itkey

Руководство по установке KeyVirt

Содержание

Список сокращений

API	Application Programming Interface	Программный интерфейс приложений, описание способов для обмена данными между приложениями
CLI	Command Line Interface	Интерфейс командной строки
CPU	Central Processor Unit	Центральный процессор
CSV	Comma-Separated Values	Текстовый формат для представления табличных данных
DRS	Distributed Resource Scheduler	Планировщик распределенных ресурсов
GPU	Graphical Processor Unit	Графический графический процессор, предназначенный для обработки графики и высокопроизводительных вычислений
HA	High Availability	Высокая доступность
IOPS	Input/Output Operations Per Second	Количество операций ввода-вывода в секунду, выполняемых системой хранения данных
IP-адрес	Internet Protocol Address	Уникальный сетевой адрес в сети передачи данных, построенный по протоколу IP (межсетевому протоколу передачи данных)
ISO-образ	Optical Disc Image	Образ оптического диска
KVM	Kernel-based Virtual Machine	Функция ПО, которую можно установить на физических компьютерах с ОС Linux в целях создания ВМ.
LAN	Local Area Network	Локальная вычислительная сеть
LUN	Logical Unit Number	Адрес блочного устройства (диска) с СХД
MAC-адрес	Media Access Control address	Уникальный аппаратный идентификатор оборудования
NAS	Network Attached Storage	Сетевое хранилище

NIC	Network Interface Controller	Сетевой адаптер
PCI passthrough	Peripheral Component Interconnect passthrough	Проброс устройств на шине PCI
RAM	Random Access Memory	Оперативная память
RDP	Remote Desktop Protocol	Протокол удаленного рабочего стола
REST	Representational State Transfer	Набор архитектурных принципов для построения распределенных масштабируемых веб-сервисов
SAN	Storage Area Network	Сеть хранения данных
SSH	Secure Shell	Сетевой протокол прикладного уровня, предназначеный для безопасного удаленного доступа к UNIX-системам
QEMU	Quick Emulator	Инструмент с открытым исходным кодом для эмуляции и виртуализации работы операционных систем на компьютере
QoS	Quality of Service	Качество обслуживания
vCPU	Virtual Central Processor Unit	Виртуальный процессор
vGPU	Virtual Graphical Processor Unit	Виртуальный графический процессор
VPN	Virtual Private Network	Виртуальная частная сеть
ВМ		Виртуальная машина
ОС		Операционная система
ПК		Персональный компьютер
ПО		Программное обеспечение
СХД		Система хранения данных
ЦОД		Дата-центр (центр обработки данных)

Список терминов

- Сервер управления (Engine, сервер управления средой виртуализации) – сервер управления средой виртуализации, для которого существует три варианта установки. В режиме Self-Hosted сервер управления (Self-Hosted Engine) – это сервер управления средой виртуализации, установленный как отдельная ВМ, размещенная на самих хостах виртуализации. Сервер управления работает как Портал администрирования.
- Менеджер управления (oVirt Engine, менеджер управления средой виртуализации) – менеджер управления средой виртуализации, т.е. Портал администрирования для управления средой виртуализации.
- Хост среды виртуализаци (oVirt Node) – это хост среды виртуализации, который работает как гипервизор.
- Affinity-группа (группа сходства) или территориальная группа – группа из двух или более виртуальных машин или хостов, для которых применяется набор идентичных условий и параметров. Такая группа используется в политике планирования ВМ. Бывают группы как с положительным, так и с отрицательным сходством.
- Affinity-метка (метка сходства) или тег соответствия – подмножество группы сходства, которое используются вместе с группами сходств для установки любого вида сходства между виртуальными машинами и хостами.
- Affinity-политика (политика сходства) – комбинация группы привязки, инструкции условия и необязательных параметров. Например, виртуальные машины A, VM B и VM C должны выполняться вместе на хосте 1.
- Alias (псевдоним) – альтернативное имя, присвоенное объекту, такому как ВМ и диск. Как правило, псевдоним представляет собой упрощенное имя объекта, которое используется для улучшения читаемости текста, который часто ссылается на данный объект.
- High Availability (HA, высокая доступность) или отказоустойчивость – способность системы или службы оставаться работоспособной и доступной для пользователей во время незапланированных сбоев или нарушений, таких как аппаратные сбои и перебои в работе сети. HA подразумевает живую миграцию ВМ.
- Infrastructure as a Service (Iaas) – модель предоставления облачных ресурсов конечному клиенту в виде единой инфраструктуры.
- IPv4 и IPv6 – группа интернет-протоколов, обеспечивающих маршрутизацию и адресацию пакетов между сетевыми устройствами внутри одной или нескольких взаимосвязанных сетей. Несмотря на то, что IPv6 – более усовершенствованная версия IPv4, четвертая версия все еще пользуется большей популярностью. Необходимости в обязательном переходе на шестой протокол нет.
- LAN (Local Area Network) – локальная вычислительная сеть, т.е. компьютерная сеть, покрывающая относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).
- MAC-адрес (Media Access Control address) – уникальный аппаратный идентификатор оборудования. Имеет длину 48 бит (6 байт) и записывается как шесть шестнадцатеричных чисел, разделенных двоеточием, тире или точками.

- Quality of Service (QoS) или качество обслуживания – технология, которая может гарантировать пропуск трафика в заданных значениях. QoS описывает уровень производительности и приоритезации обслуживания разных типов трафика в телекоммуникационной сети.
- Балансировщик нагрузки (Load Balancer) – средство, которое позволяет распределять входящий трафик между несколькими виртуальными бэкенд-серверами и тем самым обеспечивать высокую доступность для сервисов, предоставляемых этими серверами. При выходе из строя одного или нескольких серверов трафик будет перенаправлен на оставшиеся серверы. Также отдельный тип балансировщика используется для обеспечения работы других сервисов платформы.
- Брандмауэр (Firewall) или межсетевой экран – комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
- Виртуализация – предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.
- Виртуальная машина (ВМ), также известная как инстанс (Instance) и экземпляр – цельная конфигурация аппаратных ресурсов, созданная для запуска приложений и ОС. ВМ может быть представлена как компьютер или сервер, при этом есть возможность эмулировать отдельные ее компоненты. Виртуальные машины используют при тестировании ПО или для моделирования ситуаций в сетевой структуре. Это незаменимый инструмент для развертки облачной инфраструктуры (IaaS).
- Виртуальная память – энергозависимая часть компьютерной памяти, в которой временно хранятся данные и команды, необходимые процессору для выполнения операции, имеющая возможность работать в изолированной друг от друга среде.
- Гостевая операционная система (гостевая ОС) – операционная система, устанавливаемая на созданную виртуальную машину.
- Дата-центр (Data Center) – специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.
- Диск/Том (Volume) – сетевое блочное устройство, которое обеспечивает хранилище данных для ВМ. Все диски в облаке являются сетевыми и защищены репликацией данных, обеспечивающей надежность хранения и отказоустойчивость. Размер и тип дисков устанавливается индивидуально при их создании в соответствии с потребностями. Для дисков доступны операции расширения, присоединения, конвертирования, создания снимка или удаления.
- Кластер (Cluster или host cluster) – совокупность данных или аппаратных мощностей, которые объединены в один ресурс. Кластеризация необходима для обеспечения надежности и производительности инфраструктуры.
- Контейнер – программное обеспечение, предназначенное для виртуализации в условиях изолированной программной среды. Создание контейнера реализуется с помощью использования изолированного пространства. Инструменты, которые

находятся за пределами контейнера, недоступны для виртуального пространства. В отличие от виртуальной машины, которая использует отдельный пул ресурсов от ОС, контейнер требует ресурсы, а компоненты находятся в совместном использовании с основной ОС. Контейнер быстрее запускается, а степень нагрузки на контейнер во время запуска значительно меньше.

- Маршрутизатор (роутер) – специализированный сетевой компьютер, имеющий два или более сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети.
- Миграция – перенос виртуальной машины на другой узел. Существует два типа миграции: без остановки ВМ (живая миграция) — ВМ остаётся доступной во время миграции – и с остановкой ВМ — при этом ВМ становится недоступна на время миграции.
- Моментальный снимок (Snapshot) или снимок – инструмент, позволяющий запечатлеть состояние примитива хранения (например, диска ВМ) в конкретный момент времени. Благодаря нему можно в любой момент вернуть систему к сохраненной конфигурации, что особенно полезно в случае сбоя системы. В виртуальной машине снимок содержит данные виртуального диска и, по желанию, оперативной памяти. Время, необходимое для создания моментального снимка, не зависит от объема данных, что делает его более быстрым и эффективным вариантом резервного копирования.
- Облачное хранилище (Cloud Storage) – модель облачных вычислений, которая предполагает хранение данных в интернете при помощи провайдера облачных вычислительных ресурсов. Провайдер предоставляет облачное хранилище как сервис и управляет им. Пользоваться облачным хранилищем можно по необходимости, не развертывая собственную инфраструктуру.
- Hugepage (страница памяти большого размера) – специальное приложение «страниц памяти» или «виртуальных страниц». Вместо управления тысячами крошечных страниц размером 4 кБ, огромные страницы позволяют определять страницы большего размера (например, 2 или 4 МБ), уменьшая размер таблицы страниц и, таким образом, увеличивая скорость поиска. Огромные страницы не являются обязательным требованием для сквозной передачи по VGA, но они могут помочь повысить производительность ВМ.
- Оперативное запоминающее устройство (ОЗУ) – энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором.
- Проброс PCI-устройств (PCI passthrough) – метод, который позволяет гипервизору проходить через устройство PCI к виртуальной машине. Гостевая операционная система затем использует свой собственный аппаратный драйвер для прямого доступа к устройству.
- Порт – соединение (физическое или логическое), через которое принимаются и отправляются данные в компьютерах.
- Проект (Tenant) или тенант – абстракция, включающая разделение пользователей и групп между собой по каким-либо критериям. Каждый пользователь (включая администратора) должен быть подвешен в проекте для доступа к ресурсам этого проекта. Пользователь может принадлежать к нескольким проектам.

