Suristats

Éric Leblond

Freelance/OISF

18 octobre 2013

Analyse statistiques des performances

- Suricata génére un fichier stats.log
- Il contient des indicateurs de performances variés
- Des compteurs thread par thread
- Un dump régulier est effectué

Objectifs

- Analyse d'un fichier stats.log
- Stockage de chaque compteur dans une base sqlite
- Prise en compte des runs multiples

Objectifs

Basique

- Option de création de la base de données
- Option de suppression de la base de données
- Lancement en mode fichier avec display du nombre de données lues
- Lancement en mode démon (optionnel)

Stats

Après lecture et stockage des données dans une structure. Ceci permettra ensuite de multiplier les opérateurs arithmétiques.

- Ratio de drop sur un run donné
- Stats par thread et par run pour un fichier DB
  - Moyenne de paquets par seconde
  - Moyenne de drop par seconde

Requêtes

- Liste des runs stockés
  - Date de départ
  - Date de fin
  - Durée
- Liste des données pour un run
- Liste des données avec agrégation de thread pour un run

Git

- Gestionnaire de sources
- Conserver l'historique des modifications

Sqlite

- DB embarquée
- Utilisable en ligne de commande

Utilisation de la ligne de commande Sqlite

- Créer un fichier base de données
- Déclarer une table de contacts (noms prénoms mail)
- Insérer une dizaine de données
- Réaliser une requête sur les noms de domaines

Progression

- Déterminer la structure de données nécessaire
- Parsing du fichier
- Sortie texte de champ choisi
- Déterminer la structure de la base de donnée
- Se connecter à la base de donnée
- Créer une table depuis la base
- Réaliser les insertions
- Mise en place du mode stats
- Mise en place du mode continu