АННОТАЦИЯ

!!! Скорректировать цель и остальное согласно тому, что в итоге выйдет в ВКР

Цель выпускной квалификационной работы – исследование и создание кластерной инфраструктуры, которая позовлит разрабатывать и развертывать программные проекты множеством команд из нескольких человек.

В работе составлен обзор по архитектурам приложений и инфраструктур. Произведен анализ инструментов для создания инфраструктуры.

В ходе работы в рамках проекта был развернут кластер Kubernetes, его вспомогательные компоненты, настроено их взаимодействие.

Созданная инфраструктура внедрена в МИЭМ НИУ ВШЭ и происходит поэтапный процесс переноса проекта в нее.

В структуру работы входит введение, ??? глав, заключение, список использованных источников , 1 рис. и 6 источн.

Общий объем проекта составляет 35 стр.

ABSTRACT

blablabla

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

Ansible — blablabla.

Application Programming Interface — blablabla.

Block input and output — обращение на считывание и запись с хранителей данных.

Central processing unit — процессор.

Certificate — blablabla.

CertManager — blablabla.

Continuous Integration and Continuous Delivery or Deployment — blablabla.

Continuous Integration и Continuous Delivery или Deployment — этапы непрерывной интеграции разработок и непрерывной доставки кода вплоть до промышленного использования [5].

Control group — управление (контроль) групп.

Dashboard — blablabla.

DLL Hell — сбой, возникающий, когда одна часть программного обеспечения ведет себя не так, как ожидалось второй частью программного обеспечения, что в некотором роде зависит от действия первого [3].

Docker — программное обеспечение для автоматизации развертывания и управления приложениями в среде виртуализации на уровне операционной системы [4].

Docker Image — blablabla.

Docker Registry — blablabla.

Dockerfile — blablabla.

etcd — blablabla.

Git — blablabla.

GitLab Runner — blablabla.

Go — blablabla.

Helm — blablabla.

Image или образ контейнера — архив файловой системы, который используется для запуска контейнера из него.

Ingress Controller — blablabla.

Issuer — blablabla.

kubeadm — blablabla.

kubectl — blablabla.

kubelet — blablabla.

Kubernetes — blablabla.

kubespray — blablabla.

Let's Encrypt — blablabla.

master — blablabla.

Memory — память.

Mount — монтирование, например дисков как директорий. Способ подключения различных хранителей данных в OS GNU/Linux.

Multi stage approval — blablabla.

Namespaces — пространства имен.

Networking или network — сеть.

nginx — blablabla.

NodeSelector — blablabla.

PersistentVolume — blablabla.

PersistentVolumeClaim — blablabla.

playbook — blablabla.

Pod — blablabla.

PodSecurityPolicy — blablabla.

Process ID — идентификатор процесса.

Quorum approval — blablabla.

Resource management — управление и ограничение ресурсов машины.

roles — blablabla.

Service — blablabla.

Shell — средство для запуска других программ в ОС GNU/Linux.

Stateless — blablabla.

Storage Provisioner — blablabla.

StorageClass — blablabla.

tasks — blablabla.

TLS — blablabla.

Traefik — blablabla.

Uniform Resource Locator — blablabla.

User — пользователь.

volumes — blablabla.

Wildcard сертификат — blablabla.

worker — blablabla.

YAML — blablabla.

Виртуальная машина — программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы (target — целевая, или гостевая платформа) и исполняющая программы для target-платформы на host-платформе (host — хост-платформа, платформа-хозяин) или виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и даже операционные системы [1].

Гипервизор — программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере [2].

Инстанс — экземлпяр объекта.

Система контроля версий — blablabla.

Средства непрерывной интеграции и доставки артефактов — blablabla.

Токен — blablabla.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

VM — virtual machine (виртуальная машина).

OS или ОС — операционная система.

ПО — программное обеспечение.

PID — Proccess ID.

Cgroup — control group.

CPU — central processing unit.

I/O — input and output.

CI/CD — Continuous Integration и Continuous Delivery или Deployment.

K8s — Kubernetes.

IP — blablabla.

HTTP — blablabla.

HTTPS — blablabla.

DNS — blablabla.

NFS — blablabla.

SSD — blablabla.

HDD — blablabla.

CI/CD — blablabla.

API — blablabla.

URL — blablabla.

ВВЕДЕНИЕ

В настоящее время существует спрос на реализацию решений по автоматизации процессов разработки и развертывания программных продуктов. Для этого используются такие средства, как:

— Система контроля версий.

— Средства непрерывной интеграции и доставки артефактов.

— Система контенеризации.

— Оркестрация контейнеров.

— Вспомогательные инструменты.

На текущий момент в МИЭМ активно развивается проектная деятельность. Но изначально инфраструктура не была готова к такому большому количеству проектов и команд, реализующих эти проекты. В первую очередь, необходима была платформа для удобного хранения разработок, то есть система контроля версий. После этого данные наработки необходимо где-то развернуть. Ранее это представляло большую многоэтапную задачу, от поиска локальных администраторов и получения мощностей, до получение доменного имени для публикации проекта для промышленного использования.

