zVirt Containers

zVirt Containers - это комплексное решение, которое представляет из себя единую и простую в использовании среду для развертывания, масштабирования и управления приложениями в гибридной инфраструктуре. В рамках данной статьи приведена техническая информация о компонентах решения и взаимодействия между компонентами.

1. Основные компоненты решения

- zVirt — платформа виртуализации, предоставляющая вычислительные ресурсы, API для управления виртуальными машинами и хранилищами.
- Nova Container Platform — платформа на базе Kubernetes для доставки, развертывания и масштабирования приложений в контейнерах. Разворачивается в составе zVirt Containers.
- Nova Universe — сервер управления, содержащий весь необходимый код, репозитории и утилиты для установки и настройки Nova-кластеров.

2. Основные службы и сервисы

- **Zvirt-engine-backend** - это служба, которая отвечает за работу сервера управления (Hosted-Engine) в zVirt. Некоторые функции **zvirt-engine-backend**:
  - обработка запросов от интерфейса управления;
  - управление конфигурациями хостов и виртуальных машин;
  - автоматизация процессов, например, обновление хостов и сервера управления.
- **oVirt Engine** — это центр управления средой oVirt, сервис, который предоставляет графический интерфейс пользователя и REST API для управления ресурсами в этой среде. Некоторые функции **oVirt Engine**:
  - определение хостов, настройка центров данных, добавление хранилищ, определение сетей, создание виртуальных машин, управление разрешениями пользователей и использование шаблонов из одного центрального местоположения;
  - управление жизненным циклом виртуальных машин; управление сетью (добавление логических сетей и их присоединение к хостам);
  - управление хранилищем (доменами хранения и виртуальными дисками виртуальных машин); высокая доступность (автоматический перезапуск виртуальных машин с неисправных хостов на других хостах);

- менеджер обслуживания (отсутствие простоев для виртуальных машин во время запланированных окон обслуживания);
- управление образами (на основе шаблонов, тонкое provisioning и снимки);
- мониторинг (всех объектов в системе — гостей виртуальных машин, хостов, сетей, хранилищ и т. д.).

3. Логическая схема взаимодействия

Компоненты внутри решения zVirt Conteiners взаимодействуют про простейшей схеме, представленной ниже:

- Пользователь взаимодействует с кластерами исключительно через интерфейс управления zVirt.
- zvirt-engine-backend обрабатывает пользовательские запросы и осуществляет взаимодействие с Nova Universe.
- При получении команды на работу с кластерами zvirt-engine-backend инициирует вызовы к API Nova Universe. Nova Universe содержит весь необходимый функционал для подготовки, настройки и управления кластерами Nova Container Platform.
- Universe в свою очередь обращается к ovirt-engine для выполнения исходного запроса (например, создание ВМ).
- После получения доступа к созданным виртуальным машинам, Nova Universe выполняет развертывание компонентов Kubernetes и формирует рабочий кластер. В рамках этой процедуры:
  - устанавливается kubelet, kube-proxy, и другие компоненты Kubernetes;
  - запускаются сервисы, манифесты и системные поды;
  - формируется архитектура control-plane и worker-узлов;
  - выполняется настройка сети и хранилища;
  - настраивается взаимодействие между компонентами.

4. Сетевая архитектура и изоляция кластеров

Для обеспечения гибкости и безопасности при развертывании Nova Container Platform в составе zVirt Containers используется SDN.

- Universe и все управляемые кластеры размещаются в изолированной SDN-среде, отделенной от основной пользовательской сети. Объекты SDN скрыты от пользователя.
- По умолчанию эти сети изолированны снаружи, однако обеспечивается выходной трафик с помощью механизма SNAT.
- Для взаимодействия между логическими сетями (например, между Universe и кластерами) используются межроутерные сети и специальные механизмы маршрутизации.
- Для каждого развернутого кластера автоматически формируется собственная SDN-инфраструктура, логически связанная с сервером управления Universe.
- При необходимости, отдельные узлы кластера могут быть опубликованы наружу через механизм NAT на маршрутизаторах.

Такой подход позволяет обеспечить безопасное, масштабируемое и управляемое сетевое разделение между компонентами системы.

