Restrictions à appliquer aux antivirus

Sommaire

Contexte

L'installation d'un antivirus sous Linux va à l'encontre des règles préconisées pour durcir et protéger un système (*voir page : https://messervices.cyber.gouv.fr/guides/recommandations-de-securite-relatives-un-systeme-gnulinux et une copie du rapport associé : fr_np_linux_configuration-v2.0.pdf*).

L'utilisation d'un antivirus sous Linux est **déconseillée**, mais **si malgré cela** vous utilisez un antivirus, cette page fournit **nos instructions concernant sa configuration** pour **ne pas avoir d'impact** sur **l'intégrité** ou **les performances** de **Shinken**.

- REMARQUE : Voici pourquoi il est déconseillé d'utiliser un antivirus sous Linux :
  - suivant la philosophie UNIX / Linux, chaque programme (*Shinken, Apache, MongoDB, ...*) dispose de son propre utilisateur non privilégié, réduisant ainsi :la portée d'une attaque contre l'un d'eux,
    - la possibilité d'une installation du logiciel malveillant au niveau du système.
  - Les distributions Linux gèrent déjà les alertes et mises à jour de sécurité (*CVE*).
  - Un antivirus requiert les droits de l'administrateur pour pouvoir fonctionner (*analyse de tous les fichiers et processus du système*).
    - Il devient alors lui-même une cible privilégiée pour les attaques contre le système,
    - Il augmente la surface d'attaque du fait du large panel d'éléments (*fichiers, processus*) auquel il va accéder (*scan*), **affaiblissant** la sécurité du système.
  - Un antivirus peut lui-même être vulnérable à des failles de sécurité, mettant le système en danger du fait de ses droits complets sur le système, et du délai qu'il peut y avoir sur ses propres mises à jour.
  - Un antivirus n'est efficace que sur des menaces déjà connues.
  - Les virus Windows ne sont pas opérationnels sous Linux.
- Enfin, la consommation de ressources engendrée par un antivirus n'est pas compensée par ce qu'il pourrait apporter en terme de sécurité.

Exclusions relatives à MongoDB

Comme indiqué dans la documentation de MongoDB (*voir page : Security Checklist for Self-Managed Deployments - Database Manual - MongoDB Docs*) :

les **dossiers de stockage des données**, ainsi que le dossier de stockage des **fichiers de log** des différents démons MongoDB **doivent impérativement être exclus** de l'antivirus.

En effet, la suppression d'un fichier dans l'un de ces dossiers par l'antivirus peut planter le programme et corrompre l'intégralité de la base de données.

De plus, les données enregistrées dans le dossier de stockage étant compressées, leur analyse engendrerait un surcout non négligeable en ressources d'Entrées / Sorties et CPU sans apporter de bénéfice en terme de sécurité.

Pour les différents démons MongoDB, le dossier de stockage des données et le fichier de log peut être retrouvé dans leur fichier de configuration respectif :

- Pour **mongod**:
  - Fichier de configuration : **/etc/mongod.conf**
    - Parametre de configuration du fichier de log : **systemLog.path**
    - Parametre de configuration du dossier de stockage des données : **storage.dbPath**
- Pour **mongos**
  - Fichier de configuration : **/etc/mongod.conf**
    - Parametre de configuration du fichier de log : **systemLog.path**
- Pour **mongo-configsrv**
  - Fichier de configuration : **/etc/mongo-configsrv.conf**
    - Parametre de configuration du fichier de log : **systemLog.path**
    - Parametre de configuration du dossier de stockage des données : **storage.dbPath**

Exclusions relatives à Graphite

Graphite, suivant le nombre de métriques à gérer, peut déjà avoir, *naturellement*, un taux d'utilisation du disque très élevé.

- Afin d'éviter de surcharger le système, il faut exclure le dossier de stockage des métriques (***/opt/graphite/storage/whisper/***) de l'antivirus.