Цель работы – оптимизация командного взаимодействия и уменьшение метрик времени вывода в продуктив при разработке программных продуктов посредством переиспользования ресурсов контейнерных сред и общих инфраструктурных кластеров.

СТАРАЯ ТЕРМИНОЛОГИЯ

Immutable - неизменный.

Self-healing - самолечение.

Declarative - декларативность.

SLA - доступность.

Daemon или **Демон** - процесс, запущенный в фоне.

CLI (Command line interface) - консольный интерфейс приложения.

FS (File system) - файловая система раздела.

Hash или **Хэш** - результат выполнения некоторой математической хэш-функции.

Tag или **Тэг** - некоторая отметка на чем-либо для более удобного поиска объектов.

Yaml (YAML Ain't Markup Language) -"дружественный"формат сериализации данных, концептуально близкий к языкам разметки.

SSD (Solid State Drive) или *Твердотельный диск* - вид накопителя, хранящего данные.

REST API - архитектурный стиль взаимодействия компонентов распределенного приложения в сети.

Garbage Collector - "сборщик мусора".

QoS (Quality of Service) - органичения на что-либо, разграничающие по ролям.

Requested resources - запрошенные ресурсы.

Netwrok Policies - сетевые политики.

Iptables - обертка над netfilter.

Ipvs - обертка над netfilter.

OSI - сетевая модель стека сетевых протоколов.

VRRP (Virtual Router Redundancy Protocol) - сетевой протокол, предназначенный для увеличения доступности маршрутизаторов.

SSL/TLS (Secure Sockets Layer) (Transport Layer Security) - криптографические протоколы, обеспечивающие защищенную передачу данных между узлами в сети Интернет.

Hook - перехват чего-либо.

Git - одна из систем контроля версий.

HTTP (HyperText Transfer Protocol) - протокол прикладного уровня передачи данных.

Tar - архиватор.

GET Requests - метод *HTTP*.

1 Исследовательская часть работы

1.1 Виды архитектур инфраструктуры и приложений в ней

На текущий момент существует множество решений со стороны архитектуры инфраструктуры и, как следствие, приложений в ней. Для выбора конкретного решения под вышеуказанные **Указать цели выше** цели необходимо рассмотреть основные из них. Далее они будут описаны по хронологии появления.

а) Монолитная эра. Ей свойственны следующие аспекты:

- Приложения монолитные.
- Куча зависимостей.
- Долгая разработка до релиза.
- Все инстансы известны по именам.
- Использование виртуализации. Это означает:
  - Один сервер – несколько VM [1].
  - Resource Management.
  - Изоляция окружений.

Соответсвенно использовались VM:

- VMWare.
- Microsoft Hyper-V.
- VirtualBox.
- Qemu.

Подход был следующий: один большой сервер делили на несколько виртуальных машин. Это давало полную изоляцию, но недостатками были:

- Hypervisor [2].

— Большие образы.

— Как следствие больших образов с разным ПО – медленное управление VM.

б) На смену им пришла виртуализация на уровне ядра с помощью следующих инструментов:

— OpenVZ.

— Systemd-nspawn.

— LXC.

Но остались прежние проблемы:

— Большие образы с OS с большим количеством ПО.

— Нет стандарта упаковки и доставки.

— DLL Hell [3].

в) Но далее пришли контейнеры. Разница между VM и контейнером:

— Виртуальная машина подразумевает виртуализацию железа для запуска гостевой ОС.

— Контейнер использует ядро хостовой ОС.

— В VM может работать любая ОС.

— В контейнере может работать только GNU/Linux (с недавних пор и Windows).

— VM хороша для изоляции.

— Контейнеры не подходят для изоляции.

В итоге мы приходим к ситуации, изображенной на (Рис. 1.1):

