AKS / GATEWAY / KEYVAULT

TP :

Etape 1 :

Création du cluster AKS

Spec :

- 2 Nodes en Manual, 1 node virtuel
- Redondance 3 zones
- Network : Azure CNI
- Policy : Calico
- Cluster en privé
- Activer le CSI Driver

Etape 2 :

Activer l'ingress contrôler d'AKS (peut mettre du temps à se déployer)

Etape 3 :

Crée une VM linux (Ubuntu 20) dans le même subnet que le cluster :

- Installer Docker
- Installer AZ CLI

Etape 3 :

Mise en place de l'identité system sur le VMSS

Etape 4 :

Création du key vault

Spec :

- Utilisé « azure rôle based access control » pour le contrôle des accès
- Donner des accès restreints sur les VNET

Etape 5 :

Mise en place du secret dans le key vault

Etape 6 :

Accordé le rôle IAM a l'identité VMSS

- Nom du rôle « Key Vault Secrets User »

Ajouté « CAHU Moise » en tant que « Key Vault Administrator »

Etape 7 :

Modification du manifest pour prendre en charge les noms de vos ressources

Déploiement du manifest keyvault.yaml

Vérification de l’état du cluster

Etape 8 :

Modification du manifest pour prendre en charge les noms de vos ressources

Déploiement du manifest deployment-nginx.yaml

Vérification de l’état des pods lancés