Télémetrie sflow

Jean-Marc Pouchoulon

Mai 2025

1 Introduction à *sflow*

1.1 Contexte

Le TP est à réaliser de manière individuelle sur une machine virtuelle Debian. Il a pour ambition de vous montrer comment utiliser le protocole *sflow* pour surveiller les performances de votre machine virtuelle et d'un routeur.

1.2 Recherches introductives

Faites répondre votre L.L.M. favori aux questions suivantes:

1. Qu'est-ce que *sflow* ?
2. Quelles sont les différences entre les protocoles*sflow*, *netflow* et *ipfix* ?
3. Est-ce que *sflow* est open source?
4. Quel est le port et le type de protocole utilisé par un collecteur *sflow* ?
5. Sur quels types de matériels peut-on utiliser *sflow* ?

2 Utilisation de *sflow* pour surveiller une machine virtuelle Linux Debian

1. En suivant `https://sflow.net/downloads.php` installez hsflowd.
2. En suivant `https://sflow-rt.com/download.php#download` et `https://sflow-rt.com/intro.php` installez sflow-rt.
3. Configurez le fichier */etc/hsflowd.conf* afin d'alimenter sflow-rt.Aidez-vous de `https://sflow.net/host-sflow-linux-config.php`. Vous pouvez "débugguer" la configuration de hsflowd avec la commande *hsflowd -dddd*.
4. Utilisez le *flow-browser* de *sflow-rt* afin de visualiser les flux de votre machine virtuelle (port de destination , adresses IP source et destination...).
5. Retrouvez à l'aide de l'*API Browser* de sflow-rt les métriques produites par sflow. Récupérez la liste des métriques via curl
6. Installez *sampleflowtrend* avec Docker. Utilisez-le pour alimenter votre compte-rendu par des analyses intéressantes.

```
docker run -v /var/local/sflowtrend-pro:/var/local/sflowtrend-pro \
    -p 6344:6343/udp -p 8087:8087 -p 8443:8443 \
    -h sflowtrend-pro -e TZ=Europe/Paris -d --restart unless-stopped sflow/sflowtrend
```

7. Installez sflowtool (voir `https://github.com/sflow/sflowtool`).
8. Utilisez-le pour réceptionner les paquets sflow de votre machine physique sur le port 6344 afin d'éviter la collision de port avec "sflow-rt".

9. Utilisez NuShell pour afficher les flux sflow remontés en temps réel au format *json* avec la commande suivante :

```
sflowtool -p 6344 -j | from json --objects
        | flatten samples --all
        | select -i elements
        | flatten --all
        | default False udpInDatagrams
        | default False  ifSpeed
        | filter {$in.udpInDatagrams != False or $in.ifSpeed != False}
```

10. Utilisez la commande *tee* de NuShell pour sauvegarder le flux des résultats dans un fichier csv.

3 Utilisation de *sflow* pour la métrologie de routeurs Arista

On va utiliser le projet de démonstration de *sflow* sur des routeurs Arista en utilisant *containerlab*.

1. Installez containerlab avec curl sur votre machine virtuelle (voir `https://containerlab.dev/install/`)
2. Clonez le dépôt `https://github.com/pushou/sflow-arista.git`
3. Ouvrez le projet avec *vscode*. Installez l'extension "containerlab" pour vscode.
4. Utilisez cette extension pour visualiser le projet.
5. Chargez la topologie *"3 Stage Clos Topology"* et lancez-la.
6. Retrouvez l'affichage web de sflow-rt afin de visualiser la métrologie des flux.
7. Analyser le projet afin de comprendre comment il fonctionne. Illustrez par un schéma au format draw.io.