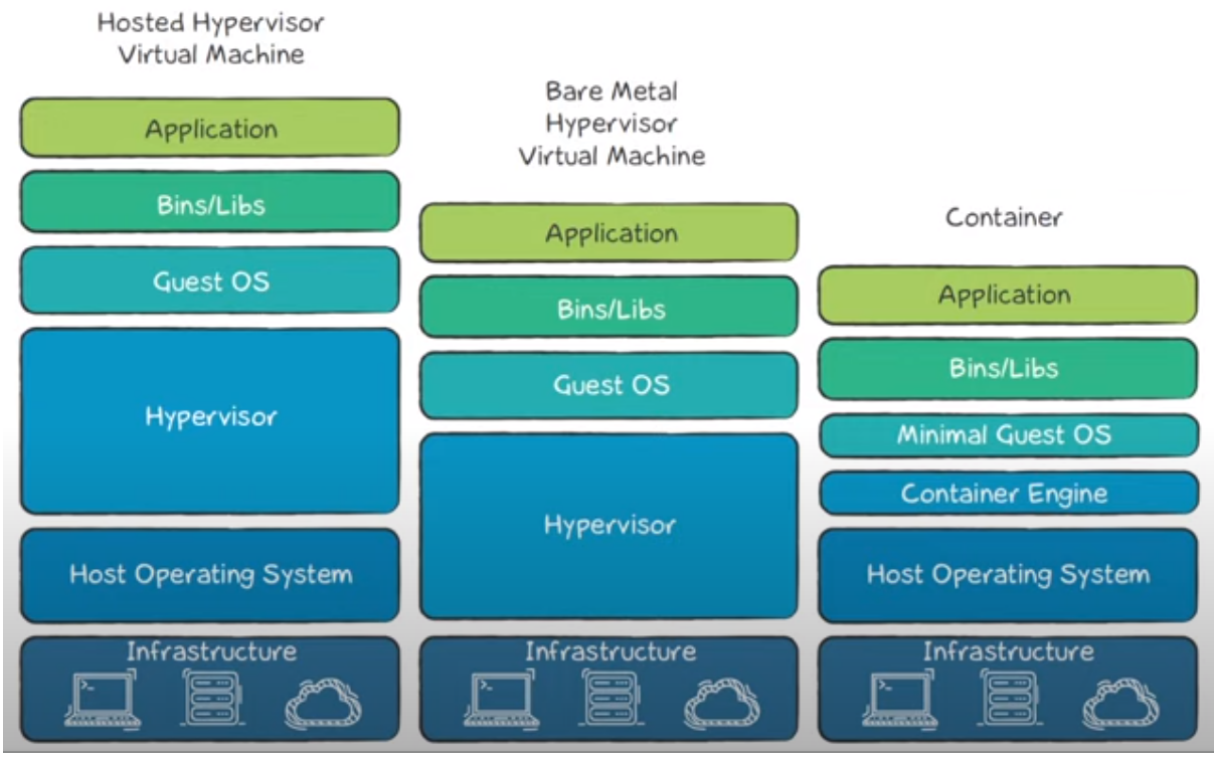

Рисунок 1.1 — Сравнение VM и контейнеров

Способ реализации контейнеризации:

— Namespaces:
  — PID.
  — Networking.
  — Mount.
  — User;
— Control Groups:
  — Memory. .
  — CPU
  — Block I/O;
  — Network;

В итоге получается следующая логика:

— Один процесс – один контейнер.

— Все зависимости в контейнере.

— Чем меньше образ контейнера – тем лучше.

— Инстансы становятся эфемерными.

И в 2014-2015 годах пришел расцвет Docker [4], который:

— Меняет философию подхода к разработке.

— Стандартизует упаковку приложения.

— Решает вопрос зависимостей.

— Гарантирует воспроизводимость.

— Обеспечивает минимум дополнительных средств для использования.

1.2 Область применения

Для большого количества проектов с множеством команд

1.3 Обзор литературы

!!! ПЕРЕПИСАТЬ

Не менее интересны и полезны статьи от IBM [15,16]. Начинаются они со сравнения виртуальных машин и контейнеров, которое было приведено выше. После идет перечисление и детальное рассмотрение каждого из преимуществ использования контейнеров в архитектуре.

По аналогии с сравнением систем CI/CD, стоит обратить внимание на сравнение систем оркестрации контейнеров [17]. Среди рассматриваемых инструментов: Swarm, Kubernetes, Mesos, Cattle. Один из немногих недостатков Kubernetes можно отметить отсутствие ограничений на обращение к диску. Но в тот же момент, среди рассматриваемых систем этим преимуществом обладает только Mesos. В остальном же Kubernetes выигрывает по

функциональности с большим отрывом. Если посмотреть на приведенные в публикации графики, то можно увидеть, что есть не один случай, когда Kubernetes выигрывает с большим отрывом от других средств. В других же случаях он на равных с большинством.

Статья [11] освещает сравнение двух популярнейших систем CI/CD - Jenkins и GitLab CI/CD. В ней рассмотрены основные особенности, возможности функционала, и преимущества двух систем. После дается достаточно объективное сравнение этих инструментов, что позволяет выбрать необходимый под создаваемую инфраструктуру.

Если рассмотреть прикладные статьи по тематике контейнеризации, то внимания заслуживает следующий материал [18]. В нем четко сформулированы простые правила написания инструкций для сборки Docker Images. Как аналогия приводится написание кода на языке программирования C или C++. Также лишними не будут листинги с примерами файлов-инструкций.

Еще одна публикация из прикладной сферы [19] освещает использование Docker. В ней рассмотрены самые часто используемые команды для взаимодействия с Docker, пояснение их работы, поведение и анализ происходящей ситуации.

