K8S 42: Kubernetes. Advanced. Cert-manager

Описание:

Вернемся на одно задание обратно к теме Ingress, поскольку теперь у нас есть кластер с внешним IP-адресом, и мы можем разобрать еще один очень важный инструмент.
Cert-manager — это демон для Kubernetes Cluster (даже точнее — для Ingress), который позволяет в автоматическом режиме получать TLS сертификаты для ваших Ingress и хранить их в системе в виде Secret, а не создавать их вручную.
Перед тем, как начать работу с данной утилитой, разберем архитектуру приложения:
Cert-manager хранит свои сущности в Custom Resource Definitions:

- issuers — данные, которые используются для получения сертификатов — определяют, откуда получать сертификат (cert-manager поддерживает не только Let's Encrypt, но и других поставщиков) и с какими данными. Применяется на уровне Namespace.
- clusterissuers — практически тоже самое, что и issuers, но применяется на весь кластер.
- orders — на время работы хранит здесь все запросы, которые требуется выполнить для получения сертификата.
- certificaterequests — во время получения сертификата сохраняет запросы на сертификаты, которые отправляются в сторону провайдера с приватным ключем.
- challenges — после получения challenge со стороны поставщика сертификата сохраняет его здесь для создания Challenge Service.
- certificates — хранит данные о сертификатах — когда они выданы, в каком секрете хранятся и для какого Ingress создавались.

Сертификат, в котором хранится сертификат и приватный ключ, согласно требованию Ingress, хранится в Secret, который указан в манифесте Ingress.
Как понятно, самый частый кейс использования Cert-manager — автоматизация получения сертификата от Let's Encrypt. И для этого в Cert-manager реализовано несколько методов получения — HTTP и DNS (для ряда провайдеров, которых поддерживает и Certbot).
Все параметры использования Cert-manager записываются в манифестах Ingress через аннотации, позволяя определить, управляется ли сертификат через Cert-manager и какой Issuer или ClusterIssuer используется для конкретного Ingress. Именно эти аннотации и вылавливает Cert-manager, подключаясь к Kubernetes Events API.
Обновлением сертификатов Cert-manager управляет сам, выставляя себе метки, когда требуется их обновлять (за сколько дней до окончания сертификата можно выставлять в параметрах запуска Cert-manager).

Полезные ссылки:

- cert-manager official docs
- JetStack/Cert-Manager (github)

Задание:

1. Установите Nginx Ingress Controller в вашем кластере (команды и вывод сохраните).
2. Запустите RabbitMQ из задания по StatefulSet (команды и вывод сохраните).
3. Из задания про OAuth2 примените все манифесты с учетом нового кластера (команды и вывод сохраните).
4. Установите Cert-Manager в вашем кластере (команды и вывод сохраните).
5. Создайте манифест для ClusterIssuer letsencrypt для получения сертификатов от Let's Encrypt production server.
6. Исправьте манифест Ingress для автоматического получения сертификата.
7. Примените манифесты из последних двух пунктов (команды и вывод сохраните).
8. Проверьте, что сертификат выдан и установился для вашего домена.
9. Выведите описание CRD Certificate через kubectl describe (команду и вывод сохраните).
10. На проверку отправьте все манифесты, ссылку на Ingress и сохраненные команды и выводы.