Mise en place d'une infrastructure e-commerce hautement disponible avec une DMZ

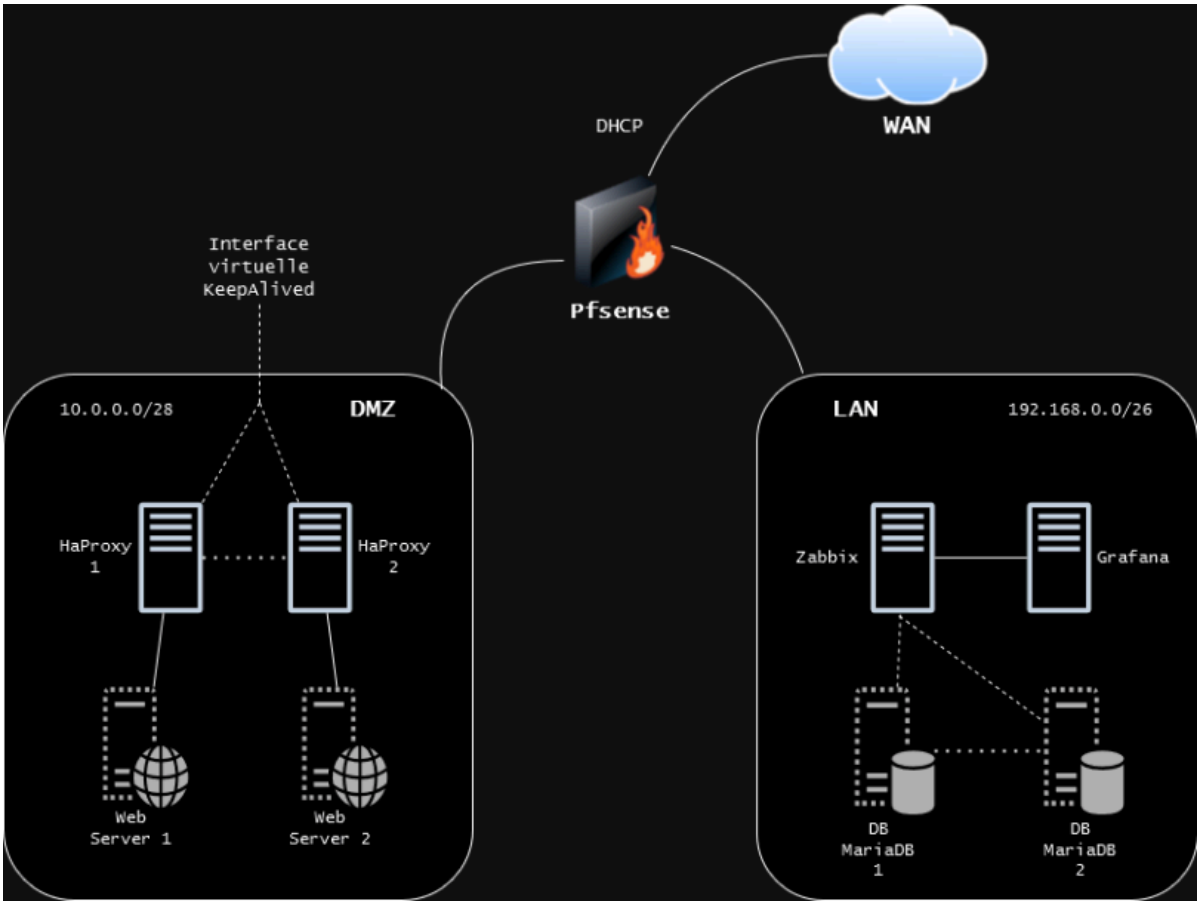
Objectif du Projet

Le projet vise à mettre en place une infrastructure hautement disponible pour le site e-commerce de **EcoFab Innovations**, une entreprise spécialisée dans la fabrication et la vente de meubles écologiques et durables. EcoFab se distingue par son engagement envers l'environnement, utilisant des matériaux recyclés et écologiques pour créer des meubles de qualité. L'entreprise gère à la fois des magasins physiques en France et une boutique en ligne où les clients peuvent acheter ses produits.

L'objectif de ce projet est de moderniser et renforcer l'infrastructure IT de la boutique en ligne, notamment pour atteindre un public plus large et répondre à une demande croissante.