- Узел (Node) – сервер с поддержкой аппаратной виртуализации. Узлы бывают разных типов в зависимости от их назначения, самые важные из них в среде KeyVirt – вычислительные узлы и контроллеры, которые размещены в одноименных кластерах (Compute и Controller). По отношению к ВМ выступают в качестве гипервизоров. Узел – более общее понятие по сравнению с гипервизором и хостом.
- Гипервизор (Hypervisor) или вычислительный узел (Compute Node) – программный или аппаратный инструмент для создания и управления ВМ на одном физическом оборудовании. Гипервизор – это сервис, предоставляемый узлом (Node).
- Хост (Host) или сервер – специализированный компьютер и/или специализированное оборудование для выполнения на нем сервисного программного обеспечения. В среде oVirt *Host* также называется гипервизором, при этом он представляет собой физический сервер, на котором работают ВМ.
- Сетевое хранилище (Network attached storage, NAS) – устройство для хранения данных, подключаемое к сети и предназначенное для обслуживания нескольких компьютеров и других устройств в офисе или домашней сети. NAS можно использовать для хранения файлов, мультимедийного контента и резервного копирования данных. Благодаря NAS компьютеры и устройства в одной сети могут работать с файлами, находящимися на устройстве, как с локальными файлами. Это может упростить процесс обмена данными между пользователями.
- Сеть хранения данных (Storage Area Network, SAN) – тип сети для подключения внешних устройств хранения данных к серверам. При этом операционная система воспринимает эти устройства как непосредственно подключенные. SAN обычно работает как выделенная сеть, отдельная от LAN. SAN преимущественно применяется для предоставления блочных устройств. SAN способствует эффективному и удобному хранению и извлечению данных для приложений корпоративного уровня.
- Дата-центр или центр обработки данных (ЦОД) – выделенное помещение или здание, в котором располагаются платформы для вычисления, оборудование связи и дисковые хранилища.
- Образ ВМ (Image) – файл, содержащий все данные ВМ на определенный момент времени, в том числе загрузочную ОС. Образ предназначен для быстрого создания диска с данными, в первую очередь загрузочного диска ВМ. На основе образа невозможно кастомизировать параметры новых ВМ, в отличие от шаблона, но можно установить ОС. Наиболее распространенный формат образов – ISO.
- Шаблон (Template) – копия виртуальной машины, которую можно использовать для упрощения последующего многократного создания похожих ВМ. Шаблоны фиксируют конфигурацию ПО и оборудования, установленного на виртуальной машине, на которой основан шаблон. Шаблоны позволяют кастомизировать параметры ВМ, создаваемых на его основе. Машина, на которой основан шаблон, известна как исходная ВМ. При создании шаблона на основе машины создается копия диска ВМ, доступная только для чтения. Этот диск, доступный только для чтения, становится базовым образом диска нового шаблона и любых ВМ, созданных на основе шаблона. Этот шаблон нельзя удалить, пока в среде существуют ВМ, созданные на основе шаблона.

- Эвакуация (Evacuation) – аварийный перенос виртуальной машины с одного узла гипервизора на другой в случае сбоя узла. Эта процедура необходима для восстановления работы виртуальной машины при неожиданных проблемах.
- Эмуляция (Emulation) – комплекс программных, аппаратных средств или их сочетание, предназначенное для копирования (или эмулирования) функций одной вычислительной системы (гостя) на другой, отличной от первой, вычислительной системе (хосте) таким образом, чтобы эмулированное поведение как можно ближе соответствовало поведению оригинальной системы (гостя).
- Фенсинг (Fencing) — это механизм исключения неисправного узла из кластера, чтобы этот узел больше не работал с ВМ. Обычно результатом фенсинга является обесточивание узла, после чего кластер возобновляет работу. Для фенсинга требуется внешнее оборудование или интерфейсы удалённого управления (redfish), способное обесточить кластер, а для взаимодействия с этим оборудованием нужны fence-агенты.
- Том – это логический набор блоков, каждый из которых представляет собой каталог экспорта на сервере в доверенном пуле хранения. Виды томов:
  - том-арбитр
  - логический том (Logical Volume)
  - общий том
- Бондинг (bonding) – объединение двух или более физических сетевых интерфейсов в один виртуальный для обеспечения отказоустойчивости и повышения пропускной способности сети.
- Блок (brick) – это базовая единица хранения в файловой системе, представленная каталогом экспорта на сервере в доверенном пуле хранения.
- DRS (Distributed Resource Scheduler) – планировщик распределенных ресурсов. Это инструмент автоматической балансировки виртуальных машин между разными хостами внутри одного кластера.
- KVM (Kernel-based Virtual Machine) – технология виртуализации для виртуальной машины. Это функция ПО, которую можно установить на физических компьютерах с ОС Linux в целях создания ВМ.
- LUN (Logical Unit Number) – это предоставление блочного устройства (диска) с СХД.
- NIC (Network Interface Controller) – контроллер сетевого интерфейса. Это аппаратное обеспечение, которое подключает компьютер к сети и позволяет ему взаимодействовать с другими устройствами. vNIC (Virtual Network Interface Controller) или виртуальный сетевой контроллер – соответственно, виртуальный аналог контроллера сетевого интерфейса.
- NAS (Network Attached Storage) или сетевое хранилище – это устройство хранения данных, предназначенное для хранения файлов, которое обеспечивает постоянный доступ к данным для эффективной совместной работы по сети.
- Сокет (socket) — это программная конечная точка, обеспечивающая двустороннюю связь между процессами по сети. Сокеты предоставляют стандартизированный интерфейс для сетевого взаимодействия, позволяя приложениям отправлять и получать данные по сети.
- Страйп (stripe) – это непрерывная последовательность дисковых блоков. Размер страйпа может достигать как одного, так и сотен блоков тома.
- Реплика (replica) – точная копия устройства, такого как виртуальная машина или диск. Репликация – это процесс создания реплики устройства с последующей

синхронизацией этой реплики с исходным устройством и поддержанием работоспособности того и другого.

1. УСТАНОВКА И ПЕРВИЧНАЯ НАСТРОЙКА KEYVIRT

1.1. Описание программного продукта

KeyVirt – это платформа для управления виртуализацией, которая позволяет управлять виртуальными машинами и хранилищем при помощи различных технологий виртуализации, включая KVM. Платформа KeyVirt была создана на базе проекта oVirt. Основные преимущества KeyVirt – это гибкость и масштабируемость, что позволяет настроить виртуальную инфраструктуру под любые нужды и требования. KeyVirt также предлагает широкий спектр функций для управления виртуальными машинами, хранилищами и сетями.

2. АРХИТЕКТУРА

Архитектура KeyVirt состоит из нескольких компонентов, каждый из которых выполняет определенную функцию и может быть развернут на отдельных серверах.

2.1. Ключевые компоненты KeyVirt

Таблица 1. Ключевые компоненты KeyVirt

Имя компонента	Описание
Менеджер управления средой виртуализации (oVirt Engine)	Портал администрирования для управления средой виртуализации. Центральный компонент, который управляет всей инфраструктурой виртуализации. Он обеспечивает управление виртуальными машинами, хранилищами и сетями, а также управление пользователями, правами доступа и журналами событий.
Хост среды виртуализации (oVirt Node)	Устанавливается на хост-серверах, на которых будут запускаться виртуальные машины. Он содержит KVM-гипервизор и необходимые драйверы устройств, которые позволяют виртуальным машинам обращаться к физическим устройствам, таким как диски и сетевые интерфейсы.
QEMU-guest-agent	Устанавливается внутри виртуальных машин. Он предоставляет информацию о состоянии виртуальной машины, такую как использование CPU и памяти, и позволяет остановить, приостановить или перезагрузить виртуальную машину.
Домен хранения среды виртуализации (oVirt Storage Domain)	Компонент, который обеспечивает управление хранилищами данных, используемыми для хранения виртуальных машин и их файлов. Он поддерживает различные типы хранилищ, включая NFS, iSCSI и Fibre Channel.

Все компоненты KeyVirt могут быть развернуты на отдельных серверах, что позволяет гибко настраивать и масштабировать инфраструктуру виртуализации в соответствии с требованиями. В целом, архитектура KeyVirt обеспечивает удобное управление виртуальными машинами и хранилищами, а также высокую надежность и производительность работы.

2.2. Обзор архитектуры KeyVirt

Система KeyVirt разворачивается в режиме, при котором менеджер управления средой виртуализации работает как виртуальная машина, размещенная на самих хостах виртуализации, т.е. менеджер управления размещен на хостах в той же среде, которой и управляет. ВМ и менеджер управления средой виртуализации создаются и настраиваются при первоначальной установке кластера.

Основное преимущество такого режима заключается в том, что отсутствует необходимость в отдельном хосте с ролью менеджера управления средой виртуализации. Кроме того, сервер управления средой виртуализации может работать в режиме высокой доступности. Если хост, на котором запущен сервер управления, переходит в режим обслуживания или неожиданно выходит из строя, виртуальная машина будет автоматически перенесена на другой хост в среде. Для режима высокой доступности требуется минимум два хоста.

