GS LABS
GS GROUP

Публичный - L0

DRE Event Server

Руководство по установке

Индекс	DREES-IG
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация

Документ предназначен для технических специалистов, занимающихся установкой, настройкой и поддержкой системы мониторинга DRE Event Server (далее - DREES). Документ рассчитан на инженеров, обладающих специальными навыками и знаниями в области программного обеспечения.

> ⚠ Данный документ опубликован исключительно с целью изучения системных требований для установки продукта, а также ознакомления с последовательностью и деталями процесса установки. Реальная установка продукта производится с использованием внутренних репозиториев ООО "Цифра", доступ к которым предоставляется заказчику по запросу.

2. Минимальные системные требования

Для установки DREES необходимо наличие не менее 3 серверов с разными именами (hostname): master, worker1, worker2. Общее количество мастеров должно быть нечетным.
Серверы должны удовлетворять следующим требованиям:

1. Операционная система Ubuntu 18.04.
2. Многоядерный центральный процессор с тактовой частотой каждого ядра 2 ГГц (не менее 20-ти ядер).
3. Объем оперативной памяти 64 ГБ.
4. Не менее 2-ух жестких дисков емкостью не менее чем по 500 ГБ. Рекомендуется наличие на каждой ноде помимо основного дискового пространства с ОС 1-го диска SSD или NVMe и 9-ти дисков HDD (SATA, SAS), не собранных в RAID и не форматированных.
5. Два интерфейса Ethernet 100 и 1000 Base-T с поддерживаемой пропускной способностью 100 и 1000 Мбит/сек соответственно. Один предназначен для сети поддержки, второй используется для вывода генерируемого транспортного потока.
6. Свободное место для папки временных файлов /tmp - 10 ГБ.

Установка должна производиться с дополнительного Ubuntu-сервера, не имеющего отношения к будущему кластеру. Требования к объему ресурсов дополнительного сервера отсутствуют.

2.1. Развертывание сервисов DREES в кластере kubernetes

Кластер развёртывается по официальной инструкции (https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/high-availability/).

Для установки DREES в имеющийся настроенный кластер Kubernetes используется процесс CI/CD, настраиваемый с помощью GitLab. Весь процесс описан в документе, который предоставляется заказчику по требованию.

Все действия возможно производить на локальной машине или на любом Ubuntu-сервере с доступом через консоль от имени любого пользователя.

Для развертывания EventServer используется CD конфигурация на базе Helm Chart и Helmfile. Ссылка на репозиторий с конфигурацией предоставляется заказчику по требованию.

Состав репозитория:

- versions.yaml - файл, содержащий последние стабильные версии сервисов
- services.yaml - файл, сожержащий данные - какие сервисы будут ставиться
- infrastructure.yaml - файл, сожержащий данные - какая инфраструктура будет развернута
- helmfile.yaml - файл, содержащий в себе список сервисов DREES

Предполагается, что DREES будет доступен по доменному имени оператора, а так же будет поддерживать Swagger UI для тестирования. Файл haproxy.cfg предоставляется заказчику по требованию.

Для балансировки сервисов между нодами, кластер использует механизм nodeAffinity, для которого нодам необходимо раздать разные лэйблы (label). Для конфигурации балансировки сервисов необходимо изменить поле nodeAffinity в используемом файле values.yaml.

NodeAffinity:

```
# Each service deploy to defined node, using this labels
nodeSelector:
  consumer:
    role.providence/consumer: ""
  events:
    role.providence/events: ""
  geoIp:
    role.providence/geo-ip: ""
  gateway:
    role.providence/gateway: ""
  envoy:
    role.providence/envoy: ""
```

3. Требования к окружению

Для развёртывания DREES предварительно необходимо соблюсти следующие требования:

1. Развернуть высоконагруженный кластер PostgreSQL с расширением TimescaleDB.
2. Разворачивать необходимо HA кластер Kubernetes.

Требования к PostgreSQL

> ⚠ Начиная с версии 4.5 может использоваться версия PostgreSQL 16.
> PostgreSQL в данном продукте - это ключевой компонент. Чем быстрее база, тем больше клиентов DREES может обслуживать. Рекомендуется использовать расширение TimescaleDB для работы с Time-series - партиционирование таблиц, функции агрегации и т.д. Последовательность действий приведена ниже.

1. Развернуть PostgreSQL. Лучше - отказоустойчивый, но главное - быстрый.
2. Развернуть пулер соединений перед ним (опционально для тестовых зон).
3. Установить расширение TimescaleDB.
4. Создать БД для DREES (в примерах будем использовать имя "event-server").
5. Создать пользователя с доступом только к этой БД (в примерах будем использовать имя "event-server-user" с паролем "event-server-password").
6. Записать артефакты конфигурации для последующей настройки DREES:
    a. IP адрес и порт мастера (пулера).
    b. Имя БД.
    c. Логин и пароль пользователя.
    d. Имя схемы, используемой в БД (по умолчанию - "public")

3.1. Обновление до pgx5

В строке подключения к postgres нужно убрать лишние параметры `statement_cache_mode` и `statement_cache_capacity`.
Также нужно добавить новый параметр `default_query_exec_mode=cache_describe`, чтобы базе было легче.

