



Apasoft Training

www.apasoft-training.com

Secrets

KUBERNETES AL COMPLETO

Secrets

- ❑ Un secret permite guardar información confidencial dentro de kubernetes. Por ejemplo contraseñas, tokens de autorización , claves SSH , etcétera
- ❑ Normalmente nos sirven como método de autenticación para acceder a distintos recursos protegidos dentro de kubernetes , desde los componentes internos hasta nuestras propias aplicaciones
- ❑ Disponemos de distintos tipos de Secrets orientados a distintos recursos dentro de la infraestructura.
- ❑ La forma más directa de utilizar estos Secrets dentro de kubernetes es asociándolos a un POD

Secrets

❑ Tipos de Secrets

- ❑ **Opaque:** Tipo por defecto que contiene cualquier información que queramos incluir y proteger.
- ❑ **Service account token:** Almacena un token que identifica un Service Account. Veremos posteriormente este recurso cuando hablemos del tema de seguridad Pero básicamente representan una identidad para los procesos que se ejecutan dentro de un POD.
- ❑ **Docker config:** Almacena las credenciales necesarias para poder acceder a un registro privado de Docker.
- ❑ **Basic authentication:** Credenciales que se utilizan para la autenticación básica contiene realmente dos propiedades obligatorias: username y password



Secrets

□ Tipos de Secrets

- **SSH:** Almacenan las credenciales para poder autenticarnos a través de SSH. vamos a necesitar una propiedad denominada ``ssh-privatekey`` que en realidad es un par de clave valor.
- **TLS:** almacenan un certificado y su clave asociada que se utilizan habitualmente para TLS. su caso más habitual es usarlo con un recurso de tipo ingres, es decir para acceder desde el exterior del clúster. en este caso deberemos de tener estos dos valores : ``tls.key`` y ``tls.crt``
- **Bootstrap:** Estos tokens son bastante especiales y se utiliza para el proceso bootstrap del nodo.