Минимальная настройка включает в себя:

- Сервер управления средой виртуализации (BM Engine);
- Один хост либо два хоста для режима высокой доступности сервера управления средой виртуализации;
- Внешнюю систему хранения данных (СХД) или локальное хранилище для размещения домена хранения данных (хранилища). Хранилище должно быть доступно всем хостам виртуализации.

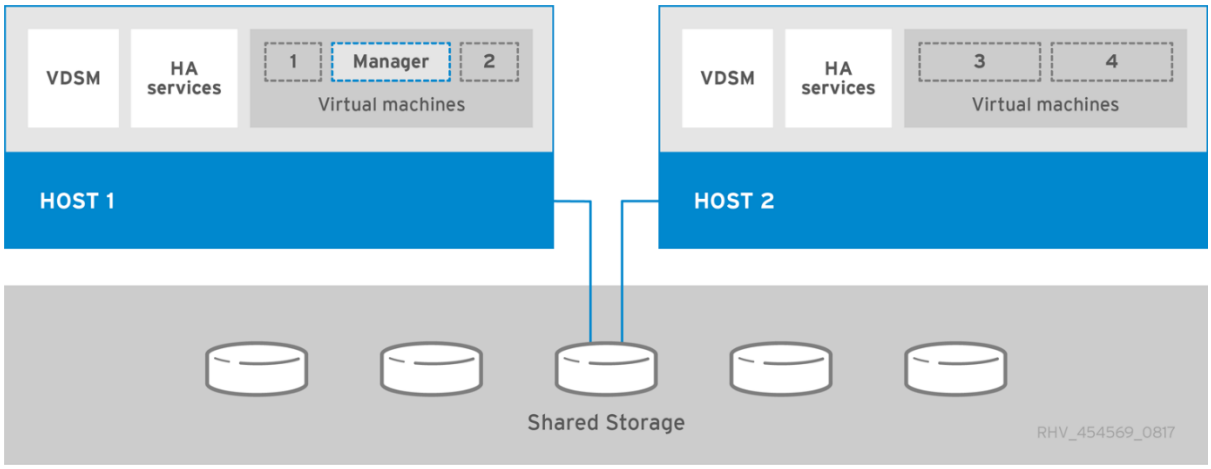

Рисунок 1. Архитектура KeyVirt

3. СИСТЕМНЫЕ ТРЕБОВАНИЯ

3.1. Требования к оборудованию для менеджера управления средой виртуализации

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.

Менеджер управления средой виртуализации работает в операционных системах Linux, таких как CentOS Linux, который является рекомендуемым вариантом Linux.

Таблица 2. Требования к оборудованию для менеджера управления средой виртуализации

Конфигурация	Минимальная	Рекомендуемая
Процессор	Двухъядерный процессор x86_64	Четырехъядерный процессор x86- 64 или несколько двухъядерных процессоров x86_64
Оперативная память	4 ГБ установленной оперативной памяти, если хранилище данных не установлено и память не используется существующими процессами	16 ГБ установленной оперативной памяти
Жесткий диск	25 ГБ доступного дискового пространства	~50 ГБ доступного дискового пространства
Сетевой интерфейс	1 сетевой интерфейс (NIC) с пропускной способностью 1 Гбит/с	1 сетевой интерфейс (NIC) с пропускной способностью 1 Гбит/с

3.1.1. Требования к браузеру

Требования к браузеру делятся на уровни (таблица 3):

Уровень 1. Полностью протестированные комбинации браузера и операционной системы.

Уровень 2. Комбинации браузера и операционной системы, которые частично протестированы и могут работать.

Уровень 3. Комбинации браузера и операционной системы, которые не протестированы, но могут работать.

Таблица 3. Требования к браузеру

Уровень поддержки	Операционная система	Браузер
Уровень 1	Enterprise Linux Любая	Mozilla Firefox Extended Support Release (ESR) version Самые последние версии Google Chrome, Mozilla

		Firefox, Microsoft Edge, Яндекс Браузер
Уровень 2	Любая	Ранние версии Google Chrome или Mozilla Firefox
Уровень 3	Любая	Другие браузеры

3.1.2. Требования к клиенту

Доступ к консолям виртуальных машин можно получить только с помощью поддерживаемых клиентов Remote Viewer (virt-viewer) в Enterprise Linux и Windows. Доступ к консолям виртуальных машин осуществляется через протоколы SPICE, VNC или RDP (только для Windows). Графический драйвер QXL может быть установлен в гостевой операционной системе для улучшения и расширения функциональных возможностей SPICE. SPICE в настоящее время поддерживает максимальное разрешение 2560x1600 пикселей.
Поддерживаемые драйверы QXL доступны в Enterprise Linux, Windows XP и Windows 7.

3.1.3. Требования к операционной системе

Менеджер управления средой виртуализации должен быть установлен на базовой установке Enterprise Linux 8.7 или более поздней версии.

Не устанавливайте дополнительных пакетов после базовой установки, так как они могут вызвать проблемы с зависимостями при попытке установить пакеты, необходимые для сервера управления средой виртуализации.

Не включайте дополнительные репозитории, кроме тех, которые необходимы для установки сервера управления средой виртуализации.

3.2. Требования к хосту

3.2.1. Требования к процессору

Все ЦП должны поддерживать расширения ЦП Intel® 64 или AMD64, а также должны быть включены расширения аппаратной виртуализации AMD-V™ или Intel VT®. Также требуется поддержка флага No eXecute (NX).

Поддерживаются следующие модели ЦП:

AMD

- Opteron G4
- Opteron G5
- EPYC

Intel

- Nehalem
- Westmere
- SandyBridge
- IvyBridge
- Haswell
- Broadwell
- Skylake Client

- Skylake Server
- Cascadelake Server

Можно проверить, какие расширения процессора доступны на системе.

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

1. Загрузите операционную систему и зарегистрируйтесь как пользователь, имеющий права администратора.
2. В командной строке определите, что ваш процессор имеет необходимые расширения и что они включены, выполнив команду:

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

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.

3.2.2. Требования к оперативной памяти

Минимально необходимый объем оперативной памяти составляет 2 ГБ. Для уровней кластера от 4.2 до 4.5 максимальный поддерживаемый объем ОЗУ на ВМ в хосте среды виртуализации составляет 6 ТБ. Для уровней кластера от 4,6 до 4,7 максимальный поддерживаемый объем ОЗУ на ВМ в хосте среды виртуализации составляет 16 ТБ.

Объем оперативной памяти зависит от требований гостевой операционной системы, 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.

3.2.3. 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. Хост среды виртуализации 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.

3.2.4. Минимальные требования и рекомендуемая схема разбиения хранилища

- / (root) – 6 ГБ
- /home – 1 ГБ
- /tmp – 1 ГБ
- /boot – 1 ГБ
- /var – 5 ГБ
- /var/crash – 10 ГБ
- /var/log – 8 ГБ
- /var/log/audit – 2 ГБ
- /var/tmp – 10 ГБ
- swap – 1 ГБ
- Anaconda резервирует 20 % размера тонкого пула в группе томов для будущего расширения метаданных. Это необходимо для предотвращения нехватки места в готовой конфигурации при нормальных условиях использования. Также не поддерживается избыточная подготовка тонких пулов во время установки.

Минимальный общий объем – 64 ГБ.

Если вы также устанавливаете Engine Appliance для самостоятельной установки ядра, размер /var/tmp должен быть не менее 10 ГБ. Если вы планируете использовать избыточное выделение памяти, добавьте достаточно места подкачки, чтобы обеспечить виртуальную память для всех виртуальных машин.

3.2.5. 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.

3.2.6. Требования к назначению устройств

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

- Процессор должен поддерживать IOMMU (например, VT-d или AMD-Vi);
- Прошивка должна поддерживать IOMMU;
- Корневые порты процессора должны поддерживать ACS или ACS-эквивалентные возможности;
- PCI-устройства должны поддерживать ACS или ACS-эквивалентные возможности.

Рекомендуется, чтобы все коммутаторы PCI и мосты между устройством PCI 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 PCI 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.

Ознакомьтесь со спецификациями и таблицами провайдеров, чтобы убедиться, что ваше оборудование соответствует этим требованиям. Команду lspci -v можно использовать для печати информации об устройствах PCI, уже установленных в системе.

3.2.7. Требования к виртуальному графическому процессору

Хост должен соответствовать следующим требованиям, чтобы виртуальные машины на этом хосте могли использовать vGPU:

- vGPU-совместимый графический процессор;
- Ядро хоста с поддержкой GPU;
- Установленный графический процессор с драйверами;
- Предварительно заданный тип mdev_type соответствует одному из типов mdev, поддерживаемых устройством;
- Драйверы с поддержкой vGPU, установлены на каждом узле кластера;
- vGPU-поддерживается операционной системой виртуальной машины с установленными графическими драйверами.

3.3. 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.

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

3.3.1. Диапазон сети для развертывания Self-hosted Engine

Процесс развертывания Self-hosted Engine временно использует /24сетевой адрес в домене 192.168. По умолчанию используется 192.168.222.0/24, и если этот адрес используется, он пробует другие /24 адреса 192.168, пока не найдет тот, который не используется. Если он не найдет неиспользуемый сетевой адрес в этом диапазоне, произойдет сбой развертывания.

При установке Self-hosted Engine с помощью командной строки вы можете настроить сценарий развертывания на использование альтернативного /24сетевого диапазона с параметром --ansible-extra-vars=he_ipv4_subnet_prefix=PREFIX, где PREFIX – префикс для диапазона по умолчанию. Например:

```
# hosted-engine --deploy --ansible-extra-vars=he_ipv4_subnet_prefix=192.168.222
```

Примечание. Вы можете установить другой диапазон, только установив KeyVirt как Self-Hosted Engine с помощью командной строки.

