

Sujet TP 5 - Mettre en place une solution de centralisation et de gestion des logs avec la suite Elastic

pour plusieurs applications dans des conteneurs

Table des matières

Présentation du Contexte.....	2
Organisation.....	2
Description détaillé des éléments attendus.....	3
Fichiers kubernetes.....	3
Configuration et creation des pipelines.....	3
Environnement d'exécution.....	3
Documentation.....	3
Rendu.....	3

Présentation du Contexte

Vous intervenez en temps que DevOps dans une équipe de prod qui doit mettre en place une solution de centralisation et de gestion des logs pour le cluster Kubernetes et les applications qu'il contient.

Vous allez donc devoir :

- Installer elasticsearch dans le cluster Kubernetes
- Mettre en place logstash et filebeats (selon ce que vous jugez nécessaire) pour récupérer les logs de la machine sur laquelle tourne le cluster Kubernetes
- Récupérer et stocker les logs des applications (pour cela vous ferez le test avec une application Nginx qui devra être déployer sur le cluster K8s). Les logs de chaque applications devront être stocker dans leur propre index, il est donc nécessaire de définir pour chaque application un pipeline logstash, et de fournir un modèle et une documentation sur comment l'utiliser pour ajouter de nouvelles applications dans le cluster.
- Récupérer et stocker les logs des conteneurs de chaque applications
- Définir une stratégie pour le stockage et la rotation des logs (il n'y a pas de contrainte réglementaire vous imposant de garder les logs X mois / années, à vous de définir les critères opérationnels qui vous permettront de savoir s'il faut garder les logs des derniers jours / semaines / mois)
- Définir les requêtes elasticsearch qui permettent
 - de connaître la liste des index disponibles
 - d'afficher les logs pour les 24 dernières heures
 - de filtrer les logs pour ne voir que ceux d'un conteneur spécifique pour une application donnée
 - de supprimer les logs plus vieux que X (X à définir en fonction de votre stratégie)

Organisation

Cet exercice se fait individuellement et sera à rendre sous la forme d'un dépôt Git public (sur github ou gitlab comme vous préférez) directement dans Teams

Le rendu sera à faire au plus tard le lundi 31/10/2023 à 23h59

Cet exercice permettra de valider vos compétences pour votre dossier d'évaluation de compétences individuelle dans le cadre de votre titre RNCP Administrateur Devops. Il concerne la validation de l'activité type 3 Superviser les services déployés

Description détaillé des éléments attendus

Fichiers kubernetes

Des fichiers Kubernetes devront être fournis pour les éléments suivants :

- déploiement et service pour elasticsearch, logstash et filebeats
- déploiement d'un nginx de démo et de son service
- tout autre déploiement utile à votre solution

Configuration et creation des pipelines

Fournir tous les fichiers de configuration, les pipelines, et les modèles nécessaire à la mise en place de la centralisation des logs

Environnement d'exécution

On considère que le cluster Kubernetes est déjà déployé pour la production et prêt à recevoir de nouveaux déploiement

Documentation

Rédiger une documentation **en anglais** qui contiendra :

- Description des fichiers fournis
- Description des pré-requis
- Schéma de présentation de l'infrastructure mise en place
- Comment déployer la solution de centralisation des logs
- Comment déployer l'application Nginx
- Comment ajouter de nouvelles applications à la centralisation des logs
- Présentation et justification de la stratégie de stockage et de rotation des logs.

Rendu

Le rendu se fait sous la forme d'un dépôt git sur Teams contenant:

- les fichiers pour le déploiement sur un cluster Kubernetes
- les fichiers de configuration et de pipeline
- une documentation sous la forme de votre choix
- Vous pouvez ajouter autant de scripts / fichiers / documents que vous jugerez nécessaire pour réaliser cet exercice