Pour ce faire, une **DMZ** sera mise en place avec deux **HAProxy** en haute disponibilité, qui redirigeront le trafic vers deux serveurs web hébergeant le site e-commerce basé sur **WordPress**. Derrière cette architecture frontale, un **cluster Galera** de bases de données **MariaDB** dans le LAN assurera la haute disponibilité et la réplication des données de manière synchrone, garantissant une continuité de service et une sécurité accrue. Le tout sera protégé par un pare-feu **pfSense** configuré pour isoler les différentes zones du réseau et surveillé par des outils comme **Zabbix** et **Grafana** pour suivre les performances en temps réel.

Ce projet permet à EcoFab de soutenir sa croissance en ligne conformément à son engagement en faveur de pratiques durables et innovantes.



Eléments techniques

Le **pare-feu pfSense** gère la segmentation du réseau et la sécurité en assurant la configuration des interfaces WAN, DMZ et LAN. PfSense filtre le trafic pour n'autoriser que les connexions légitimes. Il gère également le **NAT** (Network Address Translation) pour rediriger le trafic web entrant vers les serveurs **HAProxy** dans la **DMZ**.

Les **serveurs HAProxy** sont également protégés et situés dans la DMZ. Ces serveurs exécutent la répartition de la charge, redirigeant les requêtes HTTP/HTTPS des utilisateurs vers les serveurs **WordPress**. **Keepalived** est utilisé exclusivement pour les serveurs HAProxy afin de maintenir la haute disponibilité : en cas de panne de l'un des serveurs HAProxy, l'autre prend le relais grâce à l'adresse IP virtuelle gérée par Keepalived, assurant une continuité de service. Ainsi, le site WordPress est toujours accessible, même lors d'une défaillance matérielle.

Le **site e-commerce** est basé sur **WordPress**, hébergé sur des serveurs web derrière HAProxy dans la DMZ. WordPress permet la gestion des produits, des commandes, et des interactions utilisateurs, avec une intégration possible de WooCommerce pour transformer la plateforme en une boutique en ligne complète. Le contenu dynamique et les données des utilisateurs sont stockés dans un **cluster MariaDB Galera** situé dans le **LAN**. Ce cluster permet la réplication synchrone des données, chaque modification est immédiatement répliquée sur plusieurs serveurs de base de données pour éviter toute perte de données. Cette architecture rend le système tolérant aux pannes, car les serveurs web peuvent toujours accéder à une copie fonctionnelle des bases de données en cas de défaillance d'un nœud.

Pour une surveillance efficace de toute l'infrastructure, **Zabbix** est déployé pour surveiller les performances des serveurs HAProxy, WordPress, et du cluster MariaDB. Zabbix détecte les anomalies pour une intervention rapide avant que cela n'affecte les utilisateurs. **Grafana** est utilisé en complément pour fournir des tableaux de bord graphiques. Grafana permet une vue en temps réel des performances des composants critiques du système. On pourra suivre facilement les tendances de la charge, optimiser les performances, et faire en sorte que l'infrastructure supporte efficacement les pics de trafics.

1. Configuration du Pare-feu (pfSense)

Le pare-feu **pfSense** est le principal élément de sécurisation de l'infrastructure. Il filtre le trafic réseau et gére les différentes zones de sécurité (WAN, LAN, DMZ).

A. Configuration des interfaces réseau

pfSense nécessitera trois interfaces principales pour segmenter les réseaux :

- **WAN** : interface pour la connexion à Internet (ip publique de l'infrastructure, privé de notre LAN local pendant la simulation)
- **LAN** : interface pour la connexion des serveurs internes (base de données, etc.).
- **DMZ** : Interface dédiée à la zone démilitarisée (DMZ), qui hébergera les serveurs HAProxy et les serveurs web.

B. Mise en place de règles de filtrage

Source	Destination	Interface	Protocole	Port(s)	Action
Internet	HAProxy (DMZ)	WAN -> DMZ	TCP	80, 443	Autoriser (HTTP/HTTPS)
HAProxy (DMZ)	WebServers	DMZ	TCP	80, 443	Autoriser (HTTP/HTTPS)
WebServers	GaleraDB (LAN)	DMZ -> LAN	TCP	3306	Autoriser (SQL)
Zabbix (LAN)	HAProxy (DMZ)	LAN -> DMZ	UDP	161	Autoriser (SNMP)
Zabbix (LAN)	WebServers	LAN -> DMZ	UDP	161	Autoriser (SNMP)
Zabbix (LAN)	GaleraDB (LAN)	LAN	UDP	161	Autoriser (SNMP)
PfSense (WAN)	HAProxy (DMZ)	WAN -> DMZ	TCP	80, 443	NAT vers HAProxy VIP
PfSense	WebServers	DMZ	N/A	N/A	Redirection trafic

- Règles WAN vers DMZ

Sur l'interface WAN, vous devrez autoriser le trafic entrant vers la DMZ pour les services web. Configurez des règles pour permettre les connexions HTTP (port 80) et HTTPS (port 443) vers l'adresse IP virtuelle (VIP) des HAProxy en haute disponibilité. Bloquez tout autre trafic entrant pour renforcer la sécurité.