3.3.2. Требования к брандмауэру для защиты DNS, NTP и IPMI

Требования к брандмауэру для всех следующих тем являются особыми случаями, требующими индивидуального рассмотрения.

DNS и NTP

KeyVirt не создает сервер DNS или NTP, поэтому брандмауэру не нужно открывать порты для входящего трафика.

По умолчанию Enterprise Linux разрешает исходящий трафик к DNS и NTP по любому адресу назначения. Если вы отключите исходящий трафик, определите исключения для запросов, отправляемых на серверы DNS и NTP.

Примечания:

- Менеджер управления средой виртуализации и все хосты (хост среды виртуализации и хост Enterprise Linux) должны иметь полное доменное имя и полное, точно выровненное прямое и обратное разрешение имен.
- Запуск службы DNS в качестве виртуальной машины в среде KeyVirt не поддерживается. Все службы DNS, которые использует среда KeyVirt, должны размещаться вне среды.
- Используйте DNS вместо /etc/hosts файла для разрешения имен. Использование файла hosts обычно требует больше работы и повышает вероятность ошибок.

IPMI и другие механизмы фенсинга (по необходимости)

Для IPMI (Intelligent Platform Management Interface) и других механизмов фенсинга брандмауэру не обязательно иметь открытые порты для входящего трафика.

По умолчанию Enterprise Linux разрешает исходящий IPMI-трафик на порты с любым адресом назначения. Если вы отключите исходящий трафик, сделайте исключения для запросов, отправляемых на ваш IPMI или серверы фенсинга.

Каждый хост среды виртуализации и хост Enterprise Linux в кластере должен иметь возможность подключаться к fence-устройствам всех других хостов в кластере. Если на узлах кластера возникла ошибка (ошибка сети, ошибка хранилища) и они не могут работать как узлы, они должны иметь возможность подключаться к другим узлам в дата-центре.

Конкретный номер порта зависит от типа используемого fence-агента и его настройки.

Таблицы требований к брандмауэру в следующих разделах не представляют этот параметр.

3.3.3. Требования к брандмауэру менеджера управления средой виртуализации

Для работы менеджера управления средой виртуализации необходимо, чтобы несколько портов были открыты для пропуска сетевого трафика через системный брандмауэр.

Скрипт engine-setup может настроить брандмауэр автоматически.

По умолчанию конфигурация брандмауэра следующая:

Таблица 4. Требования к брандмауэру менеджера управления средой виртуализации

ID	Порт	Протокол	Источник	Место назначения	Предназначение	Шифрование
M1	-	ICMP	Хосты среды виртуализации	Менеджер управления	Необязательно. Может помочь в диагностике.	Нет
M2	22	TCP	Система (ы), используемая для обслуживания менеджера управления	Менеджер управления	Доступ Secure Shell (SSH). Необязательно.	Да
M3	2222	TCP	Клиенты, получающие доступ к консолям ВМ	Менеджер управления	Доступ через Secure Shell (SSH) для подключения к консолям ВМ.	Да
M4	80, 443	TCP	Клиенты Портала администрирования Клиенты Портала ВМ Хосты среды виртуализации Клиенты REST API	Менеджер управления	Предоставляет HTTP (порт 80, не зашифрован) и HTTPS (порт 443, зашифрован) доступ к менеджеру управления. HTTP перенаправляет соединения на HTTPS.	Да
M5	6100	TCP	Клиенты Портала	Менеджер	Предоставляет доступ через	Нет

			администрирования	управления	прокси-сервер веб-сокет для веб-консольного клиента noVNC, когда прокси-сервер веб-сокет работает на менеджере управления. Если прокси-сервер веб-сокет работает на другом хосте, этот порт не используется.	
			Клиенты Портала ВМ			
M6	7410	TCP	Хосты среды виртуализации	Менеджер управления	Если Kdump включен на хостах, откройте порт для fence_kdump на сервере управления. Fence_kdump не поддерживает шифрованное соединение. Вы можете вручную настроить этот порт, чтобы заблокировать доступ от хостов, которые не соответствуют требованиям.	Нет
M7	54323	TCP	Клиенты Портала администрирования	Менеджер управления (служба ovirt-imageio)	Требуется для связи со службой ovirt-imageio.	Да
M8	6642	TCP	Хосты среды виртуализации	Open Virtual Network (OVN)	Требуется для подключения к базе данных OVN.	Да
M9	9696	TCP	Клиенты провайдера внешней	Внешний сетевой провайд	OpenStack Networking API.	Да, с конфигурацие

			сети для OVN	ер для OVN		й, созданной с помощью engine-setup
M10	35357	TCP	Клиенты провайдера внешней сети для OVN	Внешний сетевой провайдер для OVN	OpenStack Identity API.	Да, с конфигурацией, созданной с помощью engine-setup
M11	53	TCP	Менеджер управления	DNS-сервер	DNS-запросы от портов с номерами более, чем 1023 к порту 53 и ответы на них. Открыты по умолчанию.	Нет
M12	123	TCP	Менеджер управления	NTP-сервер	NTP-запросы от портов с номерами более, чем 1023 к порту 123 и ответы на них. Открыты по умолчанию.	Нет

Примечание. Порт для северной базы данных OVN (6641) не указан, поскольку в конфигурации по умолчанию единственным клиентом для северной базы данных OVN (6641) является ovirt-provider-ovn. Поскольку они оба работают на одном хосте, их связь не видна в сети.

По умолчанию Enterprise Linux разрешает исходящий трафик к DNS и NTP по любому адресу назначения. Если вы отключите исходящий трафик, сделайте исключения для сервера управления для отправки запросов на DNS- и NTP-серверы. Другим узлам также могут потребоваться DNS и NTP. В этом случае ознакомьтесь с требованиями для этих узлов и соответствующим образом настройте брандмауэр.

3.3.4. Требования к брандмауэру хоста виртуализации

Хостам Enterprise Linux и хостам среды виртуализации необходимо открыть несколько портов, чтобы разрешить сетевой трафик через системный брандмауэр. Правила брандмауэра автоматически настраиваются по умолчанию при добавлении нового хоста в сервер управления средой виртуализации, перезаписывая любую ранее существовавшую конфигурацию брандмауэра.

Чтобы отключить автоматическую настройку брандмауэра при добавлении нового узла, снимите флажок Automatically configure host firewall в Advanced Parameters.

Таблица 5. Требования к брандмауэру узла виртуализации

ID	Порт	Протокол	Источник	Назначение	Предназначение	Шифрование
H1	22	TCP	Менеджер управления средой виртуализации	Хосты среды виртуализации	Secure Shell (SSH). Необязательно.	Да
H2	2223	TCP	Менеджер управления	Хосты среды виртуализации	Доступ через Secure Shell (SSH) для подключения к консолям ВМ.	Да
H3	161	UDP	Хосты среды виртуализации	Менеджер управления	Простой протокол управления сетью (SNMP). Требуется, только если вы хотите, чтобы прерывания Simple Network Management Protocol отправлялись с хоста одному или нескольким внешним SNMP-менеджерам. Необязательно.	Нет
H4	111	TCP	NFS-сервер	Хосты среды виртуализации	NFS-соединения. Необязательно.	Нет
H5	5900-6923	TCP	Клиенты Портала администрирования Клиенты Портала ВМ	Хосты среды виртуализации	Удаленный доступ к гостевой консоли через VNC и SPICE. Эти порты должны быть открыты для	Да (необязательно)

					обеспечения доступа клиентов к ВМ.	
H6	5989	TCP, UDP	Менеджер объектов общей информационной модели (CIMOM)	Хосты среды виртуализации	Используется CIMOM для Мониторинга ВМ, работающих на хосте. Требуется, только если вы хотите использовать CIMOM для мониторинга ВМ в вашей среде виртуализации. Необязательно.	Нет
H7	9090	TCP	Менеджер управления Клиентские машины	Хосты среды виртуализации	Требуется для доступа к веб-интерфейсу Cockpit, если он установлен.	Да
H8	16514	TCP	Хосты среды виртуализации	Хосты среды виртуализации	Миграция ВМ с использованием libvirt.	Да
H9	49152 - 49215	TCP	Хосты среды виртуализации	Хосты среды виртуализации	Миграция и фенсинг ВМ с использованием VDSM. Эти порты должны быть открыты для облегчения как автоматической, так и ручной миграции ВМ.	Да. В зависимости от fence-агента, миграция осуществляется через libvirt
H10	54321	TCP	Менеджер управления Хосты среды виртуализации	Хосты среды виртуализации	Хосты виртуализации.	Да
H11	54322	TCP	Менеджер управления служба ovirt-imageio	Хосты среды виртуализации	Требуется для связи со службой ovirt-imageo.	Да
H12	6081	UDP	Хосты среды виртуализации	Хосты среды виртуализации	Требуется, когда в качестве сетевого	Нет

					провайдера используется открытая виртуальная сеть (OVN), чтобы OVN мог создавать туннели между хостами.	
H13	53	TCP, UDP	Хосты среды виртуализации	DNS-сервер	DNS-запросы поиска от портов с номерами более, чем 1023 к порту 53 и ответы на них. Открыт по умолчанию.	Нет
H14	123	UDP	Хосты среды виртуализации	NTP-сервер	NTP-запросы от портов с номерами более, чем 1023 к порту 123 и ответы на них. Открыт по умолчанию.	Да
H15	4500	TCP, UDP	Хосты среды виртуализации	Хосты среды виртуализации	Internet Security Protocol (IPSec).	Да
H16	500	UDP	Хосты среды виртуализации	Хосты среды виртуализации	Internet Security Protocol (IPSec).	Да
H17	–	FY, ESP	Хосты среды виртуализации	Хосты среды виртуализации	Internet Security Protocol (IPSec).	Да

Примечание. По умолчанию Enterprise Linux разрешает исходящий трафик к DNS и NTP по любому адресу назначения. Если вы отключите исходящий трафик, сделайте исключения для хостов среды виртуализации.