Другая статья [20] рассказывает о влиянии контейнеров на примере Docker на производительность в прикладных задачах. В ней проведены детальные замеры производительности в разных задачах и условиях, что позволяет объективно оценить, насколько данный инструмент подходит для решение необходимого типа задач.

В дополнение к прикладным статьям, стоит обратить внимание на еще одну [21]. В ней также рассмотрены преимущества контейнеризации, ее особенности. Из ключевых стоит отметить:

☒простоту,

☒поддерживаемость,

☒устойчивость,

☒воспроизводимость,

☒удобство,

☒размер,

☒прозрачность.

Интересной статьей является еще одна [22]. В ней рассматривается достаточно нестандартное использование Docker для запуска приложений с графическим интерфейсом. Для этого используется дополнительный инструмент - x11docker. Он напрямую связан с графическим сервером - Xorg Windows System Server. Это позволяет выстроить безопасную экосистему, где приложения будут независимы друг от друга и уязвимость в одном из них не позволит получить доступ к другим.

Нельзя обойти стороной рассмотрение официальных лучших практик по контейнеризации от разработчиков самого Docker [23]. Первым и, пожалуй, ключевым они выделяют важность порядка инструкций, потому что если что-то изменяется выше, то все последующие инструкции будут тоже исполнятся заново, что сильно увеличивает время сборки Docker Image.

Еще одна публикация рассматривает обработку больших данных в нескольких облаках посредством контейнеров [24]. Это затрагивает такой аспект как “федерации” - когда кластер может быть разнесен географически, при этом связность данных в нем должна сохраняться. Это достаточно нетривиальная задача, так как при этом данные, поступившие в один филиал, могут еще не успеть дойти до другого, прежде чем они будут запрошены.

В другой статье [25] приводится сравнение вертикального и горизонтального масштабирования. Это давняя известная проблема: вместо наращивания мощности одного инстанса, например, сервера,

лучше взять еще один такой же конфигурации. Это позволяет экономить финансы. Но опять же, приложение архитектурно должно быть к этому готово.

Если же рассмотреть промышленное использование в больших масштабах, то стоит обратить внимание на данную книгу [26]. Она рассказывает о “кровавом энтерпрайзе”, что позволяет выявить ряд недостатков в выбранной архитектуре, так как не всегда она подходит под нужды бизнеса.

Для сравнения систем оркестрации не помешает прочитать статью об альтернативе и ее использовании [27]. С одной стороны, она тоже намного мощнее такого инструмента как docker-compose, который подходит для одного микросервиса. Но в сравнении с Kubernetes есть ряд очень ощутимых преимуществ у последнего.

Чтобы лучше понять логику “пакетного менеджера для приложений” - Helm, стоит обратить внимание на статью о его истории и будущем [28]. Как минимум, заслуживает внимание разбор гигантское обновление со второй на третью версию этого инструмента, где отказались от части логики, из-за чего отсутствует обратная совместимость.

Для малого и среднего бизнеса стоит рассмотреть использование продукта компании Flant, который они рекламируют в публикации [29]. Он может сильно упростить процессы CI/CD, то есть упростить жизнь инженерам.

И, как десерт, рассмотрение возможности автомасштабирования в Kubernetes - еще один материал от Flant [30]. Это безумно важно для пилотных проектов, так как если они “выстреливают”, то есть набирают популярность, то нагрузка вырастает в разы, если не на порядки.

Для рассмотрения связки GitLab и Kubernetes отлично подходит статья компании, которая помогает внедрять эти технологии огромному количеству малого и среднего бизнесов [5].

Более того, эта статья заслуживает внимания, так как является выдержкой с выступления на одной из крупнейших конференций в России по высоконагруженным системам - Highload++ 2017. В первую очередь хочется отметить наглядность анимированного изображения, которое позволяет наглядно увидеть разницу между разными инструментами CI/CD. . Данное изображение дает понять, что:

— Git вместе с shell дает несколько окружений и анализ кода.

— Добавление Docker позволит улучшить тестирование до тестов без окружения и добавит аспект Stateless приложения в архитектуру.

— Дополнительное использование Kubernetes и Helm позволяет довести тестирование до тестов в ”полном”окружении, а архитектуру привести к микросервисной логике.

— При пополнении стека с помощью GitLab мы получаем несколько площадок вместо нескольких окружений, а также простое разделение прав доступа. Этого набора уже зачастую предостаточно для покрытия нужд.

— Финальный аккорд - GitLab Enterprise, который привносит разные права на окружения, ”multi stage approval” или же ”quorum approval” логики.

В итоге у компании Flant используется один из самых популярных стеков технологий, за исключением dapp, который на текущий момент переименован в werf, их личная разработка, которая используется для упрощения или улучшения процессов сборки и не только.

В материалах предыдущей статьи есть ссылки на другие статьи, что позволяет глубже погрузиться в тематику. Если посмотреть на обзор другого доклада с RootConf 2017 [6], то можно заметить пересечения с вышеупомянутой историей развития

архитектуры. Но стоит дополнить тем, что еще не было освещено, а именно рядом сложностей микросервисной архитектуры:

— Сбор логов.

