниками.

Ограничьте доступ к хостам и создайте отдельные учетные записи. Не используйте одну учётную запись с правами *root* на всех хостах виртуализации.

При развертывании хостов виртуализации устанавливайте только пакеты и службы, необходимые для системы виртуализации, производительности, безопасности и мониторинга. Хосты не должны иметь дополнительных пакетов, таких как анализаторы, компиляторы или другие компоненты, которые добавляют риск для безопасности.

6.5.2 Рекомендации по хостам

Стандартизируйте хосты в одном кластере. Используйте одинаковые модели оборудования и версии микропрограммного обеспечения. Смешивание различного серверного оборудования в одном кластере может привести к нестабильности кластера.

Настройте устройства ограничения во время развертывания. Устройства ограничения необходимы для обеспечения высокой доступности.

Используйте отдельные аппаратные коммутаторы для ограждения трафика. Если мониторинг и ограждение проходят через один коммутатор, этот коммутатор становится единой точкой отказа при обеспечении высокой доступности.

6.5.3 Рекомендации по работе с сетью

Объединяйте сетевые интерфейсы, особенно на продуктивных хостах. Объединение улучшает общую доступность, а также пропускную способность сети.

Если объединения сетевых интерфейсов (bonding) предназначено для различного сетевого трафика, необходимо обеспечить надлежащее качество обслуживания (QoS) для хранилища и другого сетевого трафика.

Для оптимальной производительности и упрощения поиска и устранения неисправностей используйте виртуальные локальные сети для разделения различных типов трафика и оптимального использования сетей 10 Гбит/с или 40 Гбит/с.

Если базовые коммутаторы поддерживают jumbo frames, установите MTU на максимальный размер (например, 9000), который поддерживают базовые коммутаторы. Эта настройка обеспечивает оптимальную пропускную способность, более высокую пропускную способность и меньшее использование ЦП для большинства приложений. MTU по умолчанию определяется минимальным размером, поддерживаемым базовыми коммутаторами.

Если вы измените параметры MTU сети, вы должны распространить эти изменения на работающие виртуальные машины в сети: “Горячее” отключение и повторное подключение vNIC каждой виртуальной машины, которая должна применить настройки MTU, или перезапустите виртуальные машины. В противном случае эти интерфейсы выйдут из строя при миграции виртуальных машин на другой хост.

Сети 1 Гбит/с следует использовать только для трафика управления. Используйте 10 Гбит/с или 40 Гбит/с для виртуальных машин и хранилищ на базе Ethernet.

Если на хост добавляются дополнительные физические интерфейсы для использования хранилища, снимите флажок Сеть ВМ, чтобы VLAN назначалась непосредственно физическому интерфейсу.

6.5.4 Рекомендации по настройке сетей хоста

Всегда используйте менеджер управления для изменения сетевой конфигурации хостов в кластерах. В противном случае вы можете создать неподдерживаемую конфигурацию.

Если ваша сетевая инфраструктура сложная, возможно предварительно настроить сеть хоста вручную перед добавлением хоста в систему виртуализации.

Используйте следующие соглашения об именовании:

1. Устройства VLAN: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
2. Интерфейсы VLAN: physical_device.VLAN_ID (например, eth0.23, eth1.128, enp3s0.50).
3. Интерфейсы bond: bondnumber (например, bond0, bond1).
4. VLAN на объединенных интерфейсах (bond): bondnumber.VLAN_ID (например, bond0.50, bond1.128).

! В названии интерфейсов необходимо использовать только прописные буквы.

Используйте объединение сетей (bonding). Teaming не поддерживается в системе виртуализации и приведет к ошибкам, если хост используется для развертывания в режиме HostedEngine или добавлен в менеджер управления виртуализации.

Используйте рекомендуемые режимы объединения:

- Если сеть ovirtmgmt не используется виртуальными машинами, сеть может использовать любой поддерживаемый режим объединения.
- По умолчанию в системе виртуализации используется режим объединения (Mode 4) Dynamic Link Aggregation. Если ваш коммутатор не поддерживает протокол Link Aggregation Control Protocol (LACP), используйте режим 1 (Active-Backup).

! Не отключайте сервис firewalld (межсетевой экран).

6.5.5 Рекомендации по развертывания в режиме HostedEngine

Создайте отдельный центр данных и кластер для ВМ HostedEngine и других служб уровня инфраструктуры, если ваша инфраструктура может позволить это. Хотя виртуальная машина с менеджером управления может работать на хостах в обычном кластере, отделение от остальных виртуальных машин помогает упростить план резервного копирования, производительность, доступность и безопасность.

Домен хранения, предназначенный для ВМ HostedEngine, создается во время развертывания. Не используйте этот домен хранения для других виртуальных машин.

Если ожидается большая нагрузка на хранилище, разделите сети миграции, управления и хранения, чтобы уменьшить влияние на работоспособность ВМ HostedEngine.

Все хосты способные поддерживать работу ВМ HostedEngine должны иметь одинаковое семейство процессоров, чтобы виртуальная машина могла безопасно мигрировать между ними. Если вы планируете создание кластера с хостами, имеющими различные семейства процессоров, необходимо начинать установку с самого раннего семейства.

! После развертывания менеджера управления виртуализации запрещено изменять системные параметры ВМ HostedEngine.

7. Сбор и предоставление логов

В случае необходимости предоставления логов технической службе технической поддержки, выполнить следующие действия:

- Авторизоваться на сервере пользователем root
- Выполнить архивацию логов: tar zcf /root/logs.tar.gz /var/log
- Настроить межсетевой экран: firewall-cmd --add-port=8000/tcp
- Запустить веб-сервер: python -m SimpleHTTPServer
- С любого компьютера, находящегося в той же сети что и сервер, обратиться по адресу, например, http://172.25.1.232:8000
- Скачать файл logs.tar.gz
- Предоставить файл logs.tar.gz службе технической поддержки

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Сокращение	Описание
СУВ	Система безопасного управления виртуализацией zVirt
Менеджер управления	Служба управления виртуализацией
ВМ	Виртуальная машина
Хост	Физический сервер
IP	Internet Protocol
АРМ	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
KVM	Kernel-based Virtual Machine