MRTG : Multi Router Traffic Grapher

Monitoring de variables SNMP par MRTG

MRTG est un outil permettant de monitorer le trafic sur des liens réseaux. Il génère des pages HTML pour chaque variable SNMP monitorée. Il permet donc de visualiser l'évolution de ces variables dans le temps très simplement, à travers un browser web (Internet Explorer, Firefox, Chrome, …).

MRTG fonctionne sous Linux / Unix, et Windows NT / 2000 / 2008. Nous allons ici l'utiliser sous Linux.

Le principe est simple : après installation des paquetages adéquat, il faut créer un fichier de configuration qui permet de définir quelles variables MIBs on veut monitorer, et sur quelle machine. Une fois ce fichier créé, il suffit de lancer la commande mrtg pour aller récupérer les valeurs des variables MIBs sur la machine monitorée. Ce fichier est assez complexe à générer à la main. Il existe donc un outil qui permet de le générer automatiquement : cfgmaker.

La syntaxe classique de cfgmaker est la suivante :

```
cfgmaker --global 'WorkDir: /root/mrtg'  \
          --global 'Options[_]: bits,growright' \
          --output /root/mrtg/mrtg.cfg    \
           public@10.2.18.1
```

où `/root/mrtg` est le répertoire ou seront créés les pages HTML, `/root/mrtg/mrtg.conf` est le nom du fichier de configuration généré.

Cette commande va créer un fichier de configuration qui, par défaut, permettra de récupérer les valeurs des débits entrants et sortants de chaque interface du routeur de l'IUT.

Créez une machine virtuelle Linux qui vous servira de Manager. Créez le fichier de configuration avec cfgmaker pour monitorer les débits entrants et sortants de chaque interface du routeur. Visualisez sous un navigateur le résultat, et expliquez l'apparition des 9 fichiers différents. Rem : le répertoire d'installation des commandes mrtg : /usr/local/mrtg-2/bin

Un problème reste à résoudre. Chaque fois que l'on veut demander à mrtg d'aller chercher les valeurs des variables sur le routeur, il faut relancer « à la main » mrtg … ce qui est assez contraignant, vous l'avouerez … Heureusement, plusieurs solutions permettent de résoudre ce problème, et d'automatiser la récolte des variables SNMP.

La première solution consiste à utiliser la `crontab` de Linux, qui permet de lancer des processus à intervalles réguliers. Cette solution a pour avantage d'être générique, mais demande de bien connaître la syntaxe de la `crontab`, et de bien la programmer.

Une autre solution, beaucoup plus simple, consiste à dire à mrtg de se lancer comme un daemon, c'est-à-dire de s'exécuter tout seul toutes les X minutes. L'avantage de sa solution est sa mise en œuvre très simple. L'inconvénient est qu'on ne peut pas relancer mrtg avec des intervalles de moins de 5 mn … Si on veut dépasser cette limitation, il faut utiliser l'utilitaire rddtool (nous ne l'utiliserons pas ici …)

Pour signifier à mrtg de se lancer comme daemon, rajoutez la ligne

```
RunAsDaemon: Yes
```

dans la partie `Global` du fichier `mrtg.cfg`

Vérifiez que les fichiers HTML sont bien mis à jour toutes les 5 mn (vous pouvez commencer la suite du TP en attendant la mise à jour automatique …)

Bien entendu, on peut modifier le fichier de configuration `mrtg.conf` pour choisir les variables à monitorer, et choisir les interfaces à observer. Pour cela, on ne peut plus utiliser `cfgmaker`. En effet, ce dernier ne permet de monitorer que le nombre d'octets entrants et sortants sur chaque interface. Pour monitorer d'autres variables, il faut créer à la main son propre fichier de configuration !!

Créez le fichier mrtg2.cfg suivant :

```
EnableIPv6: no
Workdir: /root/mrtg/
options[_]: bits,growright

RunAsDaemon: Yes
Refresh: 300
MaxBytes[_]: 10000000000
```

Pour le moment, nous n'avons précisé aucune variable SNMP. Voici la syntaxe permettant de monitorer une variable :

Target[mavariable]:.1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:public@10.2.18.1:
Title[mavariable]: titre de la fenetre web

Dans la ligne Target, vous voyez répété 2 fois la même valeur de variable SNMP (.1.3.6.1.2.1.6.9.0). La première valeur correspond, sur les graphiques générés, à la variable entrante (IN), la seconde à la variable sortante (OUT). Par exemple, si on veut monitorer le nombre d'octets sur une machine, on donnera deux variables différentes, l'un pour le nombre d'octets entrants sur l'interface, l'autre pour le nombre d'octets sortants de l'interface. Si, comme dans l'exemple ci-dessus, les deux valeurs sont identiques, le graphique ne fait apparaître qu'une seule courbe (mais il faut quand même avoir mis 2 fois l'OID de la variable).