5. Этапы создания изолированной сети кластера

5.1. Этап 1. Развертывание Universe

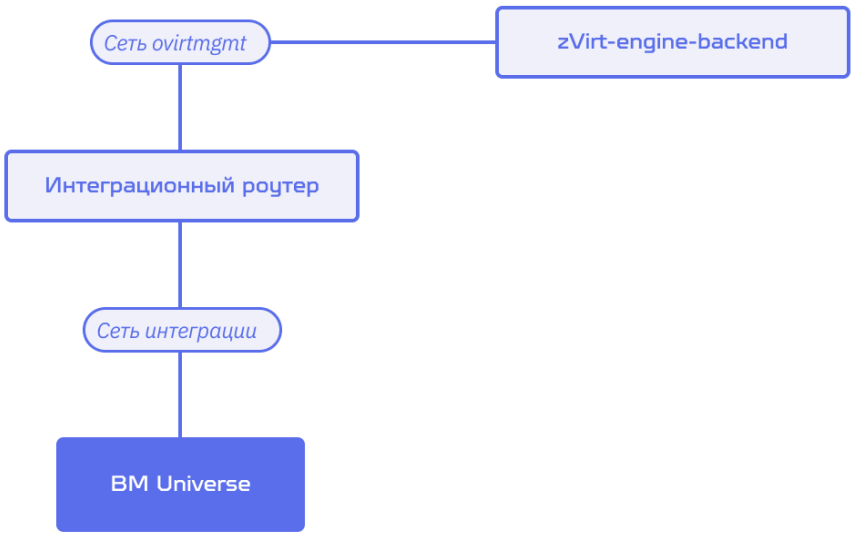
Для развертывания Universe создается логическая сеть, которая находится в SDN - сеть интеграции. В ней находится BM Universe.

Убедитесь, что IP-адрес сети интеграции не пересекается с пользовательскими адресами внутри инфраструктуры.

К сети итеграции добавляется интеграционный роутер.

Рекомендуется прикрепить интеграционный роутер к сети ovirtmgmt.

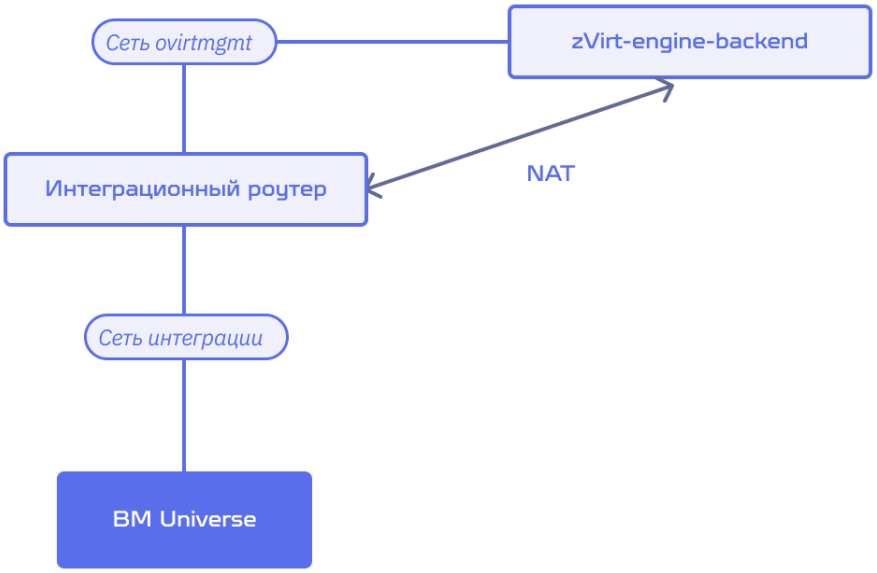
В сети также присутствует **zvirt-engine-backend**.



5.2. Этап 2. Доступ к Universe

В данном случае BM Universe находится в сети интеграции. Для обеспечения взаимодействия между zvirt-engine-backend и API Universe настраивается трансляция адресов:

Для обеспечения доступа к API Universe из управляющей сети выполняется статическая трансляция IP-адреса (NAT) на **внешний IP-адрес** (например `10.250.24.171`), который перенаправляется к внутреннему IP-адресу BM Universe в интеграционной сети. Таким образом, zvirt-engine-backend получает доступ к API Universe, не зная его внутреннего IP. Он использует публичный адрес.

