Compte rendue AvanzData

Sommaire :

1. Documentation
2. Installation clé SSH
3. Connexion et découverte du système d’exploitation Linux
4. Installation du module Apache Web Server
5. Configuration du module Apache
6. Configuration du réseau
7. HTTP à HTTPS
8. Interface Web
9. Documentation sur la gestion d’un serveur Web

**Configuration initiale :**

- Choisir un système d'exploitation approprié pour notre serveur web (Linux)

- Installer les logiciels nécessaires, ici c’est Apache

- Avoir une bonne connexion Internet et configurez les paramètres réseau de votre serveur.

**Sécurité :**

- Mettre à jour régulièrement votre système d'exploitation et les logiciels serveur pour bénéficier des derniers correctifs de sécurité.

- Configurer un pare-feu pour bloquer les accès indésirables et limiter l'exposition de votre serveur.

- Utiliser des certificats SSL/TLS pour chiffrer les communications et sécuriser les connexions.

- Mettre en place des mesures de sécurité supplémentaires, telles que la configuration de règles de sécurité applicative (WAF) ou de systèmes de détection d'intrusion (IDS).

**Gestion des ressources :**

- Surveiller l'utilisation des ressources de votre serveur, notamment le processeur, la mémoire et le stockage, pour éviter les problèmes de performances.

- Optimiser la configuration du serveur web pour maximiser son efficacité, par exemple en utilisant des caches pour réduire la charge sur le serveur.

- Mettre en œuvre une stratégie de sauvegarde régulière pour protéger vos données contre la perte ou la corruption.

**Gestion des sites web :**

- Configurer les noms de domaine et les enregistrements DNS pour diriger le trafic vers notre serveur.

- Créer des hôtes virtuels (virtual hosts) pour héberger plusieurs sites web sur un même serveur.

- Assurer que les fichiers des sites web sont organisés correctement et que les autorisations d'accès sont correctement configurées.

- Surveiller les journaux d'accès et d'erreur pour identifier les problèmes éventuels et les activités suspectes.

**Évolutivité et performances :**

- Si le site connaît une augmentation du trafic, envisager d'utiliser des techniques de mise en cache, de distribution de contenu (CDN) ou de mise à l'échelle horizontale pour gérer la charge.

- Optimiser les performances en utilisant des outils d'optimisation d'image, en activant la compression GZIP, en minimisant les fichiers CSS et JavaScript, etc.

**Surveillance et maintenance :**

- Mettre en place des outils de surveillance pour superviser les performances, la disponibilité et la sécurité de votre serveur web.

- Appliquer les correctifs de sécurité et les mises à jour logicielles dès leur disponibilité.

- Garder une sauvegarde régulière de vos données et effectuez des tests de restauration pour vous assurer de leur intégrité.

III. Connexion à la VM

**Etape 1** : Vérifier si la vm est en cours d’exécution et accessible depuis mon réseau

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

Etape 2 : Installer client SSH sur Windows → Git Bash

Information de connexion sur le serveur

|  |  |
| --- | --- |
| Adresse ip de la VM | 82.64.48.247 |
| Clé privée | id\_rsa |
| Port | 2022 |
| Pwd | Ouser123+ |

Connexion en tant qu’admin (pour avoir les accès) :

$ sudo su –

root@worker01:~# id

uid=0(root) gid=0(root) groups=0(root)

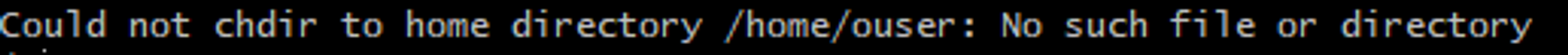
**Problèmes :**

Pas le meme nom de clé SSH

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Pas accès au répertoire /Ouser -> passer en admin



IV. Apache Web Server

**Etape 1** : Désinstallation et vérification des fichiers Apache pour ensuite le réinstaller

Une image contenant texte, capture d’écran

Description générée automatiquement

**Etape 2** : Mise à jour des informations des packages

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**Etape 3** : Vérification des modules disponibles

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

La commande **sudo apt install --assume-yes libapache2-mod-security2** a été exécutée avec succès. Les packages **liblua5.1-0**, **libyajl2**, **libapache2-mod-security2** et **modsecurity-crs** ont été installés.

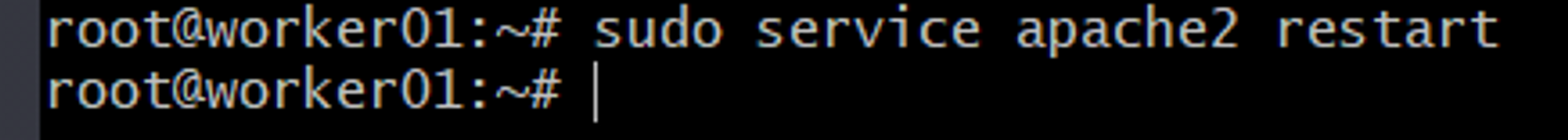
L'installation de **libapache2-mod-security2** ajoute le module **security2** à Apache. Des étapes de configuration supplémentaires peuvent être nécessaires pour activer et configurer correctement le module.