— Сбор метрик.

— Проверка состояния сервисов и их перезапуск в случае проблем.

— Автоматическое обнаружение сервисов.

— Автоматизация обновления конфигураций компонентов инфраструктуры (при добавлении/удалении новых сущностей сервисов).

— Масштабирование.

— CI/CD.

— Зависимость от выбранного "поставщика решения".

По мнению докладчика, все эти сложности можно закрыть с помощью Kubernetes и ряда вспомогательных инструментов.

Далее освещаются базовые аспекты архитектуры Kubernetes, его сущности от Pod до Ingress. Следующий раздел погружает нас в разные архитектуры Kubernetes, в зависимости от нагрузки, требований к отказоустойчивости и других параметров, что еще раз демонстрирует его гибкость как инструмента.

Если изучить еще одну статью [4], которая затрагивает первые практики Continuous Delivery с Docker, то можно раскрыть детальнее первый из этих терминов. Под Continuous Delivery имеется в виду последовательность действий, в результате который код из Git-репозитория сначала собирается, потом тестируется, после чего попадает в промышленное использование и после уходит в архив. Также в статье поднимается вопрос проблемы простоя во время выкатки в промышленное использование новой версии

продукта. На текущий момент это решается следующей последовательностью:

☒старая версия запущена,

☒в соседнем месте запускается и “прогревается” новая версия,

☒когда новая версия готова к работе, трафик переключается на нее,

☒старая версия может быть остановлена.

Не меньшего внимания заслуживает еще одна статья от компании-интегратора Flant уже про базы данных в Kubernetes [5]. Основная проблематика заключается в том, что Kubernetes ориентирован на stateless приложения, то есть приложения без сохранения состояния. А БД - яркий пример stateful приложения, которому жизненно необходимо сохранение своего состояния. В старой архитектуре приложений была следующая логика с СУБД: репликация на двух железных серверах с резервированным питанием диском сетью и всем остальным, включая инженера на дежурной смене. Это позволяло гарантировать, что если что-то или кто-то выйдет из строя, то есть возможность оперативно переключиться или заменить неисправный элемент. В архитектуре же Kubernetes ощутимо другая логика, но она тоже привносит отказоустойчивость:

☒логика кворума в купе с логикой логикой активного и запасного мастер компонентов, которые управляют кластером,

☒автоматический переезд сущностей с упавшего сервера на остальные,

☒возможность декларативно описать логику поведения при недоступности сущности.

Как простое решение с низким показателем критичности в аспекте отказоустойчивости предлагается сущность StatefulSet с одной сущностью Pod, что означает запуск СУБД или другого

stateful приложения в одном экземпляре. Этого может быть вполне достаточно для тестовых сред. Чуть более сложная схема - StatefulSet уже с двумя инстансами, между которыми настроена репликация данных с возможностью переключение с активного приложения на запасное. Но оптимальным решением будет рассмотреть приложения с сохранением состояния, которые уже умеют работать в кластере, например Kafka в роли брокера сообщений.

В одной из перечисленных выше статей поднималась проблема мониторинга большого количества сущностей в архитектуре Kubernetes. Но есть статья [6], которая освещает эти моменты. Это также обзор с доклада, в этом случае с RootConf 2018. В его начале рассказывается о ключевых аспектах мониторинга, например, что спидометр показывает скорость и усреднение его редких показателей будут сильно расходится с одометром. Также освещены специфики мониторинга в Kubernetes, основной из которых является совершенно другой масштаб того, что нужно мониторить и с какой скоростью. В статье утверждается, что ключевой выбор для такого мониторинга - Prometheus. Одним из подтверждением этого выбора следуют данные из книги о экосистеме Kubernetes [7]. Далее уже речь заходит об архитектуре самого Prometheus, и о том, какие метрики стоит собирать в Kubernetes. Для наглядного отображение всех агрегированных метрик используется такой инструмент как Grafana.

Кроме вышеперечисленных статей, начинающему стоит обратить внимание на пример или инструкцию развертывания простого проекта в Kubernetes с помощью GitLab CI/CD [10]. Если предварительно посетить и изучить курсы по GitLab, Docker, Kubernetes и Helm, то данный материал будет предельно понятен и поможет начать создание шаблонов для развертывания продуктов в инфраструктуре.

Еще одна проблема - накопление и, как следствие, необходимость умной очистки неиспользуемых Docker Images, освещается в статье от вышеупомянутой компании Flant [12]. Есть два решения данной проблемы: либо использовать фиксированное количество тегов для Docker Images, либо же каким-то образом очищать Docker Images. Во втором случае необходимо выбрать критерии актуальности образа, что также освещено в статье. Ключевой замысел реализован в подборе оптимального количества последних сохраняемых образов для каждой ветки Git-репозитория.

