**Documentation de déploiement du site Clean House Robotics en architecture 3-tiers**

**1. Introduction**

Ce document détaille le processus de déploiement de l'architecture 3-tiers pour le site web de Clean House Robotics. L'infrastructure comprend trois services principaux :

* Serveur Web (Apache et PHP)
* Serveur de base de données (MySQL)
* Serveur DNS (DNSMasq)

**2. Prérequis**

* Trois machines virtuelles sous RockyLinux.
* Accès root sur toutes les machines.
* Connexion Internet stable sur toutes les machines.

**3. Configuration du Serveur DNS avec DNSMasq**

**3.1 Installation**

sudo yum install dnsmasq

**3.2 Configuration**

Editez le fichier de configuration :

sudo nano /etc/dnsmasq.conf

Ajoutez la ligne suivante pour rediriger toutes les requêtes pour `cleanhouse.rob` vers votre serveur web :

address=/www.cleanhouse.rob/IP\_DU\_SERVEUR\_WEB

**3.3 Démarrage du service**

sudo systemctl enable dnsmasq sudo systemctl start dnsmasq

**4. Configuration du Serveur Web (Apache & PHP)**

**4.1 Installation**

sudo yum install httpd php

**4.2 Configuration**

Editez le fichier de configuration Apache :

sudo nano /etc/httpd/conf/httpd.conf

Ajoutez les lignes suivantes pour configurer le serveur :

ServerName www.cleanhouse.rob

**5. Configuration du Serveur MySQL**

**5.1 Installation**

sudo yum install mysql-server

**5.2 Configuration**

Démarrez MySQL :

sudo systemctl start mysqld

Exécutez le script de sécurisation :

sudo mysql\_secure\_installation

Créez une base de données et un utilisateur pour le site :

mysql -u root -p CREATE DATABASE cleanhouse\_db; CREATE USER 'webuser'@'IP\_DU\_SERVEUR\_WEB' IDENTIFIED BY 'password'; GRANT ALL PRIVILEGES ON cleanhouse\_db.\* TO 'webuser'@'IP\_DU\_SERVEUR\_WEB'; FLUSH PRIVILEGES;

**6. Sécurisation**

**6.1 Certificat SSL/TLS**

Générez un certificat auto-signé :

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/pki/tls/private/cleanhouse.key -out /etc/pki/tls/certs/cleanhouse.crt

Mettez à jour la configuration Apache pour utiliser SSL :

sudo nano /etc/httpd/conf.d/ssl.conf

**6.2 Fail2Ban**

Installez et configurez Fail2Ban pour surveiller et bloquer les tentatives de connexion échouées.

**6.3 Pare-feu**

Utilisez `firewalld` ou `iptables` pour sécuriser l'accès aux services.

**7. Conclusion**

Ce document fournit les étapes nécessaires pour déployer l'architecture 3-tiers pour Clean House Robotics. Assurez-vous de tester chaque étape et de valider que tout fonctionne comme prévu.