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 узлах виртуализации. Сервер управления работает как Портал администратора.
- Менеджер управления (Engine, менеджер управления средой виртуализации) – менеджер управления средой виртуализации, т.е. Портал администратора для управления средой виртуализации.
- Узел среды виртуализаци (KeyVirt Node) – это узел среды виртуализации, который работает как гипервизор.
- Affinity-группа (группа соответствия) или территориальная группа – группа из двух или более виртуальных машин или узлов, для которых применяется набор идентичных условий и параметров. Такая группа используется в политике планирования ВМ. Бывают группы как с положительным, так и с отрицательным соотвествием.
- Affinity-метка (метка соответствия) или тег соответствия – подмножество группы соответствия, которое используются вместе с группами соответствия для установки любого вида соответствия между виртуальными машинами и узлами.
- Affinity-политика (политика соответствия) – комбинация группы привязки, инструкции условия и необязательных параметров. Например, виртуальные машины A, ВМ B и ВМ C должны выполняться вместе на узле 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. Каждому пользователю (включая администратора) должены быть назначены права в проекте для доступа к ресурсам этого проекта. Пользователь может принадлежать к нескольким проектам.

- Узел (Node/Host) – 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.
- 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).
- 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 (узле) 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 узлами 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 (KeyVirt Engine)	Портал администратора 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.
Узел среды виртуализации (KeyVirt 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 (KeyVirt 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 узлах виртуализации, т.е. менеджер управления размещен на узлах 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 узле с ролью менеджера управления средой виртуализации. Кроме того, сервер управления средой виртуализации может работать в режиме высокой доступности. Если узел, на котором запущен сервер управления, переходит в режим обслуживания или неожиданно выходит из строя, виртуальная машина будет автоматически перенесена на другой узел в среде. Для режима высокой доступности требуется минимум два узла.

Минимальная настройка включает в себя:

- Сервер управления средой виртуализации (ВМ Engine);
- Один узел либо два узла 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 узлам виртуализации.

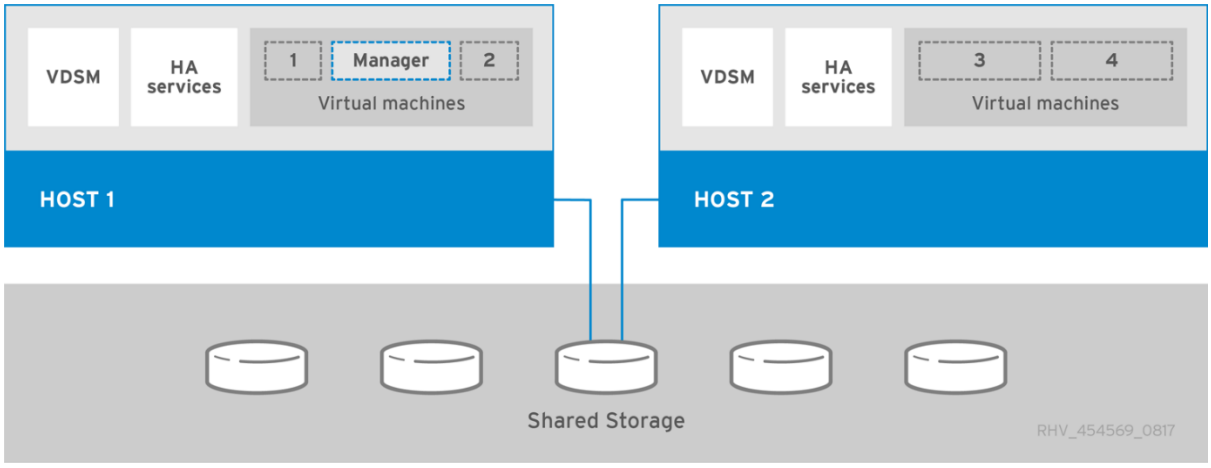

Рисунок 1. Архитектура KeyVirt

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	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.

