

TP Kubernetes

Objectifs

Étapes

1. Découpage de namespace

- Proposez-moi un découpage en namespace => Doc en Markdown qui explique vos namespaces et ce qu'ils contiennent.
- Créez les namespaces
- Attention, vos namespaces doivent posséder des Quotas !!!

2. KubeDB

- Mettre en place kubeDB qui permettra l'ajout facile de base de données.
- Comprendre le principe de CRD (se renseigner)

3. Wordpress

- Mettre en place un wordpress répliqué (ou tout autre service Web qui utilise une base de donnée)
- Des ConfigMap et/ou Secret doivent être utilisés
- Ce service doit être redondant
- Des backups de base de données doivent être mise en place
- Bonus: Les images doivent être stocké sur un volume commun ou sur un object storage

4. RBAC

- Trois rôles principaux (et au moins autant de ServiceAccount, ou de User(si 6. OIDC est fait avant)) :
 - administrateur de cluster
 - sysops chez vous
 - dev chez vous
 - client qui vous a commandé le wordpress, il ne doit pas pouvoir faire de modification, mais doit pouvoir accéder à la base de donnée depuis un port-forward (en bonus si lecture uniquement dans la bdd)
- Mettez en place une politique de sécurité avec RBAC
 - Rédigez un doc markdown pour l'expliquer
- Mettez en place cette politique
 - Vous devez utiliser un label "criticality: danger" sur les ressources qui ne doivent pas être modifiées par l tout venant

5. Monitoring

- Mettre en place une solution de monitoring
 - accessible depuis un grafana
 - qui envoie des alertes en cas de problème
- Prometheus, node-exporters, ...

6. OIDC

- à l'exception de l'administrateur général
- Mettez en place une authentification pour l'accès à votre cluster, au travers d'un service tel que Google Accounts
 - Remplacez les ServiceAccount par des users
 - Modifiez grafana pour accepter uniquement une Google Auth

7. Registry + GUI Web

- Mettre en place un docker registry
 - Stockez les images sur un Object Storage
- Mettre en place une interface Web qui permet de le configurer et de le sécuriser avec une gestion d'utilisateurs
 - Authentification Google Auth serait un plus

Tips

- Si vous bloquez ne passez pas trop de temps à deux sur le même programme.
- HELM est autorisé !