Complétez mrtg2.conf pour qu'il affiche l'évolution du nombre de connexions TCP actives sur le routeur, et le nombre d'octets entrants et sortants sur l'interface réseau du VLAN étudiant.

On peut monitorer des variables autres qu'un nombre d'octets. En fait, toute variable numérique (évidemment, pas des chaînes de caractères) dont la valeur varie régulièrement peut être monitorée.

Mise en place d'un agent snmp sur un serveur

Vous allez maintenant devoir mettre en place et configurer un agent snmp sur une autre machine virtuelle (appelé agent par la suite). Vous pourrez ainsi, à partir du Manager, observer les différents paramètres proposés par cet agent. L'objectif de cette manipulation est de vous montrer que SNMP permet de récupérer des informations sur n'importe quel type d'appareil IP (serveur, PC, imprimante, onduleur, routeur, switch, hub, …), sur lequel on a préalablement installé un agent SNMP.

Créez la machine virtuelle serveur.

Installez le module agent snmp (snmpd) sur votre machine virtuelle agent.

Il faut maintenant configurer le daemon snmpd pour qu'ils puisse répondre aux requêtes du manager. Toute la configuration se fait dans le fichier /etc/snmp/snmpd.conf. Ce fichier est assez complexe. Heureusement, l'outil snmpconf va nous permettre de le créer sans trop de difficulté …

Tapez la commande snmpconf –r none –g basic_setup

Vous ne configurerez que le contrôle d'accès snmp v1/v2c. Dans cette partie, vous définirez une communauté d'accès en lecture écriture, appelée private, et restreinte à la machine locale (127.0.0.1). Une seconde communauté en lecture seule, appelée public, sera accessible depuis toutes les machines, mais ne permettra que l'accès au sous-arbre de la mib 1.3.6.1.2.1.1

Une fois la configuration terminée, pensez à vérifier la présence dans le fichier de config de la ligne com2sec readonly default public . Si cette ligne est en commentaire (# devant), vous ne pourrez pas voir toute la MIB du l'agent. Modifiez alors le fichier de config pour prendre cette option plutôt que l'option paranoid (c'est-à-dire mettez l'option paranoid en commentaire, et décommentez l'option default – n'oubliez pas de relancer le daemon snmpd ensuite : /etc/init.d/snmpd restart).

Vous allez maintenant récupérer les valeurs de différentes variables inhérentes à votre agent :

- taille totale de la mémoire vive (RAM)
- taille de la mémoire vive libre
- taille totale du swap
- taille de la swap libre
- nb de processus actifs sur le système
- taille de la partition /
- quantité utilisée de la partition /
- quantité libre de la partition /

Bien entendu, ces différentes variables dépendent du système, et ne peuvent donc pas toutes être trouvées dans la MIB classique (1.3.6.1.2). Il va falloir donc « fouiller » dans la partie Entreprise (1.3.6.1.4) de la MIB, c'est-à-dire dans la partie propriétaire (non normalisée) de la MIB

Deux sous arbres de la MIB vous seront utiles :

- 1.3.6.1.2.1.25 dans la MIB classique
- 1.3.6.1.4.1.2021 dans la partie Entreprise

Donnez les valeurs des différents paramètres ci-dessus dans le tableau ci-après.

VARIABLE	OID (après 1.3.6.1.)	Valeur
Taille totale de la mémoire vive		
Taille de la mémoire vive libre		
Taille totale de la swap		
Taille de la swap libre		
Nbre de processus actifs sur le système		
Taille de la partition		
Quantité utilisée de la partition /		
Quantité libre de la partition /		

Supervision par MRTG du serveur

Faîtes en sorte que le répertoire /home soit supervisé par le snmpd (c'est à dire que l'on peut récupérer sa taille depuis le manager en utilisant l'agent SNMP)

Rajoutez au fichier de configuration MRTG précédent la supervision de la taille di répertoire /home du serveur. Vérifiez le bon fonctionnement.

Téléchargez un fichier dans /home du serveur, et vérifiez qu'au bout de 5mn maximum, la courbe du graphique MRTG de /home a bien variée.