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 узлу

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 узел 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 4 ГБ. Для уровней кластера от 4.2 до 4.5 максимальный поддерживаемый объем ОЗУ на ВМ в узле среды виртуализации составляет 6 ТБ. Для уровней кластера от 4,6 до 4,7 максимальный поддерживаемый объем ОЗУ на ВМ в узле 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

Узлам требуется хранилище для хранения конфигурации, журналов, дампов ядра и для использования в качестве пространства подкачки. Хранилище может быть локальным или сетевым. Узел 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 узел 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

Узлы 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 узла, 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

Узел должен соответствовать следующим требованиям, чтобы виртуальные машины на этом узле могли использовать vGPU:

- vGPU-совместимый графический процессор;
- Ядро узла 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

Узлы должны иметь хотя бы один сетевой интерфейс с минимальной пропускной способностью 1 Гбит/с. Рекомендуется, чтобы у каждого узла 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 узлах виртуализации и/или BM 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 узлы (узел среды виртуализации и узел 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 узел среды виртуализации и узел Enterprise Linux в кластере должен иметь возможность подключаться к fence-устройствам всех других узлов 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	Узлы 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 администратора Клиенты Портала ВМ Узлы 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 администратора Клиенты Портала ВМ	Менеджер управления	Предоставляет доступ через 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 узле, этот порт не используется.	Нет

M6	7410	TCP	Узлы среды виртуализации	Менеджер управления	Если Kdump включен на узлах, откройте порт для fence_kdump на сервере управления. Fence_kdump не поддерживает шифрованное соединение. Вы можете вручную настроить этот порт, чтобы заблокировать доступ от узлов, которые не соответствуют требованиям.	Нет
M7	54323	TCP	Клиенты Портала администратора	Менеджер управления (служба ovirt-imageio)	Требуется для связи со службой ovirt-imageio.	Да
M8	6642	TCP	Узлы среды виртуализации	Open Virtual Network (OVN)	Требуется для подключения к базе данных OVN.	Да
M9	9696	TCP	Клиенты провайдера внешней сети для OVN	Внешний сетевой провайдер для OVN	OpenStack Networking API.	Да, с конфигурацией, 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 узле, 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 узла виртуализации

Узлам Enterprise Linux и узлам среды виртуализации необходимо открыть несколько портов, чтобы разрешить сетевой трафик через системный брандмауэр. Правила брандмауэра автоматически настраиваются по умолчанию при добавлении нового узла 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	Узлы среды виртуализации	Secure Shell (SSH). Необязательно.	Да
H2	2223	TCP	Менеджер управления	Узлы среды виртуализации	Доступ через Secure Shell	Да

					(SSH) для подключения к консолям ВМ.	
H3	161	UDP	Узлы среды виртуализации	Менеджер управления	Простой протокол управления сетью (SNMP). Требуется, только если вы хотите, чтобы прерывания Simple Network Management Protocol отправлялись с узла одному или нескольким внешним SNMP-менеджерам. Необязательно.	Нет
H4	1111	TCP	NFS-сервер	Узлы среды виртуализации	NFS-соединения. Необязательно.	Нет
H5	5900 - 6923	TCP	Клиенты Портала администратора Клиенты Портала ВМ	Узлы среды виртуализации	Удаленный доступ к гостевой консоли через VNC и SPICE. Эти порты должны быть открыты для обеспечения доступа клиентов к ВМ.	Да (необязательно)
H6	5989	TCP, UDP	Менеджер объектов общей информационной модели (CIMOM)	Узлы среды виртуализации	Используется CIMOM для Мониторинга ВМ, работающих на узле. Требуется, только если вы хотите использовать CIMOM для мониторинга ВМ в вашей среде виртуализации. Необязательно.	Нет

H7	9090	TCP	Менеджер управления Клиентские машины	Узлы среды виртуализации	Требуется для доступа к веб-интерфейсу Cockpit, если он установлен.	Да
H8	16514	TCP	Узлы среды виртуализации	Узлы среды виртуализации	Миграция ВМ с использованием libvirt.	Да
H9	49152 - 49215	TCP	Узлы среды виртуализации	Узлы 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 Узлы среды виртуализации	Узлы среды виртуализации	Узлы виртуализации.	Да
H11	54322	TCP	Менеджер управления служба ovirt-imageio	Узлы среды виртуализации	Требуется для связи со службой ovirt-imageo.	Да
H12	6081	UDP	Узлы среды виртуализации	Узлы среды виртуализации	Требуется, когда в качестве сетевого провайдера используется открытая виртуальная сеть (OVN), чтобы OVN мог создавать туннели между узлами.	Нет
H13	53	TCP, UDP	Узлы среды виртуализации	DNS-сервер	DNS-запросы поиска от портов с номерами более, чем 1023 к порту 53 и ответы на них. Открыт	Нет

