Installation et configuration de la suite ELK

Ce tutoriel vous guide pour intégrer Elasticsearch, Kibana et Filebeat afin de créer votre propre outil de Gestion des Informations avec la stack Elastic sur Ubuntu 20.04. Les composants utilisés sont :

- Elasticsearch : pour stocker et rechercher les événements de sécurité.
- Kibana : pour visualiser et naviguer dans les journaux de sécurité.
- Filebeat : pour analyser les journaux de Suricata et les envoyer à Elasticsearch.

Prérequis

Avoir un autre serveur Ubuntu avec :

4 Go de RAM et 2 CPU.

Un utilisateur non-root avec sudo.

Les deux serveurs doivent pouvoir communiquer via des adresses IP privées.

Étape 1 — Installer Elasticsearch et Kibana

Tout d'abord, téléchargez et installez la clé publique de signature d'Elasticsearch, nécessaire pour vérifier l'intégrité des paquets.

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

Vous aurez peut-être besoin d'installer le package apt-transport-https si ce n'est pas déjà fait. Cela permet à APT d'utiliser HTTPS pour récupérer des fichiers.

sudo apt-get install apt-transport-https

Ajoutez le dépôt Elasticsearch à la liste des sources APT de votre système.

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

Après avoir ajouté le dépôt, mettez à jour l'index des paquets, puis installez Elasticsearch.

sudo apt-get update && sudo apt-get install elasticsearch

ATTENTION ! Si vous rencontrez une erreur de doublon de dépôt lors de la mise à jour (comme "Duplicate sources.list entry"), vérifiez qu'il n'y a pas de duplication dans les fichiers sources.

sudo nano /etc/apt/sources.list.d/elasticsearch-8.x.list

Supprimez toutes les lignes en double si nécessaire.

Une fois Elasticsearch installé, démarrez le service avec :

sudo systemctl start elasticsearch

Vous pouvez également activer le démarrage automatique avec :

sudo systemctl enable elasticsearch

Étape 2 — Configurer Elasticsearch

Modifier le fichier de configuration :

sudo nano /etc/elasticsearch/elasticsearch.yml

Ajoutez ces lignes :

network.bind_host: ["127.0.0.1", "votre_ip_privée"]

discovery.type: single-node

xpack.security.enabled: true

Remplacez **votre_ip_privée** par votre adresse IP.

Configurer le pare-feu sur l'interface :

sudo ufw allow in on [interface]

sudo ufw allow out on [interface]

Démarrer Elasticsearch :

sudo systemctl start elasticsearch.service

Générer des mots de passe pour les utilisateurs par défaut :

cd /usr/share/elasticsearch/bin

sudo ./elasticsearch-setup-passwords auto

Notez les mots de passe générés.

Étape 3 — Configurer Kibana

Générer des clés de chiffrement :

cd /usr/share/kibana/bin/

sudo ./kibana-encryption-keys generate -q

Notez les clés générées.

Modifier le fichier de configuration de Kibana :

sudo nano /etc/kibana/kibana.yml

Ajoutez les lignes suivantes :

xpack.encryptedSavedObjects.encryptionKey: votre_clé

xpack.reporting.encryptionKey: votre_clé

xpack.security.encryptionKey: votre_clé

server.host: "votre_ip_privée"

Remplacez **votre_clé** par les clés que vous avez générées et **votre_ip_privée** par votre adresse IP.

Configurer les identifiants de Kibana :

cd /usr/share/kibana/bin

sudo ./kibana-keystore add elasticsearch.username

sudo ./kibana-keystore add elasticsearch.password

Entrez **kibana_system** pour le nom d'utilisateur et le mot de passe que vous avez noté précédemment.

Démarrer Kibana :

sudo systemctl start kibana.service

Étape 4 — Installer Filebeat

Maintenant que vous avez configuré Elasticsearch et Kibana, passons à l'installation de Filebeat sur votre serveur.

Ajouter la clé GPG d'Elastic :

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

Ajouter la liste de sources d'Elastic :

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

Mettre à jour les paquets et installer Filebeat :

sudo apt update

sudo apt install filebeat

Configurer Filebeat :

Ouvrez le fichier de configuration de **Filebeat** :

sudo nano /etc/filebeat/filebeat.yml

Configurer Kibana : Trouvez la section **setup.kibana** (environ ligne 100) et modifiez-la pour y indiquer l'adresse IP privée de votre instance Kibana :

setup.kibana:

host: "votre_ip_privée:5601"

Configurer Elasticsearch : Trouvez la section **output.elasticsearch** (environ ligne 130) et modifiez-la pour y indiquer l'adresse IP de votre serveur Elasticsearch, ainsi que les identifiants :

output.elasticsearch:

hosts: ["votre_ip_privée:9200"]

username: "elastic"

password: "votre_mot_de_passe"

Remplacez **votre_ip_privée** et **votre_mot_de_passe** par les valeurs appropriées.

Enregistrez et fermez le fichier. (Avec nano, utilisez CTRL+X, puis Y et ENTER.)

Exécutez la commande suivante :

sudo filebeat setup

Une fois la commande terminée, vous devriez voir un message indiquant que les dashboards ont été chargés.

Démarrer Filebeat :

sudo systemctl start filebeat.service

Vous avez maintenant configuré Filebeat pour qu'il envoie des événements vers Elasticsearch.

Étape 5 — Naviguer dans les Dashboards SIEM de Kibana

Kibana est l'interface graphique de la pile Elastic. Vous l'utiliserez dans votre navigateur pour explorer les données des événements et alertes.

Connexion à Kibana avec SSH

Utilisez la commande suivante pour créer un tunnel SSH vers Kibana :

ssh -L 5601:votre_ip_privée:5601 utilisateur@adresse_publique -N

Remplacez **votre_ip_privée** par l'adresse IP privée de votre serveur Elasticsearch.

Remplacez **adresse_publique** par l'adresse IP publique de votre serveur.

Une fois le tunnel créé, ouvrez le navigateur et visitez :

http://127.0.0.1:5601

Connectez-vous avec le nom d'utilisateur elastic et le mot de passe que vous avez défini.

Après vous être connecté, vous pouvez rechercher les dashboards.

Dans ce tutoriel, on a installé et configuré Elasticsearch et Kibana, installé Filebeat et utilisé un tunnel SSH pour se connecter à Kibana. On peut désormais explorer les tableaux de bord de Kibana.