1.4 Разработка архитектуры и выбор инструментария

Картинки с разными уровнями погружений и т.д. в новую архитектуру с пояснениями

1.5 Этапы реализации инфраструктуры

Что-то типа roadmap

2 Практическая часть работы

2.1 GitLab

Первым этапом было необходимо развренуть систему контроля версий. Ранее был выбран GitLab как комплексное решение данной задачи.

2.2 Kubernetes

Далее необходимо было развернуть кластер для контейнеров. Основным инструментом, решающим эту задачу был выбран Kubernetes. Официальным инструментом для выполнения этой задачи является kubeadm, но он имеет ряд недостатков. Среди них стоит отметить сложность настройки нестандартных конфигураций, не говоря уже о сложности обновления кластера или подключения дополнительных нод. Поэтому был выбран один из самых популярных инструментов – kubespray. Этот инструмент, по своей сути – YAML-манифесты, с помощью которого описаны playbook для Ansible – средства автоматизации по развертыванию инфраструктур. В свою очередь, tasks и roles в playbook используют kubeadm, но управлять им через данные абстракции в разы проще и удобнее. Также это позволяет иметь готовый артефакт, чтобы повторно развернуть кластер в другом месте или обновить его, внеся небольшие изменения.

Далее будут рассмотрены переменные, определенные в файле для развернутого кластера, отличающиеся от заданных по умолчанию:

а) Файл `inventory.ini`:

Данный файл кардинально отличается от оригинала, так как тот является лишь примером. В нем указаны в общей группе все инстансы, которые будут использоваться как ноды кластера. Среди них master и worker ноды, за названием каждой ноды должен быть

указан ее IP адрес для подключения. Также master ноды должны быть перечислены в группе kube-master. Если etcd будет располагаться на master нодах, то их надо указать в группе etcd, иначе необходимо указать отдельные инстансы в общей группе под хранилище манифестов, и, соотвественно, указать их в группе хранилища. Worker ноды указываются в группе kube-node. Детальнее можно ознакомиться в ПРИЛОЖЕНИИ ТАКОМ-ТО.

б) Файл `group_vars/k8s-cluster/addons.yml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

— `dashboard_enabled: true`

Это позволяет получить базовый dashboard с состоянием кластера до момента поднятия полноценного мониторинга.

— `helm_enabled: true`

Эта опция устанавливает Helm вместе с кластером Kubernetes.

— `metrics_server_enabled: true`

Включает отдачу метрик.

— `ingress_nginx_enabled: false`

Это значение по умолчанию, но на первых этапах его стоит поменять на true, чтобы иметь в базовой установке кластера Ingress Controller на базе nginx.

— `ingress_nginx_host_network: true`

Данный параметр не будет задействован без предыдущего, но его стоит выставить в значение true, чтобы при включении базового контроллера он был работоспособен за счет обработки трафика с хостовой ноды.

— `ingress_nginx_namespace: "ingress-nginx"`

Здесь указано пространство в кластере, в котором будет находится контроллер. Этот параметр стоит раскомментировать, чтобы четко задать пространство, не предоставляя возможности разместить контроллер в пространстве по умолчанию или же служебном пространстве.

— `ingress_nginx_insecure_port: 80`

Порт, на который должны приходить HTTP-данные.

— `ingress_nginx_secure_port: 443`

Порт, на который должны приходить HTTPS-данные.

в) Файл `group_vars/k8s-cluster/k8-cluster.yml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

— `kube_version: v1.19.6`

На момент развертывания кластера последняя из стабильных версий kubelet.

— `kube_service_addresses: 10.10.0.0/16`

Более широкая по диапазону адресов сеть, нежели предложенная по-умолчанию. Также необходимо отслеживать, чтобы виртуальные сети кластера не пересекались с сетями на хостовых нодах.

— `kube_pods_subnet: 10.15.0.0/16`

Аналогично предыдущему параметру, указана более широкая сеть.

— `cluster_name: cluster.itsoft`

Задание имени кластера, что также влияет на внутренние DNS-имена.

— `podsecuritypolicy_enabled: true`

Включение PodSecurityPolicy в кластере, что позволит настроить ограничения работы контейнеров и других сущностей для большей безопасности.

— `kubeconfig_localhost: true`

Установка служебной утилиты на машину, с которой производится развертывание кластера.

— `kubectl_localhost: true`

Установка служебной утилиты для управления кластером на машину, с которой производится развертывание кластера.

г) Файл `group_vars/k8s-cluster/k8-net-calico.yml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

— `calico_ip_auto_method: “interface=ens3”`

Опция, позволяющая сетевому плагину для кластера автоматически определить, какую сеть использовать для работы между нодами, на основе указанного сетевого интерфейса.

д) Файл `group_vars/etcd.yml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

— `etcd_memory_limit: 0`

Такое задание значения параметра снимает ограничения по памяти на хранилище манифестов etcd, что критично для его работы.