					по умолчанию.	
H14	123	UDP	Узлы 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	Узлы среды виртуализации	Узлы среды виртуализации	Internet Security Protocol (IPSec).	Да
H16	500	UDP	Узлы среды виртуализации	Узлы среды виртуализации	Internet Security Protocol (IPSec).	Да
H17	–	FY, ESP	Узлы среды виртуализации	Узлы 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 узлов среды виртуализации.

Узлы 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 узла среды виртуализации настоятельно рекомендует сначала отключить любое существующее хранилище, не относящееся к ОС, которое подключено к узлу, 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 узле, 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 узла, что может привести к устареванию логических томов и повреждению данных. Используйте команду vdsm-tool config-lvm-filter для создания фильтров для LVM.
Если ваш узел 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 узла, что может привести к устареванию логических томов и повреждению данных.
Если ваш узел 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 узел 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 узла. Этот узел станет первым узлом с размещенным на нем сервером управления средой виртуализации. Подойдет как узел 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 узлов в сервере управления.

5.2. Установка сервера управления средой виртуализации на отдельной виртуальной машине

Сервер управления средой виртуализации можно развернуть с узла среды виртуализации или узла Enterprise Linux.

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

5.2.1. Установка узлов среды виртуализации

Узел среды виртуализации – это минимальная операционная система, основанная на Enterprise 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 имеет веб-интерфейс Cockpit для мониторинга узла и выполнения административных задач.

Узел должен соответствовать минимальным требованиям, которые описаны в разделе *Требования к узлу* выше.

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

Процедура установки:

1. Загрузите узел среды виртуализации по ссылке Installation ISO.
2. Запишите установочный ISO-образ узла среды виртуализации на USB-накопитель, компакт-диск или DVD-диск.
3. Запустите машину, на которой вы устанавливаете узел 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 узел 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 узла в поле Host Name и нажмите Done.
11. Нажмите Begin Installation.
12. Установите пароль root и, при необходимости, создайте дополнительного пользователя во время установки узла среды виртуализации.

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

13. Нажмите Reboot, чтобы завершить установку.

Примечание. Когда узел среды виртуализации перезапускается, nodectl check выполняет проверку работоспособности узла 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.

5.2.2. Установка узлов Enterprise Linux (CentOS 8-9)

Узел Enterprise Linux основан на стандартной базовой установке Enterprise Linux 8.7 или более поздней версии на физическом сервере с включенными репозиториями Enterprise Linux Server и KeyVirt. Проект KeyVirt также предоставляет пакеты для Enterprise Linux 9.

Внимание! KeyVirt поддерживает и другие дистрибутивы Linux, такие Red Hat, однако рекомендуемым дистрибутивом является CentOS.

Подробные инструкции по установке узлов Enterprise Linux см. в официальной документации в разделе *Выполнение стандартной установки EL*.

Узел должен соответствовать минимальным требованиям к узлу.

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

Внимание! Виртуализация должна быть включена в настройках BIOS вашего узла. Информацию об изменении настроек BIOS узла см. в документации по аппаратному обеспечению вашего узла.

Не устанавливайте сторонние сторожевые таймеры на узлах Enterprise Linux. Они могут мешать работе демона сторожевого таймера, предоставляемого VDSM.

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 администратора → Введите имя пользователя admin и пароль, заданный при установке системы. Откроется веб-интерфейс управления.

6.2. Добавление узлов среды виртуализации

KeyVirt поддерживает два типа узлов: узлы среды виртуализации (KeyVirt Nodes) и узлы 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 узла.

Подробнее об узлах см. в разделе *Узлы* в *Руководстве по эксплуатации KeyVirt для администратора*.