- Règles DMZ vers WAN

Pour la DMZ, autorisez le trafic sortant vers le WAN pour les mises à jour et les téléchargements nécessaires. Limitez ces connexions aux ports essentiels (par exemple, HTTP, HTTPS, et éventuellement FTP si nécessaire). Configurez ces règles pour les serveurs web et les HAProxy.

- Règles DMZ vers LAN

Créez des règles permettant aux serveurs web de la DMZ de communiquer avec le cluster Galera dans le LAN. Autorisez uniquement le trafic sur le port MySQL/MariaDB (généralement 3306) et restreignez-le aux adresses IP spécifiques des serveurs web vers les IP du cluster de bases de données.

- Règles LAN vers DMZ

Permettez au Zabbix situé dans le LAN d'accéder aux serveurs web et aux HAProxy dans la DMZ pour la supervision. Autorisez le trafic sur les ports nécessaires à Zabbix entre l'IP du serveur Zabbix et les IP des éléments supervisés dans la DMZ.

- Règles LAN vers WAN

Pour le réseau LAN, autorisez le trafic sortant vers le WAN pour permettre aux utilisateurs internes et aux serveurs d'accéder à Internet. Vous pouvez mettre en place des règles plus restrictives basées sur les besoins spécifiques de l'organisation.

- Règles de NAT

Configurez les règles de NAT (Network Address Translation) pour rediriger le trafic entrant sur les ports 80 et 443 de l'adresse IP publique vers l'adresse IP virtuelle des HAProxy dans la DMZ. Les clients externes doivent accéder à votre site e-commerce.

Explications pour Galera

Dans cette infrastructure, le **cluster Galera**, qui contient les bases de données MariaDB, est hébergé dans le **réseau LAN** plutôt que dans la DMZ. Les bases de données stockent des informations sensibles qui doivent être protégées des accès non autorisés. En plaçant le cluster dans le LAN, il bénéficie de la protection supplémentaire offerte par le pare-feu **pfSense**, empêchant tout accès direct depuis l'extérieur.

Les serveurs web situés dans la DMZ doivent être configurés pour communiquer avec le cluster Galera situé dans le LAN. Cela nécessite la configuration de flux spécifiques sur **pfSense** pour autoriser uniquement le trafic nécessaire entre la DMZ et le LAN. En particulier, des règles de filtrage doivent être définies pour permettre les requêtes SQL venant des serveurs web vers le cluster Galera tout en bloquant tout autre type de trafic. Le cluster sera accessible uniquement par les services internes autorisés (comme les serveurs web), tout en étant isolé des menaces externes.

2. Configuration des serveurs web

C'est un WordPress qui fera office de site e-commerce pour notre entreprise.

- Installer Nginx sur les deux serveurs web
- Installer PHP et les extensions nécessaires (PHP-FPM, PHP-MySQL, etc.)
- Installer les autres dépendances requises par WordPress (comme php-gd, php-xml, etc.)
- Créer un fichier de configuration Nginx spécifique pour WordPress
- Télécharger la dernière version stable de WordPress
- Extraire les fichiers dans le répertoire web approprié
- Créer le fichier wp-config.php avec les paramètres de base de données pour que la connexion à distance s'effectue correctement.

Attention : pour synchroniser les deux serveurs web hébergeant WordPress, vous devez faite en sorte que les fichiers statiques (comme les images, les thèmes, et les plugins) ainsi que la configuration de WordPress sont identiques sur les deux serveurs. Une solution rapide est d'utiliser rsync.

3. Mise en place du Cluster Galera pour MariaDB

Pour configurer un cluster Galera, il est d'abord nécessaire d'installer MariaDB et Galera sur chaque serveur qui constituera le cluster.

Ensuite, vous devez configurer les fichiers de MariaDB pour activer la réplication Galera en spécifiant les adresses IP des différents nœuds du cluster et en définissant le mode de synchronisation. Les configurations des nœuds doivent être cohérentes.