е) Файл `group_vars/all/docker.yml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

— `docker_storage_options: -s overlay2`

Так как на хостах используется свежая версия ядра ОС, то желательно использование более современного драйвера хранения данных для Docker.

После адаптации конфигурационных файлов под задачи и доступные вычислительные ресурсы, необходимо запустить playbook `cluster.yml`. При дальнейших обновлениях кластера необходимо использовать файл `upgrade-cluster.yml`.

2.3 NFS

Следующим этапом стало подключение системы хранения данных для контейнеров. Для этого была создана NFS – сетевая файловая система. Она подключена с помощью проекта NFS Subdir External Provisioner для кластера Kubernetes. Проект также пришлось адаптировать под созданные хранилища отдельно на SSD и HDD:

а) Файл `deploy/helm/values.yaml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

На месте примера с одной подключаемой NFS была переписана структура YAML-манифеста, которая теперь включает подразделы ssd и hdd, в которых уже, в свою очередь, указывается IP адрес сервера, путь до директории на сервере и опции монтирования.

б) Файл `deploy/helm/templates/deployment.yaml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

Из-за подключения двух NFS у Storage Provisioner для Kubernetes необходимо было создать, соотвественно, два контейнера: один для хранилища на SSD, второй для HDD. В связи с этим были продублирован раздел с контейнером, изменены их имена и метки, подправлены обращения к переменным в `deploy/helm/values.yaml`, и добавлены необходимые volumes для монтирования.

в) Файл `deploy/helm/templates/storageclass.yaml` (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

Также, как и в `deploy/helm/templates/deployment.yaml`, были скорректированы обращения к переменным в `deploy/helm/values.yaml`, продублирован StorageClass, поправлены имена во избежание коллизий.

После выполнения подготовки и настройки конфигурации под имеющиеся NFS, необходимые сущности Kubernetes разворачиваются с помощью Helm по инструкции проекта. Также, после развертывания проекта, необходимо написать YAML-манифесты для создания набора тестовых экземпляров сущностей Kubernetes, чтобы проверить работу хранилища: PersistentVolumeClaim, обращающегося к необходимому StorageClass, несколько Pod с PersistentVolume, который обращается к указанному ранее PersistentVolumeClaim, один из которых записывает в него данные, а другой позволяет их прочесть (ПРИЛОЖЕНИЕ ТАКОЕ-ТО).

2.4 Traefik

Далее необходимо было настроить Ingress Controller для промышленного использования, то есть обработки сетевого трафика. В качестве этого инструмента был выбран Traefik. Он, в сравнении с предлагаемым по умолчанию nginx, является намного более современным, лишенным некоторых ощутимых недостатков, которые присущи nginx. Его настройка также заслуживает внимания:

Файл values.yaml (ПРИЛОЖЕНИЕ ТАКОЕ-ТО):

— `ingressClass[enabled]: true`

Этот параметр означает, что будет создана сущность IngressClass в кластере Kubernetes для того, чтобы он корректно увидел новый Ingress Controller.

— `ingressClass[isDefaultClass]: true`

Задание Traefik как Ingress Controller по умолчанию.

— `pilot[enabled]: true`

Эта опция включает возможность управления и мониторинга активности Traefik посредством веб-интерфейса. За ней следует еще одна, содержащая токен.

— `volumes`

Этот раздел параметров указывает сущности Kubernetes, которые необходимо подключить к Pod Traefik. На данном этапе это используется, чтобы подключить wildcard сертификаты для сайтов.

— `ports[web][hostPort]: 80`

Это значение позволяет включить проброс сетевого трафика с 80-го порта инстанса, на котором будет находиться Pod Traefik на заданный по умолчанию порт самого Pod Traefik.

— `ports[web][redirectTo]: websecure`

Эта опция включает перенаправления трафика с HTTP на HTTPS.

— `ports[websecure][hostPort]: 443`

Аналогично подобной опции в разделе `web`, позволяет проброс трафика с хостовой машины внутрь Pod Traefik.

— `ports[websecure][tls][enabled]: true`

Эту опцию необходимо включать для того, чтобы работали сертификаты для HTTPS. Далее, в разделе tls, указываются пути до сертификатов и обслуживаемые доменные имена.

— `service[enabled]: false`

Так как у нас Traefik является входным узлом, то для него не требуется сущность Service Kubernetes.

— `persistence[enabled]: true`

Использование PerstistentVolumeClaim Kubernetes для хранения TLS сертификатов. Далее также необходимо указать корректный StorageClass, который был создан ранее.

— `podSecurityPolicy[enabled]: true`

Включение аспектов безопасности Pod Traefik.

— `resources`

Этот раздел аргументов позволяет задать минимальные требования по ресурсам для запуска Traefik, а также его лимиты, за которые он не сможет выйти по потреблению.