Таблица 7. Типы узлов

Тип узла	Другие названия	Описание
Узел среды виртуализации	KeyVirt Node, тонкий узел	Это минимальная операционная система на базе Enterprise Linux. Он распространяется в виде файла ISO с портала клиентов и содержит только те пакеты, которые необходимы машине для работы в качестве узла.
Обычный узел	Узел Linux (например, CentOS), толстый узел	В качестве узлов можно использовать Linux-системы с включенными соответствующими репозиториями, такие как CentOS Linux.

Совместимость узлов

При создании нового дата-центра вы можете установить версию совместимости. Выберите версию совместимости, подходящую для всех узлов 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 об узлах см. в разделе *Узлы* в *Руководстве по эксплуатации KeyVirt для администратора*.

6.2.1. Узлы среды виртуализации

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

Установка стороннего пакета на KeyVirt-node

Если вам нужен пакет, который не включен в репозиторий, предоставленный KeyVirt, вам необходимо предоставить репозиторий, прежде чем вы сможете установить пакет.

Требования

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

Процедура:

1. Откройте существующий файл .repo или создайте новый в /etc/yum.repos.d/.
2. Добавьте запись в файл .repo. Например, чтобы установить sssd-ldap, добавьте следующую запись в новое имя .repo файла third-party.repo:

```
# imgbased: set-enabled
[custom-sssd-ldap]
name = Provides sssd-ldap
mirrorlist=http://mirrorlist.centos.org/?release=$stream&arch=$basearch&repo=BaseOS&infra=$infra
#baseurl=http://mirror.centos.org/$contentdir/$stream/BaseOS/$basearch/os/
```

gpgcheck=1
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-centosofficial
ncludepkgs = sssd-ldap

3. Установите ` sssd-ldap`:

   # dnf install sssd-ldap

6.2.2. Развертывание Engine с помощью командной строки

1. Подготовьте полные доменные имена и их IP-адреса для менеджера управления виртуализации и узлов перед развертыванием, в DNS должны существовать соответствующие записи в зонах прямого и обратного просмотра. Ниже приведён **пример планирования доменных имён и IP-адресов** развёртываемой системы управления виртуализацией KeyVirt. Не используйте верхний регистр при указании fqdn Менеджера управления.

Объект	FQDN	IP адрес
Менеджер управления	e.keyvirt.local	10.10.10.10
Узел 1	u1.keyvirt.local	10.10.10.11
Узел 2	u2.keyvirt.local	10.10.10.12
Узел 3	u3.keyvirt.local	10.10.10.13

2. После установки имя HostedEngine будет являться именем виртуальной машины с менеджером управления и веб-интерфейсом управления средой виртуализации. Задаваемый адрес должен быть свободен.
3. В случае невозможности использования внешнего DNS добавьте в файл **/etc/hosts** IP-адреса и FQDN узла виртуализации и разворачиваемого менеджера управления.
4. Скачайте rpm пакеты
5. Откройте сессию запустив терминальный мультиплексор tmux, чтобы избежать потери сессии в случае сбоя в работе сети или терминала:

tmux

6. Запустите процесс развертывания:

hosted-engine –deploy

В случае развертывания в среде dual-stack при запуске развертывания без опций --4 или --6 по умолчанию будет использоваться IPv4.
Для указания использования конкретной версии IP используйте соответствующую опцию. Например, для IPv6:

hosted-engine --deploy --6

7. Следуйте сообщениям в консоли:
   - Подтвердите готовность развернуть ВМ HostedEngine.
     Are you sure you want to continue? (Yes, No) [Yes]:

В случае запуска развертывания без опций --4 или --6 появится предупреждение. Убедитесь, что запустили развертывание корректно и подтвердите ответ Yes

If you run "hosted-engine --deploy" without the "--4" or "--6" option
in a dual-stack environment, the default is IPv4.
You must ensure that your DNS returns only IPv4 addresses.
See: https://keyvirt.ru

- По указанному пути будет расположен файл, содержащий лог развертывания.