Activer le module

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

Redémarrer Apache pour prendre en compte les modifications



V. Configuration du module

* Accès au répertoire contenant les fichiers de configuration du module **libapache2-mod-security2**. Ubuntu, le répertoire est **/etc/apache2/mods-enabled/**.

cd /etc/apache2/mods-enabled/

* Créer un nouveau fichier de config pour le module **libapache2-mod-security2**.

sudo nano custom-modsecurity.conf

* À l'intérieur du fichier, on ajoute des directives de configuration spécifiques.

Par exemple, -> activer/désactiver certaines règles en utilisant les directives **SecRuleRemoveById** ou **SecRule** avec l'option **id**. On peut également ajouter nos propres règles personnalisées.

Une image contenant texte, logiciel, Logiciel multimédia, Police

Description générée automatiquement

Ici, la règle avec l'ID 123456 est désactivée à l'aide de la directive **SecRuleRemoveById**. De plus, une nouvelle règle est ajoutée pour vérifier si le paramètre **password** contient la valeur **"mypassword"**. Si c'est le cas, la requête est refusée.

Etapes Optionnel :

Pour tester soigneusement votre application et surveiller les journaux d'Apache, vous pouvez suivre les étapes suivantes :

1. Test de l'application : Accédez à votre application Web et effectuez différentes actions pour vous assurer que tout fonctionne correctement. Cela peut inclure la navigation sur le site, la soumission de formulaires, l'accès aux fonctionnalités principales, etc. Vérifiez que toutes les fonctionnalités de votre application sont accessibles et fonctionnent comme prévu.
2. Génération d'activités suspectes : Pour tester la réaction du module de sécurité aux activités suspectes, vous pouvez essayer de générer des attaques connues ou des activités malveillantes sur votre application. Cela peut inclure des tentatives d'injection SQL, des tentatives de cross-site scripting (XSS), des explorations de répertoire, etc. Observez comment le module de sécurité réagit à ces activités et si elles sont correctement bloquées ou signalées.
3. Surveillance des journaux d'Apache : Les journaux d'Apache contiennent des informations précieuses sur les activités du serveur Web, y compris les activités bloquées ou détectées par le module de sécurité. Vous pouvez consulter les journaux pour détecter toute activité suspecte ou tout problème lié à la configuration du module de sécurité. Les fichiers de journaux d'Apache se trouvent généralement dans le répertoire **/var/log/apache2/**.
   * Accédez au répertoire des journaux d'Apache : **cd /var/log/apache2/**
   * Visualisez le contenu du fichier de journal : **sudo cat nom-du-fichier.log** (remplacez "nom-du-fichier.log" par le nom réel du fichier de journal)
   * Utilisez des outils de recherche ou des commandes de filtrage pour extraire les informations pertinentes, par exemple :
     + Filtrer les entrées liées à ModSecurity : **sudo cat nom-du-fichier.log | grep ModSecurity**
     + Afficher les activités bloquées : **sudo cat nom-du-fichier.log | grep "ModSecurity: Access denied"**
     + Vérifier les erreurs ou avertissements liés à ModSecurity : **sudo cat nom-du-fichier.log | grep "ModSecurity: Warning"**

En surveillant les journaux d'Apache, vous pourrez détecter toute activité suspecte, analyser les problèmes de configuration, identifier les erreurs et les avertissements, et prendre les mesures appropriées pour renforcer la sécurité de votre application.

Assurez-vous de mettre en place une surveillance régulière des journaux d'Apache et de suivre les meilleures pratiques en matière de sécurité pour maintenir votre application Web sécurisée.

**Commandes Linux Pour l’authentification :**

cd ~/.ssh

ssh -i id\_rsa -p 2022 [ouser@82.64.48.247](mailto:ouser@82.64.48.247)7

pwd

userid ouser ; passwd : Ouser123+

$ sudo su - root@worker01: ~# id uid=0(root) gid=0(root) groups=0(root)

root@worker01:/var/log# apt install telnet Reading package lists... Done Building dependency tree

Reading state information... Done telnet is already the newest version (0.17-41.2build1). Telnet set to manually installed.

VII. HTTP à HTTPS

Installer le certificat SSl (Let’s Encypt):

Une image contenant texte, capture d’écran

Description générée automatiquement

sudo apt install certbot sudo certbot certonly --webroot --webroot-path /var/www/html -d avanzdata.com

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Erreur lors d’entrée du nom de domaine dans la commande + adresse mail à confirmer avec l’admin

Tache à réaliser :

* + Configurer Apache pour utiliser HTTPS :

sudo a2enmod ssl

sudo a2ensite default-ssl

sudo systemctl restart apache2

Ces commandes activent le module SSL pour Apache et activent la configuration du site par défaut pour HTTPS. Le service Apache est redémarré pour prendre en compte les modifications.

* + Rediriger le trafic http vers HTTPS :

sudo nano /etc/apache2/sites-available/000-default.conf

* + Ajouter le code suivant avant la balise </VirtualHost> :

Redirect permanent / <https://avanzdata.com/>

* + Redémarrer Apache pour mettre à jour les modifs :

sudo systemctl restart apache2