— `nodeSelector`

С помощью сущности NodeSelector можно указать, на каком хосте или группе хостов должен оказаться конкретный Pod. В данном случае, это позволяет расположить Pod Traefik именно там, куда проброшен трафик из Интернета.

— `tolerations`

С помощью данной сущности Kubernetes можно обойти какие-либо ограничения. В текущем случае, это ограничение на планирование запуска Pod на master ноде.

2.5 CI/CD

После этого была начата разработка тестового проекта для развертывания в кластере с помощью CI/CD. За основу был взят минимальный веб-сервер на языке программирования Go, который отдавал статичную страницу. Далее был написан Dockerfile с командами для сборки и запуска веб-сервера. Первая его часть основан на Docker Image `golang:1.8-alpine`. Далее код копируется внутрь Docker Image посредством директивы texttttADD и компилируется с помощью директивы `RUN`. После этого берется второй Docker Image `alpine:latest`, в который переносится

скомпилированный веб-сервер директивой `COPY`. Также объявляется порт для прослушивания трафика директивой `ENV`. И последней директивой `CMD` запускается веб-сервер.

Далее было необходимо написать Helm-chart для развертывания контейнера Docker и всех необходимых для его работы сущностей Kubernetes в кластере. В качестве ключевых файлов выступают `.helm/values.yaml` и `.helm/Chart.yaml`, в которых содержатся:

— Название проекта.

— Описание проекта.

— Версия проекта.

— Версия используемого API.

— Название Docker Image.

— Тег Docker Image.

— Политика скачивания образа.

— Количество копий образа, которое должно быть запущено.

— Порт, на котором веб-сервер образа слушает трафик.

На основе этих переменных все остальные файлы в директории `.helm/templates` будут описывать сущности кластера Kubernetes:

— `helm/templates/deployment-app.yaml`

— `helm/templates/service-app.yaml`

— `helm/templates/ingress.yaml`

Далее был написан файл `.gitlab-ci.yml`, который является YAML-манифестом для описания этапов CI/CD для развертывание проекта в кластере. Он состоит из трех этапов:

— `build`.

— `push`.

— `deploy`.

Этап `build` выполняется в одну команду `docker build` с указанием тега самим GitLab Runner.

Этап `push` требует предварительной аутентификации в Docker Registry, для этого был взят пример из официальной документации по GitLab. После этого выполняется `docker push`.

Этап `deploy`, относящийся к CD уже намного сложнее. Для этого требуется задать в GitLab API URL кластера Kubernetes, а также его токен. После чего в начале выполнения этапа мы задаем эти переменные в окружение с помощью `kubectl`, после чего происходит проверка на то, существуют ли уже данный проект в кластере. Если проект существет, то будет выполнена команда `helm upgrade`, в противном случае будет выполнена команда `helm install`. Детальнее эти вещи можно увидеть в ПРИЛОЖЕНИЕ ТАКОМ-ТО.

2.6 Certs

Последним этапом развертывания кластера стало автоматическое получение сертификатов для проекта. Для этого был установлен проект CertManager в кластер Kubernetes. После чего был доработан Helm-chart, в котором появились сущности Certificate и Issuer, которые взаимодействуют с центром сертификации Let's Encrypt через CertManager. Их содержимое отображено в ПРИЛОЖЕНИИ ТАКОМ-ТО.

3 Документация

3.1 Инструкция для пользователя

Скирны веб-морды от Матвея + прописывание данных в GitLab

3.2 Руководство администратора

Как обновить GitLab, K8s, мб еще что

3.3 Документация разработчика

Ознакомиться со всей вкр и другими доками

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Wikipedia. Виртуальная машина — Википедия. — 2021. — Режим доступа: https://ru.wikipedia.org/w/index.php?title=%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0&stable=1 (дата обращения: 07.05.2021).

2. Wikipedia. Гипервизор — Википедия. — 2021. — Режим доступа: https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%B5%D1%80%D0%B2%D0%B8%D0%B7%D0%BE%D1%80 (дата обращения: 07.05.2021).

3. Dick Stephanie, Volmar Daniel. DLL hell: software dependencies, failure, and the maintenance of microsoft windows // IEEE Annals of the History of Computing. — 2018. — Vol. 40, no. 4. — P. 28–51.

4. Демидова ТС, Соболев АА. Использование Docker для развёртывания вычислительного программного комплекса // Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем. — 2019. — P. 432–435.

5. Хабр. Лучшие практики CI/CD с Kubernetes и GitLab (обзор и видео доклада) / Блог компании Флант / Хабр. — 2021. — Режим доступа: https://habr.com/ru/company/flant/blog/345116/ (дата обращения: 10.05.2021).

6. Хабр. Наш опыт с Kubernetes в небольших проектах (обзор и видео доклада) / Блог компании Флант / Хабр. — 2021. — Режим доступа: https://habr.com/ru/company/flant/blog/331188/ (дата обращения: 10.05.2021).