Log file: /var/log/ovirt-hosted-engine-setup/ovirt-hosted-engine-setup-***.log

- Введите или подтвердите адрес шлюза

--== HOST NETWORK CONFIGURATION ==--
Please indicate the gateway IP address [10.10.10.254]:

- Укажите сетевой интерфейс, который будет использоваться для создания сетевого моста для ВМ.

Please indicate a nic to set ovirtmgmt bridge on (ens192) [ens192]:

- Укажите, каким образом будет выполняться проверка сети. Рекомендуется использовать метод проверки сети - dns.

Please specify which way the network connectivity should be checked (ping, dns, tcp, none) [dns]:

ping - Попытка выполнить ping шлюза.
dns - Проверяет соединение с DNS-сервером.
tcp - Создает TCP-соединение с комбинацией узла и порта. Необходимо указать IP-адрес и порт назначения. После успешного создания соединения сеть считается "живой". Убедитесь, что указанный узел способен принимать входящие TCP-соединения на указанный порт.
None - Сеть всегда считается подключенной.

- Укажите название создаваемого центра данных или подтвердите имя по умолчанию (Default).
  --== VM CONFIGURATION ==--
  Please enter the name of the data center where you want to deploy this hosted-engine host.
  Data center [Default]:

- Укажите название создаваемого кластера или подтвердите имя по умолчанию (Default).
  Please enter the name of the cluster where you want to deploy this hosted-engine host.
  Cluster [Default]:

- Подтвердите или откажитесь от интеграции с Keycloak.
  Configure Keycloak integration on the engine(Yes, No) [Yes]:

Рекомендуем предварительно принять решение о необходимости его использования, исходя из следующих особенностей:
Если на данном этапе отказаться от интеграции с Keycloak, будет использоваться провайдер по умолчанию AAA-JDBC. После развертывания можно перейти с AAA-JDBC на Keycloak, но при этом всю конфигурацию AAA необходимо будет переносить в Keycloak вручную.
Если на данном согласиться с интеграцией с Keycloak, в дальнейшем можно будет переключиться на AAA, но это необходимо делать вручную. Кроме того, мы настоятельно не рекомендуем выполнять такой переход. На текущий момент не существует никаких средств автоматизации, упрощающих миграцию между AAA JDBC/LDAP и keycloak.

- Укажите количество vCPU (минимально -4) и ОЗУ (минимально - 4096 МБ, рекомендуется - не менее 16384 МБ) выделяемых для **BM HostedEngine**.
  Please specify the number of virtual CPUs **for** the VM. The default is the appliance OVF value [4]:
  Please specify the memory size of the VM in MB. The default is the appliance OVF value [16384]:
- Укажите подготовленное доменное имя для **BM HostedEngine**.
  Engine VM FQDN: e.keyvirt.local

Вводимое имя менеджера должно разрешаться в IP-адрес, иначе сценарий выдаст ошибку [ERROR] Host name is not valid

- Введите имя домена, в котором будет находиться сервер управления или подтвердите предложенное.
  Engine VM domain [keyvirt.local]:
- Введите и подтвердите пароль для пользователя *root* **BM HostedEngine**.
  Enter root password that will be used **for** the engine appliance:
  Confirm appliance root password:
- При необходимости введите открытый ключ ssh для пользователя *root*, который будет использоваться для **BM HostedEngine**.
  SSH public key []:
- Укажите хотите ли включить доступ по ssh для пользователя *root* в **BM HostedEngine**.
  Do you want to enable ssh access **for** the root user (yes, no, withoutpassword) [yes]:
- Подтвердите ответ No или, если данная функция необходима, наберите Yes на предложение применить профиль безопасности OpenSCAP.
  Do you want to apply a default OpenSCAP security profile (Yes, No) [No]:
- Подтвердите сгенерированный mac-адрес для BM HostedEngine или введите свой.
  Please specify a unicast MAC address for the VM, or accept a randomly generated default [00:16:3e:48:d5:0d]:
- Используйте статическую конфигурацию сети BM HostedEngine.
  How should the engine VM network be configured? (DHCP, Static)[Static]:
- Введите IP-адрес **BM HostedEngine**.
  Please enter the IP address to be used **for** the engine VM []:10.10.10.10

IP-адрес BM **HostedEngine** должен принадлежать той же сети, что и адрес узла, на котором происходит развертывание.

