% Supervision NetFlow
%
% Gestion et Surveillance de Réseau

Introduction

Objectifs

* Apprendre à installer les outils nfdump et NfSen

Notes

* Les commandes précédées de "$" signifient que vous devez exécuter
  la commande en tant qu'utilisateur général - et non en tant
  qu'utilisateur root.
* Les commandes précédées de "#" signifient que vous devez
travailler
  en tant qu'utilisateur root.
* Les commandes comportant des lignes de commande plus spécifiques
  (par exemple "RTR-GW>" ou "mysql>") signifient que vous exécutez
  des commandes sur des équipements à distance, ou dans un autre
  programme.

Prérequis

Il est attendu que vous ayez déja configuré votre routeur pour
exporter
les flux vers un PC dans votre groupe et que votre groupe voisin a
configuré
leur routeur pour qu'il exporte les flux vers le même PC. Voir
l'exercice 1
pour les détails.

Configurer votre collecteur

Installer Nfdump et les outils associés.

Nfdump fait partie des outils de collection Netflow. Nous allons
installer plusieurs outils supplémentaires dont nous aurons besoin
un peu plus tard.

~~~~~~
~~~~~~~
$ sudo apt-get install rrdtool mrtg librrds-perl librrdp-perl
librrd-dev \
libmailtools-perl php5 bison flex
~~~~~~
~~~~~~

Si on vous demande "Make /etc/mrtg.cfg owned by and readable only by root?"
choisir "<Yes>" et appuyer sur ENTREE pour continuer.

Compilation et installation de nfdump

Il nous manque des outils:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

Il y a un paquetage dans Ubuntu mais celui ci est trop ancien.
Nous avons donc re-compilé un paquetage plus récent, prêt à être téléchargé du NOC:

```
cd /tmp/
wget http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1_i386.deb
wget http://noc.ws.nsrc.org/downloads/nfdump-flow-tools_1.6.6-1_i386.deb
```

Installation:

```
sudo dpkg --install nfdump_1.6.6-1_i386.deb
sudo dpkg --install nfdump-flow-tools_1.6.6-1_i386.deb
```

Test et installation de nfcapd et nfdump

```
mkdir /tmp/nfcap-test
nfcapd -E  -p 9001 -l /tmp/nfcap-test
```

... au bout d'un certain temps, une série de flux devrait être affichée
sur votre écran.

Arrêtez l'outil avec CTRL-C, et inspectez le contenu de /tmp/nfcap-test

```
$ ls -l /tmp/nfcap-test
```

Vous devriez voir un ou plusieurs fichiers nommés nfcapd.2013xxyyzz

Inspectez ce(s) fichier(s) avec nfdump:

```
nfdump -r /tmp/nfcap-test/nfcapd.2013xxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.2013xxyyzz -s srcip/bytes
```

Vous devriez y trouvez quelques informations utiles :)

Installation et configuration de NfSen

```
cd /usr/local/src
sudo wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
sudo tar xvzf nfsen-1.3.6p1.tar.gz
cd nfsen-1.3.6p1
sudo wget http://noc.ws.nsrc.org/downloads/nfsen-socket6.patch
sudo patch -p0 < nfsen-socket6.patch
cd etc
sudo cp nfsen-dist.conf nfsen.conf
sudo editor nfsen.conf
```

Ajuster la variable $BASEDIR

```
$BASEDIR="/var/nfsen";
```

Ajuster le chemin où résident les outils:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
# nfdump tools path
$PREFIX = '/usr/bin';
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Configurer le bon utilisateur afin qu'Apache puisse accéder aux fichiers:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data';
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Paramétrer la taille du buffer (tampon) à une petite taille, pour qu'on
reçoive des données rapidement:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
# Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = 2000;
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Trouver la section avec la définition des sources (%sources), et la modifier ainsi:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
%sources=(
'rtr1' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
'rtr2' => {'port'=>'9002','col'=>'#00ff00','type'=>'netflow'},
 );
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Maintenaint, sauver le fichier et quitter l'éditeur.

Créer l'utilisateur netflow sur le système

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ sudo useradd -d /var/netflow -G www-data -m -s /bin/false netflow
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Installer NfSen et commencer à l'utiliser

Assurons nous que nous sommes au bon endroit:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ cd /usr/local/src/nfsen-1.3.6p1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Enfin, on peut installer:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ sudo perl install.pl etc/nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Appuyer sur ENTREE quand on vous demande le chemin de Perl.

Installer le script de démarrage (initialisation)

Afin que nfsen démarre et s'arrête automatiquement quand votre machine démarre, ajoutez un lien depuis le répertoire init.d pointant sur le script d'initialisation de nfsen:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
sudo ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen
sudo update-rc.d nfsen defaults 20
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Démarrer nfsen

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
sudo service nfsen start
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

View flows via the web:

La page nfsen se trouve ici:

~~~~~~
~~~~~~~
http://pcX.ws.nsrc.org/nfsen/nfsen.php
~~~~~~
~~~~~~~

Si vous voyez un message similaire:

~~~~~~
~~~~~~~
Frontend - Backend version missmatch!
~~~~~~
~~~~~~~

... ce n'est pas grave, il suffit de recharder la page et il
disparaît.

Fini! Continuons avec le labo 3, exercice3-NfSen-PortTracker

* NOTES:

Ajour de sources supplémentaires

Pour ajouter de nouvelles sources à nfsen, il suffit de faire ainsi:

- rédiger /var/nfsen/etc/nfsen.conf, and ajouter les sources, par
exemple:

~~~~~~
~~~~~~~
```
%sources = (
    'rtrX'  => { 'port' => '900X', 'col' => '#0000ff', 'type' =>
'netflow' },
    'rtrY'  => { 'port' => '900Y', 'col' => '#00ff00', 'type' =>
'netflow' },
    'rtr10' => { 'port' => '9010', 'col' => '#ff0000', 'type' =>
'netflow' }, # <- new
);
```
~~~~~~
~~~~~~~

- Reconfigurer NfSen.

Il faudra faire ceci chaque fois que aller modifier /var/nfsen/etc/nfsen.conf:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
$ sudo /etc/init.d/nfsen reconfig
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```

Vous devriez alors voir:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
New sources to configure : rtr10
Continue? [y/n] y

Add source 'rtr10'

Reconfig done!
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~
```