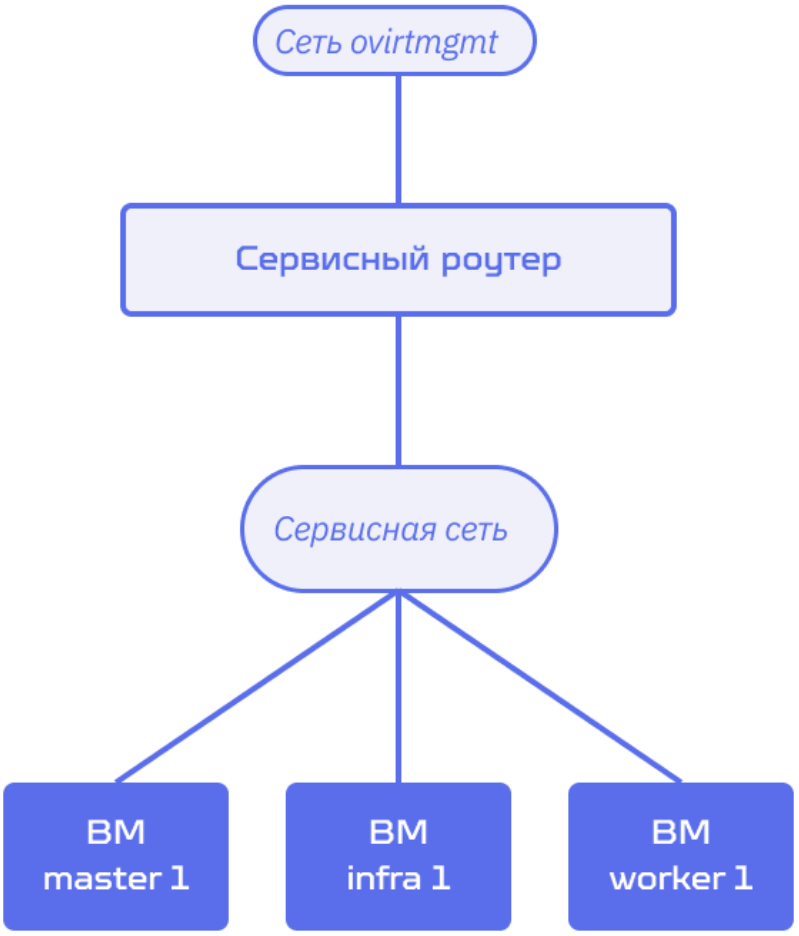


Внешний IP-адрес может быть зарегистрирован в DNS, как имя для Universe.

5.3. Этап 3. Инфраструктура кластера

Для развертывания кластеров в начале необходимо подготовить инфраструктуру:

- Формируется логическая сервисная сеть, к которой подключаются виртуальные машины кластера.
- Сервисный маршрутизатор связан с доступным внешним VLAN (на выбор), чтобы обеспечить выход кластера наружу.
- Вся исходящая активность из кластера также маршрутизируется через SNAT.
- Для обеспечения управления кластером необходимо настроить устойчивый канал связи между Universe и узлами кластера, чтобы обеспечить загрузку компонентов, передачу манифестов и запуск сервисов.



5.4. Этап 4. Межсетевая маршрутизация

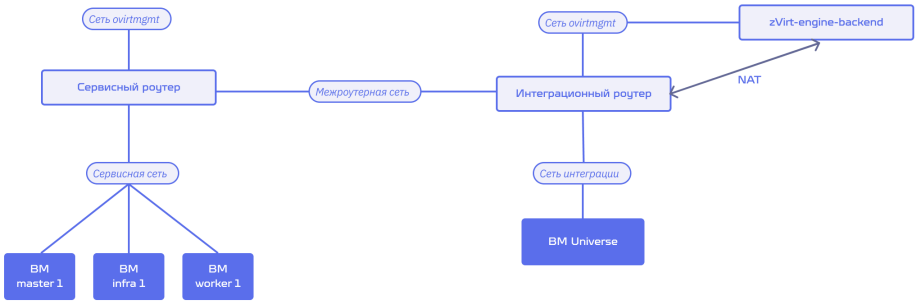
Для организации взаимодействия между Universe и отдельными кластерами используется межсетевая (межроутерная) сеть. Эта сеть подключается одновременно к интеграционному маршрутизатору (интеграционная сеть, в которой размещается Universe) и к маршрутизатору сервисной сети каждого кластера.

На обоих маршрутизаторах (Universe и кластеров) настраиваются маршруты, обеспечивающие двустороннюю связность. Таким образом, Universe получает прямой

сетевой доступ ко всем узлам любого из развернутых кластеров.