- Подтвердите или введите адрес DNS сервера.
  Engine VM DNS (leave it empty to skip) [10.10.10.10]:

- Укажите добавить ли запись о узле в файл hosts на **BM HostedEngine**.
  Add lines to /etc/hosts? (Yes, No)[Yes]:

- Введите имя SMTP сервера, через который будут отсылаться уведомления или примите значение по умолчанию.
  Please provide the name of the SMTP server through which we will send notifications [localhost]:

- Введите порт для SMTP сервера или примите значение по умолчанию.
  Please provide the TCP port number of the SMTP server [25]:

- Введите e-mail адрес, откуда будут отсылаться уведомления или примите значение по умолчанию.
  Please provide the email address from which notifications will be sent [root@localhost]:

- Введите список адресов e-mail через запятую, которые будут получать уведомления или примите значение по умолчанию.
  Please provide a comma-separated list of email addresses which will get notifications [root@localhost]:

- Введите и подтвердите пароль для пользователя *admin* (учётная запись используется для авторизации в веб-интерфейсе среды виртуализации).
  Enter engine admin password:
  Confirm engine admin password:

Не используйте простые пароли. Это может вызывать ошибки в работе некоторых сервисов.
В случае, если ранее была выбрана интеграция с Keycloak, заданный в этом пункте пароль также будет назначен пользователю **admin@ovirt**.

- Укажите имя узла для сети управления или примите предложенное значение.
  Please provide the hostname of this host on the management network [u1.keyvirt.local]:

- Укажите тип хранилища, которое вы хотите использовать для размещения **BM HostedEngine**.
  Please specify the storage you would like to use (glusterfs, iscsi, fc, nfs)[nfs]:
  - Для NFS введите версию, полный адрес и путь к хранилищу, а также необходимые параметры монтирования:
    Please specify the nfs version you would like to use (auto, v3, v4, v4_1)[auto]:
    Please specify the full shared storage connection path to use (example: host:/path): storage.example.com:/hosted_engine/nfs
    If needed, specify additional mount options **for** the connection to the hosted-engine storage domain []:

  - Для iSCSI введите данные портала и выберите цель и LUN из автоматически определяемых списков. Во время развертывания

можно выбрать только одну цель iSCSI, но поддерживается многоканальность для подключения всех порталов одной группы порталов.
Please specify the storage you would like to use (glusterfs, iscsi, fc, nfs)[nfs]:iscsi
Please specify the iSCSI portal IP address:10.220.162.2
Please specify the iSCSI portal port [3260]:
Please specify the iSCSI discover user:
Please specify the iSCSI discover password:
Please specify the iSCSI portal login user:
Please specify the iSCSI portal login password:
The following targets have been found:
[1] iqn.1991-05.com.microsoft:dc-hor-tst-sber-23-target
TPGT: 1, portals:
10.220.162.2:3260

Please select a target (1) [1]:

The following luns have been found on the requested target:
[1] 360003ff44dc75adc8f7f2de3f74461b6 90.0GiB MSFT Virtual HD
status: free, paths: 1 active
Please select the destination LUN (1) [1]:

- Для хранилища Gluster введите полный адрес и путь к хранилищу, а также необходимые параметры монтирования:
  Please specify the full shared storage connection path to use (example: host:/path):
  storage.example.com:/hosted_engine/gluster_volume
  If needed, specify additional mount options **for** the connection to the hosted-engine storage domain []:

- Для Fibre Channel выберите LUN из списка автоматического обнаружения. Адаптеры шины узла должны быть настроены и подключены, а LUN не должен содержать существующих данных.
  The following luns have been found on the requested target:
  [1] 3514f0c5447600451 30GiB XtremIO XtremApp
  status: free, paths: 2 active
  [2] 3514f0c5447600452 30GiB XtremIO XtremApp
  status: used, paths: 2 active
  Please select the destination LUN (1, 2) [1]:

- Укажите другой размер диска для ВМ HostedEngine, если это необходимо.
  Please specify the size of the VM disk **in** GiB: [51]:

