Installation de Wazuh Server sur CentOS 8 | RHEL 8 | AlmaLinux 8

Cette procédure décrit l'installation sans assistance de Wazuh Server sur les systèmes d'exploitation CentOS 8, RHEL 8 et AlmaLinux 8. Cette méthode est la plus rapide et utilise un script d'installation automatisé.

Prérequis

- Assurez-vous d'avoir un accès root ou sudo sur votre machine.
- Une connexion internet stable est requise pour télécharger le script d'installation.

Procédure d'installation

1. **Téléchargement du script d'installation:**
   Ouvrez un terminal et connectez-vous en tant que root ou avec sudo.
   Bash
   ```
   cd ~/
   curl -so wazuh-installation.sh
   https://packages.wazuh.com/resources/4.2/open-distro/unattended-ins
   tallation/unattended-installation.sh
   ```

   Cette commande télécharge le script d'installation unattended-installation.sh depuis le dépôt officiel de Wazuh et l'enregistre dans votre répertoire personnel.

2. **Exécution du script d'installation:**
   Exécutez le script d'installation téléchargé avec la commande suivante :

   ```
   sudo bash ./wazuh-installation.sh
   ```

   Le processus d'installation automatisé commencera. Il affichera des messages d'information sur les différentes étapes de l'installation, telles que l'installation des utilitaires nécessaires, l'ajout du dépôt Wazuh, l'installation des composants Wazuh (manager, Elasticsearch, Filebeat, Kibana), la configuration d'Elasticsearch et la génération de certificats.

3. **Enregistrement des informations de connexion:**
   Une fois l'installation terminée, le script affichera les informations de connexion pour les différents services Wazuh, y compris :

- Wazuh manager
- Elasticsearch
- Kibana
- Filebeat
- Utilisateurs par défaut (admin, readall, etc.)

Important : Notez ces informations de connexion en lieu sûr, car vous en aurez besoin pour accéder à l'interface web de Wazuh et aux différents services.

4. **Accès à l'interface web de Wazuh:**
   Vous pouvez accéder à l'interface web de Kibana (pour la visualisation des logs) en utilisant l'URL suivante :
   `https://<adresse_ip_du_serveur>`

   Remplacez <adresse_ip_du_serveur> par l'adresse IP réelle de votre machine où Wazuh Server est installé.
   Utilisez les informations de connexion fournies par le script d'installation (utilisateur wazuh et son mot de passe) pour vous authentifier sur l'interface web.

5. **Configuration du pare-feu avec Firewalld**

   Pour garantir la communication entre les différents composants de Wazuh, il est nécessaire d'ouvrir les ports suivants sur votre pare-feu :

   - **1514/TCP**: Communication des agents
   - **1515/TCP**: Inscription via demande automatique d'agent
   - **55000/TCP**: Inscription via l'API du gestionnaire

   En utilisant Firewalld :

   1. Vérifier le statut du Firewalld

      ```
      sudo systemctl status firewalld
      ```

   2. Ouvrir les ports :

      ```
      sudo firewall-cmd --permanent --add-port=1514/tcp
      sudo firewall-cmd --permanent --add-port=1515/tcp
      sudo firewall-cmd --permanent --add-port=55000/tcp
      ```

   3. Recharger la configuration :

      ```
      sudo firewall-cmd --reload
      ```

4. Vérification :

```
sudo firewall-cmd --list-ports
```

- Assurez-vous que les ports 1514/tcp, 1515/tcp et 55000/tcp sont présents dans la liste.

Résumé

En suivant ces étapes, vous aurez installé et configuré Wazuh Server avec succès sur votre système CentOS 8, RHEL 8 ou AlmaLinux 8. Vous pouvez maintenant commencer à utiliser Wazuh pour la détection d'intrusion, la gestion des vulnérabilités et la conformité aux réglementations.

Remarque: N'oubliez pas de consulter la documentation officielle de Wazuh pour plus d'informations sur la configuration et l'utilisation de la plateforme : https://documentation.wazuh.com/current/index.html

Doc créer par Romain le 03/04/2024