Это решение сохраняет изоляцию логических сетей, обеспечивая при этом контролируемую маршрутизацию трафика и необходимый уровень сетевой безопасности.

Пример использования межроутерной сети показан на схеме ниже.



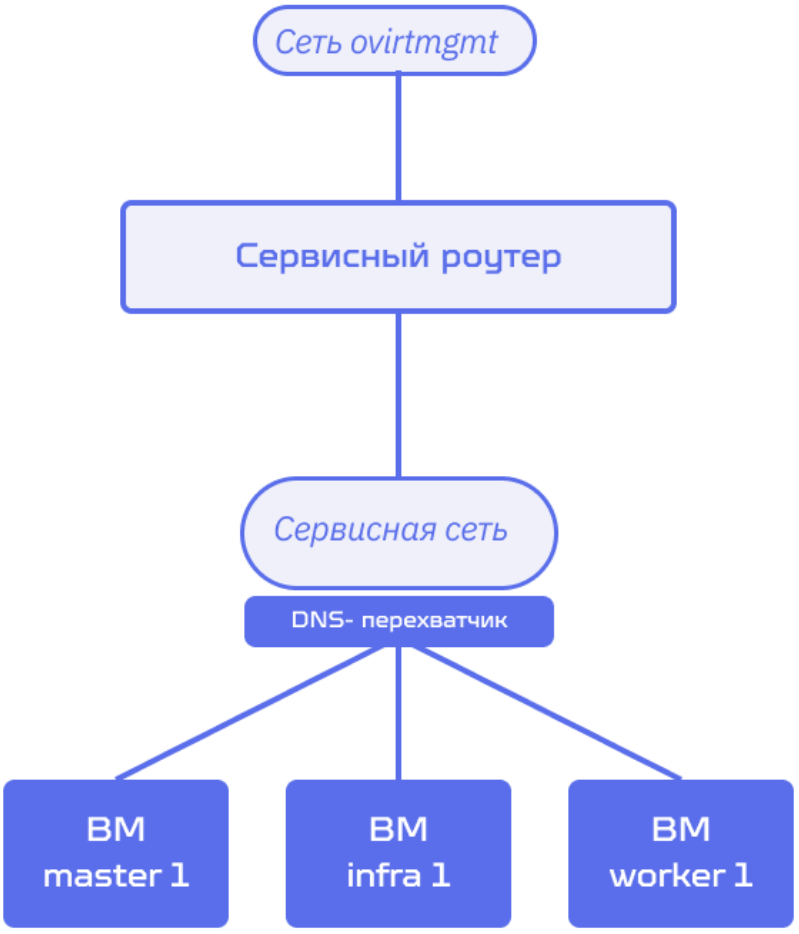
5.5. Этап 5. DNS-перехватчик

Внутренние компоненты Nova взаимодействуют между собой с использованием DNS-имен (например, для обращения к Universe). Однако автоматическая регистрация этих имен во внешней системе DNS не предусмотрена, так как они, как правило, относятся к внутренней изолированной инфраструктуре.

Для решения этой задачи в логических сетях используются DNS-перехватчики (interceptors). Они работают следующим образом:

- Все DNS-запросы, проходящие через сеть (UDP/53), анализируются перехватчиком.
- Если в запросе содержится имя, заранее определенное как «внутреннее» (например, universe.local), перехватчик немедленно возвращает подмененный DNS-ответ — с нужным IP-адресом.
- Таким образом, даже при отсутствии записи во внешнем DNS, система получает корректный ответ и может продолжать взаимодействие.

Это позволяет обеспечить работоспособность сервисов и разрешение имен в пределах изолированной инфраструктуры без необходимости настраивать внешний DNS-сервер или раскрывать внутренние адреса.



В результате прохождения всех этапов проектирования сетевая инфраструктура zVirt Containers формируется как изолированная, но функционально связанная система. Каждый кластер получает собственную логическую сеть с управляемым выходом наружу. Компонент Universe, размещенный в интеграционной сети, обеспечивает **централизованное управление и настройку кластеров**.

Межроутерная сеть обеспечивает взаимодействие между Universe и сервисными сетями кластеров, сохраняя при этом их независимость. Использование DNS-перехватчиков позволяет безопасно и прозрачно разрешать внутренние имена, необходимые для взаимодействия между компонентами.

Такой подход обеспечивает надежную, масштабируемую и изолированную среду для автоматического развертывания и управления Nova Container Platform в рамках zVirt.