- После успешного развёртывания менеджера управления виртуализации будет выведено сообщение:
  [INFO] Hosted Engine successfully deployed

6.2.3. 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:

   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.
```

6.2.4. Узлы Enterprise Linux

Установка узлов Enterprise Linux

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

Установка Cockpit на узлах Enterprise Linux

Вы можете установить Cockpit для мониторинга ресурсов узла 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 узлов 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 узла 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 узла в ядро, настройте сеть на Портале администратора после добавления узла 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 KeyVirt 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 администратора после добавления узла в Engine. Подробнее см. раздел *Настройка правил брандмауэра узла* в *Руководстве по эксплуатации KeyVirt для администратора*.

6.2.5. 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 администратора выберите *Виртуализация* > *Узлы*.
2. Нажмите *Новый*.
3. Используйте раскрывающийся список, чтобы выбрать Data Center и Host Cluster – дата-центр и кластер для нового узла.
4. Заполните поля *Имя* и *Адрес* для нового узла. 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 узлу:
   - Вводить пароль пользователя root, чтобы использовать аутентификацию по паролю.
   - Копировать ключ, отображаемый в поле SSH PublicKey, в /root/.ssh/authorized_keys на узле для использования аутентификации с открытым ключом.
6. При необходимости настройте управление питанием, если на узле имеется поддерживаемая карта управления питанием.
7. Перейдите на вкладку Hosted Engine.
8. Выберите *Развернуть*.
9. Нажмите OK.

6.2.6. Добавление стандартных узлов в менеджер управления средой виртуализации

Всегда используйте менеджер управления средой виртуализации для изменения сетевой конфигурации узлов в ваших кластерах. В противном случае вы можете создать неподдерживаемую конфигурацию.

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

1. На Портале администратора выберите *Виртуализация* > *Узлы*.
2. Нажмите *Новый*.
3. Используйте раскрывающийся список, чтобы выбрать Data Center и Host Cluster – дата-центр и кластер для нового узла.
4. Заполните поля *Имя* и *Адрес* для нового узла. Стандартный порт SSH, порт 22, автоматически заполняется в поле SSH Port.
5. Выберите метод аутентификации, который будет использоваться Engine для доступа к узлу:
   - Вводить пароль пользователя root, чтобы использовать аутентификацию по паролю.
   - Копировать ключ, отображаемый в поле SSH PublicKey, в /root/.ssh/authorized_keys на узле для использования аутентификации с открытым ключом.
6. При желании нажмите кнопку *Расширенные параметры*, чтобы изменить следующие дополнительные настройки узла:
   - Отключить автоматическую настройку брандмауэра.
   - Добавить отпечаток SSH узла для повышения безопасности. Вы можете добавить его вручную или получить автоматически.
7. При необходимости настройте управление питанием, если на узле имеется поддерживаемая карта управления питанием.
8. Нажмите OK.

Новый узел отображается в списке узлов со статусом Installing, и вы можете просмотреть ход установки в разделе Events (на панели уведомлений Notification Drawer). После небольшой задержки статус узла изменится на Up.

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 узлы 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 узле, где в данный момент не работает сервер управления средой виртуализации.

1. Если в вашей среде имеется более одного узла, убедитесь, что другой узел 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 узле:

   # 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 узла из базы данных глобального статуса. Это заставляет все остальные узлы забыть об этом узле. Убедитесь, что целевой узел 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 узла 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 узел 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 узле 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 локальную 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 узел 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 узлов 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 узлах 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 узлах или виртуальных машинах.
Создайте индивидуальные учетные записи администраторов, вместо того чтобы допускать использование одной учетной записи администратора несколькими сотрудниками.
Ограничьте доступ к узлам и создайте отдельные учетные записи. Не используйте одну учётную запись с правами root на всех узлах виртуализации.
При развертывании узлов виртуализации устанавливайте только пакеты и службы, необходимые для системы виртуализации, производительности, безопасности и мониторинга. Узлы не должны иметь дополнительных пакетов, таких как анализаторы, компиляторы или другие компоненты, которые добавляют риск для безопасности.