

## **SLA – Amélioration de la Résilience - MPL\_10**



## Points d'amélioration de la résilience identifiés:

### **Ajout de notifications par mail ou téléphone :**

Pour améliorer notre capacité de réponse aux incidents, il est recommandé d'ajouter des notifications par mail ou téléphone. Cela nous permettra d'être informés rapidement en cas de défaillance ou de situation critique, afin de pouvoir prendre des mesures immédiates pour rétablir les services.

intégrer un système de notifications par mail ou téléphone dans notre infrastructure peut être réalisé en utilisant des outils tels que Nagios, Zabbix ou des services de messagerie en ligne. Ces notifications nous permettront de réagir rapidement et efficacement en cas d'incidents, minimisant ainsi l'impact sur nos utilisateurs.

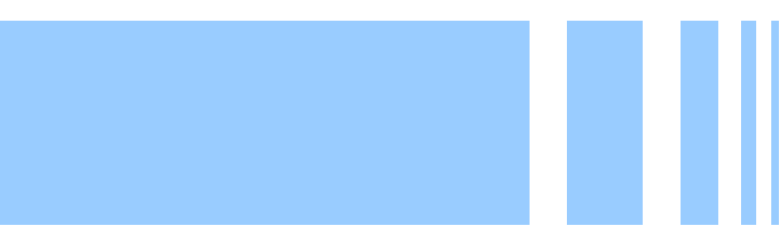
### **Automatisation avec Ansible :**

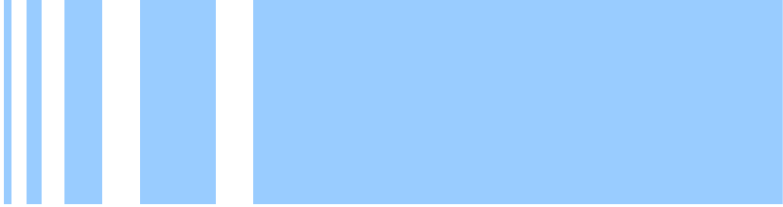
Pour simplifier et accélérer la gestion de notre infrastructure, il est recommandé d'utiliser Ansible pour l'automatisation des tâches. Ansible nous permettra de déployer et de configurer facilement nos serveurs, en garantissant une cohérence et une reproductibilité des configurations.

Implémenter Ansible dans notre infrastructure nous permettrait d'utiliser Ansible pour automatiser les tâches de déploiement, de configuration et de gestion des services. Cela nous permettra de gagner du temps et de réduire les erreurs humaines, améliorant ainsi la résilience et la stabilité de notre infrastructure.

### **Containerisation avec Kubernetes :**

Pour améliorer la flexibilité, l'évolutivité et la résilience de notre infrastructure, il est recommandé d'adopter la containerisation avec Kubernetes. Kubernetes est une plateforme d'orchestration de conteneurs qui facilite la gestion des applications et des services distribués.





Implémenter Kubernetes dans notre infrastructure nous permettrait de déployer et gérer nos applications sous forme de conteneurs, ce qui permet une isolation des ressources et une gestion plus efficace des charges de travail. Kubernetes offre également des mécanismes de haute disponibilité, de mise à l'échelle automatique et de reprise sur incident, renforçant ainsi la résilience de notre infrastructure.

### **Mise en place de Fail2ban :**

Fail2ban est un outil de prévention d'intrusion qui peut surveiller nos journaux de serveur et protéger contre les attaques de force brute et les tentatives d'intrusion répétées. En détectant les adresses IP malveillantes, il bloque automatiquement leur accès à notre système pour une période définie.

Implémenter Fail2ban sur nos serveurs d'application et serveurs de base de données permettrait de renforcer la sécurité et de protéger nos services contre les attaques par force brute ou par injection de code malveillant. Cela nous aidera à réduire les risques d'indisponibilité et à garantir la continuité de nos services.

### **Mise en place de la haute disponibilité (HA):**

La haute disponibilité est une stratégie qui vise à assurer la continuité de nos services en cas de défaillance matérielle ou logicielle d'un composant de notre infrastructure. Cela implique la mise en place de redondance et de mécanismes de basculement automatique pour maintenir un fonctionnement ininterrompu du service.

Mettre en place une architecture haute disponibilité pour nos composants critiques tels que les serveurs d'application et les serveurs de base de données peut être réalisé en configurant des clusters, des systèmes de réplication, des mécanismes de basculement automatique, ou en utilisant des solutions de conteneurisation et d'orchestration telles que Kubernetes. Cette approche nous permettra d'assurer une disponibilité continue et de minimiser les interruptions de service en cas de défaillance d'un nœud ou d'une instance.