Après avoir configuré chaque serveur, vous initialisez le premier nœud du cluster en démarrant MariaDB avec une configuration spécifique. Une fois le premier nœud en place, les autres nœuds peuvent être ajoutés en démarrant MariaDB normalement sur chacun d'eux, et ils rejoindront automatiquement le cluster. Une fois tous les nœuds connectés, ils partageront et répliqueront les données en temps réel.

4. Utilisation de Keepalived

Keepalived est utilisé dans cette infrastructure pour la haute disponibilité des serveurs **HAProxy**. Dans ce projet, deux instances de HAProxy sont déployées dans la **DMZ** pour répartir le trafic entre les serveurs web hébergeant le site e-commerce. Keepalived assure qu'en cas de défaillance d'une des instances de HAProxy, l'autre prend immédiatement le relais sans interruption du service, grâce à l'utilisation d'une **adresse IP virtuelle (VIP)**. Cette VIP est partagée entre les deux serveurs HAProxy, et Keepalived surveille en continu la santé de chaque instance. Si une instance devient indisponible, la VIP bascule automatiquement sur l'autre instance encore fonctionnelle, garantissant ainsi une **répartition de charge continue** et une **haute disponibilité** pour le site e-commerce.

5. Sécurité et surveillance

Utilisez **Nginx avec un module WAF**, **ModSecurity**, pour protéger votre site WordPress contre les attaques web courantes.

Installez **Zabbix** pour surveiller les performances de vos serveurs **Nginx**, de votre infrastructure WordPress, et du **cluster Galera**. Zabbix peut suivre les métriques telles que la charge CPU, l'utilisation de la mémoire, le temps de réponse HTTP des serveurs Nginx, l'utilisation des disques, et les connexions SQL à la base de données.

Intégrez **Grafana** avec Zabbix pour visualiser les métriques de performance sous forme de tableaux de bord interactifs. Grafana vous permet de suivre en temps réel les performances des serveurs web, les requêtes SQL sur le cluster Galera, ainsi que les tendances de trafic.

Zabbix, Grafana et le cluster de BDD sont dans le LAN.

Votre mission est de maquetter et configurer correctement l'infrastructure. Vous devez produire toute documentation utile ainsi qu'effectuer un test de charge pour montrer la résilience de celle-ci.

6. Livrables attendus

Architecture détaillée de l'infrastructure :

- Schéma de l'architecture réseau avec les différentes zones (WAN, DMZ, LAN) et les composants de l'infrastructure (HAProxy, serveurs web, cluster Galera, pfSense).

Configuration des serveurs HAProxy :

- Fichiers de configuration de HAProxy.
- Mise en place de Keepalived pour la haute disponibilité.

Configuration des serveurs web (WordPress) :

- Détails de l'installation et de la configuration de WordPress sur les serveurs.

- Synchronisation des fichiers et configuration du serveur Nginx.

Configuration du cluster Galera (MariaDB) :

- Fichiers de configuration MariaDB pour la réplication synchrone.
- Documentation sur la mise en place du cluster et des procédures de synchronisation des bases de données.

Configuration du pare-feu pfSense :

- Règles de filtrage et de sécurité configurées pour chaque zone (WAN, DMZ, LAN).
- NAT et redirection du trafic vers HAProxy.

Surveillance et monitoring :

- Documentation de la configuration de Zabbix pour la surveillance des serveurs (HAProxy, WordPress, Galera).
- Tableaux de bord Grafana pour le suivi des performances.

Tests de haute disponibilité :

- Rapport de test de basculement automatique avec Keepalived pour HAProxy.
- Tests de performance et de montée en charge.

Vous devrez utiliser youtrack de JetBrains pour organiser les taches du projet. Votre premier travail sera de réaliser les WBS et PBS du projet de façon à déterminer l'ensemble des tâches à effectuer sur le projet et de définir qui les réalisera.

Groupe	**Élève**
Groupe 1	BOUDET Anthony
	PARMA Charles
	LEFEBVRE Jacky
	ESCAFFRE Benjamin
Groupe 2	RAGOT Naim
	MENIER Clément
	DAILLE Clément
	GRIMA Hugo
Groupe 3	D'AGUANNO Morgane
	DAUBA-MAROT Mathias
	KLEIN Joffrey
	ORTOLI Louis
Groupe 4	MOURET Adéodat
	DE TREE Ryan

Groupe	Élève
	AZAFAD Ilyesse
	BARRAUD Arthur