3.2. Установка Nats JetStream

Поддерживается NATS JetStream с версии 2.9.7 и выше. Установка Nats JetStream выполняется при включении ссылки на файл infrastructure.yaml из релизного проекта в helmfile проекта установки следующим образом:

helmfile.yaml:

```
helmfiles:
  - path: ingress.helmfile.yaml
  - path: ceph.helmfile.yaml
    values:
    - production.yaml
  - path: providence/helmfile.yaml
    values:
      - providence/versions.yaml
      - providence/default.yaml
      - production.yaml
```

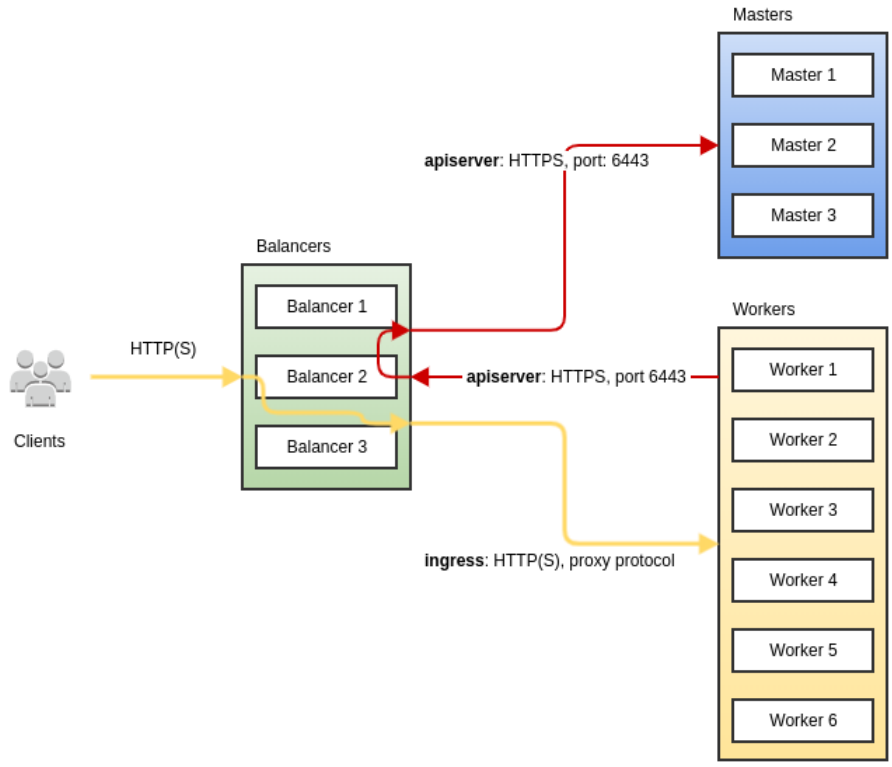
3.3. Распределение узлов

Необходимо разделить узлы логически на две роли:

Роль	Компоненты	Пример распределения ресурсов	Требования к количеству узлов	Требования к физическому местоположению	Резервное копирование
Master	• apiserver • control plane • etcd	• 2 CPU cores • 2GB RAM	1. Не менее трёх 2. Нечётное количество	Распределить по физическим машинам. Рекомендуется 1 физическая машина - 1 master нода.	Каждый час - полный snapshot etcd. (Документация https://etcd.io/docs/v3.3.12/op-guide/recovery/)
Worker	• kubelet	• 4 CPU cores • 16GB RAM	1. Не менее двух	Распределить по физическим машинам. Рекомендуется 1 физическая машина - 2 worker-ноды.	Не требуется

3.3.1. Общая схема

Перед Kubernetes кластером необходимо разместить балансировщики на базе haproxy для балансировки как внутреннего трафика kubernetes (workermaster), так и внешнего (ingress). Балансировщики должны иметь общий Virtual IP адрес, который настраивается через keepalived. Этот адрес должен использоваться как адрес мастера при создании кластера. Таким образом, в случае отказа мастера, трафик с воркеров будет успешно достигать одного из мастеров. Схематически процесс изображен ниже:



3.4. Конфигурация Ingress

IIngress Controller, который используется - nginx-ingress, и для правильной его работы с proxy protocol, в его конфигурации потребуется установка дополнительных опций. Для каждого worker узла необходимо выполнить эту команду:

```
kubectl label node <node> node-role.kubernetes.io/ingress=
```

Конфигурация Ingress задается в файле ingress.helmfile.yaml, который подключается в файле helmfile.yaml.

База данных географического отношения адресов не используется.

Конфигурация Ingress предоставляется заказчику по требованию.

3.5. Конфигурация TLS

Nginx не поддерживает автоматическое определение протокола между HTTP1.1 и HTTP/2 если не используется TLS. Именно поэтому установка DREES невозможно в среду с отсутствующим TLS шифрованием.

В наличии необходимо иметь сертификат, подходящий к доменному имени metrics.tricolor.tv. Дла загрузки сертификата в кластер используйте команду:

```
$ kubectl --namespace events providence secret tls [domain.name] --cert <path_to_cert_file> --key
<path_to_key_file>
```

3.6. Конфигурация Envoy

Envoy используется для отказоустойчивой балансировки нагрузки между подами events server. Развертывается автоматически, при помощи helm чарта event server, в дополнительной конфигурации не нуждается.

© ООО "Цифра", 2019-2024

Документация "DRE Event Server. Руководство по установке" является объектом авторского права. Воспроизведение всего произведения или любой его части воспрещается без письменного разрешения правообладателя.