Хосты Enterprise Linux нужны для отправки запросов на серверы DNS и NTP. Другим узлам также могут потребоваться DNS и NTP. В этом случае ознакомьтесь с требованиями для этих узлов и соответствующим образом настройте брандмауэр.

3.3.5. Требования к брандмауэру сервера базы данных

KeyVirt поддерживает использование удаленного сервера базы данных для базы данных сервера управления средой виртуализации (engine) и базы данных хранилища данных (ovirt-engine-history). Если вы планируете использовать удаленный

сервер базы данных, он должен разрешать подключения от сервера управления и службы хранилища данных (которая может быть отделена от сервера управления).

Точно так же, если вы планируете получить доступ к локальной или удаленной базе данных хранилища данных из внешней системы, база данных должна разрешать подключения из этой системы.

Внимание! Доступ к базе данных сервера управления средой виртуализации из внешних систем не поддерживается.

Таблица 6. Требования к брандмауэру сервера базы данных

ID	Порт	Протокол	Источник	Назначение	Предназначение	Шифрование
D1	5432	TCP, UDP	Менеджер управления Сервис Data Warehouse	Сервер базы данных сервера управления средой виртуализации (engine) Сервер базы данных Data Warehouse (ovirt-engine-history)	Порт по умолчанию для соединений с базой данных PostgreSQL.	По умолчанию — нет
D2	5432	TCP, UDP	Внешние системы	Сервер базы данных Data Warehouse (ovirt-engine-history)	Порт по умолчанию для соединений с базой данных PostgreSQL.	По умолчанию — нет

3.3.6. Максимальные требования к блоку передачи

Рекомендуемое значение Максимального количества единиц передачи (MTU) для узлов во время развертывания – 1500. Этот параметр можно обновить после настройки среды на другое значение MTU.

4. ПОДГОТОВКА К УСТАНОВКЕ

4.1. Подготовка хранилища

Вам необходимо подготовить хранилище, которое будет использоваться для доменов хранения в новой среде. В среде KeyVirt должен быть хотя бы один домен хранения данных, но рекомендуется добавить больше.

Внимание! При установке или переустановке операционной системы хоста среды виртуализации настоятельно рекомендует сначала отключить любое существующее хранилище, не относящееся к ОС, которое подключено к хосту, чтобы избежать случайной инициализации этих дисков и потенциальной потери данных.

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 типы хранилища:

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

Требования:

- Самостоятельно размещенные модули должны иметь дополнительный домен данных с объемом не менее 74 ГБ, выделенным для виртуальной машины сервера управления средой виртуализации. Установщик сервера управления средой виртуализации создает этот домен. Перед установкой подготовьте хранилище для этого домена.

Внимание! Расширение или иное изменение домена хранилища локального ядра после развертывания локального ядра не поддерживается. Любое такое изменение может помешать загрузке сервера управления средой виртуализации.

- При использовании домена блочного хранилища, либо FCP, либо iSCSI, единственный целевой LUN является единственной поддерживаемой установкой для сервера управления средой виртуализации.
- Если вы используете хранилище iSCSI, домен хранилища сервера управления средой виртуализации должен использовать выделенную цель iSCSI. Любые дополнительные домены хранения должны использовать другую цель iSCSI.
- Настоятельно рекомендуется создавать дополнительные домены хранения данных в том же дата-центре, что и самостоятельный домен хранилища ядра. Если вы развернете самостоятельный модуль в дата-центре только с одним активным доменом хранения данных, и этот домен хранения будет поврежден, вы не сможете добавить новые домены хранения или удалить поврежденный домен хранения. Вы должны повторно развернуть локальный сервер управления средой виртуализации.

4.1.1. Подготовка хранилища NFS

Для KeyVirt требуются определенные учетные записи системных пользователей и группы системных пользователей, чтобы сервер управления средой виртуализации мог хранить данные в доменах хранения, представленных экспортируемыми каталогами. Следующая процедура устанавливает разрешения для одного каталога. Вы должны повторить шаги chown и chmod для всех каталогов, которые вы собираетесь использовать в качестве доменов хранения в KeyVirt.
Требования:

1. Установите пакет NFS utils:

   # dnf install nfs-utils -y

2. Проверьте включенные версии:

   # cat /proc/fs/nfsd/versions

3. Включите следующие службы:

   # systemctl enable nfs-server
   # systemctl enable rpcbind

Процедура**:**

1. Создайте группу kvm:

   # groupadd kvm -g 36

2. Создайте пользователя vdsm в группе kvm:

   # useradd vdsm -u 36 -g kvm

3. Создайте storage каталог и измените права доступа.

   # mkdir /storage
   # chmod 0755 /storage
   # chown 36:36 /storage/

4. Добавьте storage каталог /etc/exports с соответствующими разрешениями.

   # vi /etc/exports
   # cat /etc/exports
   /storage *(rw)

5. Перезапустите следующие службы:

   # systemctl restart rpcbind
   # systemctl restart nfs-server

6. Чтобы увидеть, какой экспорт доступен для определенного IP-адреса:

   # exportfs
   /nfs_server/srv
   10.46.11.3/24
   /nfs_server <world>

Если изменения /etc/exports были внесены после запуска служб, exportfs -r a команду можно использовать для перезагрузки изменений. После выполнения всех вышеперечисленных этапов каталог экспорта должен быть готов, и его можно протестировать на другом хосте, чтобы убедиться, что его можно использовать.

4.1.2. Подготовка хранилища iSCSI

KeyVirt 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. Используйте команду vdsm-tool config-lvm-filter для создания фильтров для LVM.

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, добавьте 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 boot_LUN_wwid
      no_path_retry queue
   }
```

4.1.3. Подготовка FCP-хранилища

KeyVirt 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.
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, добавьте 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 boot_LUN_wwid
      no_path_retry queue
   }
```


4.2. Настройка конфигураций Multipath для провайдеров SAN

Если ваша среда RHV настроена на использование многолучевых соединений с SAN, вы можете настроить параметры многолучевой конфигурации в соответствии с требованиями, указанными вашим провайдером хранилища. Эти настройки могут переопределять как параметры по умолчанию, так и параметры, указанные в файлах /etc/multipath.conf.
Чтобы переопределить настройки многолучевости, не настраивайте файлы /etc/multipath.conf. Поскольку VDSM владеет /etc/multipath.conf, установка или обновление VDSM или KeyVirt может перезаписать этот файл, включая любые содержащиеся в нем настройки. Эта перезапись может привести к серьезным сбоям в хранении.

Вместо этого вы создаете в каталоге файл /etc/multipath/conf.d, содержащий параметры, которые вы хотите настроить или переопределить.
VDSM выполняет файлы /etc/multipath/conf.d в алфавитном порядке. Таким образом, чтобы контролировать порядок выполнения, вы начинаете имя файла с числа, которое делает его последним. Например, /etc/multipath/conf.d/90-myfile.conf.
Чтобы избежать серьезных сбоев хранилища, следуйте рекомендациям:

- Не меняйте/etc/multipath.conf. Если файл содержит изменения, внесенные пользователем, и файл перезаписывается, это может вызвать непредвиденные проблемы с хранением.
- Не переопределяйте настройки user_friendly_names и find_multipaths. Подробнее см. в разделе *Рекомендуемые настройки для Multipath.conf*.
- Избегайте переопределения параметров no_path_retry и polling_interval, если провайдер хранилища специально не требует от вас этого.

Несоблюдение этих рекомендаций может привести к катастрофическим ошибкам хранения.

Требования:

- VDSM настроен на использование многолучевого модуля. Чтобы убедиться в этом, введите:
  # vdsm-tool is-configured --module multipath

Процедура:

1. Создайте новый файл конфигурации в каталоге /etc/multipath/conf.d.
2. Скопируйте отдельные настройки, которые вы хотите переопределить, /etc/multipath.conf в новый файл конфигурации в формате /etc/multipath/conf.d/<my_device>.conf. Удалите все метки комментариев, отредактируйте значения параметров и сохраните изменения.
3. Примените новые параметры конфигурации, введя:
   # systemctl reload multipathd

Не перезапускайте службу multipathd. Это приводит к ошибкам в журналах VDSM.
Этапы проверки:

1. Проверьте, что новая конфигурация работает должным образом на нерабочем кластере в различных сценариях отказа. Например, отключите все подключения к хранилищу.
2. Включайте одно подключение за раз. Повторите несколько раз и убедитесь, что это делает домен хранения доступным.

4.2.1. Рекомендуемые настройки для Multipath.conf

Не переопределяйте следующие настройки:

- **user_friendly_names no**

Имена устройств должны быть согласованы во всех гипервизорах. Например, /dev/mapper/{WWID}. Значение по умолчанию для этого параметра no предотвращает присвоение произвольных и непоследовательных имен устройств, например, /dev/mapper/mpath{N} в различных гипервизорах, что может привести к

непредсказуемому поведению системы. Не меняйте этот параметр на user_friendly_names yes. Дружественные имена могут вызвать непредсказуемое поведение системы или сбои и не поддерживаются.

