TD : Administration réseau avec SNMP

Principes de fonctionnement de l'architecture

- *Simple Network Management Protocol* (SNMP) est un protocole de communication qui permet aux administrateurs de réseaux de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
- Les systèmes de gestion de réseau sont basés sur trois éléments principaux : un superviseur, des nœuds et des agents. Dans la terminologie SNMP, le superviseur est appelé *manager*. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de *management*. Les agents sont des entités qui se trouvent au niveau de chaque interface, connectant au réseau l'équipement géré (nœud) et permettant de récupérer des informations sur différents objets. Commutateurs, concentrateurs, routeurs, postes de travail et serveurs (physiques ou virtuels) sont des exemples d'équipements contenant des objets gérables. Ces objets gérables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données arborescente appelée *Management Information Base* (MIB). SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.
- L'architecture de gestion du réseau proposée par le protocole SNMP est donc fondée sur trois principaux éléments :
    - Les équipements gérés (*managed devices*) sont des éléments du réseau contenant des objets de gestion (*managed objects*) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques.
    - Les agents, c'est-à-dire les applications de gestion de réseau résidant dans un périphérique, sont chargés de transmettre les données locales de gestion du périphérique au format SNMP.
    - Les systèmes de gestion de réseau (*network management systems*) notés NMS sont les consoles à travers lesquelles les administrateurs peuvent réaliser des tâches d'administration.
- Le protocole SNMP version 1 est défini dans la RFC 1157 qui est récupérable ici http://www.ietf.org/rfc/rfc1157. Le protocole SNMP version 2 est défini dans la RFC 1901 qui est récupérable ici http://www.ietf.org/rfc/rfc1901. Le protocole SNMP version 3 est défini dans la RFC 2571 qui est récupérable ici http://www.ietf.org/rfc/rfc2571.

Mise en place

1. Ce TD utilise l'émulateur système **`QEMU`** avec le module noyau d'accélération matérielle **`KVM`** qui est installé sur les machines du CREMI. Pour configurer ces outils, il faut taper les commandes suivantes (dans cet ordre) dans un terminal :
   ```
   source /net/ens/vince/virt/nemu-init.rc
   nemu-kvm start
   ```

2. Récupérez la documentation de Vyatta située sur **`/net/stockage/dmagoni`** pour savoir comment configurer les routeurs. Les commandes de bases pour **Debian** sont aussi données dans le fichier `TD-Instructions.pdf` et celles pour **NEmu** sont dans `TD-Nemu-Guide.pdf`.
3. Ce TD utilise trois machines virtuelles émulant des PC standards exécutant une distribution **Debian** d'un système d'exploitation GNU/Linux. Elles serviront d'hôtes ou de routeurs selon les cas. Lancez le script suivant pour démarrer ces machines :
   ```
   nemu-vnet /net/ens/vince/virt/config/netsnmp.py
   ```

4. Lorsqu'une machine a fini de démarrer, revenez sur la fenêtre du script et tapez sur la touche **`Entrée`**. Repétez ceci trois fois afin de démarrer les trois machines virtuelles.
5. Connectez-vous en tant qu'administrateur **`root`** sur chaque machine virtuelle en utilisant le mot de passe suivant : **`plop`**. Sur **Vyatta**, le login est **`vyatta`** et le mot de passe est **`vyatta`**.
6. Les commandes **Debian** et **Vyatta** données ci-dessous sont **à compléter correctement**, grâce aux documents fournis avec les images et au Web.
7. Pour chaque machine virtuelle, son interface **`eth0`** est connectée à l'Internet par SLIRP et elle est configurée par DHCP. Vous pouvez ainsi télécharger des paquets logiciels en utilisant la commande **`apt-get install`**. Pour mettre à jour la gestion des paquets, tapez d'abord la commande **`apt-get update`**.

Réseau supervisé

Un réseau intranet simple est présenté sur la figure 1a. Le réseau intranet est un réseau local de type Ethernet connecté à l'Internet via un routeur d'accès. Le réseau intranet est privé, donc le routeur fait du NAT et toutes les machines ont des adresses IP privées.

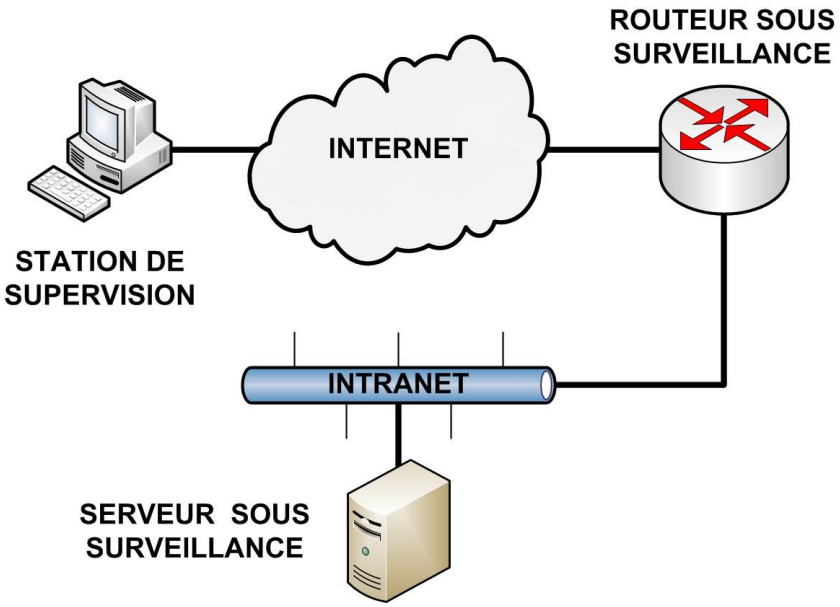

Figure 1a. Réseau intranet à superviser.