- **find_multipaths no**

Этот параметр определяет, будет ли хост среды виртуализации пытаться получить доступ к устройствам через многолучевой доступ только в том случае, если доступно более одного пути. Текущее значение (no) позволяет KeyVirt получать доступ к устройствам по множеству путей, даже если доступен только один путь. Избегайте переопределения следующих параметров, если это не требуется провайдером системы хранения:

- **no_path_retry 4**

Этот параметр определяет количество повторных попыток опроса при отсутствии доступных путей. Если предположить, что интервал опроса по умолчанию составляет 5 секунд, проверка путей занимает 20 секунд. Если нет пути, multipathd сообщает ядру, что нужно прекратить ставить в очередь, и прерывает все незавершенные и будущие операции ввода-вывода до тех пор, пока путь не будет восстановлен. Когда путь восстанавливается, 20-секундная задержка сбрасывается для следующего отказа всех путей.

- **polling_interval 5**

Этот параметр определяет количество секунд между попытками опроса для определения того, открыт ли путь или произошел сбой. Если провайдер не указал четкую причину увеличения значения, оставьте созданное VDSM значение по умолчанию, чтобы система быстрее реагировала на сбои пути.

5. УСТАНОВКА

5.1. Описание процесса установки

Установка включает следующие основные шаги:

1. Установка узла развертывания хоста. Этот хост станет первым хостом с размещенным на нем сервером управления средой виртуализации. Подойдет как хост среды виртуализации, так и Enterprise Linux.
2. Подготовка хранилища для домена хранения сервера управления и для стандартных доменов хранения. Вы можете использовать один из следующих типов хранения: NFS, ISCSI и Fibre Channel (FCP).
3. Установка и настройка сервера управления.
4. (Дополнительно) добавление узлов сервера управления и стандартных хостов в сервере управления.

5.2. Установка сервера управления средой виртуализации на отдельной виртуальной машине

Сервер управления средой виртуализации можно развернуть с хоста среды виртуализации или хоста Enterprise Linux, CenOS и дериативы RedHat.

При установке или переустановке операционной системы хоста среды виртуализации настоятельно рекомендует сначала отключить любое существующее хранилище, не относящееся к ОС, которое подключено к хосту, чтобы избежать случайной инициализации этих дисков и потенциальной потери данных.

5.2.1. Установка хостов среды виртуализации

Хост среды виртуализации – это минимальная операционная система, основанная на Linux, предназначенная для обеспечения простого метода настройки физической машины для работы в качестве гипервизора в среде KeyVirt. Минимальная операционная система содержит только пакеты, необходимые для работы компьютера в качестве гипервизора, и опционально имеет веб-интерфейс Cockpit для мониторинга хоста и выполнения административных задач. Хост должен соответствовать минимальным требованиям к хосту.

Хост должен соответствовать минимальным требованиям, которые описаны в разделе *Требования к хосту* выше.

Внимание! При установке или переустановке операционной системы хоста среды виртуализации настоятельно рекомендует сначала отключить любое существующее хранилище, не связанное с ОС, которое подключено к хосту, чтобы избежать случайной инициализации этих дисков и, как следствие, потенциальной потери данных.

Процедура установки:

1. Скачайте установочный ISO-образ, содержащий подготовленную к установке ОС с набором необходимых пакетов.
2. Запишите установочный ISO-образ хоста среды виртуализации на USB-накопитель, компакт-диск или DVD-диск.
3. Запустите машину, на которой вы устанавливаете хост среды виртуализации, загрузившись с подготовленного установочного носителя.
4. В меню загрузки выберите **Install KeyVirt Node** и нажмите Enter.

Примечание. Вы также можете нажать клавишу Tab для редактирования параметров ядра. Параметры ядра должны быть разделены пробелом, и вы можете загрузить систему, используя указанные параметры ядра, нажав клавишу Enter. Нажмите клавишу Esc, чтобы отменить любые изменения параметров ядра и вернуться в меню загрузки.

5. Выберите язык и нажмите Continue.
6. Выберите раскладку клавиатуры на экране Keyboard Layout и нажмите Done.
7. Выберите устройство, на которое необходимо установить хост среды виртуализации, на экране Installation Destination. При желании включите шифрование. Нажмите Done.

Внимание! Используйте параметр Automatically configure partitioning.

8. Выберите часовой пояс на экране Time & Date и нажмите Done.
9. Выберите сеть на экране Network & Host Name и нажмите Configure, чтобы настроить детали подключения.
10. Введите имя хоста в поле Host Name и нажмите Done.
11. Нажмите Begin Installation.
12. Установите пароль root и, при необходимости, создайте дополнительного пользователя во время установки хоста среды виртуализации.

Внимание! Не создавайте ненадежных пользователей на хосте среды виртуализации, так как это может привести к использованию локальных уязвимостей безопасности.

13. Нажмите Reboot, чтобы завершить установку.

Примечание. Когда хост среды виртуализации перезапускается, nodectl check выполняет проверку работоспособности хоста и отображает результат при входе в систему в командной строке. Сообщение node status: OK или node status: DEGRADED указывает на состояние здоровья. Запустите nodectl check, чтобы получить больше информации.

5.3. Подготовка хранилища

Подготовка хранилища описана в разделе *Подготовка к установке* выше.

6. ПОСЛЕ УСТАНОВКИ

6.1. Проверка работоспособности

Зайдите в веб-интерфейс по адресу, который вы задали для сервера управления средой виртуализации, например, http://...→ Портал администрирования → Введите имя пользователя admin и пароль, заданный при установке системы. Откроется веб-интерфейс управления.

6.2. Добавление хостов среды виртуализации

KeyVirt поддерживает два типа хостов: хосты среды виртуализации (oVirt Nodes) и хосты Enterprise Linux. В зависимости от вашей среды вы можете использовать только один тип или оба. Для таких функций, как миграция и высокая доступность, требуется как минимум два хоста.

Подробнее о хостах см. в разделе *Хосты* в *Руководстве по эксплуатации KeyVirt для администратора*.

Таблица 7. Типы хостов

Тип хоста	Другие названия	Описание

Хост среды виртуализации	KeyVirt Node, тонкий хост	Это минимальная операционная система на базе Linux систем.
Обычный хост	Хост Linux (например, CentOS), толстый хост	В качестве хостов можно использовать Linux-системы с включенными соответствующими репозиториями, такие как CentOS Linux.

Совместимость хостов

При создании нового дата-центра вы можете установить версию совместимости. Выберите версию совместимости, подходящую для всех хостов в дата-центре. После установки регрессия версии не допускается. Для новой установки KeyVirt последняя версия совместимости устанавливается в дата-центре и кластере по умолчанию; для использования более ранней версии совместимости необходимо создать дополнительные дата-центры и кластеры.

Подробнее о хостах см. в разделе *Хосты* в *Руководстве по эксплуатации KeyVirt для администратора*.

6.2.1. Хосты среды виртуализации

Процедуру установки узлов см. в разделе *Установка хостов среды виртуализации* выше.

Требования

- Путь к репозиторию, содержащему пакет, который вы хотите установить.
- Авторизация на хосте с правами root.

Процедура:

1. Остановите и выключите службы iscsid и multipathd, с помощью команд:
   systemctl stop iscsid.socket
   systemctl stop iscsid.service
   systemctl disable iscsid.socket
   systemctl disable iscsid.service
   systemctl stop multipathd multipathd.socket
   systemctl disable multipathd multipathd.socket

2. Создайте группы и пользователей с помощью команд:

   groupadd -g 36 kvm

   groupmod -g 36 kvm

   groupadd -g 987 ovirt-vmconsole

   groupadd -g 986 openvswitch

   groupadd -g 989 ovirtimg

   groupadd -g 179 sanlock

   groupadd -g 42435 neutron

useradd -c "oVirt VM Console" -d /usr/share/ovirt-vmconsole/empty -u 991 -g 987 -s /bin/sh ovirt-vmconsole

useradd -c "Open vSwitch Daemons" -d / -u 990 -g 986 -s /sbin/nologin openvswitch

useradd -c "oVirt imageio" -d /run/ovirt-imageio -u 985 -g 989 -s /sbin/nologin ovirtimg

useradd sanlock -u 179 -d /run/sanlock -c sanlock -g 179

useradd vdsm -u 36 -s /sbin/nologin -d /var/lib/vdsm -g 36 -c "Node Virtualization Manager"

useradd -u 42435 -g 42435 -d /home/neutron -s /bin/sh neutron

usermod -aG qemu ovirtimg

usermod -aG kvm ovirtimg

usermod -aG kvm sanlock

usermod -aG kvm qemu

usermod -aG qemu sanlock

usermod -aG qemu vdsm

usermod -aG sanlock vdsm

usermod -aG disk sanlock

usermod -aG cdrom qemu

usermod -aG hugetlbfs openvswitch

3. Создайте каталоги с помощью команд:

mkdir -p /etc/pki/ovirt-vmconsole

mkdir -p /var/lib/vdsm

mkdir -p /run/{openvswitch,ovn}

mkdir -p /etc/libvirt/

mkdir -p /etc/pki/{CA,vdsm,libvirt}

mkdir -p /var/log/keyvirt/{openvswitch,ovn,vdsm,ovirt-imageio,libvirt}

mkdir -p /var/lib/iscsi

mkdir -p /rhev/data-center

mkdir -p /var/lib/{libvirt,vdsm}

mkdir -p /usr/lib/firewalld/{services,zones}

mkdir -p /var/log/kolla/neutron/

mkdir -p /etc/kolla/neutron-openvswitch-agent/

mkdir -p /dev/hugepages1G

4. Скопируйте файлы настроек с помощью команд:

cp multipathd/conf.d/multipath.conf /etc/

cp ./sysctl.vdsm.conf /etc/sysctl.d/vdsm.conf

"/sbin/sysctl" -q -p "/etc/sysctl.d/vdsm.conf"

cp vdsm/etc/modules-load.d/vdsm.conf /etc/modules-load.d/

cp vdsm-lvm.rules /usr/lib/udev/rules.d/57-vdsm-lvm.rules

cp setup/firewalld/services/*.xml /usr/lib/firewalld/services

cp setup/firewalld/zones/*.xml /usr/lib/firewalld/zones

5. Создайте файлы, с помощью команд:

   touch /etc/libvirt/qemu.conf

   touch /var/log/keyvirt/sanlock.log

6. Назначьте права на каталоги с помощью команд:

   chown openvswitch:hugetlbfs /run/openvswitch

   chown openvswitch:openvswitch /run/ovn

   chown openvswitch:hugetlbfs /var/log/keyvirt/openvswitch

   chown openvswitch:openvswitch /var/log/keyvirt/ovn

   chown vdsm:root /var/log/keyvirt/vdsm

   chown vdsm:kvm /rhev/data-center

   chown neutron:neutron /var/log/kolla/neutron/

7. Смонтируйте директорию пользователю hugetlbfs с параметрами, с помощью команды:

   mount -t hugetlbfs -o pagesize=1G none /dev/hugepages1G

6.2.2. Установка QEMU Guest Agent на CentOS 8 / RHEL 8 Linux guest

Установка QEMU Guest Agent на CentOS 8

1. Выполните следующие команды в CentOS 8, чтобы установить Guest Agent oVirt:

   sudo yum -y install qemu-guest-agent

2. Установите и включите сервис:

   sudo systemctl enable --now qemu-guest-agent

3. Проверьте статус службы, чтобы убедиться, что она работает:

   $ systemctl status qemu-guest-agent
   ● qemu-guest-agent.service - QEMU Guest Agent
   Loaded: loaded (/usr/lib/systemd/system/qemu-guest-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-01-03 15:02:16 EAT; 24min ago
   Main PID: 756 (qemu-ga)

```
 Tasks: 1 (limit: 23985)
Memory: 2.7M
CGroup: /system.slice/qemu-guest-agent.service
        └─756 /usr/bin/qemu-ga --method=virtio-serial --path=/dev/virtio-
ports/org.qemu.guest_agent.0 --blacklist=guest-file-open,guest-file-close,g>
Jan 03 15:02:16 localhost.localdomain systemd[1]: Started QEMU Guest Agent.
```

6.2.3. Хосты Enterprise Linux

Установка хостов Enterprise Linux

Инструкции по установке хостов Enterprise Linux см. в разделе *Установка хостов Enterprise Linux (CentOS 8-9)* выше.

Установка Cockpit на хостах Enterprise Linux

Вы можете установить Cockpit для мониторинга ресурсов хоста и выполнения административных задач.

Процедура:

1. Установите пакеты панели мониторинга:

   ```
   # dnf install cockpit-ovirt-dashboard
   ```
2. Включите и запустите службу cockpit.socket:

   ```
   # systemctl enable cockpit.socket
   # systemctl start cockpit.socket
   ```
3. Проверьте, является ли Cockpit активной службой в брандмауэре:

   ```
   # firewall-cmd --list-services
   ```
4. Вы должны увидеть cockpit в списке. Если его там нет, введите следующую команду с правами root, чтобы добавить cockpit в качестве службы к вашему брандмауэру:

   ```
   # firewall-cmd --permanent --add-service=cockpit
   ```
5. Опция --permanent сохраняет активность службы cockpit после перезагрузки.
6. Вы можете войти в веб-интерфейс Cockpit по адресу: https://HostFQDNorIP:9090

Рекомендуемые методы настройки хост-сетей

Внимание! Всегда используйте менеджер управления средой виртуализации для изменения конфигурации сети хостов в ваших кластерах. В противном случае вы можете создать неподдерживаемую конфигурацию.

Если у вас сложная сетевая среда, вам может потребоваться вручную настроить хост-сеть перед добавлением хоста в менеджер управления средой виртуализации.

Рассмотрим следующие методы настройки хост-сети:

- Настройте сеть с помощью Cockpit. Альтернативно вы можете использовать nmtui или nmcli.
- Если сеть не требуется для самостоятельного развертывания ядра или для добавления хоста в ядро, настройте сеть на Портале администрирования после добавления хоста в ядро. Подробнее см. раздел *Создание новой логической сети в дата-центре или кластере* в *Руководстве по эксплуатации KeyVirt для администратора*.
- Используйте следующие соглашения об именах:
  - Устройства VLAN: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
  - Интерфейсы VLAN: physical_device.VLAN_ID (например, eth0.23, eth1.128, enp3s0.50)

  - Интерфейсы связи: bondnumber (например, bond0, bond1)
  - VLAN на связных интерфейсах: bondnumber.VLAN_ID (например, bond0.50, bond1.128)
- Используйте объединение сетевых адаптеров (network bonding). KeyVirt поддерживает следующий тип объединения сетевых адаптеров: 802.3ad.
- Используйте рекомендуемые режимы объединения сетевых адаптеров:
  - Если сеть ovirtmgmt не используется виртуальными машинами, сеть может использовать любой поддерживаемый режим объединения сетевых адаптеров.
  - Если сеть ovirtmgmt используется виртуальными машинами, см. раздел *Какие режимы объединения сетевых адаптеров работают при использовании с мостом, к которому подключаются гости или контейнеры виртуальных машин* в официальной документации KeyVirt.
  - Режим объединения сетевых адаптеров oVirt по умолчанию – (Mode 4) Dynamic Link Aggregation. Если ваш коммутатор не поддерживает протокол управления агрегацией каналов (LACP), используйте (Mode 1) Active-Backup.
- Настройте VLAN на физическом сетевом адаптере, как показано в следующем примере (хотя используется nmcli, вы можете использовать любой инструмент):

  ```
  # nmcli connection add type vlan con-name vlan50 ifname eth0.50 dev eth0 id 50
  # nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24
  +ipv4.gateway 123.123.0.254
  ```
- Настройте VLAN на объединении сетевых адаптеров, как показано в следующем примере (хотя используется nmcli, вы можете использовать любой инструмент):

  ```
  # nmcli connection add type bond con-name bond0 ifname bond0 bond.options
  "mode=active-backup,miimon=100" ipv4.method disabled ipv6.method ignore
  # nmcli connection add type ethernet con-name eth0 ifname eth0 master bond0 slave-
  type bond
  # nmcli connection add type ethernet con-name eth1 ifname eth1 master bond0 slave-
  type bond
  # nmcli connection add type vlan con-name vlan50 ifname bond0.50 dev bond0 id 50
  # nmcli con mod vlan50 +ipv4.dns 8.8.8.8 +ipv4.addresses 123.123.0.1/24
  +ipv4.gateway 123.123.0.254
  ```
- Не отключайте firewalld.
- Настройте правила брандмауэра на Портале администрирования после добавления хоста в Engine. Подробнее см. раздел *Настройка правил брандмауэра хоста* в *Руководстве по эксплуатации KeyVirt для администратора*.

6.2.4. Добавление узлов сервера управления средой виртуализации в менеджер управления средой виртуализации

Добавьте узлы сервера управления средой виртуализации так же, как стандартный узел, с дополнительным шагом для развертывания узла в качестве узла сервера управления. Домен общего хранилища определяется автоматически, и узел можно использовать в качестве резервного узла для размещения виртуальной машины сервера управления, когда это необходимо.
Требования:

- Все узлы сервера управления средой виртуализации должны находиться в одном кластере.
- Если вы повторно используете узел сервера управления, удалите его существующую конфигурацию сервера управления.

Процедура:

1. На Портале администрирования выберите Compute > Hosts.
2. Нажмите New.
3. Используйте раскрывающийся список, чтобы выбрать Data Center и Host Cluster – дата-центр и кластер для нового хоста.
4. Заполните поля Name и Address для нового хоста. Стандартный порт SSH, порт 22, автоматически заполняется в поле SSH Port.
5. Выберите метод аутентификации, который будет использоваться сервер управления средой виртуализации для доступа к хосту:
   - Вводить пароль пользователя root, чтобы использовать аутентификацию по паролю.
   - Копировать ключ, отображаемый в поле SSH PublicKey, в /root/.ssh/authorized_keys на хосте для использования аутентификации с открытым ключом.
6. При необходимости настройте управление питанием, если на хосте имеется поддерживаемая карта управления питанием.
7. Перейдите на вкладку Hosted Engine.
8. Выберите Deploy.
9. Нажмите OK.

6.2.5. Добавление хостов в менеджер управления средой виртуализации

Добавление хоста в вашу среду KeyVirt может занять некоторое время, так как платформа выполняет следующие шаги: проверки виртуализации, установка пакетов и создание моста.

1. Со стороны Engine хост появиться в статусе «pending approve».
   Необходимо подтвердить добавление хоста в кластер «Approve», снять галку reboot, и согласиться на добавления хоста в кластер.
2. Хост отображается в списке хостов со статусом Installing, и вы можете просмотреть ход установки в разделе Events (на панели уведомлений Notification Drawer). После небольшой задержки статус хоста изменится на Up.

Примечание: после перезапуска гипервизора, возможно отключение привязки управляющей сети ovirt manager, вследствие чего необходима повторная привязка интерфейса через web-интерфейс Engine.

6.3. Добавление хранилища

Добавьте хранилище в качестве доменов данных в новой среде. В среде KeyVirt должен быть хотя бы один домен данных, но рекомендуется добавить больше.

Добавьте хранилище, которое вы подготовили ранее. Подробнее о всех доступных типах хранилища см. в разделе *Хранилище* в *Руководстве по эксплуатации KeyVirt для администратора*.