Pour le TD vous allez mettre en place la topologie présentée dans la figure 1b ci-dessous et que l'on considérera équivalente à celle de la figure 1a ci-dessus.

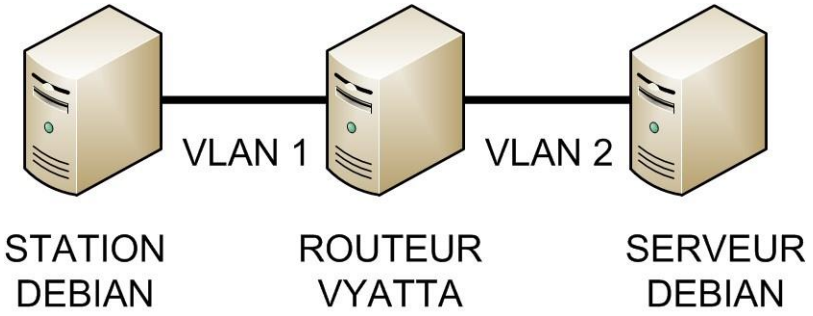

Figure 1b. Réseau 1a implémenté sur Qemu avec Debian / Vyatta.

8. Créez les interfaces **eth1** dans les machines **Debian** avec la commande **ip link set eth1 up**.
9. Choisissez des plages d'adresses pour chaque sous-réseau. Etablir un plan d'adressage précisant les adresses de toutes les interfaces des machines puis configurez-les.
10. Remplissez les tables de routage des machines de manière statique. Ne remplacez pas la route par défaut. Vérifiez que toutes les machines peuvent communiquer entre elles par des **ping**.

Utilisation de SNMP

11. Installez les paquets **snmp, snmpd** et **snmp-mibs-downloader** sur la station et le serveur. Si besoin ajouter les mots : **contrib non-free** aux lignes se terminant par main dans **/etc/apt/sources.list**. et retapez **apt-get update**.
12. Lancez la commande **download-mibs** pour récuperer les MIBS.
13. Sur le serveur, étudiez et configurez les fichiers **/etc/snmp/snmpd.conf** et **/etc/snmp/snmptrapd.conf**. Les fichiers des MIBs se trouvent dans le répertoire **/usr/share/snmp/mib2c-data/**. Commentez la ligne **mibs:** dans le fichier **snmp.conf**.
14. Démarrez le service avec **/etc/init.d/snmpd restart**.
15. Testez le serveur SNMP avec **snmpwalk -v1 -cpublic localhost**.
16. Affichez l'arbre de la hiérarchie **system** avec la commande **snmptranslate -Tp**.
17. Utilisez la commande **snmpget** pour obtenir la description de la station.
18. Modifiez la ligne **view system included** dans le fichier **snmpd.conf** pour accéder à toute la MIB v2.
19. Utilisez **snmpgetnext** pour parcourir la MIB manuellement et **snmpwalk** pour la parcourir automatiquement.
20. Utilisez **snmpset** pour changer la valeur de la description de la station.
21. Activez SNMP sur Vyatta.

```
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server host 192.168.130.20 version snmp
```

22. Utilisez les browsers graphiques de MIB tels que **mbrowse** et **tkmib** pour visualiser l'arborescence des MIB du serveur et du routeur.
23. Utilisez **snmpconf** pour créer un fichier de configuration sur le serveur.
24. Configurez le serveur pour activer l'envoi des *traps* SNMP avec **snmptrap** et **snmptrapd**.
25. Configurez le routeur pour activer l'envoi des *traps* SNMP avec **snmptrap** et **snmptrapd**.
26. Installez Multi Router Traffic Grapher (MRTG) qui nécessite Apache2, PHP et Perl.
27. Observez et tracez les messages SNMP échangés avec **wireshark**.

Utilisation de nagios

28. Installez *nagios* sur la station en récupérant les archives sur **/net/stockage/dmagoni**. Voir les instructions à : `http://wiki.monitoring-fr.org/nagios/debian-install`.
    Alternativement, vous pouvez aussi installer *nagios* à partir des paquets **Debian**.
29. Installez NRPE et les *plugins* sur le serveur.
30. Configurez les fichiers dans **/etc/nagios**.
31. Configurez les fichiers :
    a. /usr/local/nagios/etc/timeperiods.cfg
    b. /usr/local/nagios/etc/contacts.cfg
    c. /usr/local/nagios/etc/contactgroups.cfg
    d. /usr/local/nagios/etc/hosts.cfg

    e. /usr/local/nagios/etc/hostgroups.cfg
32. Vérifiez les fichiers de configuration avec **`nagios -v /etc/nagios/nagios.cfg`**.
33. Relancez *nagios* avec **`/etc/init.d/nagios restart`**.
34. Surveillez les services suivants en modifiant **`services.cfg`** et **`checkcommands.cfg`** :
    a. ping, load, swap, disk
    b. http, ftp, ssh
35. Développez un plugin en *bash* ou en C utilisant les commandes SNMP pour superviser le routeur **Vyatta**.

Travail à rendre

A la fin des séances de ce TD, vous rendrez un rapport de TD, au format PDF, que vous enverrez par e-mail à votre chargé de TD. Ce rapport contiendra les réponses aux questions posées dans ce sujet en y incluant tous les justificatifs nécessaires :

- Extraits pertinents des fichiers de configuration des machines **Debian** et du routeur **Vyatta**.
- Extraits pertinents des listings des commandes **Debian** et **Vyatta** utilisées pour résoudre les questions.
- Extraits pertinents des captures de trames prises par **`wireshark`**.