6.4. Устранение неполадок при установке сервера управления средой виртуализации

Чтобы убедиться, что сервер управления средой виртуализации уже развернут, запустите hosted-engine --check-deployed. Ошибка будет отображаться только в том случае, если сервер управления не был развернут.

6.4.1. Устранение неполадок сервера управления средой виртуализации

Проверьте состояние сервера управления, запустив hosted-engine --vm-status. В зависимости от выходных данных Engine status см. следующие предложения, чтобы найти или устранить проблему.

Engine status: "health": "good", "vm": "up" "detail": "up"

1. Если сервер управления средой виртуализации запущен и работает как обычно, вы увидите следующий вывод:

   ```
   --== Host 1 status ==--
   Status up-to-date              : True
   Hostname                       : hypervisor.example.com
   Host ID                        : 1
   Engine status                  : {"health": "good", "vm": "up", "detail": "up"}
   Score                          : 3400
   stopped                        : False
   Local maintenance              : False
   crc32                          : 99e57eba
   Host timestamp                 : 248542
   ```

2. Если вывод в норме, но вы не можете подключиться к серверу управления, проверьте сетевое соединение.

Engine status: "reason": "failed liveliness check", "health": "bad", "vm": "up", "detail": "up"

1. Если значение health равно bad, а значение vm – up, службы HA попытаются перезапустить сервер управления, чтобы восстановить его. Если в течение нескольких минут это не удастся, включите режим глобального обслуживания из командной строки, чтобы хосты больше не управлялись службами HA.

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

2. Подключитесь к консоли. При появлении запроса введите пароль root операционной системы.

   ```
   # hosted-engine --console
   ```

3. Убедитесь, что операционная система сервера управления работает, войдя в систему.
4. Проверьте состояние службы ovirt-engine:

```
# systemctl status -l ovirt-engine
 # journalctl -u ovirt-engine
```

5. Проверьте следующие журналы: /var/log/messages, /var/log/ovirt -engine/engine.log и /var/log/ovirt-engine/server.log.
6. После устранения проблемы перезагрузите сервер управления вручную с одного из локальных узлов сервер управления:

```
# hosted-engine --vm-shutdown
 # hosted-engine --vm-start
```

Примечание. Когда узлы сервера управления средой виртуализации находятся в режиме глобального обслуживания, сервер управления необходимо перезагрузить вручную. Если вы попытаетесь перезагрузить сервер управления, отправив команду reboot из командной строки, сервер управления останется выключенным, как и запланировано в этой ситуации.

7. На сервере управления средой виртуализации убедитесь, что служба ovirt-engine запущена и работает:

```
# systemctl status ovirt-engine.service
```

8. Убедившись, что сервер управления запущен и работает, закройте сеанс консоли и отключите режим обслуживания, чтобы снова включить службы HA:

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

Engine status: "vm": "down", "health": "bad", "detail": "unknown", "reason": "vm not running on this host"

Это сообщение появляется на хосте, где в данный момент не работает сервер управления средой виртуализации.

1. Если в вашей среде имеется более одного хоста, убедитесь, что другой хост в данный момент не пытается перезапустить сервер управления.
2. Убедитесь, что вы не находитесь в режиме глобального обслуживания.
3. Проверьте журналы ovirt-ha-agent в /var/log/ovirt-hosted- engine-ha/agent.log.
4. Попробуйте перезагрузить сервер управления средой виртуализации вручную с одного из узлов сервера управления:

```
# hosted-engine--vm-shutdown
# hosted-engine --vm-start
```

Engine status: "vm": "unknown", "health": "unknown", "detail": "unknown", "reason": "failed to getVmStats"

Этот статус означает, что ovirt-ha-agent не удалось получить сведения о ВМ от VDSM.

1. Проверьте журналы VDSM в /var/log/vdsm/vdsm.log.
2. Проверьте журналы ovirt-ha-agent в /var/log/ovirt-hosted- engine-ha/agent.log.

Engine status: The self-hosted engine’s configuration has not been retrieved from shared storage

При возникновении проблемы со службой ovirt-ha-agent, с хранилищем, или с тем и другим будет следующий статус: The hosted engine configuration has not been

retrieved from shared storage. Please ensure that ovirt-ha-agent is running and the storage server is reachable.

Проверьте состояние ovirt-ha-agent на хосте:

```
# systemctl status -l ovirt-ha-agent
# journalctl -u ovirt-ha-agent
```

Если ovirt-ha-agent не работает, перезапустите его:

```
# systemctl start ovirt-ha-agent
```

Проверьте логи ovirt-ha-agent в /var/log/ovirt-hosted-engine-ha/agent.log.

Убедитесь, что вы можете пропинговать общее хранилище.

Проверьте, смонтировано ли общее хранилище.

Дополнительные команды для устранения неполадок

- hosted-engine --reinitialize-lockspace: эта команда используется, когда пространство блокировки sanlock нарушено. Перед повторной инициализацией пространства блокировок sanlock убедитесь, что режим глобального обслуживания включен и сервер управления средой виртуализации остановлен.
- hosted-engine --clean-metadata: удалить метаданные агента хоста из базы данных глобального статуса. Это заставляет все остальные хосты забыть об этом хосте. Убедитесь, что целевой хост не работает и включен режим глобального обслуживания.
- hosted-engine --check-liveliness: Эта команда проверяет страницу активности службы ovirt-engine. Вы также можете проверить, подключившись в веб-браузере к https://engine-fqdn/ovirt-engine/services/health/
- hosted-engine --connect-storage: эта команда дает указание VDSM подготовить все подключения к хранилищу, необходимые для хоста и сервера управления средой виртуализации. Обычно она запускается на серверной стороне во время развертывания сервера управления. Убедитесь, что режим глобального обслуживания включен, если вам нужно запустить эту команду для устранения проблем с хранилищем.

6.4.2. Очистка неудачного развертывания сервера управления средой виртуализации

Если развертывание сервера управления средой виртуализации было прервано, последующие развертывания завершится с сообщением об ошибке. Ошибка будет отличаться в зависимости от этапа, на котором развертывание не удалось.

Внимание! Если выполнение данной процедуры не устранило проблему, тогда необходимо удалить узел, на котором установлен сервер управления средой виртуализации, и поставить хост среды виртуализации и менеджер управления заново согласно инструкциям, приведенным в разделе *Установка сервера управления средой виртуализации на отдельной виртуальной машине* выше.

Если вы получили сообщение об ошибке, вы можете запустить сценарий очистки на хосте развертывания, чтобы удалить неудачное развертывание. Однако

лучше всего переустановить базовую операционную систему и начать развертывание с самого начала.

Сценарий очистки имеет следующие ограничения:

- Нарушение сетевого подключения во время работы сценария может привести к тому, что сценарий не сможет удалить мост управления или воссоздать рабочую конфигурацию сети.
- Сценарий не предназначен для очистки любого общего устройства хранения, использованного во время неудачного развертывания. Вам необходимо очистить общее запоминающее устройство, прежде чем вы сможете повторно использовать его при последующем развертывании.

Процедура:

1. Запустите /usr/sbin/ovirt-hosted-engine-cleanup и выберите y, чтобы удалить все, что осталось от неудачного развертывания сервера управления средой виртуализации.

   ```
   # /usr/sbin/ovirt-hosted-engine-cleanup
    This will de-configure the host to run ovirt-hosted-engine-setup from scratch.
    Caution, this operation should be used with care.
    Are you sure you want to proceed? [y/n]
   ```

2. Определите, следует ли переустанавливать на то же общее запоминающее устройство или выбрать другое общее запоминающее устройство.
   - Чтобы развернуть установку в том же домене хранения, очистите домен хранения, выполнив следующую команду в соответствующем каталоге на сервере для NFS, PosixFS или локальных доменов хранения:

     ```
     # rm -rf storage_location/*
     ```

   - Перезагрузите локальный хост-систему или выберите другое общее запоминающее устройство. Перезагрузка нужна, чтобы убедиться, что все соединения с хранилищем очищены перед следующей попыткой.
3. Повторно разверните сервер управления средой виртуализации.

6.5. Резервное копирование/восстановление сервер управления средой виртуализации

Процедура:

1. Создайте резервную копию сервера управления средой виртуализации:

   ```
   engine-backup --mode=backup --file=имя_файла.bcp --log=имя_файла.log
   ```

2. Установите новый сервер управления, как описано выше в разделе *Установка менеджера управления средой виртуализации (служб управления виртуализацией)*.
3. Восстановите конфигурацию сервера управления. Параметр --no-restore-permissions сбросит привилегии пользователей. Если же выбран пареметр --restore-permissions, то привилегии пользователей сохранятся:

   ```
   engine-backup --mode=restore --log=имя_файла.log --file=имя_файла.bcp --provision-db --provision-dwh-db --no-restore-permissions
   ```

4. Запустите установку:

   engine-setup --offline

5. Запустите службу сервера управления:

   systemctl start ovirt-engine

7. РЕКОМЕНДАЦИИ

7.1. Общие рекомендации

Сразу после завершения развертывания создайте полную резервную копию менеджера управления средой виртуализации 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 средой виртуализации, 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 средой виртуализации, имеет достаточную энтропию. Значения ниже 200 могут привести к сбою установки менеджера управления средой виртуализации. Чтобы проверить значение энтропии, выполните команду cat /proc/sys/kernel/random/entropy_avail. Чтобы увеличить энтропию, установите пакет rngtools.
Вы можете автоматизировать развертывание хостов и виртуальных машин с помощью PXE, Kickstart, Satellite, CloudForms, Ansible или их комбинации. Развертывание сервера управления средой виртуализации на отдельной виртуальной машине 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.

7.2. Рекомендации по безопасности

Не отключайте функции безопасности (такие как HTTPS, SELinux и брандмауэр) 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.